Lorenz J. Halbeisen

Combinatorial Set Theory

with a gentle introduction to forcing

November 17, 2011

Springer
Berlin Heidelberg New York
Hong Kong London
Milan Paris Tokyo

To Joringel,
Meredith, Andrin, and Salome

As the original design of casting Peals of Bells was in order to make pleasant Musick thereon; so the Notes in every Peal are formed apt for that end and purpose, every Peal of Bells being tun'd according to the principles of Musick.
Yet the Notes may be so placed in ringing that their Musick may be rendred much more pleasant: for in Musick there are Concords, which indeed may be term'd the very life and soul of it.
For this Musical end were changes on Bells first practiced, changes being nothing else but a moving and placing of the Notes in ringing; wherein 'tis to be observed as a general Rule, That every change must be made betwixt two notes that strike next to each other.

Fabian Stedman
Campanalogia, 1677

By the campanologist, the playing of tunes is considered to be a childish game; the proper use of bells is to work out mathematical permutations and combinations.
His passion finds its satisfaction in mathematical completeness and mechanical perfection.

Dorothy L. Sayers
The Nine Tailors, 1934

Preface

This book provides a self-contained introduction to *Axiomatic Set Theory* with main focus on *Infinitary Combinatorics* and the *Forcing Technique*. The book is intended to be used as a textbook in undergraduate and graduate courses of various levels, as well as for self-study. To make the book valuable for experienced researchers also, some historical background and the sources of the main results have been provided in the NOTES, and some topics for further studies are given in the section RELATED RESULTS — where those containing open problems are marked with an asterisk.

The axioms of Set Theory ZFC, consisting of the axioms of *Zermelo-Fraenkel Set Theory* (denoted ZF) and the *Axiom of Choice*, are the foundation of Mathematics in the sense that essentially all Mathematics can be formalised within ZFC. On the other hand, Set Theory can also be considered as a mathematical theory, like Group Theory, rather than the basis for building general mathematical theories. This approach allows us to drop or modify axioms of ZFC in order to get, for example, a Set Theory without the *Axiom of Choice* (see Chapter 4) or in which just a weak form of the *Axiom of Choice* holds (see Chapter 7). In addition, we are also allowed to extend the axiomatic system ZFC in order to get, for example, a Set Theory in which, in addition to the ZFC axioms, we also have *Martin's Axiom* (see Chapter 13), which is a very powerful axiom with many applications for *Infinitary Combinatorics* as well as other fields of Mathematics. However, this approach prevents us from using any kind of Set Theory which goes beyond ZFC, which is used, for example, to prove the existence of a countable model of ZFC (see the *Löwenheim-Skolem Theorem* in Chapter 15).

Most of the results presented in this book are combinatorial results, in particular the results in *Ramsey Theory* (introduced in Chapter 2 and further developed in Chapter 11), or those results whose proofs have a combinatorial flavour. For example, we get results of the latter type if we work in Set Theory without the *Axiom of Choice*, since in the absence of the *Axiom of Choice*, the proofs must be constructive and therefore typically have a much more combinatorial flavour than proofs in ZFC (examples can be found in Chapters 4 & 7). On the other hand, there are also elegant combinatorial proofs using the *Axiom of Choice*. An example is the proof in Chapter 6, where it is shown that one can divide the solid unit ball into five parts, such that one can build two solid unit balls out of these five parts — another such paradoxical result is given in Chapter 17, where it is shown that it might be possible in ZF to decompose a square into more parts than there are points on the square.

Even though the ZFC axiomatic system is the foundation of Mathematics, by *Gödel's Incompleteness Theorem* — briefly discussed at the end of Chapter 3 — no axiomatic system of Mathematics is complete in the sense that every statement can either be proved or disproved; in other words, there are always statements which are independent of the axiomatic system. The main tool to show that a certain statement is independent of the axioms of Set Theory is Cohen's *Forcing Technique*, which he originally developed in the early 1960s in order to show that there are models of ZF in which the *Axiom of Choice* fails (see Chapter 17) and that the *Continuum Hypothesis* is independent of ZFC (see Chapter 14). The *Forcing Technique* is introduced and discussed in great detail in Part II, and in Part III it is used to investigate combinatorial properties of the set of real numbers. This is done by comparing the *Cardinal Characteristics of the Continuum* introduced in Chapter 8.

The following table indicates which of the main topics appear in which chapter, where $***$ means that it is the main topic of that chapter, $**$ means that some new results in that topic are proved or at least that the topic is important for understanding certain proofs, and $*$ means that the topic appears somewhere in that chapter, but not in an essential way:

Chapter	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Forcing Technique	*											***	**	***	*	***	**	**	**	***	**	**	**	**	**	**	**
Axiom of Choice & ZF	*	*	***	***	***	**	***										***										
Ramsey Theory	*	***		*	**		*	**	***	***	***		**	*				*					*	*	**	***	
Cardinal Characteristics	*	*						***	***	*			**					**	**		**	**	**	**	**	**	***

Part I **Part II** **Part III**

For example *Ramsey's Theorem*, which is the nucleus of *Ramsey Theory*, is the main topic in Chapter 2, it is used in some proofs in Chapters 4 & 7, it is used as a choice principle in Chapter 5, it is related to two *Cardinal Characteristics* defined in Chapter 8, it is used to define what is called a Ramsey ultrafilter in Chapter 10, it is used in the proof of the *Hales-Jewett Theorem* in Chapter 11, and it is used to formulate a combinatorial feature of Mathias reals in

Chapter 24. Furthermore, one can see that *Cardinal Characteristics* are our main tool in Part III in the investigation of combinatorial properties of various forcing notions, even in the cases when — in Chapters 25 & 26 — the existence of Ramsey ultrafilters are investigated. Finally, in Chapter 27 we show how *Cardinal Characteristics* can be used to shed new light on a classical problem in Measure Theory. On the other hand, the *Cardinal Characteristics* are used to describe some combinatorial features of different forcing notions. In particular, it will be shown that the cardinal characteristic $\mathfrak{h}$ (introduced in Chapter 8 and investigated in Chapter 9) is closely related to Mathias forcing (introduced in Chapter 24), which is used in Chapter 25 to show that the existence of Ramsey ultrafilters is independent of ZFC.

I tried to write this book like a piece of music, not just writing note by note, but using various themes or voices — like *Ramsey's Theorem* and the cardinal characteristic $\mathfrak{h}$ — again and again in different combinations. In this undertaking, I was inspired by the English art of bell ringing and tried to base the order of the themes on Zarlino's introduction to the art of counterpoint.

Acknowledgement. First of all, I would like to thank Andreas Blass for his valuable remarks and comments, as well as for his numerous corrections, which improved the quality of the book substantially. Furthermore, I would like to thank my spouse Stephanie Halbeisen, not only for reading Chapters 1 & 12 and parts of Chapters 5 & 13, but also for her patience during the last seven years. I would also like to thank Dandolo Flumini for reading Chapters 2, 3, 13, 14, 15, Ioanna Dimitriou for reading Chapters 16 & 17, and Gearóidín Diserens for reading Chapter 1 as well as the introductory comments of several chapters. Finally, I would like to thank Jörg Sixt, editor of Springer-Verlag, for making every effort to ensure that the book was published in the optimal style.

Winterthur, October 2011 *Lorenz Halbeisen*

Contents

Part III Combinatorics of Forcing Extensions

1 The Setting

For one cannot order or compose anything, or understand the nature of the composite, unless one knows first the things that must be ordered or combined, their nature, and their cause.

Gioseffo Zarlino
Le Istitutioni Harmoniche, 1558

Combinatorics with all its various aspects is a broad field of Mathematics which has many applications in areas like Topology, Group Theory and even Analysis. A reason for its wide range of applications might be that Combinatorics is rather a way of thinking than a homogeneous theory, and consequently Combinatorics is quite difficult to define. Nevertheless, let us start with a definition of Combinatorics which will be suitable for our purpose:

> *Combinatorics is the branch of Mathematics which studies collections of objects that satisfy certain criteria, and is in particular concerned with deciding how large or how small such collections might be.*

Below we give a few examples which should illustrate some aspects of infinitary Combinatorics. At the same time, we present the main topics of this book, which are the *Axiom of Choice*, *Ramsey Theory*, *cardinal characteristics of the continuum*, and *forcing*.

Let us start with an example from Graph Theory: A *graph* is a set of *vertices*, where some pairs of vertices are connected by an *edge*. Connected pairs of vertices are called *neighbours*. A graph is *infinite* if it has an infinite number of vertices. A *tree* is a *cycle-free* (*i.e.*, one cannot walk in proper cycles along edges), *connected* (*i.e.*, any two vertices are connected by a path of edges) graph, where one of its vertices is designated as the *root*. A tree is *finitely branching* if every vertex has only a finite number of neighbours. Furthermore, a *branch* through a tree is a maximal edge-path beginning at the root, in which no edge appears twice.

Now we are ready to state König's Lemma, which is often used implicitly in fields like Combinatorics, Topology, and many other branches of Mathematics.

> König's Lemma: *Every infinite, finitely branching tree contains an infinite branch.*

At first glance, this result looks straightforward and one would construct an infinite branch as follows: Let v_0 be the root. Since the tree is infinite but finitely branching, there must be a neighbour of v_0 from which we reach infinitely many vertices without going back to v_0. Let v_1 be such a neighbour of v_0. Again, since we reach infinitely many vertices from v_1 (without going back to v_1) and the tree is finitely branching, there must be a neighbour of v_1, say v_2, from which we reach infinitely many vertices without going back to v_2. Proceeding in this way, we finally get the infinite branch $(v_0, v_1, v_2, \ldots)$.

Let us now have a closer look at this proof: Firstly, in order to prove that the set of neighbours of v_0 from which we reach infinitely many vertices without going back to v_0 is not empty, we need an infinite version of the so-called Pigeon-Hole Principle. The Pigeon-Hole Principle can be seen as the fundamental principle of Combinatorics.

> Pigeon-Hole Principle: *If $n+1$ pigeons roost in n holes, then at least two pigeons must share a hole. More prosaically: If m objects are coloured with n colours and $m > n$, then at least two objects have the same colour.*

An infinite version of the Pigeon-Hole Principle reads as follows:

> Infinite Pigeon-Hole Principle: *If infinitely many objects are coloured with finitely many colours, then infinitely many objects have the same colour.*

Using the Infinite Pigeon-Hole Principle we are now sure that the set of neighbours of v_0 from which we reach infinitely many vertices without going back to v_0 is not empty. However, the next problem we face is which element we should choose from that non-empty set. If the vertices are ordered in some way, then we can choose the first element with respect to that order, but otherwise, we would need some kind of choice function which selects *infinitely often* (and this is the crucial point!) one vertex from a given non-empty set of vertices. Such a choice function is guaranteed by the Axiom of Choice, denoted AC, which is discussed in Chapter 5.

> Axiom of Choice: *For every family $\mathscr{F}$ of non-empty sets, there is a function f — called choice function — which selects one element from each member of $\mathscr{F}$ (i.e., for each $x \in \mathscr{F}$, $f(x) \in x$); or equivalently, every Cartesian product of non-empty sets is non-empty.*

The Axiom of Choice is one of the main topics of this book: In Chapter 3, the axioms of Zermelo-Fraenkel Set Theory (*i.e.*, the usual axioms of Set Theory except AC) are introduced. In Chapter 4 we shall introduce the reader to Zermelo-Fraenkel Set Theory and show how combinatorics can, to some extent, replace the Axiom of Choice. Subsequently, the Axiom of Choice (and some of its weaker forms) is introduced in Chapter 5. From then on, we always work in Zermelo-Fraenkel Set Theory *with* the Axiom of Choice — even in the case as in Chapters 7 & 17 when we construct models of Set Theory in which AC fails.

Now, let us turn back to König's Lemma. In order to prove König's Lemma we do not need full AC, since it would be enough if every family of non-empty *finite* sets had a choice function — the family would consist of all subsets of neighbours of vertices. However, as we will see later, even this weaker form of AC is a proper axiom and is independent of the other axioms of Set Theory (*cf.* PROPOSITION 7.7). Thus, depending on the axioms of Set Theory we start with, AC — as well as some weakened forms of it — may fail, and consequently, König's Lemma may become unprovable. On the other hand, as we will see in Chapter 5, König's Lemma may be used as a non-trivial choice principle.

Thus, this first example shows that — with respect to our definition of Combinatorics given above — some "objects satisfying certain criteria," may, but need not, exist.

The next example can be seen as a problem in infinitary *Extremal Combinatorics*. The word "extremal" describes the nature of problems dealt with in this field and refers to the second part of our definition of Combinatorics, namely "how large or how small collections satisfying certain criteria might be."

If the objects considered are infinite, then the answer, how large or how small certain sets are, depends again on the underlying axioms of Set Theory, as the next example shows.

> REAPING FAMILIES: *A family $\mathscr{R}$ of infinite subsets of the natural numbers $\mathbb{N}$ is said to be reaping if for every colouring of $\mathbb{N}$ with two colours there exists a monochromatic set in the family $\mathscr{R}$.*

For example, the set of all infinite subsets of $\mathbb{N}$ is such a family. The *reaping number* $\mathfrak{r}$ — a so-called *cardinal characteristic of the continuum* — is the smallest cardinality (*i.e.*, size) of a reaping family. In general, a *cardinal characteristic of the continuum* is typically defined as the smallest cardinality of a subset of a given set S which has certain combinatorial properties, where S is of the same cardinality as the continuum $\mathbb{R}$.

Consider the cardinal characteristic $\mathfrak{r}$ (*i.e.*, the size of the smallest reaping family). Since $\mathfrak{r}$ is a well-defined cardinality we can ask: How large is $\mathfrak{r}$? Can it be countable? Is it always equal to the cardinality of the continuum?

Let us just show that a reaping family can never be countable: Let $\mathscr{A} = \{A_i : i \in \mathbb{N}\}$ be any countable family of infinite subsets of $\mathbb{N}$. For each $i \in \mathbb{N}$, pick n_i and m_i from the set A_i in such a way that, at the end, for all i we have $n_i < m_i < n_{i+1}$. Now we colour all n_i's blue and all the other numbers red. For this colouring, there is no monochromatic set in $\mathscr{A}$, and hence, $\mathscr{A}$ cannot be a reaping family. The *Continuum Hypothesis*, denoted CH, states that every subset of the continuum $\mathbb{R}$ is either countable or of cardinality $\mathfrak{c}$, where $\mathfrak{c}$ denotes the cardinality of $\mathbb{R}$. Thus, if we assume CH, then any reaping family is of cardinality $\mathfrak{c}$. The same holds if we assume Martin's Axiom which will be introduced in Chapter 13.

On the other hand, with the *forcing technique* — invented by Paul Cohen in the early 1960s — one can show that the axioms of Set Theory do not decide whether or not the cardinals $\mathfrak{r}$ and $\mathfrak{c}$ are equal. The forcing technique is introduced in Part II and a model in which $\mathfrak{r} < \mathfrak{c}$ is given in Chapter 18.

Thus, the second example shows that — depending on the additional axioms of Set Theory we start with — we can get different answers when we try to "decide how large or how small certain collections might be."

Many more cardinal characteristics like $\mathfrak{hom}$ and $\mathfrak{par}$ (see below) are introduced in Chapter 8. Possible (*i.e.*, consistent) relations between these cardinals are investigated in Part II and more systematically in Part III — where the cardinal characteristics are also used to distinguish the combinatorial features of certain forcing notions.

Another field of Combinatorics is the so-called Ramsey Theory, and since many results in this work rely on Ramsey-type theorems, let us give a brief description of Ramsey Theory.

Loosely speaking, *Ramsey Theory* (which can be seen as a part of extremal Combinatorics) is the branch of Combinatorics which deals with structures preserved under partitions, or colourings. Typically, one looks at the following kind of question: If a particular object (*e.g.*, algebraic, geometric or combinatorial) is arbitrarily coloured with finitely many colours, what kinds of monochromatic structures can we find?

For example, van der Waerden's Theorem, which will be proved in Chapter 11, tells us that *for any positive integers r and n, there is a positive integer N such that for every r-colouring of the set $\{0, 1, \dots, N\}$ we find always a monochromatic (non-constant) arithmetic progression of length n.*

Even though van der Waerden's Theorem is one of the earliest results in Ramsey Theory, the most famous result in Ramsey Theory is surely Ramsey's Theorem (which will be discussed in detail in the next chapter):

> RAMSEY'S THEOREM: *Let n be any positive integer. If we colour all n-element subsets of $\mathbb{N}$ with finitely many colours, then there exists an infinite subset of $\mathbb{N}$ all of whose n-element subsets have the same colour.*

There is also a finite version of RAMSEY'S THEOREM which gives an answer to problems like the following:

How many people must be invited to a party in order to make sure that three of them mutually shook hands on a previous occasion or three of them mutually did not shake hands on a previous occasion?

It is quite easy to show that at least six people must be invited. On the other hand, if we ask how many people must get invited such that there are five people who all mutually shook hands or did not shake hands on a previous occasion, then the precise number is not known — but it is conjectured that it is sufficient to invite 43 people.

As we shall see later, RAMSEY'S THEOREM has many — sometimes unexpected — applications. For example, if we work in Set Theory without AC, then RAMSEY'S THEOREM can help to construct a choice function, as we will see in Chapter 4. Sometimes we get Ramsey-type (or anti-Ramsey-type) results even for partitions into infinitely many classes (*i.e.*, using infinitely many colours). For example, one can show that there is a colouring of the points in the Euclidean plane with countably many colours, such that no two points of any "copy of the rationals" have the same colour. This result can be seen as an anti-Ramsey-type theorem (since we are far away from "monochromatic structures"), and it shows that Ramsey-type theorems cannot be generalised arbitrarily. However, concerning RAMSEY'S THEOREM, we can ask for a "nice" family $\mathscr{F}$ of infinite subsets of $\mathbb{N}$, such that for every colouring of the n-element subsets of $\mathbb{N}$ with finitely many colours, there exists a homogenous set in the family $\mathscr{F}$, where an infinite set $x \subseteq \mathbb{N}$ is called *homogeneous* if all n-element subsets of x have the same colour. Now, "nice" could mean "as small as possible" but also "being an ultrafilter." In the former case, this leads to the *homogeneous number* $\mathfrak{hom}$, which is the smallest cardinality of a family $\mathscr{F}$ which contains a homogeneous set for every 2-colouring of the 2-element subsets of $\mathbb{N}$. One can show that $\mathfrak{hom}$ is uncountable and — like for the reaping number — that the axioms of Set Theory do not decide whether or not $\mathfrak{hom}$ is equal to $\mathfrak{c}$ (see Chapter 18). The latter case, where "nice" means "being an ultrafilter," leads to so-called *Ramsey ultrafilters*. It is not difficult to show that Ramsey ultrafilters exist if one assumes CH or Martin's Axiom (see Chapter 10), but on the other hand, the axioms of Set Theory alone do not imply the existence of Ramsey ultrafilters (see PROPOSITION 25.11). A somewhat anti-Ramsey-type question would be to ask how many 2-colourings of the 2-element subsets of $\mathbb{N}$ we need to make sure that no single infinite subset of $\mathbb{N}$ is almost homogeneous for all these colourings, where a set H is called *almost homogeneous* if there is a finite set K such that $H \setminus K$ is homogeneous. This question leads to the *partition number* $\mathfrak{par}$. Again, $\mathfrak{par}$ is uncountable and the axioms of Set Theory do not decide whether or not $\mathfrak{par}$ is equal to $\mathfrak{c}$ (see for example Chapter 18).

RAMSEY'S THEOREM, as well as Ramsey Theory in general, play an important role throughout this book. Especially in all chapters of Part I, except for Chapter 3, we shall meet — sometimes unexpectedly — RAMSEY'S THEOREM in one form or other.

NOTES

Gioseffo Zarlino. All citations of Zarlino (1517 – 1590) are taken from Part III of his book entitled *Le Istitutioni Harmoniche* (*cf.* [1]). This section of Zarlino's *Institutioni* is concerned primarily with the art of counterpoint, which is, according to Zarlino, *the concordance or agreement born of a body with diverse parts, its various melodic lines accommodated to the total composition, arranged so that voices are separated by commensurable, harmonious intervals.* The word "counterpoint" presumably originated at the beginning of the 14^{th} century and was derived from "punctus contra punctum," i.e., point against point or note against note. Zarlino himself was an Italian music theorist and composer. While he composed a number of masses, motets and madrigals, his principal claim to fame is as a music theorist: For example, Zarlino was ahead of his time in proposing that the octave should be divided into twelve equal semitones — for the lute, that is to say, he advocated a practice in the 16^{th} century which was universally adopted three centuries later. He also advocated equal temperament for keyboard instruments and just intonation for unaccompanied vocal music and strings — a system which has been successfully practiced up to the present day. Furthermore, Zarlino arranged the modes in a different order of succession, beginning with the Ionian mode instead of the Dorian mode. This arrangement seems almost to have been dictated by a prophetic anticipation of the change which was to lead to the abandonment of the modes in favour of a newer tonality, for his series begins with a form which corresponds exactly with our modern major mode and ends with the prototype of the descending minor scale of modern music. (For the terminology of music theory we refer the interested reader to Benson [2].)

Zarlino's most notable student was the music theorist and composer Vincenzo Galilei, the father of Galileo Galilei.

König's Lemma and Ramsey's Theorem. A proof of König's Lemma can be found in König's book on Graph Theory [3, VI, §2, Satz 6], where he called the result *Unendlichkeitslemma*. As a first application of the *Unendlichkeitslemma* he proved the following theorem of de la Vallée Poussin: *If E is a subset of the open unit interval $(0,1)$ which is closed in $\mathbb{R}$ and I is a set of open intervals covering E, then there is a natural number n, such that if one partitions $(0,1)$ into 2^n intervals of length 2^{-n}, each of these intervals containing a point of E is contained in an interval of I.* Using the *Unendlichkeitslemma*, König also showed that VAN DER WAERDEN'S THEOREM is equivalent to the following statement: *If the positive integers are finitely coloured, then there are arbitrarily long monochromatic arithmetic progressions.* In a similar way we will use König's Lemma to derive the FINITE RAMSEY THEOREM from RAMSEY'S THEOREM (*cf.* COROLLARY 2.3).

At first glance, König's Lemma and Ramsey's Theorem seem to be quite unrelated statements. In fact, König's Lemma is a proper (but rather weak) choice principle, whereas Ramsey's Theorem is a very powerful combinatorial tool. However, as we shall see in Chapter 5, Ramsey's Theorem can also be considered as a proper choice principle which turns out to be even stronger than König's Lemma (see Theorem 5.17).

References

1. Gioseffo Zarlino, ***The Art of Counterpoint,*** Part Three of *Le Istitutioni Harmoniche, 1558*, [translated by Guy A. Marco and Claude V. Palisca], Yale University Press, New Haven and London, 1968.
2. David J. Benson, ***Music: a mathematical offering***, Cambridge University Press, Cambridge, 2007.
3. Dénes König, ***Theorie der endlichen und unendlichen Graphen. Kombinatorische Topologie der Streckenkomplexe***, Akademische Verlagsgesellschaft, Leipzig, 1936 [reprint: Chelsea, New York, 1950].

Part I

Topics in Combinatorial Set Theory

2

Overture: Ramsey's Theorem

Musicians in the past, as well as the best of the moderns, believed that a counterpoint or other musical composition should begin on a perfect consonance, that is, a unison, fifth, octave, or compound of one of these.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

The Nucleus of Ramsey Theory

Most of this text is concerned with sets of subsets of the natural numbers, so, let us start there: The set $\{0, 1, 2, \dots\}$ of **natural numbers** (or of non-negative integers) is denoted by ω. It is convenient to consider a natural number n as an n-element subset of ω, namely as the set of all numbers smaller than n, so, $n = \{k \in \omega : k < n\}$. In particular, $0 = \emptyset$, where $\emptyset$ is the **empty set**. For any $n \in \omega$ and any set S, let $[S]^n$ denote the set of all n-element subsets of S (*e.g.*, $[S]^0 = \{\emptyset\}$). Further, the set of all finite subsets of a set S is denoted by $[S]^{<\omega}$.

For a finite set S let $|S|$ denote the number of elements in S, also called the **cardinality** of S.

A set S is called **countable** if there is an enumeration of S, *i.e.*, if $S = \emptyset$ or $S = \{x_i : i \in \omega\}$. In particular, every finite set is countable. However, when we say that a set is countable we usually mean that it is a countably infinite set. For any set S, $[S]^\omega$ denotes the set of all countably infinite subsets of S, in particular, since every infinite subset of ω is countable, $[\omega]^\omega$ is the set of *all* infinite subsets of ω.

Let S be an arbitrary non-empty set. A binary relation "$\sim$" on S is an **equivalence relation** if it is

- *reflexive* (*i.e.*, for all $x \in S$: $x \sim x$),

- *symmetric* (*i.e.*, for all $x, y \in S$: $x \sim y \leftrightarrow y \sim x$), and
- *transitive* (*i.e.*, for all $x, y, z \in S$: $x \sim y \wedge y \sim z \ \rightarrow \ x \sim z$).

The **equivalence class** of an element $x \in S$, denoted $[x]\tilde{}$, is the set $\{y \in S : x \sim y\}$. We would like to recall the fact that, since "$\sim$" is an equivalence relation, for any $x, y \in S$ we have *either* $[x]\tilde{} = [y]\tilde{}$ *or* $[x]\tilde{} \cap [y]\tilde{} = \emptyset$. A set $A \subseteq S$ is a set of **representatives** if for each equivalence class $[x]\tilde{}$ we have $|A \cap [x]\tilde{}| = 1$; in other words, A has exactly one element in common with each equivalence class. It is worth mentioning that in general, the existence of a set of representatives relies on the Axiom of Choice (see Chapter 5).

For sets A and B, let ${}^{A}B$ denote the set of all functions $f : A \to B$. For $f \in {}^{A}B$ and $S \subseteq A$ let $f[S] := \{f(x) : x \in S\}$ and let $f|_S \in {}^{S}B$ (the restriction of f to S) be such that for all $x \in S$, $f(x) = f|_S(x)$.

Further, for sets A and B, let the set-theoretic difference of A and B be the set $A \setminus B := \{a \in A : a \notin B\}$.

For some positive $n \in \omega$, let us colour all n-element subsets of ω with three colours, say red, blue, and yellow. In other words, each n-element set of natural numbers $\{k_1, \dots, k_n\}$ is coloured either red, or blue, or yellow. Now one can ask whether there is an infinite subset H of ω such that all its n-element subsets have the same colour (*i.e.*, $[H]^n$ is **monochromatic**). Such a set we would call **homogeneous** (for the given colouring). In the terminology above, this question reads as follows: Given any colouring (*i.e.*, function) $\pi : [\omega]^n \to 3$, where $3 = \{0, 1, 2\}$, does there exist a set $H \in [\omega]^\omega$ such that $\pi|_{[H]^n}$ is constant? Alternatively, one can define an equivalence relation "$\sim$" on $[\omega]^n$ by stipulating $x \sim y$ *iff* $\pi(x) = \pi(y)$ and ask whether there exists a set $H \in [\omega]^\omega$ such that $[H]^n$ is included in one equivalence class. The answer to this question is given by RAMSEY'S THEOREM 2.1 below, but before we state and prove this theorem, let us say a few words about its background.

Ramsey proved his theorem in order to investigate a problem in formal logic, namely the problem of finding a regular procedure to determine the truth or falsity of a given logical formula in the language of *First-Order Logic*, which is also the language of Set Theory (*cf.* Chapter 3). However, RAMSEY'S THEOREM is a purely combinatorial statement and was the nucleus — but not the earliest result — of a whole combinatorial theory, the so-called *Ramsey Theory*. We would also like to mention that Ramsey's original theorem, which will be discussed later, is somewhat stronger than the theorem stated below but is, like König's Lemma, not provable without assuming some form of the Axiom of Choice (see PROPOSITION 7.8).

THEOREM 2.1 (RAMSEY'S THEOREM). *For any number $n \in \omega$, for any positive number $r \in \omega$, for any $S \in [\omega]^\omega$, and for any colouring $\pi : [S]^n \to r$, there is always an $H \in [S]^\omega$ such that H is homogeneous for π, i.e., the set $[H]^n$ is monochromatic.*

Before we prove RAMSEY'S THEOREM, let us consider a few examples: In the first example we colour the set of prime numbers $\mathbb{P}$ with two colours.

A **Wieferich prime** is a prime number p such that p^2 divides $2^{p-1}-1$, denoted $p^2 \mid 2^{p-1}-1$ — recall that by FERMAT'S LITTLE THEOREM we have $p \mid 2^{p-1}-1$ for any prime p. Now, define the 2-colouring π_1 of $\mathbb{P}$ by stipulating

$$\pi_1(p) = \begin{cases} 0 & \text{if } p \text{ is a Wieferich prime,} \\ 1 & \text{otherwise.} \end{cases}$$

Let $H_0 = \{p \in \mathbb{P} : p^2 \mid 2^{p-1}-1\}$ and $H_1 = \mathbb{P} \setminus H_0$. The only numbers which are known to belong to H_0 are 1093 and 3511. On the other hand, it is not known whether H_1 is infinite. However, by the Infinite Pigeon-Hole Principle we know that at least one of the two sets H_0 and H_1 is infinite, which gives us a homogeneous set for π_1.

As a second example, define the 2-colouring π_2 of the set of 2-element subsets of $\{7l : l \in \omega\}$ by stipulating

$$\pi_2\big(\{n,m\}\big) = \begin{cases} 0 & \text{if } n^m + m^n + 1 \text{ is prime,} \\ 1 & \text{otherwise.} \end{cases}$$

An easy calculation modulo 3 shows that the set $H = \{42k+14 : k \in \omega\} \subseteq \{7l : l \in \omega\}$ is homogeneous for π_2; in fact, for all $\{n,m\} \in [H]^2$ we have $3 \mid (n^m + m^n + 1)$.

Before we give a third example, we prove the following special case of RAMSEY'S THEOREM.

PROPOSITION 2.2. *For any positive number $r \in \omega$, for any $S \in [\omega]^\omega$, and for any colouring $\pi : [S]^2 \to r$, there is always an $H \in [S]^\omega$ such that $[H]^2$ is monochromatic.*

Proof. The proof is in fact just a consequence of the Infinite Pigeon-Hole Principle; firstly, the Infinite Pigeon-Hole Principle is used to construct homogeneous sets for certain 2-colourings τ and then it is used to show the existence of a homogeneous set for π.

Let $S_0 = S$ and let $a_0 = \min(S_0)$. Define the r-colouring $\tau_0 : S_0 \setminus \{a_0\} \to r$ by stipulating $\tau_0(b) := \pi\big(\{a_0, b\}\big)$. By the Infinite Pigeon-Hole Principle there is an infinite set $S_1 \subseteq S_0 \setminus \{a_0\}$ such that $\tau_0|_{S_1}$ is constant (*i.e.*, $\tau_0|_{S_1}$ is a constant function) and let $\rho_0 := \tau_0(b)$, where b is any member of S_1. Now, let $a_1 = \min(S_1)$ and define the r-colouring $\tau_1 : S_1 \setminus \{a_1\} \to r$ by stipulating $\tau_1(b) := \pi\big(\{a_1, b\}\big)$. Again we find an infinite set $S_2 \subseteq S_1 \setminus \{a_1\}$ such that $\tau_1|_{S_2}$ is constant and let $\rho_1 := \tau_1(b)$, where b is any member of S_2. Proceeding this way we finally get infinite sequences $a_0 < a_1 < \ldots < a_n < \ldots$ and $\rho_0, \rho_1, \ldots$. Notice that by construction, for all $n \in \omega$ and all $k > n$ we have $\pi\big(\{a_n, a_k\}\big) = \tau_n(a_k) = \rho_n$. Define the r-colouring $\tau : \{a_n : n \in \omega\} \to r$ by stipulating $\tau(a_n) := \rho_n$. Again by the Infinite Pigeon-Hole Principle there is an infinite set $H \subseteq \{a_n : n \in \omega\}$ such that $\tau|_H$ is constant, which implies that H is homogeneous for π, *i.e.*, $[H]^2$ is monochromatic. ⊣

As a third example, consider the 17-colouring π_3 of the set of 9-element subsets of $\mathbb{P}$ defined by stipulating

$$\pi_3\big(\{p_1, \dots, p_9\}\big) = c \iff p_1 \cdot p_2 \cdot \ldots \cdot p_9 \equiv c \mod 17 .$$

For $0 \leq k \leq 16$ let $P_k = \{p \in \mathbb{P} : p \equiv k \mod 17\}$. Then, by Dirichlet's theorem on primes in arithmetic progression, P_k is infinite whenever $\gcd(k, 17) = 1$, *i.e.*, for all positive numbers $k \leq 16$. Thus, by an easy calculation modulo 17 we get that for $1 \leq k \leq 16$, P_k is homogeneous for π_3.

Now we give a complete proof of RAMSEY'S THEOREM 2.1:

Proof of Ramsey's Theorem. The proof is by induction on n. For $n = 2$ we get PROPOSITION 2.2. So, we assume that the statement is true for $n \geq 2$ and prove it for $n + 1$. Let $\pi : [\omega]^{n+1} \to r$ be any r-colouring of $[\omega]^{n+1}$. For each integer $a \in \omega$ let π_a be the r-colouring of $\big[\omega \setminus \{a\}\big]^n$ defined as follows:

$$\pi_a(x) = \pi\big(x \cup \{a\}\big)$$

By induction hypothesis, for each $S' \in [\omega]^\omega$ and for each $a \in S'$ there is an $H_a^{S'} \in \big[S' \setminus \{a\}\big]^\omega$ such that $H_a^{S'}$ is homogeneous for π_a. Construct now an infinite sequence $a_0 < a_1 < \ldots < a_i < \ldots$ of natural numbers and an infinite sequence $S_0 \supseteq S_1 \supseteq \ldots \supseteq S_i \supseteq \ldots$ of infinite subsets of ω as follows: Let $S_0 = S$ and $a_0 = \min(S)$, and in general let

$$S_{i+1} = H_{a_i}^{S_i}, \text{ and } a_{i+1} = \min\big\{a \in S_{i+1} : a > a_i\big\} .$$

It is clear that for each $i \in \omega$, the set $\big[\{a_m : m > i\}\big]^n$ is monochromatic for π_{a_i}; let $\tau(a_i)$ be its colour (*i.e.*, τ is a colouring of $\{a_i : i \in \omega\}$ with at most r colours). By the Infinite Pigeon-Hole Principle there is an $H \subseteq \{a_i : i \in \omega\}$ such that τ is constant on H, which implies that $\pi|_{[H]^{n+1}}$ is constant, too. Indeed, for any $x_0 < \ldots < x_n$ in H we have $\pi\big(\{x_0, \dots, x_n\}\big) = \pi_{x_0}\big(\{x_1, \dots, x_n\}\big) = \tau(x_0)$, which completes the proof. ⊣

Corollaries of Ramsey's Theorem

In finite Combinatorics, the most important consequence of RAMSEY'S THEOREM 2.1 is its finite version:

COROLLARY 2.3 (FINITE RAMSEY THEOREM). *For all $m, n, r \in \omega$, where $r \geq 1$ and $n \leq m$, there exists an $N \in \omega$, where $N \geq m$, such that for every colouring of $[N]^n$ with r colours, there exists a set $H \in [N]^m$, all of whose n-element subsets have the same colour.*

Proof. Assume towards a contradiction that the FINITE RAMSEY THEOREM fails. So, there are $m, n, r \in \omega$, where $r \geq 1$ and $n \leq m$, such that for all $N \in \omega$

with $N \geq m$ there is a colouring $\pi_N : [N]^n \to r$ such that no $H \in [N]^m$ is homogeneous, *i.e.*, $[H]^n$ is not monochromatic. We shall construct an r-colouring π of $[\omega]^n$ such that no infinite subset of ω is homogeneous for π, contradicting RAMSEY'S THEOREM. The r-colouring π will be induced by an infinite branch through a finitely branching tree, where the infinite branch is obtained by König's Lemma. Thus, we first need an infinite, finitely branching tree. For this, consider the following graph G: The vertex set of G consists of $\emptyset$ and all colourings $\pi_N : [N]^n \to r$, where $N \geq m$, such that no $H \in [N]^m$ is homogeneous for π_N. There is an edge between $\emptyset$ and each r-colouring π_m of $[m]^n$, and there is an edge between the colourings π_N and π_{N+1} *iff* $\pi_N \equiv \pi_{N+1}|_N$ (*i.e.*, for all $x \in [N]^n$, $\pi_{N+1}(x) = \pi_N(x)$). In particular, there is no edge between two different r-colouring of $[N]^n$. By our assumption, the graph G is infinite. Further, by construction, it is cycle-free, connected, finitely branching, and has a root, namely $\emptyset$. In other words, G is an infinite, finitely branching tree and therefore, by König's Lemma, contains an infinite branch of r-colourings, say $(\emptyset, \pi_m, \pi_{m+1}, \ldots, \pi_{m+i}, \ldots)$, where for all $i, j \in \omega$, the colouring π_{m+i+j} is an extension of the colouring π_{m+i}.

At this point we would like to mention that since for any $N \in \omega$ the set of all r-colouring of $[N]^n$ can be ordered, for example lexicographically, we do not need any non-trivial form of the Axiom of Choice to construct an infinite branch.

Now, the infinite branch $(\emptyset, \pi_m, \pi_{m+1}, \ldots)$ induces an r-colouring π of $[\omega]^n$ such that no m-element subset of ω is homogeneous. In particular, there is no infinite set $H \in [\omega]^\omega$ such that $\pi|_{[H]^n}$ is constant, which is a contradiction to RAMSEY'S THEOREM 2.1 and completes the proof. ⊣

The following corollary is a geometrical consequence of the FINITE RAMSEY THEOREM 2.3:

COROLLARY 2.4. *For every positive integer n there exists an $N \in \omega$ with the following property: If P is a set of N points in the Euclidean plane without three collinear points, then P contains n points which form the vertices of a convex n-gon.*

Proof. By the FINITE RAMSEY THEOREM 2.3, let N be such that for every 2-colouring of $[N]^3$ there is a set $H \in [N]^n$ such that $[H]^3$ is monochromatic. Now let N points in the plane be given, and number them from 1 to N in an arbitrary but fixed way. Colour a triple (i, j, k), where $i < j < k$, red, if travelling from i to j to k is in clockwise direction; otherwise, colour it blue. By the choice of N, there are n ordered points so that every triple has the same colour (*i.e.*, orientation) from which one verifies easily (*e.g.*, by considering the convex hull of the n points) that these points form the vertices of a convex n-gon. ⊣

The following theorem — discovered more than a decade before RAMSEY'S THEOREM — is perhaps the earliest result in Ramsey Theory:

COROLLARY 2.5 (SCHUR'S THEOREM). *If the positive integers are finitely coloured (i.e., coloured with finitely many colours), then there are three distinct positive integers x, y, z of the same colour, with $x + y = z$.*

Proof. Let r be a positive integer and let π be any r-colouring of $\omega \setminus \{0\}$. Let $N \in \omega$ be such that for every r-colouring of $[N]^2$ there is a homogeneous 3-element subset of N. Define the colouring $\pi^* : [N]^2 \to r$ by stipulating $\pi^*(i,j) = \pi(|i-j|)$, where $|i-j|$ is the modulus or absolute value of the difference $i - j$. Since N contains a homogeneous 3-element subset (for π^*), there is a triple $0 \leq i < j < k < N$ such that $\pi^*(i,j) = \pi^*(j,k) = \pi^*(i,k)$, which implies that the numbers $x = j - i$, $y = k - j$, and $z = k - i$, have the same colour, and in addition we have $x + y = z$. ⊣

The next result is a purely number-theoretical result and follows quite easily from RAMSEY'S THEOREM. However, somewhat surprisingly, it is unprovable in Number Theory, or more precisely, in *Peano Arithmetic* (which will be discussed in Chapter 3). Before we can state the corollary, we have to introduce the following notion: A non-empty set $S \subseteq \omega$ is called *large* if S has more than $\min(S)$ elements. Further, for $n, m \in \omega$ let $[n, m] := \{i \in \omega : n \leq i \leq m\}$.

COROLLARY 2.6. *For all $n, k, r \in \omega$ with $r \geq 1$, there is an $m \in \omega$ such that for any r-colouring of $\big[[n,m]\big]^k$, there exists a large homogeneous set.*

Proof. Let $n, k, r \in \omega$, where $r \geq 1$, be some arbitrary but fixed numbers. Let $\pi : [\omega \setminus n]^k \to r$ be any r-colouring of the k-element subsets of $\{i \in \omega : i \geq n\}$. By RAMSEY'S THEOREM 2.1 there exists an infinite homogeneous set $H \in [\omega \setminus n]^\omega$. Let $a = \min(H)$ and let S denote the least $a+1$ elements of H. Then S is large and $[S]^k$ is monochromatic.

The existence of a finite number m with the required properties now follows — using König's Lemma — in the very same way as the FINITE RAMSEY THEOREM followed from RAMSEY'S THEOREM (see the proof of the FINITE RAMSEY THEOREM 2.3). ⊣

Generalisations of Ramsey's Theorem

Even though Ramsey's theorems are very powerful combinatorial results, they can still be generalised. The following result will be used later in Chapter 7 in order to prove that the Prime Ideal Theorem — introduced in Chapter 5 — holds in the ordered Mostowski permutation model (but it will not be used anywhere else in this book).

In order to illustrate the next theorem, as well as to show that it is optimal to some extent, we consider the following two examples: Firstly, define the 2-colouring π_1 of $[\omega]^2 \times [\omega]^3 \times [\omega]^1$ by stipulating

$$\pi_1\big(\{x_1,x_2\},\{y_1,y_2,y_3\},\{z_1\}\big) = \begin{cases} 1 & \text{if } 2^{x_1 \cdot x_2} + 13^{y_1 \cdot y_2 \cdot y_3} + 17^{z_1} - 3 \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Let $H_1 = \{3 \cdot k : k \in \omega\}$, $H_2 = \{2 \cdot k : k \in \omega\}$, and $H_3 = \{6 \cdot k : k \in \omega\}$. Then an easy calculation modulo 7 shows that $[H_1]^2 \times [H_2]^3 \times [H_3]^1$ is an infinite monochromatic set.

Secondly, define the 2-colouring π_2 of $[\omega]^1 \times [\omega]^1$ by stipulating

$$\pi_2\big(\{x\},\{y\}\big) = \begin{cases} 1 & \text{if } x < y, \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that whenever H_1 and H_2 are *infinite* subsets of ω, then $[H_1]^1 \times [H_2]^1$ is not monochromatic; on the other hand, we easily find arbitrarily large *finite* sets $M_1, M_2 \subseteq \omega$ such that $[M_1]^1 \times [M_2]^1$ is monochromatic.

Thus, if $[\omega]^{n_1} \times \ldots \times [\omega]^{n_l}$ is coloured with r colours, then, in general, we cannot expect to find infinite subsets of ω, say $H_1, \ldots, H_l$, such that $[H_1]^{n_1} \times \ldots \times [H_l]^{n_l}$ is monochromatic; but we always find arbitrarily large finite subsets of ω:

THEOREM 2.7. *Let $r, l, n_1, \ldots, n_l \in \omega$ with $r \geq 1$ be given. For every $m \in \omega$ with $m \geq \max\{n_1, \ldots, n_l\}$ there is some $N \in \omega$ such that whenever $[N]^{n_1} \times \ldots \times [N]^{n_l}$ is coloured with r colours, then there are $M_1, \ldots, M_l \in [N]^m$ such that $[M_1]^{n_1} \times \ldots \times [M_l]^{n_l}$ is monochromatic.*

Proof. The proof is by induction on l and the induction step uses a so-called *product-argument*. For $l = 1$ the statement is equivalent to the FINITE RAMSEY THEOREM 2.3. So, assume that the statement is true for $l \geq 1$ and let us prove it for $l + 1$. By induction hypothesis, for every $r \geq 1$ there is an N_l (depending on r) such that for *every* r-colouring of $[N_l]^{n_1} \times \ldots \times [N_l]^{n_l}$ there are $M_1, \ldots, M_l \in [N_l]^m$ such that $[M_1]^{n_1} \times \ldots \times [M_l]^{n_l}$ is monochromatic. Now, the crucial idea in order to apply the FINITE RAMSEY THEOREM is to consider the coloured l-tuples in $\big([N_l]^m\big)^l$ as new colours. More precisely, let u_l be the number of different l-tuples in $\big([N_l]^m\big)^l$ and let $r_l := u_l \cdot r$. Notice that each colour in r_l corresponds to a pair $\langle t, c\rangle$, where t is an l-tuple in $\big([N_l]^m\big)^l$ and c is one of r colours. Notice also that r_l is very large compared to r. Now, by the FINITE RAMSEY THEOREM 2.3, there is a number $N_{l+1} \in \omega$ such that whenever $[N_{l+1}]^{n_{l+1}}$ is coloured with r_l colours, then there exists an $M_{l+1} \in [N_{l+1}]^m$ such that $[M_{l+1}]^{n_{l+1}}$ is monochromatic. Let $N = \max\{N_l, N_{l+1}\}$ and let π be any r-colouring of $[N_l]^{n_1} \times \ldots \times [N_l]^{n_l} \times [N]^{n_{l+1}}$. For every $F \in [N]^{n_{l+1}}$ let π^F be the r-colouring of $[N_l]^{n_1} \times \ldots \times [N_l]^{n_l}$ defined by stipulating

$$\pi^F(X) = \pi\big(\langle X, F\rangle\big).$$

By the definition of N, for every $F \in [N]^{n_{l+1}}$ there is a lexicographically first l-tuple $\big(M_1^F, \ldots, M_l^F\big) \in \big([N_l]^m\big)^l$ such that $\big[M_1^F\big]^{n_1} \times \ldots \times \big[M_l^F\big]^{n_l}$ is monochromatic for π^F. By definition of r_l we can define an r_l-colouring π_{l+1} on $[N]^{n_{l+1}}$ as follows: Every set $F \in [N]^{n_{l+1}}$ is coloured according to the l-tuple $t = \big(M_1^F, \ldots, M_l^F\big)$ (which can be encoded as one of u_l numbers) and the colour $c = \pi^F(X)$, where X is any element of the set $\left[M_1^F\right]^{n_1} \times \ldots \times \left[M_l^F\right]^{n_l}$; because $\left[M_1^F\right]^{n_1} \times \ldots \times \left[M_l^F\right]^{n_l}$ is monochromatic for π^F, c is well-defined and one of r colours. In other words, for every $F \in [N]^{n_{l+1}}$, $\pi_{l+1}(F)$ correspond to a pair $\langle t, c\rangle$, where $t \in \left([N_l]^m\right)^l$ and c is one of r colours. Finally, by definition of N, there is a set $M_{l+1} \in [N]^m$ such that $[M_{l+1}]^{n_{l+1}}$ is monochromatic for π_{l+1}, which implies that for all $F, F_1, F_2 \in [M_{l+1}]^{n_{l+1}}$ we have:

- $\left[M_1^F\right]^{n_1} \times \ldots \times \left[M_l^F\right]^{n_l}$ is monochromatic for π^F,
- $\left(M_1^{F_1}, \ldots, M_l^{F_1}\right) = \left(M_1^{F_2}, \ldots, M_l^{F_2}\right)$,
- and restricted to the set $\left[M_1^F\right]^{n_1} \times \ldots \times \left[M_l^F\right]^{n_l}$, the colourings $\pi_l^{F_1}$ and $\pi_l^{F_2}$ are identical.

Hence, there are $M_1, \ldots, M_{l+1} \in [N]^m$ such that $\pi|_{[M_1]^{n_1} \times \ldots \times [M_{l+1}]^{n_{l+1}}}$ is constant, which completes the proof. $\dashv$

A very strong generalisation of RAMSEY'S THEOREM in terms of partitions is the PARTITION RAMSEY THEOREM 11.4. However, since the proof of this generalisation is quite involved, we postpone the discussion of that result until Chapter 11 and consider now some other possible generalisations of RAMSEY'S THEOREM: Firstly one could finitely colour all finite subsets of ω, secondly one could colour $[\omega]^n$ with infinitely many colours, and finally, one could finitely colour all the infinite subsets of ω. However, below we shall see that none of these generalisations works, but first, let us consider Ramsey's original theorem, which is — at least in the absence of the Axiom of Choice — also a generalisation of RAMSEY'S THEOREM.

Ramsey's Original Theorem.

The theorem which Ramsey proved originally is somewhat stronger than what we proved above. In our terminology, it states as follows:

RAMSEY'S ORIGINAL THEOREM. *For any infinite set A, for any number $n \in \omega$, for any positive number $r \in \omega$, and for any colouring $\pi : [A]^n \to r$, there is an infinite set $H \subseteq A$ such that $[H]^n$ is monochromatic.*

Notice that the difference is just that the infinite set A is not necessarily a subset of ω, and therefore, it does not necessarily contain a countable infinite subset. However, this difference is crucial, since one can show that, like König's Lemma, this statement is not provable without assuming some form of the Axiom of Choice (AC). On the other hand, if one has AC, then every infinite set has a countably infinite subset, and so RAMSEY'S THEOREM implies the original version. Ramsey was aware of this fact and stated explicitly that he is assuming the *axiom of selections* (*i.e.*, AC). Even though we do not need full AC in order to prove RAMSEY'S ORIGINAL THEOREM, there is no way to avoid some non-trivial kind of choice, since there are models of Set Theory in which RAMSEY'S ORIGINAL THEOREM fails (*cf.* PROPOSITION 7.8). Consequently, RAMSEY'S ORIGINAL THEOREM can be used as a choice principle, which will be discussed in Chapter 5.

Finite Colourings of $[\omega]^{<\omega}$

Assume we have coloured all the finite subsets of ω with two colours, say red and blue. Can we be sure that there is an infinite subset of ω such that all its finite subsets have the same colour? The answer to this question is negative and it is not hard to find a counterexample (*e.g.*, colour a set $x \in [\omega]^{<\omega}$ blue, if $|x|$ is even; otherwise, colour it red).

Thus, let us ask for slightly less. Is is there at least an infinite subset of ω such that for each $n \in \omega$, all its n-element subsets have the same colour? The answer to this question is also negative: Colour a non-empty set $x \in [\omega]^{<\omega}$ red, if x has more than $\min(x)$ elements (*i.e.*, x is large); otherwise, colour it blue. Now, let I be an infinite subset of ω and let $n = \min(I)$. We leave it as an exercise to the reader to verify that $[I]^{n+1}$ is dichromatic.

The picture changes if we are asking just for an almost homogeneous sets: An infinite set $H \subseteq \omega$ is called **almost homogeneous** for a colouring $\pi : [\omega]^n \to r$ (where $n \in \omega$ and r is a positive integer), if there is a finite set $K \subseteq \omega$ such that $H \setminus K$ is homogeneous for π. Now, for a positive integer r consider any colouring $\bar{\pi} : [\omega]^{<\omega} \to r$. Then, for each $n \in \omega$, $\bar{\pi}|_{[\omega]^n}$ is a colouring $\pi_n : [\omega]^n \to r$. Is there an infinite set $H \subseteq \omega$ which is almost homogeneous for all π_n's simultaneously? The answer to this question is affirmative and is given by the following result.

PROPOSITION 2.8. *Let $\{r_k : k \in \omega\}$ and $\{n_k : k \in \omega\}$ be two (possibly finite) sets of positive integers, and for each $k \in \omega$ let $\pi_k : [\omega]^{n_k} \to r_k$ be a colouring. Then there exists an infinite set $H \subseteq \omega$ which is almost homogeneous for each π_k $(k \in \omega)$.*

Proof. A first attempt to construct the required almost homogeneous set would be to start with an $I_0 \in [\omega]^\omega$ which is homogeneous for π_0, then take an $I_1 \in [I_0]^\omega$ which is homogeneous for π_1, *et cetera*, and finally take the intersection of all the I_k's. Even though this attempt fails — since it is very likely that we end up with the empty set — it is the right direction. In fact, if the intersection of the I_k's would be non-empty, it would be homogeneous for all π_k's, which is more than what is required. In order to end up with an infinite set we just have to modify the above approach — the trick, which is used almost always when the word "almost" is involved, is called *diagonalisation*.

The proof is by induction on k: By RAMSEY'S THEOREM 2.1 there exists an $H_0 \in [\omega]^\omega$ which is homogeneous for π_0. Assume we have already constructed $H_k \in [\omega]^\omega$ (for some $k \geq 0$) such that H_k is homogeneous for π_k. Let $a_k = \min(H_k)$ and let $S_k = H_k \setminus \{a_k\}$. Then, again by RAMSEY'S THEOREM 2.1, there exists an $H_{k+1} \in [S_k]^\omega$ such that H_{k+1} is homogeneous for π_{k+1}. Let $H = \{a_k : k \in \omega\}$. Then, by construction, for every $k \in \omega$ we have that

$H \setminus \{a_0, \dots, a_{k-1}\}$ is homogeneous for π_k, which implies that H is almost homogeneous for all π_k's simultaneously. ⊣

Now we could ask what is the least number of 2-colourings of 2-element subsets of ω we need in order to make sure that no single infinite subset of ω is almost homogeneous for all colourings simultaneously? By PROPOSITION 2.8 we know that countably many colourings are not sufficient, but as we will see later, the axioms of Set Theory do not decide how large this number is (*cf.* Chapter 18).

The dual question would be as follows: How large must a family of infinite subsets of ω be, in order to make sure that for each 2-colouring of the 2-element subsets of ω we find a set in the family which is homogeneous for this colouring? Again, the axioms of Set Theory do not decide how large this number is (*cf.* Chapter 18).

Going to the Infinite

There are two parameters involved in a colouring $\pi : [\omega]^n \to r$, namely n and r. Let first consider the case when $n = 2$ and $r = \omega$. In this case, we obviously cannot hope for any infinite homogeneous or almost homogeneous set. However, there are still infinite subsets of ω which are homogeneous in a broader sense which leads to the CANONICAL RAMSEY THEOREM. Even though the CANONICAL RAMSEY THEOREM is a proper generalisation of RAMSEY'S THEOREM, we will not discuss it here (but see RELATED RESULT 0).

In the case when $n = \omega$ and $r = 2$ we cannot hope for an infinite homogeneous set, as the following example illustrates (compare this result with Chapter 5 | RELATED RESULT 38):

In the presence of the Axiom of Choice *there is a 2-colouring of $[\omega]^\omega$ such that there is no infinite set, all whose infinite subsets have the same colour.*

The idea is to construct (or more precisely, to prove the existence of) a colouring of $[\omega]^\omega$ with say red and blue in such a way that whenever an infinite set $x \in [\omega]^\omega$ is coloured blue, then for each $a \in x$, $x \setminus \{a\}$ is coloured red, and vice versa.

For this, define an equivalence relation on $[\omega]^\omega$ as follows: for $x, y \in [\omega]^\omega$ let

$$x \sim y \iff x \triangle y \text{ is finite}$$

where $x \triangle y = (x \setminus y) \cup (y \setminus x)$ is the **symmetric difference** of x and y. It is easily checked that the relation "$\sim$" is indeed an equivalence relation on $[\omega]^\omega$. Further, let $\mathscr{A} \subseteq [\omega]^\omega$ be any set of representatives, *i.e.*, $\mathscr{A}$ has exactly one element in common with each equivalence class. Since the existence of the set $\mathscr{A}$ relies on the Axiom of Choice, the given proof is not entirely constructive.

Colour now an infinite set $x \in [\omega]^\omega$ blue, if $|x \triangle r_x|$ is even, where $r_x \in (\mathscr{A} \cap [x]^{\tilde{}})$; otherwise, colour it red. Since two sets $x, y \in [\omega]^\omega$ with finite symmetric difference are always equivalent, every infinite subset of ω must contain blue as well as red coloured infinite subsets.

So, there is a colouring $\pi : [\omega]^\omega \to \{0,1\}$ such that for no $x \in [\omega]^\omega$, $\pi|_{[x]^\omega}$ is constant. On the other hand, if the colouring is not too sophisticated we may find a homogeneous set: For $\mathscr{A} \subseteq [\omega]^\omega$ define $\pi_{\mathscr{A}} : [\omega]^\omega \to \{0,1\}$ by stipulating $\pi_{\mathscr{A}}(x) = 1$ *iff* $x \in \mathscr{A}$. Now we say that the set $\mathscr{A} \subseteq [\omega]^\omega$ has the **Ramsey property** if there exists an $x_h \in [\omega]^\omega$ such that $\pi_{\mathscr{A}}|_{[x]^\omega}$ is constant. In other words, $\mathscr{A} \subseteq [\omega]^\omega$ has the Ramsey property if and only if there exists an $x_h \in [\omega]^\omega$ such that either $[x_h]^\omega \subseteq \mathscr{A}$ or $x_h]^\omega \cap \mathscr{A} = \emptyset$. The Ramsey property is related to the cardinal $\mathfrak{h}$ (*cf.* Chapter 8) and will be discussed in Chapter 9.

A slightly weaker property than the Ramsey property is the so-called *doughnut property*: If a and b are subsets of ω such that $b \setminus a$ is infinite, then we call the set $[a,b]^\omega := \{x \in [\omega]^\omega : a \subseteq x \subseteq b\}$ a **doughnut**. (Why such sets are called "doughnuts" is left to the reader's imagination.) Now, a set $\mathscr{A} \subseteq [\omega]^\omega$ is said to have the **doughnut property** if there exists an doughnut $[a,b]^\omega$ (for some a and b) such that either $[a,b]^\omega \subseteq \mathscr{A}$ or $[a,b]^\omega \cap \mathscr{A} = \emptyset$. Obviously, every set with the Ramsey property has also the doughnut property (consider doughnuts of the form $[\emptyset, b]^\omega$). On the other hand, it is not difficult to show that, in the presence of the Axiom of Choice, there are sets with the doughnut property which fail to have the Ramsey property (just modify the example given above).

Notes

Ramsey's Theorem. Frank Plumpton Ramsey (1903-1930), the elder brother of Arthur Michael Ramsey (who was Archbishop of Canterbury from 1961 to 1974), proved his famous theorem in [34] and the part of the volume in which his article appeared was issued on the 16^{th} of December in 1929, but the volume itself belongs to the years 1929 and 1930 (which caused some confusion about the year Ramsey's article was actually published). However, Ramsey submitted his paper already in November 1928. For Ramsey's paper and its relation to First-Order Logic, as well as for an introduction to Ramsey Theory in general, we refer the reader to the classical textbook by Graham, Rothschild, and Spencer [16] (for Ramsey's other papers on Logic see [35]). In [34], RAMSEY'S THEOREM 2.1 appears as THEOREM A and the FINITE RAMSEY THEOREM 2.3 is proved as a corollary and appears as THEOREM B. Although RAMSEY'S THEOREM is accurately attributed to Ramsey, its popularisation stems from the classical paper of Erdős and Szekerés [9], where they proved (independently of Ramsey) COROLLARY 2.4 — which can be seen as a variant of the FINITE RAMSEY THEOREM 2.3 in a geometrical context (see also Morris and Soltan [27]). The elegant proof we gave for COROLLARY 2.4 is due to Tarsy (*cf.* Lewin [25] or Graham, Rothschild, and Spencer [16, p. 26]).

Schur's Theorem. Schur's original paper [36] was motivated by FERMAT'S LAST THEOREM, and he actually proved the following result: *For all natural numbers m, if p is prime and sufficiently large, then the equation $x^m + y^m = z^m$ has a non-zero solution in the integers modulo p.* A proof of this theorem can also be found in

Graham, Rothschild, and Spencer [16, Section 3.1]. For some historical background and for the early development of Ramsey Theory (before Ramsey) see Soifer [38].
The Paris-Harrington Result. As mentioned above, COROLLARY 2.6 is true but unprovable in *Peano Arithmetic* (also called *First-Order Arithmetic*). This result was the first natural example of such a statement and is due to Paris and Harrington [31] (see also Graham, Rothschild, and Spencer [16, Section 6.3]). For other statements of that type see Paris [30].

It is worth mentioning that Peano Arithmetic is, in a suitable sense, equivalent to Zermelo-Fraenkel Set Theory with the Axiom of Infinity replaced by its negation, which is a reasonable formalisation of standard combinatorial reasoning about finite sets.

Rado's generalisation of the Finite Ramsey Theorem. THEOREM 2.7, which is the only proper generalisation of the FINITE RAMSEY THEOREM shown in this book so far, is due to Rado [32] (see also page 113, Problems 4 & 5 of Jech [23]).

Ramsey sets and doughnuts. Even though the Ramsey property and the doughnut property look very similar, there are sets which have the Ramsey property, but which fail to have the doughnut property. For the relation between the doughnut property and other regularity properties see for example Halbeisen [18] or Brendle, Halbeisen, and Löwe [4] (see also Chapter 9 | RELATED RESULT 60).

RELATED RESULTS

0. *Canonical Ramsey Theorem.* The following result, known as the CANONICAL RAMSEY THEOREM, is due to Erdős and Rado (*cf.* [8, Theorem I]): *Whenever we have a colouring π of $[\omega]^n$, for some $n \in \omega$, with an arbitrary (e.g., infinite) set of colours, there exist an infinite set $H \subseteq \omega$ and a set $I \subseteq \{1, 2, \ldots, n\}$ such that for any ordered n-element subsets $\{k_1 < \ldots < k_n\}, \{l_1 < \ldots < l_n\} \in [H]^n$ we have $\pi(\{k_1, \ldots, k_n\}) = \pi(\{l_1, \ldots, l_n\}) \iff k_i = l_i$ for all $i \in I$.* The 2^n possible choices for I correspond to the so-called *canonical colourings* of $[\omega]^n$. As an example let us consider the case when $n = 2$: Let π be an arbitrary colouring of $[\omega]^2$ and let $H \in [\omega]^\omega$ and $I \subseteq \{1, 2\}$ be as above. Then we are in exactly one of the following four cases for *all* $\{k_1 < k_2\}, \{l_1 < l_2\} \in [H]^2$ (*cf.* [8, Theorem II]):

   (1) If $I = \emptyset$, then $\pi(\{k_1, k_2\}) = \pi(\{l_1, l_2\})$.
   (2) If $I = \{1, 2\}$, then $\pi(\{k_1, k_2\}) = \pi(\{l_1, l_2\})$ *iff* $\{k_1, k_2\} = \{l_1, l_2\}$.
   (3) If $I = \{1\}$, then $\pi(\{k_1, k_2\}) = \pi(\{l_1, l_2\})$ *iff* $k_1 = l_1$.
   (4) If $I = \{2\}$, then $\pi(\{k_1, k_2\}) = \pi(\{l_1, l_2\})$ *iff* $k_2 = l_2$.

   Obviously, if π is a finite colouring of $[\omega]^n$, then we are always in case (1), which gives us just RAMSEY'S THEOREM 2.1.

1. *Ramsey numbers.* The least number of people that must be invited to a party, in order to make sure that n of them mutually shook hands before or m of them mutually did not shake hands before, is denoted by $R(n, m)$, and the numbers $R(n, m)$ are called **Ramsey numbers**. Notice that by the FINITE RAMSEY THEOREM, Ramsey numbers $R(n, m)$ exist for all integers $n, m \in \omega$. Very few Ramsey numbers are actually known. It is easy to show that $R(2, 3) = 3$ (in

general, $R(2,n) = n$), and we leave it as an exercise to show that $R(3,3) = 6$. A comprehensive list of what is known about small Ramsey numbers is maintained by Radziszowski [33].

2. *Monochromatic triangles in K_6-free graphs.* Erdős and Hajnal [10] asked for a graph which contains no K_6 (*i.e.*, no complete graph on 6 vertices) but has the property that whenever its edges are 2-coloured there must be a monochromatic triangle. A minimal example for such a graph was provided by Graham [14]: On the one hand he showed that if a 5-cycle is deleted from a K_8, then the resulting graph contains no K_6 and has the property that whenever its edges are 2-coloured there is a monochromatic triangle. On the other hand, if a graph on 7 vertices contains no K_6, then there is a 2-colouring of the edges with no monochromatic triangle.

3. *Hindman's Theorem.* If $F \in [\omega]^{<\omega}$, then we write ΣF for $\Sigma_{a\in F}\, a$, where as usual we define $\Sigma\emptyset := 0$. HINDMAN'S THEOREM states that if ω is finitely coloured, then there is an $x \in [\omega]^{\omega}$ such that $\{\Sigma F : F \in [x]^{<\omega} \wedge F \neq \emptyset\}$ is monochromatic (*cf.* Hindman [21, Theorem 3.1] or Hindman and Strauss [22, Corollary 5.10] where references to alternative proofs are given on page 102). Using HINDMAN'S THEOREM as a strong Pigeon-Hole Principle, Milliken proved in [26] a strengthened version of RAMSEY'S THEOREM 2.1 which includes HINDMAN'S THEOREM as well as RAMSEY'S THEOREM 2.1. Since Milliken's result was proved independently by Taylor (*cf.* [39]), it is usually called MILLIKEN-TAYLOR THEOREM. In order to state this result we have to introduce some notation. Two finite sets $K_1, K_2 \subseteq \omega$ are said to be *unmeshed* if $\max(K_1) < \min(K_2)$ or $\max(K_2) < \min(K_1)$. If I and H are two sets of pairwise unmeshed finite subsets of ω and every member of I is the union of (finitely many) members of H, then we write $I \sqsubseteq H$. Further, let $\langle\omega\rangle^{\omega}$ denote the set of all infinite sets of pairwise unmeshed finite subsets of ω, and for $H \in \langle\omega\rangle^{\omega}$ let $\langle H\rangle^{n} := \{I : |I| = n \text{ and } I \sqsubseteq H\}$. Now, the MILLIKEN-TAYLOR THEOREM states as follows: *If all the n-element sets of pairwise unmeshed finite subsets of ω are finitely coloured, then there exists an $H \in \langle\omega\rangle^{\omega}$ such that $\langle H\rangle^{n}$ is monochromatic.*

4. *Colourings of the plane.* Erdős [7] proved that there is a colouring of the Euclidean plane with countably many colours, such that any two points at a rational distance have different colours. This result was strengthened by Komjáth [24] in the following way: *Let $\mathbb{Q}$ be the set of rational numbers and let $Q := \{(q,0) : q \in \mathbb{Q}\}$ be a copy of the rationals in the Euclidean plane. Then there exists a colouring of the Euclidean plane with countably many colours, such that for any rigid motion σ of the plane, every colour occurs in $\sigma[Q] = \big\{\sigma(p) : p \in Q\big\}$ exactly once.*

5. *Finite colourings of $\mathbb{Q}$.* If we colour the rational numbers $\mathbb{Q}$ with finitely many colours, is there always an infinite homogeneous set which is order-isomorphic to $\mathbb{Q}$? In general, this is not the case: Let $\{q_n : n \in \omega\}$ be an enumeration of $\mathbb{Q}$ (see Chapter 4, in particular RELATED RESULT 14) and colour a pair $\{q_i, q_j\}$ blue if $q_i < q_j \leftrightarrow i < j$, otherwise, colour it red. Then it is easy to see that an infinite homogeneous set which is order-isomorphic to $\mathbb{Q}$ would yield an infinite decreasing sequence of natural numbers, which is obviously not possible. On the other hand, for every positive integer $n \in \omega$ there is a smallest number

$t_n \in \omega$ such that if $[\mathbb{Q}]^n$ is finitely coloured then there is an infinite set $X \subseteq \mathbb{Q}$ which is order-isomorphic to $\mathbb{Q}$ such that $[X]^n$ is coloured with at most t_n colours. For this see Devlin [6] or Vuksanović [41], where it is shown that such numbers exist and that the sequence of numbers t_n coincides with the so-called *tangent numbers* (*cf.* Sloane [37, A000182]). In particular, $t_1 = 1$ and for $n \geq 2$, $t_n = \sum_{i=1}^{n-1} \binom{2n-2}{2i-1} t_i t_{n-i}$.

6. *Symmetry and colourings.* Banakh and Protasov investigated in [2] the following problem: Is it true that for every n-colouring of the group $\mathbb{Z}^n$ there exists an infinite monochromatic subset of $\mathbb{Z}^n$ which is symmetric with respect to a central reflection. It turns out that the answer is always positive (for all n). However, there exists a 4-colouring of $\mathbb{Z}^3$ without infinite, symmetric, monochromatic set. For more general results we refer the reader to Banakh, Verbitski, and Vorobets [3].

7. *Wieferich primes*.* The so-called Wieferich primes were first introduced by Wieferich in [42] in relation to FERMAT'S LAST THEOREM. As mentioned above, the only known Wieferich primes (less than $1.25 \cdot 10^{15}$) are 1093 and 3511 (found in 1913 and 1922 respectively). It is not known if there are infinitely many primes of this type, even though it is conjectured that this is the case (see for example Halbeisen and Hungerbühler [19]). Moreover, it is not even known whether there are infinitely many non-Wieferich primes — although it is very likely to be the case.

8. *Sums and products.* As a consequence of RAMSEY'S THEOREM we get that if ω is finitely coloured, then there are infinite sequences of positive integers $(x_0, x_1, \ldots, x_k, \ldots)$ and $(y_0, y_1, \ldots, y_k, \ldots)$ such that $\{x_i + x_j : i, j \in \omega \wedge i < j\}$ as well as $\{y_i \cdot y_j : i, j \in \omega \wedge i < j\}$ is monochromatic (but not necessarily of the same colour). On the other hand, it is known (*cf.* Hindman and Strauss [22, Chapter 17.2]) that *one can colour the positive integers with finitely many colours in such a way that there is* no *infinite sequence* $(x_0, x_1, \ldots, x_k, \ldots)$ *such that* $\{x_i + x_j : i, j \in \omega \wedge i < j\} \cup \{x_i \cdot x_j : i, j \in \omega \wedge i < j\}$ *is monochromatic.*

9. *The graph of pairwise sums and products*.* One can show that if ω is 2-coloured, then there are infinitely many pairs of distinct positive integers x and y such that $x + y$ has the same colour as $x \cdot y$. For this consider the graph on ω with n joined to m if for some distinct $x, y \in \omega$ we have $x + y = n$ and $x \cdot y = m$. Now, notice that it is enough to show that this so-called *graph of pairwise sums and products* contains infinitely many triangles (*cf.* Halbeisen [17]).
Suppose now that ω is finitely coloured. Are there two distinct positive integers x and y such that $x + y$ has the same colour as $x \cdot y$? This problem — which is equivalent to asking whether the chromatic number of the graph of pairwise sums and products is finite or infinite — is still open (*cf.* Hindman and Strauss [22, Question 17.18]). A partial result is given in Halbeisen [17], where it is shown that such numbers x and y exist if ω is 3-coloured.

10. *Problems in Ramsey Theory*.* For a variety of open problems from Ramsey Theory we refer the reader to Graham [15] (it might be worth mentioning that Graham is offering modest rewards for most of the presented problems).

11. *Applications of Ramsey Theory to Banach Space Theory.* There are many — and sometimes quite unexpected — applications of Ramsey Theory to Banach Space

Theory (see for example Odell [28], Gowers [13], or Argyros and Todorčević [1]). Let us mention just the following two applications:

An unexpected application of Ramsey Theory to Banach Space Theory is due to Brunel and Sucheston [5]: *If $x_1, x_2, \ldots$ is an infinite normalised basic sequence in a Banach space X and $\varepsilon_n \searrow 0$ (a sequence of positive real numbers which tends to 0), then one can find an infinite subsequence $y_1, y_2, \ldots$ of $x_1, x_2, \ldots$ which has the following property: For any positive $n \in \omega$, any sequence of scalars $(a_1, \ldots, a_n) \in [-1,1]^n$ and any natural numbers $n \leq i_0 < \ldots < i_{n-1}$ and $n \leq j_0 < \ldots < j_{n-1}$ we have*

$$\left| \Big\| \sum_{k=1}^{n} a_k y_{i_k} \Big\| - \Big\| \sum_{k=1}^{n} a_k y_{j_k} \Big\| \right| < \varepsilon_n \,.$$

The limit $\| \sum_{k=1}^{n} a_k \tilde{e}_k \|$ we obtain for each finite sequence $(a_1, \ldots, a_n) \in [-1,1]^n$ leads to the sequence $\tilde{e}_1, \tilde{e}_2, \ldots$, and the Banach space generated by $\tilde{e}_1, \tilde{e}_2, \ldots$ is called a *spreading model* of X. The notion of spreading models was generalised (*e.g.*, using the MILLIKEN-TAYLOR THEOREM) and investigated by Halbeisen and Odell in [20].

Another example is due to Gowers [11, 12] (see also Todorčević [40, Section 2.3]), who discovered the long sought *Block Ramsey Theorem* — a genuinely new Ramsey-type result — for Banach spaces, which he used to prove his famous DICHOTOMY THEOREM (see also Gowers [13, Section 5] or Odell [29]): *Every Banach space X contains a subspace Y which either has an unconditional basis or is hereditarily indecomposable (i.e., Y contains no subspaces having a non-trivial complemented subspace).*

REFERENCES

1. SPIROS A. ARGYROS AND STEVO TODORČEVIĆ, ***Ramsey Methods in Analysis***, [Advanced Courses in Mathematics – CRM Barcelona], Birkhäuser, Basel, 2005.
2. TARAS O. BANAKH AND IGOR V. PROTASOV, *Symmetry and colorings: some results and open problems*, ***Izdatel'stvo Gomel'skogo Universiteta. Voprosy Algebry***, vol. 17 (2001), 5–16.
3. TARAS O. BANAKH, OLEG V. VERBITSKI, AND YAROSLAV B. VOROBETS, *A Ramsey treatment of symmetry*, ***The Electronic Journal of Combinatorics***, vol. 7 #R52 (2000), 25pp.
4. JÖRG BRENDLE, LORENZ HALBEISEN, AND BENEDIKT LÖWE, *Silver measurability and its relation to other regularity properties*, ***Mathematical Proceedings of the Cambridge Philosophical Society***, vol. 138 (2005), 135–149.
5. ANTOINE BRUNEL AND LOUIS SUCHESTON, *B-convex Banach spaces*, ***Mathematical Systems Theory***, vol. 7 (1973), 294–299.
6. DENNIS DEVLIN, *Some partition theorems and ultrafilters on ω*, Ph.D. thesis (1979), Dartmouth College, Hanover (USA).
7. PAUL ERDŐS, *Problems and results in chromatic number theory*, in ***Proof Techniques in Graph Theory*** (F. Harary, ed.), Academic Press, New York, 1969, pp. 47–55.
8. PAUL ERDŐS AND RICHARD RADO, *A combinatorial theorem*, ***Journal of the London Mathematical Society***, vol. 25 (1950), 249–255.

9. Paul Erdős and George Szekerés, *A combinatorial problem in geometry*, ***Compositio Mathematica***, vol. 2 (1935), 463–470.
10. Paul Erdős and András Hajnal, *Research problem 2-5*, ***Journal of Combinatorial Theory***, vol. 2 (1967), 105.
11. W. Timothy Gowers, *A new dichotomy for Banach spaces*, ***Geometric and Functional Analysis***, vol. 6 (1996), 1083–1093.
12. ______, *An infinite Ramsey theorem and some Banach-space dichotomies*, ***Annals of Mathematics (2)***, vol. 156 (2002), 797–833.
13. ______, *Ramsey methods in Banach spaces*, in ***Handbook of the geometry of Banach spaces, Vol. 2*** (William B. Johnson and Joram Lindenstrauss, eds.), North-Holland, Amsterdam, 2003, pp. 1071–1097.
14. Ronald L. Graham, *On edgewise 2-colored graphs with monochromatic triangles and containing no complete hexagon*, ***Journal of Combinatorial Theory***, vol. 4 (1968), 300.
15. ______, *Some of my favorite problems in Ramsey theory*, in ***Combinatorial Number Theory*** (Bruce Landman, Melvyn B. Nathanson, Jaroslav Nešetřil, Richard J. Nowakowski, and Carl Pomerance, eds.), Proceedings of the 'Integers Conference 2005' in Celebration of the 70th Birthday of Ronald Graham. Carrollton, Georgia, USA, October 27–30, 2005, Walter de Gruyter, Berlin, 2007, pp. 229–236.
16. Ronald L. Graham, Bruce L. Rothschild, and Joel H. Spencer, ***Ramsey Theory***, 2nd ed., J. Wiley & Sons, New York, 1980.
17. Lorenz Halbeisen, *Fans and bundles in the graph of pairwise sums and products*, ***The Electronic Journal of Combinatorics,*** 11(1) (2004) #R6, 11pp.
18. ______, *Making doughnuts of Cohen reals*, ***Mathematical Logic Quarterly***, vol. 49 (2003), 173–178.
19. Lorenz Halbeisen and Norbert Hungerbühler, *On generalized Carmichael numbers*, ***Hardy-Ramanujan Journal***, vol. 22 (1999), 8–22.
20. Lorenz Halbeisen and Edward W. Odell, *On asymptotic models in Banach spaces*, ***Israel Journal of Mathematics***, vol. 139 (2004), 253–291.
21. Neil Hindman, *Finite sums from sequences within cells of a partition of N*, ***Journal of Combinatorial Theory (A)***, vol. 17 (1974), 1–11.
22. Neil Hindman and Dona Strauss, ***Algebra in the Stone-Čech Compactification: Theory and Applications***, [De Gruyter Expostitions in Mathematics], Walter de Gruyter, New York, 1998.
23. Thomas Jech, ***The Axiom of Choice***, Studies in Logic and the Foundations of Mathematics 75, North-Holland, Amsterdam, 1973.
24. Péter Komjáth, *A coloring result for the plane*, ***Journal of Applied Analysis***, vol. 5 (1999), 113–117.
25. Mordechai Lewin, *A new proof of a theorem of Erdős and Szekerés*, ***The Mathematical Gazette***, vol. 60 (1976), 136–138 (correction ibid., p. 298).
26. Keith R. Milliken, *Ramsey's theorem with sums or unions*, ***Journal of Combinatorial Theory (A)***, vol. 18 (1975), 276–290.
27. Walter D. Morris and Valeriu Soltan, *The Erdős-Szekeres problem on points in convex position – a survey*, ***Bulletin of the American Mathematical Society***, vol. 37 (2000), 437–458.
28. Edward W. Odell, *Applications of Ramsey theorems to Banach space theory*, in ***Notes in Banach Spaces*** (H.E. Lacey, ed.), University Press, Austin and London, Austin TX, 1980, pp. 379–404.

29. ______, *On subspaces, asymptotic structure, and distortion of Banach spaces; connections with logic*, in ***Analysis and Logic*** (Catherine Finet and Christian Michaux, eds.), [London Mathematical Society Lecture Note Series 262], Cambridge University Press, Cambridge, 2002, pp. 189–267.
30. Jeff B. Paris, *Combinatorial statements independent of arithmetic*, in ***Mathematics of Ramsey Theory*** (J. Nešetřil and V. Rödl, eds.), Springer-Verlag, Berlin, 1990, pp. 232–245.
31. Jeff B. Paris and Leo Harrington, *A mathematical incompleteness in Peano arithmetic*, in ***Handbook of Mathematical Logic*** (J. Barwise, ed.), North-Holland, Amsterdam, 1977, pp. 1133–1142.
32. Richard Rado, *Direct decomposition of partitions*, ***Journal of the London Mathematical Society***, vol. 29 (1954), 71–83.
33. Stanisław P. Radziszowski, *Small Ramsey numbers*, ***The Electronic Journal of Combinatorics,*** Dynamic Surveys 1, (August 1, 2006), 60pp.
34. Frank P. Ramsey, *On a problem of formal logic*, ***Proceedings of the London Mathematical Society, Ser. II***, vol. 30 (1930), 264–286.
35. ______, ***The Foundations of Mathematics and other Logical Essays***, edited by R. B. Braithwaite, Kegan Paul, Trench, Trubner & Co., London, 1931.
36. Issai Schur, *Über die Kongruenz $x^m + y^m = z^m$ (mod p)*, ***Jahresbericht der Deutschen Mathematiker-Vereinigung***, vol. 25 (1916), 114–117.
37. Neil J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, available online at: http://www.research.att.com/~njas/sequences/.
38. Alexander Soifer, *Issai Schur: Ramsey theory before Ramsey*, ***Geombinatorics***, vol. 5 (1995), 6–23.
39. Alan D. Taylor, *A canonical partition relation for finite subsets of ω*, ***Journal of Combinatorial Theory (A)***, vol. 21 (1976), 137–146.
40. Stevo Todorčević, ***Introduction to Ramsey Spaces***, [Annals of Mathematics Studies 174], Princeton University Press, Princeton (New Jersey), 2010.
41. Vojkan Vuksanović, *A proof of a partition theorem for $[\mathbb{Q}]^n$*, ***Proceedings of the American Mathematical Society***, vol. 130 (2002), 2857–2864.
42. Arthur Wieferich, *Zum letzten* Fermat*schen Theorem*, ***Journal für die Reine und Angewandte Mathematik***, vol. 136 (1909), 293–302.

3

The Axioms of Zermelo-Fraenkel Set Theory

Every mathematical science relies upon demonstration rather than argument and opinion. Certain principles, called premises, are granted, and a demonstration is made which resolves everything easily and clearly. To arrive at such a demonstration the means must be found for making it accessible to our judgment. Mathematicians, understanding this, devised signs, not separate from matter except in essence, yet distant from it. These were points, lines, planes, solids, numbers, and countless other characters, which are depicted on paper with certain colours, and they used these in place of the things symbolised.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

Why Axioms?

In the middle and late 19^{th} century, members of the then small mathematical community began to look for a rigorous foundation of Mathematics. In accordance with the Euclidean model for reason, the ideal foundation consists of a few simple, clear principles, so-called *axioms*, on which the rest of knowledge can be built via firm and reliable thoughts free of contradictions. However, at the time it was not clear what assumptions should be made and what operations should be allowed in mathematical reasoning.

At the beginning of the last book of *Politeia*, Plato develops his theory of ideas. Translated into the mathematical setting, Plato's theory of ideas reads as follows: Even though there may be more than one human approach to Mathematics, there is only *one* idea of Mathematics (*i.e.*, a unique mathematical world), and from this idea alone we can attain real knowledge — all human approaches are just opinions. In particular, the mathematical world already exists and is just waiting to be discovered. So, from a Platonic point of view it would make sense to search for the unique set of true axioms for Set Theory — also because the axioms of Set Theory are supposed to describe the world of "real" Mathematics.

However, if we consider Set Theory as a mathematical discipline, then, like in any other field of Mathematics, there is no true axiom system, and moreover, we are even allowed to weaken the axioms or to extend them by additional assumptions in order to get weaker or stronger theories. This is done for example in Group Theory in order to study *semigroups* or *monoids*, or to focus on *abelian groups*.

It is often the case that a mathematical theory is developed long before its formal axiomatisation, and in rare instances, mathematical theories were already partially developed before mathematicians were aware of them, which happened with Group Theory: Around the year 1600 in England it was discovered that by altering the fittings around each bell in a bell tower, it was possible for each ringer to maintain precise control of when his (there were no female ringers then) bell sounded. This enabled the ringers to ring the bells in any particular order, and either maintain that order or permute the order in a precise way. (For technical reasons, not every permutation is allowed. In fact, just products of mutually disjoint elementary transpositions may be used, that means that two bells can exchange their places only if they are adjacently rung before-hand.) So, in the first half of the 17^{th} century the ringers tried to continuously change the order of the bells for as long as possible, while not repeating any particular order, and return to rounds at the end. This game evolved into a challenge to ring the bells in every possible order, without any repeats, and return to rounds at the end. Thus, bell-ringers began to investigate permutations and Stedman's work *Campanologia* (Cambridge, 1677) can fairly be said to be the first work in which Group Theory was successfully applied to a "musical" situation and consequently, Stedman can be regarded as the first group theorist. This also shows that permutations — the prototype of finite groups — were first studied in the 17^{th} century in the context of the change-ringing, and therefore had a practical application long before they were used in Lagrange's work of 1770–1771 on the theory of algebraic equations.

Let us now turn back to Set Theory. The history of Set Theory is rather different from the history of most other areas of Mathematics. Usually a long process can be traced in which ideas evolve until an ultimate flash of inspiration, often by a number of mathematicians almost simultaneously, produces a discovery of major importance. Set Theory however is the creation of only one person, namely of Georg Cantor (1845–1918), who first discovered that infinite sets may have different sizes, *i.e.*, cardinalities. In fact, the birth of Set Theory dates to 1873 when Cantor proved that the set of real numbers is uncountable. Until then, no one envisioned the possibility that infinities come in different sizes, and moreover, mathematicians had no use for the *actual in-*

finite — in contrast to the *potential infinite*, as it is introduced by Aristotle in *Physics* Book III. The difference between actual and potential infinite is that the latter just means "unlimited" or "arbitrarily large" (*e.g.*, there are arbitrarily large — and therefore arbitrarily many — prime numbers), whereas the former means that there are infinite objects which actually exist (*e.g.*, there exists a set containing all, *i.e.*, infinitely many, prime numbers). Moreover, Cantor also showed that for every infinite set, there is a set of larger cardinality, which implies that there is no largest set. Cantor never introduced formal axioms for Set Theory, even though he was tacitly using most of the axioms introduced later by Zermelo and Fraenkel. However, Cantor considered a set as any collection of well-distinguished objects of our mind, which leads directly to RUSSELL'S PARADOX: Firstly, the collection of all sets is a set which is a member of itself. Secondly, the set of negative natural numbers is empty, and hence cannot be a member of itself (otherwise, it would not be empty). Now, call a set x *good* if x is not a member of itself and let C be the collection of all sets which are good. Is C, as a set, good or not? If C is good, then C is *not* a member of itself, but since C contains all sets which are good, C *is* a member of C, a contradiction. Otherwise, if C is a member of itself, then C must be good, again a contradiction. In order to avoid this paradox we have to exclude the collection C from being a set, but then, we have to give reasons why certain collections are sets and others are not. The axiomatic way to do this is described by Zermelo as follows: *Starting with the historically grown Set Theory, one has to search for the principles required for the foundations of this mathematical discipline. In solving the problem we must, on the one hand, restrict these principles sufficiently to exclude all contradictions and, on the other hand, take them sufficiently wide to retain all the features of this theory.*

The principles, which are called axioms, will tell us how to get new sets from already existing ones. In fact, most of the axioms of Set Theory are constructive to some extent, *i.e.*, they tell us how new sets are *constructed* from already existing ones and what elements they contain.

However, before we state the axioms of Set Theory we would like to introduce informally the formal language in which these axioms will be formulated.

First-Order Logic in a Nutshell

First-Order Logic is the system of Symbolic Logic concerned not only to represent the logical relations between sentences or propositions as wholes (like *Propositional Logic*), but also to consider their internal structure in terms of subject and predicate. First-Order Logic can be consider as a kind of language which is distinguished from higher-order languages in that it does not allow quantification over subsets of the domain of discourse or other objects of higher type. Nevertheless, First-Order Logic is strong enough to formalise all of Set Theory and thereby virtually all of Mathematics. In other words, First-Order Logic is an abstract language that in one particular case is the language of Group Theory, and in another case is the language of Set Theory.

The goal of this brief introduction to First-Order Logic is to illustrate and summarise some of the basic concepts of this language and to show how it is applied to fields like Group Theory and Peano Arithmetic (two theories which will accompany us for a while).

Syntax: Formulae, Formal Proofs, and Consistency

Like any other written language, First-Order Logic is based on an *alphabet*, which consists of the following *symbols*:

(a) **Variables** such as $v_0, v_1, x, y, \ldots$ which are place holders for objects of the *domain* under consideration (which can for example be the elements of a group, natural numbers, or sets).

(b) **Logical operators** which are "$\neg$" (*not*), "$\wedge$" (*and*), "$\vee$" (*or*), "$\rightarrow$" (*implies*), and "$\leftrightarrow$" (*if and only if*, abbreviated *iff*).

(c) **Logical quantifiers** which are the *existential quantifier* "$\exists$" (*there is* or *there exists*) and the *universal quantifier* "$\forall$" (*for all* or *for each*), where quantification is restricted to objects only and not to formulae or sets of objects (but the objects themselves may be sets).

(d) **Equality symbol** "$=$", which stands for the particular binary *equality relation*.

(e) **Constant symbols** like the number $\mathtt{0}$ in Peano Arithmetic, or the neutral element $\mathtt{e}$ in Group Theory. Constant symbols stand for fixed individual objects in the domain.

(f) **Function symbols** such as $\circ$ (the operation in Group Theory), or $+$, $\cdot$, $\mathtt{s}$ (the operations in Peano Arithmetic), Function symbols stand for fixed functions taking objects as arguments and returning objects as values. With each function symbol we associate a positive natural number, its co-called "arity" (*e.g.*, "$\circ$" is a 2-ary or binary function, and the successor operation "$\mathtt{s}$" is a 1-ary or unary function).

(g) **Relation symbols** or **predicate constants** (such as $\in$ in Set Theory) stand for fixed relations between (or properties of) objects in the domain. Again we associate an "arity" with each relation symbol (*e.g.*, "$\in$" is a binary relation).

The symbols in (a)–(d) form the core of the alphabet and are called **logical symbols**. The symbols in (e)–(g) depend on the specific topic we are investigating and are called **non-logical symbols**. The set of non-logical symbols which are used in order to formalise a certain mathematical theory is called the **language** of this theory, denoted by $\mathscr{L}$, and *formulae* which are formulated in a language $\mathscr{L}$ are usually called $\mathscr{L}$-formulae. For example if we investigate groups, then the only non-logical symbols we use are "$\mathtt{e}$" and "$\circ$", thus, $\mathscr{L} = \{\mathtt{e}, \circ\}$ is the language of Group Theory.

A first step towards a proper language is to build words (*i.e.*, *terms*) with these symbols.

Terms:

(T1) Each variable is a term.

(T2) Each constant symbol is a term.

(T3) If $t_1, \ldots, t_n$ are terms and F is an n-ary function symbol, then $Ft_1 \cdots t_n$ is a term.

It is convenient to use auxiliary symbols like brackets in order to make terms, relations, and other expressions easier to read. For example we usually write $F(t_1, \ldots, t_n)$ rather than $Ft_1 \cdots t_n$.

To some extent, terms correspond to words, since they denote objects of the domain under consideration. Like real words, they are not statements and cannot express or describe possible relations between objects. So, the next step is to build sentences (*i.e.*, *formulae*) with these terms.

Formulae:

(F1) If t_1 and t_2 are terms, then $t_1 = t_2$ is a formula.

(F2) If $t_1, \ldots, t_n$ are terms and R is an n-ary relation symbol, then $Rt_1 \cdots t_n$ is a formula.

(F3) If φ is a formula, then $\neg\varphi$ is a formula.

(F4) If φ and ψ are formulae, then $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, and $(\varphi \leftrightarrow \psi)$ are formulae. (To avoid the use of brackets one could write these formulae for example in *Polish notation*, *i.e.*, $\wedge\varphi\psi$, $\vee\varphi\psi$, *et cetera*.)

(F5) If φ is a formula and x a variable, then $\exists x \varphi$ and $\forall x \varphi$ are formulae.

Formulae of the form (F1) or (F2) are the most basic expressions we have, and since every formula is a logical connection or a quantification of these formulae, they are called **atomic formulae**.

For binary relations R it is convenient to write xRy instead of $R(x, y)$. For example we write $x \in y$ instead of $\in(x, y)$, and we write $x \notin y$ rather than $\neg(x \in y)$.

If a formula φ is of the form $\exists x \psi$ or of the form $\forall x \psi$ (for some formula ψ) and x occurs in ψ, then we say that x is in the *range* of a logical quantifier. A variable x occurring at a particular place in a formula φ is either in the range of a logical quantifier or it is not in the range of any logical quantifier. In the former case this particular instance of the variable x is **bound** in φ, and in the latter case it is **free** in φ. Notice that it is possible that a certain variable occurs in a given formula bound as well as free (*e.g.*, in $\exists z(x = z) \wedge \forall x(x = y)$, the variable x is both bound and free, whereas z is just bound and y is just free). However, one can always rename the bound variables occurring in a given formula φ such that each variable in φ is either bound or free. For formulae φ, the set of variables occurring free in φ is denoted by free(φ). A formula φ is a **sentence** if it contains no free variables (*i.e.*, $\text{free}(\varphi) = \emptyset$). For example $\forall x(x = x)$ is a sentence but $(x = x)$ is not.

Sometimes it is useful to indicate explicitly which variables occur free in a given formula φ, and for this we usually write $\varphi(x_1, \dots, x_n)$ to indicate that $\{x_1, \dots, x_n\} \subseteq \text{free}(\varphi)$.

If $\varphi(x)$ is a formula (*i.e.*, $x \in \text{free}(\varphi)$), and t a term, then $\varphi(x/t)$ is the formula we get after replacing all *free* instances of x by t. A so-called **substitution** $\varphi(x/t)$ is **admissible** *iff* no free occurrence of x in φ is in the range of a quantifier that binds any variable contained in t (*i.e.*, for each variable v appearing in t, no place where x occurs free in φ is in the range of "$\exists v$" or "$\forall v$").

So far we have letters, and we can build words and sentences. However, these sentences are just strings of symbols without any inherent meaning. Later we shall interpret formulae in the intuitively natural way by giving the symbols the intended meaning (*e.g.*, "$\wedge$" meaning "and", "$\forall x$" meaning "for all x", *et cetera*). But before we shall do so, let us stay a little bit longer on the syntactical side — nevertheless, one should consider the formulae also from a semantical point of view.

Below we shall label certain formulae or types of formulae as **axioms**, which are used in connection with *inference rules* in order to derive further formulae. From a semantical point of view we can think of axioms as "true" statements from which we deduce or prove further results. We distinguish two types of axioms, namely *logical axioms* and *non-logical axioms* (which will be discussed later). A **logical axiom** is a sentence or formula φ which is universally valid (*i.e.*, φ is true in any possible universe, no matter how the variables, constants, *et cetera*, occurring in φ are interpreted). Usually one takes as logical axioms some minimal set of formulae that is sufficient for deriving all universally valid formulae (such a set is given below).

If a symbol is involved in an axiom which stands for an arbitrary relation, function, or even for a first-order formula, then we usually consider the statement as an **axiom schema** rather than a single axiom, since each instance of the symbol represents a single axiom. The following list of axiom schemata is a system of logical axioms.

Let φ, φ_1, φ_2, and ψ, be arbitrary first-order formulae:

$\mathsf{L}_1 : \varphi \rightarrow (\psi \rightarrow \varphi)$

$\mathsf{L}_2 : \big(\psi \rightarrow (\varphi_1 \rightarrow \varphi_2)\big) \rightarrow \big((\psi \rightarrow \varphi_1) \rightarrow (\psi \rightarrow \varphi_2)\big)$

$\mathsf{L}_3 : (\varphi \wedge \psi) \rightarrow \varphi$

$\mathsf{L}_4 : (\varphi \wedge \psi) \rightarrow \psi$

$\mathsf{L}_5 : \varphi \rightarrow \big(\psi \rightarrow (\psi \wedge \varphi)\big)$

$\mathsf{L}_6 : \varphi \rightarrow (\varphi \vee \psi)$

$\mathsf{L}_7 : \psi \rightarrow (\varphi \vee \psi)$

$\mathsf{L}_8 : (\varphi_1 \rightarrow \varphi_3) \rightarrow \big((\varphi_2 \rightarrow \varphi_3) \rightarrow \big((\varphi_1 \vee \varphi_2) \rightarrow \varphi_3\big)\big)$

$\mathsf{L}_9 : (\varphi \rightarrow \psi) \rightarrow \big((\varphi \rightarrow \neg\psi) \rightarrow \neg\varphi\big)$

L_{10}: $\neg\varphi \to (\varphi \to \psi)$

L_{11}: $\varphi \vee \neg\varphi$

If t is a term and the substitution $\varphi(x/t)$ is admissible, then:

L_{12}: $\forall x\varphi(x) \to \varphi(t)$

L_{13}: $\varphi(t) \to \exists x\varphi(x)$

If ψ is a formula such that $x \notin \mathrm{free}(\psi)$, then:

L_{14}: $\forall x\big(\psi \to \varphi(x)\big) \to \big(\psi \to \forall x\varphi(x)\big)$

L_{15}: $\forall x\big(\varphi(x) \to \psi\big) \to \big(\exists x\varphi(x) \to \psi\big)$

What is not covered yet is the symbol "$=$", so, let us have a closer look at the binary equality relation. The defining properties of equality can already be found in Book VII, Chapter 1 of Aristotle's *Topics*, where one of the rules to decide whether two things are the same is as follows: ... *you should look at every possible predicate of each of the two terms and at the things of which they are predicated and see whether there is any discrepancy anywhere. For anything which is predicated of the one ought also to be predicated of the other, and of anything of which the one is a predicate the other also ought to be a predicate.*

In our formal system, the binary equality relation is defined by the following three axioms.

If $t, t_1, \ldots, t_n, t'_1, \ldots, t'_n$ are any terms, R an n-ary relation symbol (*e.g.*, the binary relation symbol "$=$"), and F an n-ary function symbol, then:

L_{16}: $t = t$

L_{17}: $\big(t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n\big) \to \big(R(t_1, \ldots, t_n) \to R(t'_1, \ldots, t'_n)\big)$

L_{18}: $\big(t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n\big) \to \big(F(t_1, \ldots, t_n) = F(t'_1, \ldots, t'_n)\big)$

Finally, we define the logical operator "$\leftrightarrow$" by stipulating

$$\varphi \leftrightarrow \psi \iff (\varphi \to \psi) \wedge (\psi \to \varphi)\,,$$

i.e., $\varphi \leftrightarrow \psi$ is just an abbreviation for $(\varphi \to \psi) \wedge (\psi \to \varphi)$.

This completes the list of our logical axioms. In addition to these axioms, we are allowed to state arbitrarily many theory-specific assumptions, so-called **non-logical axioms**. Such axioms are for example the three axioms of *Group Theory*, denoted GT, or the axioms of *Peano Arithmetic*, denoted PA.

GT: The language of Group Theory is $\mathscr{L}_{\mathsf{GT}} = \{\mathsf{e}, \circ\}$, where "$\mathsf{e}$" is a constant symbol and "$\circ$" is a binary function symbol.

GT_0: $\forall x\forall y\forall z\big(x\circ(y\circ z) = (x\circ y)\circ z\big)$ (*i.e.*, "$\circ$" is *associative*)

GT_1: $\forall x(\mathsf{e}\circ x = x)$ (*i.e.*, "e" is a *left-neutral* element)

GT_2: $\forall x\exists y(y\circ x = \mathsf{e})$ (*i.e.*, every element has a *left-inverse*)

PA: The language of Peano Arithmetic is $\mathscr{L}_{\mathsf{PA}} = \{\mathtt{0}, \mathtt{s}, +, \cdot\}$, where "$\mathtt{0}$" is a constant symbol, "$\mathtt{s}$" is a unary function symbol, and "$+$" and "$\cdot$" are binary function symbols.

PA_1: $\forall x\big(\mathtt{s}(x) \neq \mathtt{0}\big)$

PA_2: $\forall x \forall y\big(\mathtt{s}(x) = \mathtt{s}(y) \rightarrow x = y\big)$

PA_3: $\forall x(x + \mathtt{0} = x)$

PA_4: $\forall x \forall y\big(x + \mathtt{s}(y) = \mathtt{s}(x + y)\big)$

PA_5: $\forall x(x \cdot \mathtt{0} = \mathtt{0})$

PA_6: $\forall x \forall y\big(x \cdot \mathtt{s}(y) = (x \cdot y) + x\big)$

If φ is any $\mathscr{L}_{\mathsf{PA}}$-formula with $x \in \mathrm{free}(\varphi)$, then:

PA_7: $\big(\varphi(\mathtt{0}) \wedge \forall x\big(\varphi(x) \rightarrow \varphi(\mathtt{s}(x))\big)\big) \rightarrow \forall x \varphi(x)$.

It is often convenient to add certain *defined symbols* to a given language so that the expressions get shorter or at least are easier to read. For example in Peano Arithmetic — which is an axiomatic system for the natural numbers — we usually replace the expression $\mathtt{s}(\mathtt{0})$ with $\mathtt{1}$ and consequently $\mathtt{s}(x)$ by $x + \mathtt{1}$. Probably, we would like to introduce an ordering "$<$" on the natural numbers. We can do this by stipulating

$$\mathtt{1} := \mathtt{s}(\mathtt{0}), \quad x < y \iff \exists z\big((x + z) + \mathtt{1} = y\big).$$

We usually use ":=" to define constants or functions, and "$\iff$" to define relations. Obviously, all that can be expressed in the language $\mathscr{L}_{\mathsf{PA}} \cup \{\mathtt{1}, <\}$ can also be expressed in $\mathscr{L}_{\mathsf{PA}}$.

So far we have a set of logical and non-logical axioms in a certain language and can define, if we wish, as many new constants, functions, and relations as we like. However, we are still not able to deduce anything from the given axioms, since we have neither *inference rules* nor the notion of *formal proof*.

Surprisingly, just two **inference rules** are sufficient, namely:

Modus Ponens: $\dfrac{\varphi \rightarrow \psi,\ \varphi}{\psi}$ and **Generalisation:** $\dfrac{\varphi}{\forall x\, \varphi}$

In the former case we say that ψ is obtained from $\varphi \rightarrow \psi$ and φ by Modus Ponens, and in the latter case we say that $\forall x \varphi$ (where x can be any variable) is obtained from φ by Generalisation.

Using these two inference rules, we are able to define the notion of **formal proof**: Let T be a possibly empty set of non-logical axioms (usually sentences), formulated in a certain language $\mathscr{L}$. An $\mathscr{L}$-formula ψ is **provable** from T (or provable in T), denoted $\mathsf{T} \vdash \psi$, if there is a *finite* sequence $\varphi_1, \ldots, \varphi_n$ of $\mathscr{L}$-formulae such that φ_n is equal to ψ (*i.e.*, the formulae φ_n and ψ are identical), and for all i with $1 \leq i \leq n$ we have:

- φ_i is a logical axiom, or
- $\varphi_i \in \mathsf{T}$, or
- there are $j, k < i$ such that φ_j is equal to the formula $\varphi_k \to \varphi_i$, or
- there is a $j < i$ such that φ_i is equal to the formula $\forall x\, \varphi_j$.

If a formula ψ is not provable in T, *i.e.*, if there is no formal proof for ψ which uses just formulae from T, then we write $\mathsf{T} \nvdash \psi$.

Formal proofs, even of very simple statements, can get quite long and tricky. So, before we give an example of a formal proof, let us state a theorem which allows us to simplify formal proofs:

THEOREM 3.1 (DEDUCTION THEOREM). *If* $\{\psi_1, \dots, \psi_n\} \cup \{\varphi_1, \dots, \varphi_k\} \vdash \varphi$*, where* Generalisation *is not applied to the free variables of the formulae* $\varphi_1, \dots, \varphi_k$ *(e.g., if these formulae are sentences), then*

$$\{\psi_1, \dots, \psi_n\} \vdash \big(\varphi_1 \wedge \dots \wedge \varphi_k\big) \to \varphi\,.$$

Now, as an example of a formal proof let us show the equality relation is symmetric. We first work with $\mathsf{T}_{x=y}$, consisting only of the formula $x = y$, and show that $\mathsf{T}_{x=y} \vdash y = x$, in other words we show that $\{x = y\} \vdash y = x$:

φ_1:	$(x = y \wedge x = x) \to (x = x \to y = x)$	*instance of* L_{17}
φ_2:	$(x = y \wedge x = x) \to x = x$	*instance of* L_4
φ_3:	$\varphi_1 \to \big(\varphi_2 \to \big((x = y \wedge x = x) \to y = x\big)\big)$	*instance of* L_2
φ_4:	$\varphi_2 \to \big((x = y \wedge x = x) \to y = x\big)$	*from* φ_3 *and* φ_1 *by* Modus Ponens
φ_5:	$(x = y \wedge x = x) \to y = x$	*from* φ_4 *and* φ_2 *by* Modus Ponens
φ_6:	$x = x$	*instance of* L_{16}
φ_7:	$x = y$	$(x = y) \in \mathsf{T}_{x=y}$
φ_8:	$x = x \to \big(x = y \to (x = y \wedge x = x)\big)$	*instance of* L_5
φ_9:	$x = y \to (x = y \wedge x = x)$	*from* φ_8 *and* φ_6 *by* Modus Ponens
φ_{10}:	$x = y \wedge x = x$	*from* φ_9 *and* φ_7 *by* Modus Ponens
φ_{11}:	$y = x$	*from* φ_5 *and* φ_9 *by* Modus Ponens

Thus, we have $\{x = y\} \vdash y = x$, and by the DEDUCTION THEOREM 3.1 we get that $\vdash x = y \to y = x$, and finally, by Generalisation we get

$$\vdash \forall x \forall y (x = y \to y = x)\,.$$

We leave it as an exercise to the reader to show that the equality relation is also transitive, and since the equality relation is also reflexive (by L_{16}), it is an equivalence relation.

Furthermore, we say that two formulae φ and ψ are **equivalent**, denoted $\varphi \equiv \psi$, if $\vdash \varphi \leftrightarrow \psi$. In other words, if $\varphi \equiv \psi$, then — from a logical point of view — φ and ψ state exactly the same, and therefore we could call $\varphi \leftrightarrow \psi$ a tautology, which means *saying the same thing twice*. However, in Logic, a formula φ is a **tautology** if $\vdash \varphi$. Thus, the formulae φ and ψ are equivalent if and only if $\varphi \leftrightarrow \psi$ is a tautology.

A few examples:

- $\varphi \vee \psi \equiv \psi \vee \varphi$, $\varphi \wedge \psi \equiv \psi \wedge \varphi$ This shows that "$\vee$" and "$\wedge$" are commutative (up to equivalence). Moreover, "$\vee$" and "$\wedge$" are (up to equivalence) also associative — a fact which we tacitly used already.
- $\neg\neg\varphi \equiv \varphi$, $(\varphi \vee \psi) \equiv \neg(\neg\varphi \wedge \neg\psi)$ This shows for example how "$\vee$" can be replaced with "$\neg$" and "$\wedge$".
- $(\varphi \rightarrow \psi) \equiv (\neg\varphi \vee \psi)$ This shows how the logical operator "$\rightarrow$" can be replaced with "$\neg$" and "$\vee$".
- $\forall x\varphi \equiv \neg\exists x\neg\varphi$ This shows how "$\forall$" can be replaced with "$\neg$" and "$\exists$".

Thus, some of the logical operators are redundant and we could work for example with just "$\neg$", "$\wedge$", and "$\exists$". However, it is more convenient to use all of them.

Let T be a set of $\mathscr{L}$-formulae. We say that T is **consistent**, denoted $\mathrm{Con}(\mathsf{T})$, if there is *no* $\mathscr{L}$-formula φ such that $\mathsf{T} \vdash (\varphi \wedge \neg\varphi)$, otherwise T is called **inconsistent**, denoted $\neg\,\mathrm{Con}(\mathsf{T})$.

PROPOSITION 3.2. *Let T be a set of $\mathscr{L}$-formulae.*

(a) If $\neg\,\mathrm{Con}(\mathsf{T})$, then for every $\mathscr{L}$-formula ψ we have $\mathsf{T} \vdash \psi$.
(b) If $\mathrm{Con}(\mathsf{T})$ and $\mathsf{T} \vdash \varphi$ for some $\mathscr{L}$-formula φ, then $\mathsf{T} \nvdash \neg\varphi$.

Proof. (a) Let ψ be any $\mathscr{L}$-formula and assume that $\mathsf{T} \vdash (\varphi \wedge \neg\varphi)$ for some $\mathscr{L}$-formula φ. Then $\mathsf{T} \vdash \psi$:

φ_1:	$\varphi \wedge \neg\varphi$	*provable from* T *by assumption*
φ_2:	$(\varphi \wedge \neg\varphi) \rightarrow \varphi$	*instance of* L_3
φ_3:	φ	*from* φ_2 *and* φ_1 *by* Modus Ponens
φ_4:	$(\varphi \wedge \neg\varphi) \rightarrow \neg\varphi$	*instance of* L_4
φ_5:	$\neg\varphi$	*from* φ_4 *and* φ_1 *by* Modus Ponens
φ_6:	$\neg\varphi \rightarrow (\varphi \rightarrow \psi)$	*instance of* L_{10}
φ_7:	$\varphi \rightarrow \psi$	*from* φ_6 *and* φ_5 *by* Modus Ponens
φ_8:	ψ	*from* φ_7 *and* φ_3 *by* Modus Ponens

(b) Assume that $\mathsf{T} \vdash \varphi$ and $\mathsf{T} \vdash \neg\varphi$. Then $\mathsf{T} \vdash (\varphi \wedge \neg\varphi)$, *i.e.*, $\neg\,\mathrm{Con}(\mathsf{T})$:

φ_1:	φ	*provable from* T *by assumption*
φ_2:	$\neg\varphi$	*provable from* T *by assumption*
φ_3:	$\varphi \to \big(\neg\varphi \to (\varphi \wedge \neg\varphi)\big)$	*instance of* L_5
φ_4:	$\neg\varphi \to (\varphi \wedge \neg\varphi)$	*from* φ_3 *and* φ_1 *by* Modus Ponens
φ_5:	$\varphi \wedge \neg\varphi$	*from* φ_4 *and* φ_2 *by* Modus Ponens

$\dashv$

Notice that PROPOSITION 3.2.(a) implies that from an inconsistent set of axioms T one can prove everything and T would be completely useless. So, if we design a set of axioms T, we have to make sure that T is consistent. However, as we shall see later, in many cases this task is impossible.

Semantics: Models, Completeness, and Independence

Let T be any set of $\mathscr{L}$-formulae (for some language $\mathscr{L}$). There are two different ways to approach T, namely the *syntactical* and the *semantical* way. The above presented syntactical approach considers the set T just as a set of well-formed formulae — regardless of their intended sense or meaning — from which we can prove some other formulae.
On the other hand, we can consider T also from a semantical point of view by interpreting the symbols of the language $\mathscr{L}$ in a reasonable way, and then seeking for a *model* in which all formulae of T are true. To be more precise, we first have to define how models are built and what "true" means:

Let $\mathscr{L}$ be an arbitrary but fixed language. An **$\mathscr{L}$-structure** $\mathfrak{A}$ consists of a (non-empty) set or collection A, called the **domain** of $\mathfrak{A}$, together with a mapping which assigns to each constant symbol $c \in \mathscr{L}$ an element $c^{\mathfrak{A}}$ of A, to each n-ary relation symbol $R \in \mathscr{L}$ a set of n-tuples $R^{\mathfrak{A}}$ of elements of A, and to each n-ary function symbol $F \in \mathscr{L}$ a function $F^{\mathfrak{A}}$ from n-tuples of A to A. Further, the interpretation of variables is given by a so-called assignment: An **assignment** in an $\mathscr{L}$-structure $\mathfrak{A}$ is a mapping j which assigns to each variable an element of the domain A. Finally, an **$\mathscr{L}$-interpretation $\mathbf{I}$** is a pair $(\mathfrak{A}, j)$ consisting of an $\mathscr{L}$-structure $\mathfrak{A}$ and an assignment j in $\mathfrak{A}$. For a variable x, an element $a \in A$, and an assignment j in $\mathfrak{A}$ we define the assignment $j\frac{a}{x}$ by stipulating

$$j\tfrac{a}{x}(y) = \begin{cases} a & \text{if } y = x, \\ j(y) & \text{otherwise.} \end{cases}$$

Further, for an interpretation $\mathbf{I} = (\mathfrak{A}, j)$ let $\mathbf{I}\frac{a}{x} := (\mathfrak{A}, j\frac{a}{x})$.

We associate with every interpretation $\mathbf{I} = (\mathfrak{A}, j)$ and every term t an element $\mathbf{I}(t)$ from the domain A as follows:

- For a variable x let $\mathbf{I}(x) := j(x)$.
- For a constant symbol $c \in \mathscr{L}$ let $\mathbf{I}(c) := c^{\mathfrak{A}}$.
- For an n-ary function symbol $F \in \mathscr{L}$ and terms $t_1, \ldots, t_n$ let

$$\mathbf{I}\big(F(t_1, \ldots, t_n)\big) := F^{\mathfrak{A}}\big(\mathbf{I}(t_1), \ldots, \mathbf{I}(t_n)\big).$$

Now, we are able to define precisely the notion of a formula φ being true under an interpretation $\mathbf{I} = (\mathfrak{A}, j)$, in which case we write $\mathbf{I} \vDash \varphi$ and say that φ holds in $\mathbf{I}$. The definition is by induction on the complexity of the formula φ (where it is enough to consider formulae containing — besides terms and relations — just the logical operators "$\neg$" and "$\wedge$", and the logical quantifier "$\exists$"):

- If φ is of the form $t_1 = t_2$, then

$$\mathbf{I} \vDash t_1 = t_2 \iff \mathbf{I}(t_1) \textit{ is the same element as } \mathbf{I}(t_2).$$

- If φ is of the form $R(t_1, \ldots, t_n)$, then

$$\mathbf{I} \vDash R(t_1, \ldots, t_n) \iff \big(\mathbf{I}(t_1), \ldots, \mathbf{I}(t_n)\big) \textit{ belongs to } R^{\mathfrak{A}}.$$

- If φ is of the form $\neg\psi$, then

$$\mathbf{I} \vDash \neg\psi \iff \textit{it is not the case that } \mathbf{I} \vDash \psi.$$

- If φ is of the form $\exists x\psi$, then

$$\mathbf{I} \vDash \exists x\psi \iff \textit{there is an element } a \in A \textit{ such that } \mathbf{I}\tfrac{a}{x} \vDash \psi.$$

- If φ is of the form $\psi_1 \wedge \psi_2$, then

$$\mathbf{I} \vDash \psi_1 \wedge \psi_2 \iff \mathbf{I} \vDash \psi_1 \textit{ and } \mathbf{I} \vDash \psi_2.$$

Notice that since the domain of $\mathbf{I}$ is non-empty we always have $\mathbf{I} \vDash \exists x(x = x)$.

Now, let T be an arbitrary set of $\mathscr{L}$-formulae. Then an $\mathscr{L}$-structure $\mathfrak{A}$ is a **model** of T if for every assignment j in $\mathfrak{A}$ and for each formula $\varphi \in \mathsf{T}$ we have $(\mathfrak{A}, j) \vDash \varphi$, *i.e.*, φ holds in the $\mathscr{L}$-interpretation $\mathbf{I} = (\mathfrak{A}, j)$. We usually denote models by bold letters like $\mathbf{M}$, $\mathbf{N}$, $\mathbf{V}$, *et cetera*. Instead of saying "$\mathbf{M}$ is a model of T" we just write $\mathbf{M} \vDash \mathsf{T}$. If φ fails in $\mathbf{M}$, then we write $\mathbf{M} \nvDash \varphi$, which is equivalent to $\mathbf{M} \vDash \neg\varphi$ (this is because for any $\mathscr{L}$-formula φ we have *either* $\mathbf{M} \vDash \varphi$ *or* $\mathbf{M} \vDash \neg\varphi$).

For example S_7 (*i.e.*, the set of all permutations of seven different items) is a model of GT, where the interpretation of the binary operation is composition and the neutral element is interpreted as the identity permutation. In this case, the elements of the domain of S_7 can be real and can even be heard, namely when the seven items are seven bells and a peal of for example Stedman Triples consisting of all 5040 permutations of the seven bells is rung — which happens quite often, since Stedman Triples are very popular with change-ringers. However, the objects of models of mathematical theories usually do not belong to our physical world and are not more real than for example the *number zero* or the *empty set*.

The following two theorems, which we state without proofs, are the main connections between the syntactical and the semantical approach to first-order theories. On the one hand, the SOUNDNESS THEOREM 3.3 just tells us that our deduction system is sound, *i.e.*, if a sentence φ is provable from T then φ is true in each model of T. On the other hand, GÖDEL'S COMPLETENESS THEOREM 3.4 tells us that our deduction system is even complete, *i.e.*, every sentence which is true in all models of T is provable from T. As a consequence we get that $\mathsf{T} \vdash \varphi$ if and only if φ is true in each model of T. In particular, if T is empty, this implies that every tautology (*i.e.*, universally valid formula) is provable.

THEOREM 3.3 (SOUNDNESS THEOREM). *Let T be a set of $\mathscr{L}$-sentences and let φ be any $\mathscr{L}$-sentence. If $\mathsf{T} \vdash \varphi$, then in any model $\mathbf{M}$ such that $\mathbf{M} \vDash \mathsf{T}$ we have $\mathbf{M} \vDash \varphi$.*

THEOREM 3.4 (GÖDEL'S COMPLETENESS THEOREM). *Let T be a set of $\mathscr{L}$-sentences and let φ be any $\mathscr{L}$-sentence. Then $\mathsf{T} \vdash \varphi$ or there is a model $\mathbf{M}$ such that $\mathbf{M} \vDash \mathsf{T} \cup \{\neg\varphi\}$. In other words, if for every model $\mathbf{M} \vDash \mathsf{T}$ we have $\mathbf{M} \vDash \varphi$, then $\mathsf{T} \vdash \varphi$. (Notice that this does not imply the existence of a model of T.)*

One of the main consequences of GÖDEL'S COMPLETENESS THEOREM 3.4 is that formal proofs — which are usually quite long and involved — can be replaced with informal ones: Let T be a consistent set of $\mathscr{L}$-formulae and let φ be any $\mathscr{L}$-sentence. Then, by GÖDEL'S COMPLETENESS THEOREM 3.4, in order to show that $\mathsf{T} \vdash \varphi$ it is enough to show that $\mathbf{M} \vDash \varphi$ whenever $\mathbf{M} \vDash \mathsf{T}$. In fact, we would take an arbitrary model $\mathbf{M}$ of T and show that $\mathbf{M} \vDash \varphi$.

As an example let us show that $\mathsf{GT} \vdash (y \circ x = \mathsf{e}) \to (x \circ y = \mathsf{e})$: Firstly, let $\mathbf{G}$ be a model of GT, with domain G, and let x and y be any elements of G. By GT_2 we know that every element of G has a left-inverse. In particular, y has a left-inverse, say $\bar{y}$, and we have $\bar{y} \circ y = \mathsf{e}$. By GT_1 we have $x \circ y = (\bar{y} \circ y) \circ (x \circ y)$, and by GT_0 we get $(\bar{y} \circ y) \circ (x \circ y) = \bar{y} \circ \big((y \circ x) \circ y\big)$. Now, if $y \circ x = \mathsf{e}$, then we have $x \circ y = \bar{y} \circ y$ and consequently we get $x \circ y = \mathsf{e}$. Notice that we tacitly used that the equality relation is symmetric and transitive.

We leave it as an exercise to the reader to find the corresponding formal proof of this basic result in Group Theory. In a similar way one can show that every left-neutral element is also a right-neutral element (called *neutral element*) and that there is just one neutral element in a group.

The following result, which is a consequence of GÖDEL'S COMPLETENESS THEOREM 3.4, shows that *every* consistent set of formulae has a model.

PROPOSITION 3.5. *Let* T *be any set of* $\mathscr{L}$*-formulae. Then* $\mathrm{Con}(\mathsf{T})$ *if and only if* T *has a model.*

Proof. ($\Rightarrow$) If T has no model, then, by GÖDEL'S COMPLETENESS THEOREM 3.4, for *every* $\mathscr{L}$-formula ψ we have $\mathsf{T} \vdash \psi$ (otherwise, there would be a model of $\mathsf{T} \cup \{\neg\psi\}$, and in particular for T). So, for ψ being $\varphi \wedge \neg\varphi$ we get $\mathsf{T} \vdash (\varphi \wedge \neg\varphi)$, hence T is inconsistent.

($\Leftarrow$) If T is inconsistent, then, by PROPOSITION 3.2.(a), for every $\mathscr{L}$-formula ψ we have $\mathsf{T} \vdash \psi$, in particular, $\mathsf{T} \vdash \varphi \wedge \neg\varphi$. Now, the SOUNDNESS THEOREM 3.3 implies that in all models $\mathbf{M} \vDash \mathsf{T}$ we have $\mathbf{M} \vDash \varphi \wedge \neg\varphi$; thus, there are no models of T. $\dashv$

A set of *sentences* T is usually called a **theory**. A consistent theory T (in a certain language $\mathscr{L}$) is said to be **complete** if for every $\mathscr{L}$-sentence φ, *either* $\mathsf{T} \vdash \varphi$ *or* $\mathsf{T} \vdash \neg\varphi$. If T is not complete, we say that T is **incomplete**.

The following result is an immediate consequence of PROPOSITION 3.5.

COROLLARY 3.6. *Every consistent theory is contained in a complete theory.*

Proof. Let T be a theory in the language $\mathscr{L}$. If T is consistent, then it has a model, say $\mathbf{M}$. Now let $\bar{\mathsf{T}}$ be the set of all $\mathscr{L}$-sentences φ such that $\mathbf{M} \vDash \varphi$. Obviously, $\bar{\mathsf{T}}$ is a complete theory which contains T. $\dashv$

Let T be a set of $\mathscr{L}$-formulae and let φ be any $\mathscr{L}$-formula not contained in T. φ is said to be **consistent relative to** T (or that φ is **consistent with** T) if $\mathrm{Con}(\mathsf{T})$ implies $\mathrm{Con}(\mathsf{T} \cup \{\varphi\})$ (later we usually write $\mathsf{T} + \varphi$ instead of $\mathsf{T} \cup \{\varphi\}$). If both φ and $\neg\varphi$ are consistent with T, then φ is said to be **independent** of T. In other words, if $\mathrm{Con}(\mathsf{T})$, then φ is independent of T if *neither* $\mathsf{T} \vdash \varphi$ *nor* $\mathsf{T} \vdash \neg\varphi$. By GÖDEL'S COMPLETENESS THEOREM 3.4 we get that if $\mathrm{Con}(\mathsf{T})$ and φ is independent of T, then there are models $\mathbf{M}_1$ and $\mathbf{M}_2$ of T such that $\mathbf{M}_1 \vDash \varphi$ and $\mathbf{M}_2 \vDash \neg\varphi$. A typical example of a statement which is independent of GT is $\forall x \forall y (x \circ y = y \circ x)$ (*i.e.*, the binary operation is commutative), and indeed, there are abelian as well as non-abelian groups.

In order to prove that a certain statement φ is independent of a given (consistent) theory T, one could try to find two different models of T such that φ holds in one model and fails in the other. However, this task is quite difficult, in particular if one cannot prove that T has a model at all (as it happens for Set Theory).

Limits of First-Order Logic

We begin this section with a useful result, called COMPACTNESS THEOREM. On the one hand, it is just a consequence of the fact that formal proofs are finite (*i.e.*, finite sequences of formulae). On the other hand, the COMPACTNESS THEOREM is the main tool to prove that a certain sentence (or a set of sentences) is consistent with a given theory. In particular, the COMPACTNESS

THEOREM is implicitly used in every set-theoretic consistency proof which is obtained by forcing (for details see Chapter 16).

THEOREM 3.7 (COMPACTNESS THEOREM). *Let* T *be an arbitrary set of* $\mathscr{L}$*-formulae. Then* T *is consistent if and only if every finite subset* Φ *of* T *is consistent.*

Proof. Obviously, if T is consistent, then every finite subset Φ of T must be consistent. On the other hand, if T is inconsistent, then there is a formula φ such that $\mathsf{T} \vdash \varphi \wedge \neg\varphi$. In other words, there is a proof of $\varphi \wedge \neg\varphi$ from T. Now, since every proof is finite, there are only finitely many formulae of T involved in this proof, and if Φ is this finite set of formulae, then $\Phi \vdash \varphi \wedge \neg\varphi$, which shows that Φ, a finite subset of T, is inconsistent. $\dashv$

A simple application of the COMPACTNESS THEOREM 3.7 shows that if PA is consistent, then there is more than one model of PA (*i.e.*, beside the intended model of natural numbers with domain $\mathbb{N}$, there are also so-called *non-standard* models of PA with larger domains):

Firstly we extend the language $\mathscr{L}_{\mathsf{PA}} = \{\mathtt{0}, \mathtt{s}, +, \cdot\}$ by adding a new constant symbol $\mathtt{n}$. Secondly we extend PA by adding the formulae

$$\underbrace{\mathtt{n} \neq \mathtt{0}}_{\varphi_0}, \quad \underbrace{\mathtt{n} \neq \mathtt{s}(\mathtt{0})}_{\varphi_1}, \quad \underbrace{\mathtt{n} \neq \mathtt{s}\big(\mathtt{s}(\mathtt{0})\big)}_{\varphi_2}, \ldots$$

and let Ψ be the set of these formulae. Now, if PA has a model $\mathbf{N}$ with domain say $\mathbb{N}$, and Φ is any finite subset of Ψ, then, by interpreting $\mathtt{n}$ in a suitable way, $\mathbf{N}$ is also a model of $\mathsf{PA} \cup \Phi$, which implies that $\mathsf{PA} \cup \Phi$ is consistent. Thus, by the COMPACTNESS THEOREM 3.7, $\mathsf{PA} \cup \Psi$ is also consistent and therefore has a model, say $\tilde{\mathbf{N}}$. Now, $\tilde{\mathbf{N}} \vDash \mathsf{PA} \cup \Psi$, but since $\mathtt{n}$ is different from every standard natural number of the form $\mathtt{s}(\mathtt{s}(\ldots\mathtt{s}(\mathtt{0})\ldots))$, the domain of $\tilde{\mathbf{N}}$ must be essentially different from $\mathbb{N}$ (since it contains a kind of infinite number, whereas all standard natural numbers are finite).

This example shows that we cannot axiomatise Peano Arithmetic in First-Order Logic in such a way that all the models we get have essentially the same domain $\mathbb{N}$.

By PROPOSITION 3.5 we know that a set of first-order formulae T is consistent if and only if it has a model, *i.e.*, there is a model $\mathbf{M}$ such that $\mathbf{M} \vDash \mathsf{T}$. So, in order to prove for example that the axioms of Set Theory are consistent we only have to find a single model in which all these axioms hold. However, as a consequence of the following theorems — which we state again without proof — this turns out to be impossible (at least if one restricts oneself to methods formalisable in Set Theory).

THEOREM 3.8 (GÖDEL'S INCOMPLETENESS THEOREM). *Let* T *be a consistent set of first-order* $\mathscr{L}$*-formulae which is sufficiently strong to define the concept of natural numbers and to prove certain basic arithmetical facts (e.g.,*

PA *is such a theory, but also slightly weaker theories would suffice). Then there is always an* $\mathscr{L}$*-sentence* φ *which is independent of* T*, i.e., neither* $\mathsf{T} \vdash \varphi$ *nor* $\mathsf{T} \vdash \neg\varphi$ *(or in other words, there are models* $\mathbf{M}_1$ *and* $\mathbf{M}_2$ *of* T *such that* $\mathbf{M}_1 \vDash \varphi$ *and* $\mathbf{M}_2 \vDash \neg\varphi$*).*

In particular we get that there are number-theoretic statements which can neither be proved nor disproved in PA (*i.e.*, the theory PA is incomplete). Moreover, the following consequence of GÖDEL'S INCOMPLETENESS THEOREM 3.4 shows that not even the consistency of PA can be proved with number-theoretical methods.

THEOREM 3.9 (GÖDEL'S SECOND INCOMPLETENESS THEOREM). *Let* T *be a set of first-order* $\mathscr{L}$*-formulae. Then the statement* $\mathrm{Con}(\mathsf{T})$*, which says that* $\mathsf{T} \nvdash \varphi \wedge \neg\varphi$ *for some* $\mathscr{L}$*-formula* φ*, can be formulated as a number-theoretic sentence* $\mathrm{Con}^{\mathsf{T}}$*. Now, if* T *is consistent and is sufficiently strong to define the concept of natural numbers and to prove certain basic arithmetical facts, then* $\mathsf{T} \nvdash \mathrm{Con}^{\mathsf{T}}$*, i.e.,* T *cannot prove its own consistency. In particular,* $\mathsf{PA} \nvdash \mathrm{Con}^{\mathsf{PA}}$*.*

On the one hand, GÖDEL'S INCOMPLETENESS THEOREM tells us that in any theory T which is sufficiently strong, there are always statements which are independent of T (*i.e.*, which can neither be proved nor disproved in T). On the other hand, statements which are independent of a given theory (*e.g.*, of Set Theory or of Peano Arithmetic) are often very interesting, since they say something unexpected, but in a language we can understand. From this point of view it is good to have GÖDEL'S INCOMPLETENESS THEOREM which guarantees the existence of such statements in theories like Set Theory or Peano Arithmetic.

In Part II we shall present a technique with which we can prove the independence of certain set-theoretical statements from the axioms of Set Theory, which are introduced and discussed below.

The Axioms of Zermelo-Fraenkel Set Theory

In 1905, Zermelo began to axiomatise Set Theory and in 1908 he published his first axiomatic system consisting of seven axioms. In 1922, Fraenkel and Skolem independently improved and extended Zermelo's original axiomatic system, and the final version was presented again by Zermelo in 1930. In this chapter we give the resulting axiomatic system called *Zermelo-Fraenkel Set Theory*, denoted ZF, which contains all axioms of Set Theory except the Axiom of Choice, which will be introduced and discussed in Chapter 5. Alongside the axioms of Set Theory we develop the theory of ordinals and give various notations which will be used throughout this book.

The language of Set Theory contains only one non-logical symbol, namely the binary **membership relation**, denoted by $\in$, and there exists just one type of objects, namely sets. In other words, every object in the domain is a set and there are no other objects than sets. However, to make life easier, instead of $\in(a, b)$ we write $a \in b$ (or on rare occasions also $b \ni a$) and say that "a is an element of b", or that "a belongs to b". Later we will extend the language of Set Theory by defining some constants (like "$\emptyset$" and "ω"), relations (like "$\subseteq$"), and operations (like the power set operation "$\mathscr{P}$"), but in fact, all that can be formulated in Set Theory, can be written as a formula containing only the non-logical relation "$\in$" (but for obvious reasons, we will usually not do so).

0. The Axiom of Empty Set

$$\exists x \forall z (z \notin x)$$

This axiom not only postulates the existence of a set without any elements, *i.e.*, an empty set, it also shows that the set-theoretic universe is non-empty, because it contains at least an empty set (of course, the logical axioms L_{16} and L_{13} already incorporate this fact).

1. The Axiom of Extensionality

$$\forall x \forall y \big(\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y\big)$$

This axiom says that any sets x and y having the same elements are equal. Notice that the converse — which is $x = y$ implies that x and y have the same elements — is just a consequence of the logical axiom L_{17}.

The Axiom of Extensionality also shows that the empty set, postulated by the Axiom of Empty Set, is unique. For assume that there are two empty sets x_0 and x_1, then we have $\forall z (z \notin x_0 \wedge z \notin x_1)$, which implies that $\forall z (z \in x_0 \leftrightarrow z \in x_1)$, and therefore, $x_0 = x_1$.

Let us introduce the following notation: If $\varphi(x)$ is any first-order formula with free variable x (*i.e.*, x occurs at a particular place in the formula φ where it is not in the range of any logical quantifier), then

$$\exists! x\, \varphi(x) \iff \exists x \big(\varphi(x) \wedge \forall z \big(\varphi(z) \rightarrow z = x\big)\big)$$

With this definition we can reformulate the Axiom of Empty Set as follows:

$$\exists! x \forall z (z \notin x)$$

and this unique empty set is denoted by $\emptyset$.

We say that y is a **subset** of x, denoted $y \subseteq x$, if $\forall z (z \in y \rightarrow z \in x)$. Notice that the empty set is a subset of every set. If y is a **proper subset** of x, *i.e.*, $y \subseteq x$ and $y \neq x$, then this is sometimes denoted by $y \subsetneq x$.

One of the most important concepts in Set Theory is the notion of *ordinal number*, which can be seen as a transfinite extension of the natural numbers.

In order to define the concept of ordinal numbers, we have to give first some definitions: Let $z \in x$. Then z is called an **$\in$-minimal element** of x, if $\forall y(y \notin z \vee y \notin x)$, or equivalently, $\forall y(y \in z \rightarrow y \notin x)$. A set x is **ordered by $\in$** if for any sets $y_1, y_2 \in x$ we have $y_1 \in y_2$, or $y_1 = y_2$, or $y_1 \ni y_2$, but we do not require the three cases to be mutually exclusive. Now, a set x is called **well-ordered by $\in$** if it is ordered by $\in$ and every non-empty subset of x has an $\in$-minimal element. Further, a set x is called **transitive** if $\forall y(y \in x \rightarrow y \subseteq x)$. Notice that if x is transitive and $z \in y \in x$, then this implies $z \in x$. A set is called an **ordinal number**, or just an **ordinal**, if it is transitive and well-ordered by $\in$. Ordinal numbers are usually denoted by Greek letters like α, β, γ, λ, *et cetera*, and the collection of all ordinal numbers is denoted by Ω. We will see later, when we know more properties of ordinals, that Ω is not a set. However, we can consider "$\alpha \in \Omega$" just as an abbreviation for "α is an ordinal", and thus, there is no harm in using the symbol Ω in this way, even though Ω is *not* an object of the set-theoretic universe.

FACT 3.10. *If $\alpha \in \Omega$, then either $\alpha = \emptyset$ or $\emptyset \in \alpha$.*

Proof. Since $\alpha \in \Omega$, α is well-ordered by $\in$. Thus, either $\alpha = \emptyset$, or, since $\alpha \subseteq \alpha$, α contains an $\in$-minimal element, say x_0. Now, by transitivity of α, for all $z \in x_0$ we have $z \in \alpha$, and since x_0 is $\in$-minimal we get $x_0 = \emptyset$. $\dashv$

Notice that until now, we cannot prove the existence of any ordinal — or even of any set — beside the empty set, postulated by the Axiom of Empty Set. This will change with the following axiom.

2. The Axiom of Pairing

$$\forall x \forall y \exists! u\big(u = \{x, y\}\big)$$

where $\{x, y\}$ denotes the set which contains just the elements x and y. In order to write this axiom in a more formal way, let us introduce the following notation: If $\varphi(z)$ is any first-order formula with free variable z, and x is any set, then

$$\forall z \in x\,\big(\varphi(z)\big) \iff \forall z\big((z \in x) \rightarrow \varphi(z)\big)\,,$$

and similarly

$$\exists z \in x\,\big(\varphi(z)\big) \iff \exists z\big((z \in x) \wedge \varphi(z)\big)\,.$$

More formally the Axiom of Pairing reads as follows:

$$\forall x \forall y \exists u\big(x \in u \wedge y \in u \wedge \forall z \in u(z = x \vee z = y)\big)$$

If in the above formula we set $x = y$, then $u = \{x, x\}$, which is, by the Axiom of Extensionality, the same as $\{x\}$. Thus, by the Axiom of Pairing, if x is a set, then also $\{x\}$ is a set. Starting with $\emptyset$, an iterated application of the Axiom of Pairing yields for example the sets $\emptyset, \{\emptyset\}, \big\{\{\emptyset\}\big\}, \big\{\big\{\{\emptyset\}\big\}\big\}, \dots,$

and $\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$ Among these sets, $\emptyset$, $\{\emptyset\}$, and $\{\emptyset, \{\emptyset\}\}$ are ordinals, but for example $\{\{\emptyset\}\}$ is not an ordinal.

So far, we did not exclude the possibility that a set may be an element of itself, and in fact, we need the Axiom of Foundation in order to do so. However, we can already show that no ordinal is an element of itself:

FACT 3.11. *If* $\alpha \in \Omega$, *then* $\alpha \notin \alpha$.

Proof. Assume towards a contradiction that $\alpha \in \alpha$. Then $\{\alpha\}$ is a non-empty subset of α and therefore contains an $\in$-minimal element. Now, since $\{\alpha\}$ just contains the element α, the $\in$-minimal element of $\{\alpha\}$ must be α, but on the other hand, $\alpha \in \alpha$ implies that α is not $\in$-minimal, a contradiction. ⊣

For any sets x and y, the Axiom of Extensionality implies that $\{x, y\} = \{y, x\}$. So, it does not matter in which order the elements of a 2-element set are written down. However, with the Axiom of Pairing we can easily define **ordered pairs**, denoted $\langle x, y\rangle$, as follows:

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}$$

Notice that $\langle x, y\rangle = \langle x', y'\rangle$ *iff* $x = x'$ *and* $y = y'$, and further notice that this definition also makes sense in the case when $x = y$ — at least as long as we know that $\{\{x\}\}$ is supposed to denote an ordered pair. By a similar trick, one can also define ordered triples by stipulating for example $\langle x, y, z\rangle := \langle x, \langle y, z\rangle\rangle$, ordered quadruples, *et cetera*, but the notation becomes hard to read and it requires additional methods to distinguish for example between ordered pairs and ordered triples. However, when we have more axioms at hand we can define arbitrary tuples more elegantly.

3. The Axiom of Union

$$\forall x \exists u \forall z \big(z \in u \leftrightarrow \exists w \in x\, (z \in w)\big)$$

More informally, for all sets x there exists the union of x, denoted $\bigcup x$, consisting of all sets which belong to a member of x.

For sets x and y, let $x \cup y := \bigcup\{x, y\}$ denote the **union** of x and y. Notice that $x = \bigcup\{x\}$. For $x \cup y$, where x and y are disjoint (*i.e.*, do not have any common elements) we sometimes write $x \,\dot\cup\, y$, and for $x = \{y_\iota : \iota \in I\}$ we sometimes write $\bigcup_{\iota \in I} y_\iota$ instead of $\bigcup x$.

Now, with the Axiom of Union and the Axiom of Pairing, and by stipulating $x+1 := x \cup \{x\}$, we can for example build the following sets (which are in fact ordinals): $0 := \emptyset$, $1 := 0 + 1 = 0 \cup \{0\} = \{0\}$, $2 := 1 + 1 = 1 \cup \{1\} = \{0, 1\}$, $3 := 2 + 1 = 2 \cup \{2\} = \{0, 1, 2\}$, and so on. In particular, if a set x of this type is already defined, we get that $x + 1 = \{0, 1, 2, \ldots, x\}$. This construction leads to the following definition:

A set x such that $\forall y\big(y \in x \rightarrow (y \cup \{y\}) \in x\big)$ is called **inductive**. On the one hand, $\emptyset$ is inductive. On the other hand, we cannot prove the existence of a non-empty inductive set without the aid of the following axiom.

4. The Axiom of Infinity

$$\exists I\big(\emptyset \in I \land \forall y \in I\big((y \cup \{y\}) \in I\big)\big)$$

More informally, the Axiom of Infinity postulates the existence of a non-empty inductive set containing $\emptyset$. All the sets $0, 1, 2, \ldots$ constructed above — which we recognise as natural numbers — must belong to every inductive set and in fact, the "smallest" inductive set contains just these sets.

5. The Axiom Schema of Separation

For each first-order formula $\varphi(z, p_1, \ldots, p_n)$ with $\text{free}(\varphi) \subseteq \{z, p_1, \ldots, p_n\}$, the following formula is an axiom:

$$\forall x \forall p_1 \ldots \forall p_n \exists y \forall z\big(z \in y \leftrightarrow \big(z \in x \land \varphi(z, p_1, \ldots, p_n)\big)\big)$$

Informally, for each set x and every first-order formula $\varphi(z)$, $\big\{z \in x : \varphi(z)\big\}$ is a set.

One can think of the sets $p_1, \ldots, p_n$ as parameters of φ, which are usually some fixed sets. For example for $\varphi(z, p) \equiv z \in p$ we get that for any sets x and p there exists a set y such that $z \in y \leftrightarrow (z \in x \land z \in p)$. In other words, for any sets x_0 and x_1, the collection of all sets which belong to both, x_0 and x_1, is a set. This set is called the **intersection** of x_0 and x_1 and is denoted by $x_0 \cap x_1$. In general, for non-empty sets x we define

$$\bigcap x = \big\{z \in \bigcup x : \forall y \in x\,(z \in y)\big\}$$

which is the intersection of all sets which belong to x. (In order to see that $\bigcap x$ is a set, let $\varphi(z, x) \equiv \forall y \in x\,(z \in y)$ and apply the Axiom Schema of Separation to $\bigcup x$.) Notice also that $x \cap y = \bigcap\{x, y\}$. Furthermore, for $x = \{y_\iota : \iota \in I\}$ we sometimes write $\bigcap_{\iota \in I} y_\iota$ instead of $\bigcap x$. Another example is when $\varphi(z, p) \equiv z \notin p$. In this case, for $p = y$, we get that $\{z \in x : z \notin y\}$ is a set, denoted $x \setminus y$, which is called the **set-theoretic difference** of x and y.

Let us now turn back to ordinal numbers:

THEOREM 3.12. *(a) If $\alpha, \beta \in \Omega$, then $\alpha \in \beta$ or $\alpha = \beta$ or $\alpha \ni \beta$, where these three cases are mutually exclusive.*

(b) If $\alpha \in \beta \in \Omega$, then $\alpha \in \Omega$.

(c) If $\alpha \in \Omega$, then also $\big(\alpha \cup \{\alpha\}\big) \in \Omega$.

(d) Ω is transitive and is well-ordered by $\in$, or more precisely, Ω is transitive, is ordered by $\in$, and every non-empty class $C \subseteq \Omega$ has an $\in$-minimal element.

Proof. (a) Firstly, notice that by FACT 3.11 the three cases $\alpha \in \beta$, $\alpha = \beta$, $\alpha \ni \beta$, are mutually exclusive.

Let $\alpha, \beta \in \Omega$ be given. If $\alpha = \beta$, then we are done. So, let us assume that $\alpha \neq \beta$. Without loss of generality we may assume that $\alpha \setminus \beta \neq \emptyset$.

We first show that $\alpha \cap \beta$ is the $\in$-minimal element of $\alpha \setminus \beta$: Let γ be an $\in$-minimal element of $\alpha \setminus \beta$. Since α is transitive and $\gamma \in \alpha$, $\forall u(u \in \gamma \to u \in \alpha)$, and since γ is an $\in$-minimal element of $\alpha \setminus \beta$, $\forall u(u \in \gamma \to u \in \beta)$, which implies $\gamma \subseteq \alpha \cap \beta$. On the other hand, if there is a $w \in (\alpha \cap \beta) \setminus \gamma$, then, since α is ordered by $\in$ and $\gamma \neq w$ ($\gamma \notin \beta \ni w$), we must have $\gamma \in w$, and since β is transitive and $w \in \beta$, this implies that $\gamma \in \beta$, which contradicts the fact that $\gamma \in (\alpha \setminus \beta)$. Hence, $\gamma = \alpha \cap \beta$ is the $\in$-minimal element of $\alpha \setminus \beta$. Now, if also $\beta \setminus \alpha \neq \emptyset$, then we would get that $\alpha \cap \beta$ is also the $\in$-minimal element of $\beta \setminus \alpha$, which is obviously a contradiction.

Thus, $\alpha \setminus \beta \neq \emptyset$ implies that $\beta \setminus \alpha = \emptyset$, or in other words, $\beta \subseteq \alpha$, which is the same as saying $\beta = \alpha \cap \beta$. Consequently we get that β is the $\in$-minimal element of $\alpha \setminus \beta$, in particular, $\beta \in \alpha$.

(b) Let $\alpha \in \beta \in \Omega$. Since β is transitive, α is ordered by $\in$. So, it remains to show that α is transitive and well-ordered by $\in$.
well-ordered by $\in$: Because β is transitive, every subset of α is also a subset of β and consequently contains an $\in$-minimal element.
transitive: Let $\delta \in \gamma \in \alpha$. We have to show that $\delta \in \alpha$. Since β is transitive, $\delta \in \beta$, and since β is ordered by $\in$, we have either $\delta \in \alpha$ or $\delta = \alpha$ or $\alpha \in \delta$. If $\delta \in \alpha$, we are done, and if $\delta = \alpha$ or $\alpha \in \delta$, then the set $\{\alpha, \gamma, \delta\} \subseteq \beta$ does not have an $\in$-minimal element, which contradicts the fact that β is well-ordered by $\in$.

(c) We have to show that $\alpha \cup \{\alpha\}$ is transitive and well-ordered by $\in$.
transitive: If $\beta \in (\alpha \cup \{\alpha\})$, then either $\beta \in \alpha$ or $\beta = \alpha$, and in both cases we have $\beta \subseteq (\alpha \cup \{\alpha\})$.
well-ordered by $\in$: Since α is an ordinal, $\alpha \cup \{\alpha\}$ is ordered by $\in$. Let now $x \subseteq (\alpha \cup \{\alpha\})$ be a non-empty set. If $x = \{\alpha\}$, then α is obviously an $\in$-minimal element of x. Otherwise, $x \cap \alpha \neq \emptyset$, and since $\alpha \in \Omega$, $x \cap \alpha$ has an $\in$-minimal element, say γ. Since α is transitive we have $x \cap \gamma = \emptyset$ (otherwise, γ would not be $\in$-minimal in $x \cap \alpha$), which implies that γ is $\in$-minimal in x.

(d) Ω *is transitive and ordered by* $\in$: This is part (b) and part (a) respectively.
Ω *is well-ordered by* $\in$: Let $C \subseteq \Omega$ be a non-empty class of ordinals. If $C = \{\alpha\}$ for some $\alpha \in \Omega$, then α is the $\in$-minimal element of C. Otherwise, C contains an ordinal δ_0 such that $\delta_0 \cap C \neq \emptyset$ and let $x := \delta_0 \cap C$. Then x is a non-empty *set* of ordinals. Now, let $\alpha \in x$ and let γ be an $\in$-minimal element of $x \cap (\alpha \cup \{\alpha\})$. By definition, $\gamma \in (\alpha \cup \{\alpha\})$, and since $(\alpha \cup \{\alpha\}) \in \Omega$, $\gamma \subseteq (\alpha \cup \{\alpha\})$. Thus, every ordinal $\gamma' \in \gamma$ belongs to $\alpha \cup \{\alpha\}$, but by the definition of γ, γ' cannot belong to $x \cap (\alpha \cup \{\alpha\})$, which implies that γ is also $\in$-minimal in x, and consequently in C. ⊣

By THEOREM 3.12.(d) we get that Ω is transitive and well-ordered by $\in$. Thus, if Ω would be a set, Ω would be an ordinal number and therefore would belong to itself, but this is a contradiction to FACT 3.11.

In general, a collection of sets, satisfying for example a certain formula, which is not necessarily a set is called a **class**. For example Ω is a class which is *not* a set (it consists of all transitive sets which are well-ordered by $\in$). Even though proper classes (*i.e.*, classes which are not sets) do not belong to the set-theoretic universe, it is sometimes convenient to handle them like sets, *e.g.*, taking intersections or extracting certain subsets or subclasses from them.

By THEOREM 3.12.(c) we know that if $\alpha \in \Omega$, then also $\big(\alpha \cup \{\alpha\}\big) \in \Omega$. Now, for ordinals $\alpha \in \Omega$ let $\alpha+1 := \alpha \cup \{\alpha\}$. Part (a) of the following result — which is just a consequence of THEOREM 3.12 — motivates this notation.

COROLLARY 3.13. *(a) If $\alpha, \beta \in \Omega$ and $\alpha \in \beta$, then $\alpha+1 \subseteq \beta$. In other words, $\alpha+1$ is the least ordinal which contains α.*

(b) For every ordinal $\alpha \in \Omega$ we have either $\alpha = \bigcup \alpha$ or there exists $\beta \in \Omega$ such that $\alpha = \beta + 1$.

Proof. (a) Assume $\alpha \in \beta$, then $\{\alpha\} \subseteq \beta$, and since β is transitive, we also have $\alpha \subseteq \beta$; thus, $\alpha + 1 = \alpha \cup \{\alpha\} \subseteq \beta$.

(b) Since α is transitive, $\bigcup \alpha \subseteq \alpha$. Thus, if $\alpha \neq \bigcup \alpha$, then $\alpha \setminus \bigcup \alpha \neq \emptyset$. Let β be $\in$-minimal in $\alpha \setminus \bigcup \alpha$. Then $\beta \in \alpha$ and $\beta + 1 \in \Omega$, and by part (a) we have $\beta + 1 \subseteq \alpha$. On the one hand, $\alpha \in \beta + 1$ would imply that $\alpha \in \alpha$, a contradiction to FACT 3.11. On the other hand, $\beta + 1 \in \alpha$ would imply that $\beta \in \bigcup \alpha$, which contradicts the choice of β. Thus, we must have $\beta+1 = \alpha$. $\dashv$

This leads to the following definitions: An ordinal α is called a **successor ordinal** if there exists an ordinal β such that $\alpha = \beta+1$; otherwise, it is called a **limit ordinal**. In particular, $\emptyset$ (or equivalently 0) is a limit ordinal.

We are now ready to define the set of *natural numbers* ω, which will turn out to be the least non-empty limit ordinal. By the Axiom of Infinity we know that there exists an inductive set I. Below we show that there exists also a smallest inductive set. For this, let $I_\Omega = I \cap \Omega$; more precisely,

$$I_\Omega = \{\alpha \in I : \alpha \textit{ is an ordinal}\}.$$

Then I_Ω is a set of ordinals and by THEOREM 3.12.(c), I_Ω is even an inductive set. Now, if there exists no $\alpha \in I_\Omega$ such that α is non-empty and inductive, let $\omega := I_\Omega$, otherwise, define

$$\omega = \bigcap \big\{\alpha \in I_\Omega : \emptyset \in \alpha \textit{ and } \alpha \textit{ is inductive}\big\}.$$

By definition, $\emptyset \in \omega$ and for all $\beta \in \omega$ we have $\beta+1 \in \omega$, *i.e.*, ω is inductive and contains $\emptyset$. In particular, $\bigcup \omega = \omega$, which shows that ω is a limit ordinal. Again by definition, ω does not properly contain any inductive set which contains $\emptyset$.

In particular, ω does not contain any limit ordinal other than $\emptyset$ (since such an ordinal would be an inductive set containing $\emptyset$), and therefore, ω is the smallest non-empty limit ordinal.

The ordinals belonging to ω are called **natural numbers**. One can also define natural numbers inductively as we have done above: $0 := \emptyset$, and for any natural number n, $n+1 := n \cup \{n\} = \{0,1,2,\dots,n\}$. Notice that each natural number n is the set $\{k \in \omega : k < n\}$, where $k < n \iff k \in n$. Further notice that since ω is the smallest non-empty limit ordinal, all natural numbers except 0 are successor ordinals. Now, a set A is called **finite** if there exists a bijection between A and a natural number $n \in \omega$, otherwise, A is called **infinite**. Thus, all natural numbers are finite and ω is the smallest infinite (*i.e.*, not finite) ordinal number.

The following theorem is a consequence of the fact that Ω is transitive and well-ordered by $\in$ (which is just THEOREM 3.12.(d)).

THEOREM 3.14 (TRANSFINITE INDUCTION THEOREM). *Let $C \subseteq \Omega$ be a class of ordinals and assume that:*

(a) if $\alpha \in C$, then $\alpha + 1 \in C$,
(b) if α is a limit ordinal and $\forall \beta \in \alpha(\beta \in C)$, then $\alpha \in C$.

Then C is the class of all ordinals. (Notice that by (b) we have $0 \in C$, in particular, $C \neq \emptyset$.)

Proof. Assume towards a contradiction that $C \neq \Omega$ and let α_0 be the $\in$-minimal ordinal which does not belong to C (such an ordinal exists by THEOREM 3.12.(d)). Now, α_0 can be *neither* a successor ordinal, since this would contradict (a), *nor* a limit ordinal, since this would contradict (b). Thus, α_0 does not exist which implies that $\Omega \setminus C = \emptyset$, *i.e.*, $C = \Omega$. ⊣

The following result is just a reformulation of the TRANSFINITE INDUCTION THEOREM.

COROLLARY 3.15. *For any first-order formula $\varphi(x)$ with free variable x we have*

$$\forall \alpha \in \Omega \left(\forall \beta \in \alpha\big(\varphi(\beta)\big) \to \varphi(\alpha)\right) \to \forall \alpha \in \Omega \left(\varphi(\alpha)\right).$$

Proof. Let $C \subseteq \Omega$ be the class of all ordinals $\alpha \in \Omega$ such that $\varphi(\alpha)$ holds and apply the TRANSFINITE INDUCTION THEOREM 3.14. ⊣

When some form of COROLLARY 3.15 is involved we usually do not mention the corresponding formula φ and just say "by induction on ..." or "by transfinite induction".

6. The Axiom of Power Set

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

Informally, the Axiom of Power Set states that for each set x there is a set $\mathscr{P}(x)$, called the **power set** of x, which consists of all subsets of x.

With the Axiom of Power Set (and other axioms like the Axiom of Union or the Axiom Schema of Separation) we can now define notions like functions, relations, and sequences: Let A and B be arbitrary sets. Then

$$A \times B = \big\{\langle x, y\rangle : x \in A \wedge y \in B\big\}$$

where $\langle x, y\rangle = \big\{\{x\}, \{x, y\}\big\}$; thus, $A \times B \subseteq \mathscr{P}\big(\mathscr{P}(A \cup B)\big)$. Further, let

$${}^{A}B = \big\{f \subseteq A \times B : \forall x \in A\, \exists! y \in B\, (\langle x, y\rangle \in f)\big\}.$$

An element $f \in {}^{A}B$, usually denoted by $f : A \to B$, is called a **function** or **mapping** from A to B, where A is called the **domain** of f, denoted $\mathrm{dom}(f)$.

For $f : A \to B$ we usually write $f(x) = y$ instead of $\langle x, y\rangle \in f$. If S is a set, then the **image** of S under f is denoted by $f[S] = \big\{f(x) : x \in S\big\}$ and $f|_S = \big\{\langle x, y\rangle \in f : x \in S\big\}$ is the restriction of f to S. Furthermore, for a function $f : A \to B$, $f[A]$ is called the **range** of f, denoted $\mathrm{ran}(f)$.

A function $f : A \to B$ is **surjective**, or **onto**, if $\forall y \in B\, \exists x \in A\big(f(x) = y\big)$. We sometimes emphasise the fact that f is surjective by writing $f : A \twoheadrightarrow B$.

A function $f : A \to B$ is **injective**, also called **one-to-one**, if we have $\forall x_1 \in A\, \forall x_2 \in A\big(f(x_1) = f(x_2) \to x_1 = x_2\big)$. To emphasise the fact that f is injective we sometimes write $f : A \hookrightarrow B$.

A function $f : A \to B$ is **bijective** if it is injective and surjective. If $f : A \to B$ is bijective, then

$$\forall y \in B\, \exists! x \in A\big(\langle x, y\rangle \in f\big)$$

and therefore,

$$f^{-1} := \big\{\langle y, x\rangle : \langle x, y\rangle \in f\big\} \in {}^{B}A$$

is a function which is even bijective. So, if there is a bijective function from A to B, then there is also one from B to A and we sometimes just say that there is a **bijection between** A and B. Notice that if $f : A \to B$ is injective, then f is a bijection between A and $f[A]$.

Let x be any non-empty set and assume that for each $i \in x$ we have assigned a set A_i. For $A = \bigcup_{i\in x} A_i$, where $\bigcup_{i\in x} A_i := \bigcup\{A_i : i \in x\}$, the set

$$\prod_{i\in x} A_i = \big\{f \in {}^{x}A : \forall i \in x\, \big(f(i) \in A_i\big)\big\}$$

is called the **Cartesian product** of the sets A_i ($i \in x$). Notice that if all sets A_i are equal to a given set A, then $\prod_{i\in x} A_i = {}^{x}A$. If $x = n$ for some $n \in \omega$, in abuse of notation we also write A^n instead of ${}^{n}A$ by identifying ${}^{n}A$ with the set

$$A^n = \underbrace{A \times \ldots \times A}_{n\text{-times}}.$$

Similarly, for $\alpha \in \Omega$ we sometimes identify a function $f \in {}^{\alpha}A$ with the **sequence** $\langle f(0), f(1), \dots, f(\beta), \dots \rangle_\alpha$ of length α, and vice versa. Sequences (of length α) are usually denoted by using angled brackets (and by using α as a subscript), *e.g.*, $\langle s_0, \dots, s_\beta, \dots \rangle_\alpha$ or $\langle s_\beta : \beta < \alpha \rangle$.
For any set A and any $n \in \omega$, a set $R \subseteq A^n$ is called an ***n*-ary relation** on A. If $n = 2$, then $R \subseteq A \times A$ is also called a **binary relation**. A binary relation R on A is a **well-ordering** of A, if there is an ordinal $\alpha \in \Omega$ and a bijection $f : A \to \alpha$ such that

$$R(x, y) \iff f(x) \in f(y) \,.$$

For any set A, let $\operatorname{seq}(A)$ be the set of all finite sequences which can be formed with elements of A, or more formally:

$$\operatorname{seq}(A) = \bigcup_{n \in \omega} A^n$$

Furthermore, let $\operatorname{seq}^{1\text{-}1}(A)$ be those sequences of $\operatorname{seq}(A)$ in which no element appears twice. Again more formally, this reads as follows:

$$\operatorname{seq}^{1\text{-}1}(A) = \big\{\sigma \in \operatorname{seq}(A) : \sigma \textit{ is injective}\big\}$$

The last notion we introduce in this section is the notion of cardinality: Two sets A and B are said to have the same **cardinality**, denoted $|A| = |B|$, if there is a bijection between A and B. Notice that cardinality equality is an equivalence relation. For example $|\omega \times \omega| = |\omega|$, *e.g.*, define the bijection $f : \omega \times \omega \to \omega$ by stipulating $f\big(\langle n, m\rangle\big) = m + \frac{1}{2}(n + m)(n + m + 1)$.

If $|A| = |B'|$ for some $B' \subseteq B$, then the cardinality of A is less than or equal to the cardinality of B, denoted $|A| \leq |B|$. Notice that $|A| \leq |B|$ *iff* there is an injection from A into B. Finally, if $|A| \neq |B|$ but $|A| \leq |B|$, then cardinality of A is said to be strictly less than the cardinality of B, denoted $|A| < |B|$. Notice that the relation "$\leq$" is reflexive and transitive. The notation suggests that $|A| \leq |B|$ and $|B| \leq |A|$ implies $|A| = |B|$. This is indeed the case and a consequence of the following result.

LEMMA 3.16. *Let A_0, A_1, A be sets such that $A_0 \subseteq A_1 \subseteq A$. If $|A| = |A_0|$, then $|A| = |A_1|$.*

Proof. If $A_1 = A$ or $A_1 = A_0$, then the statement is trivial. So, let us assume that $A_0 \subsetneq A_1 \subsetneq A$ and let $C = A \setminus A_1$, *i.e.*, $A \setminus C = A_1$. Further, let $f : A \to A_0$ be a bijection and define $g : \mathscr{P}(A) \to \mathscr{P}(A_0)$ by stipulating $g(D) := f[D]$. Let $\varphi(z, p_1, p_2, p_3)$ be the following formula:

$$z \in p_1 \wedge \langle 0, p_2\rangle \in z \wedge \forall n \in \omega \exists u \exists v \,\big(\langle n, u\rangle \in z \wedge \langle u, v\rangle \in p_3 \wedge \langle n+1, v\rangle \in z\big)$$

By the Axiom Schema of Separation, for $x = p_1 = {}^{\omega}\mathscr{P}(A)$, $p_2 = C$, and $p_3 = g$, there exists a set y such that $z \in y \leftrightarrow \big(z \in {}^{\omega}\mathscr{P}(A) \wedge \varphi(z, {}^{\omega}\mathscr{P}(A), C, g)\big)$. By induction on n and by assembling the various partial functions produced by the induction into a single function, one gets that y contains just a single function, say $z_0 : \omega \to \mathscr{P}(A)$. In fact, $z_0(0) = C$ and for all $n \in \omega$ we have $z_0(n+1) = f\big[z_0(n)\big]$. Now, let

$$\bar{C} = \bigcup \{z_0(n) : n \in \omega\}$$

and define the function $\tilde{f} : A \to A$ by stipulating

$$\tilde{f}(x) = \begin{cases} f(x) & x \in \bar{C}, \\ x & \text{otherwise.} \end{cases}$$

By definition of $\tilde{f}$ and since f is a bijection which maps C into A_0, $\tilde{f}[\bar{C}] = \bar{C} \setminus C$. Moreover, the function $\tilde{f}$ is injective. To see this, let $x, y \in A$ be *distinct* and consider the following three cases:

(1) If $x, y \in \bar{C}$, then $\tilde{f}(x) = f(x)$ and $\tilde{f}(y) = f(y)$, and since f is injective we get $\tilde{f}(x) \neq \tilde{f}(y)$.

(2) If $x, y \in A \setminus \bar{C}$, then $\tilde{f}(x) = x$ and $\tilde{f}(y) = y$, and hence, $\tilde{f}(x) \neq \tilde{f}(y)$.

(3) If $x \in \bar{C}$ and $y \in A \setminus \bar{C}$, then $\tilde{f}(x) = f(x) \in \bar{C}$ and $\tilde{f}(y) = y \notin \bar{C}$, and therefore, $\tilde{f}(x) \neq \tilde{f}(y)$.

We already know that $\tilde{f}[\bar{C}] = \bar{C} \setminus C$ and by definition we have $\tilde{f}[A \setminus \bar{C}] = A \setminus \bar{C}$. Hence,

$$\tilde{f}[A] = (A \setminus \bar{C}) \mathbin{\dot\cup} (\bar{C} \setminus C) = A \setminus C = A_1$$

which shows that $|A| = |A_1|$. ⊣

THEOREM 3.17 (CANTOR-BERNSTEIN THEOREM). *Let A and B be any sets. If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Proof. Let $f : A \hookrightarrow B$ be a one-to-one mapping from A into B, and $g : B \hookrightarrow A$ be a one-to-one mapping from B into A. Further, let $A_0 := (g \circ f)[A]$ and $A_1 := g[B]$. Then $|A_0| = |A|$ and $A_0 \subseteq A_1 \subseteq A$, hence, by LEMMA 3.16, $|A| = |A_1|$, and since $|A_1| = |B|$ we have $|A| = |B|$. ⊣

As an application of the CANTOR-BERNSTEIN THEOREM 3.17 let us show that the set of **real numbers**, denoted by $\mathbb{R}$, has the same cardinality as $\mathscr{P}(\omega)$.

PROPOSITION 3.18. $|\mathbb{R}| = |\mathscr{P}(\omega)|$.

Proof. Cantor showed that every real number $r > 1$ can be written in a unique way as a product of the form

$$r = \prod_{n \in \omega} \Big(1 + \frac{1}{q_n}\Big)$$

where all q_n's are positive integers and for all $n \in \omega$ we have $q_{n+1} \geq q_n^2$. Such products are called *Cantor products*. So, for every real number $r > 1$ there exists a unique infinite sequence $q_0(r), q_1(r), \dots, q_n(r), \dots$ of positive integers with $q_{n+1} \geq q_n^2$ (for all $n \in \omega$) such that $r = \prod_{n\in\omega} \left(1 + \frac{1}{q_n}\right)$.

Let us first show that $|\mathbb{R}| \leq |\mathscr{P}(\omega)$: For $r \in \mathbb{R}$ let

$$f(r) = \Big\{ \sum_{j \leq n} q_j(r)(2^j + 1) : n \in \omega \Big\} .$$

Define the function $h : \mathbb{R} \to \mathbb{R}$ by stipulating $h(x) := 1 + e^x$, where e is the *Euler number* and $e^x = \sum_{n\in\omega}(x^n/n!)$. Then h is a bijection between $\mathbb{R}$ and the set of real numbers $r > 1$. We leave it as an exercise to the reader to verify that the composition $f{\circ}h$ is an injective mapping from $\mathbb{R}$ into $\mathscr{P}(\omega)$.

To see that $|\mathscr{P}(\omega)| \leq |\mathbb{R}|$, consider for example the function $g(x) = \displaystyle\sum_{n \in x} 3^{-n}$, where $g(\emptyset) := 0$, which is obviously a injective mapping from $\mathscr{P}(\omega)$ into $\mathbb{R}$ (or more precisely, into the interval $[0, \frac{3}{2}]$).

So, by the CANTOR-BERNSTEIN THEOREM 3.17, $|\mathbb{R}| = |\mathscr{P}(\omega)|$. ⊣

7. The Axiom Schema of Replacement

For every first-order formula $\varphi(x, y, p)$ with $\mathrm{free}(\varphi) \subseteq \{x, y, p\}$, where p can be an ordered n-tuple of parameters, the following formula is an axiom:

$$\forall A\, \forall p \big(\forall x \in A\, \exists! y\, \varphi(x, y, p) \to \exists B\, \forall x \in A\, \exists y \in B\, \varphi(x, y, p)\big)$$

In other words, for every set A and for each class function F (*i.e.*, a certain class of ordered pairs of sets) defined on A, $F[A] = \{F(x) : x \in A\}$ is a set. Or even more informally, images of sets under functions are sets.

The Axiom Schema of Replacement is needed to build sets like $\big\{\mathscr{P}^n(\omega) : n \in \omega\big\}$, where $\mathscr{P}^0(\omega) := \omega$ and $\mathscr{P}^{n+1}(\omega) := \mathscr{P}\big(\mathscr{P}^n(\omega)\big)$.

Another application of the Axiom Schema of Replacement is the following result, which will be used for example to define ordinal addition (see THEOREM 3.20) or to build the cumulative hierarchy of sets (see THEOREM 3.22).

THEOREM 3.19 (TRANSFINITE RECURSION THEOREM). *Let F be a class function which is defined for all sets. Then there is a unique class function G defined on Ω such that for each $\alpha \in \Omega$ we have*

$$G(\alpha) = F(G|_\alpha)\,, \quad \textit{where} \;\; G|_\alpha = \big\{\langle \beta, G(\beta)\rangle : \beta \in \alpha\big\}\,.$$

Proof. If such a class function G exists, then, by the Axiom Schema of Replacement, for *every* ordinal α, $\mathrm{ran}(G|_\alpha)$ is a set, and consequently, $G|_\alpha$ is a function with $\mathrm{dom}(G|_\alpha) = \alpha$. This leads to the following definition: For $\delta \in \Omega$, a function g with $\mathrm{dom}(g) = \delta$ is called a *δ-approximation* if

$$\forall \beta \in \delta \big(g(\beta) = F(g|_\beta)\big)\,.$$

In other words, g is an δ-approximation if and only if g has the following properties:

(a) If $\beta+1 \in \delta$, then $g(\beta+1) = F\big(g|_\beta \cup \{\langle \beta, g(\beta)\rangle\}\big)$.
(b) If $\beta \in \delta$ is a limit ordinal, then $g(\beta) = F(g|_\beta)$.

In particular, by (b) we get $g(0) = F(\emptyset)$. For example $g_1 = \big\{\langle 0, F(\emptyset)\rangle\big\}$ is a 1-approximation; in fact, g_1 is the unique 1-approximation. Similarly, $g_2 = \big\{\langle 0, F(\emptyset)\rangle, \big\langle 1, F(\langle 0, F(\emptyset)\rangle)\big\rangle\big\}$ is the unique 2-approximation.

Firstly, notice that for all ordinals δ and δ', if g is an δ-approximation and g' is an δ'-approximation, then $g|_{\delta\cap\delta'} = g'|_{\delta\cap\delta'}$. Otherwise, there would be a smallest ordinal β_0 such that $g(\beta_0) \neq g'(\beta_0)$, but by (a) and (b), β_0 would be neither a successor ordinal nor a limit ordinal.

Secondly, notice that for each ordinal δ there exists a δ-approximation. Otherwise, by THEOREM 3.12.(d), there would be a smallest ordinal δ_0 such that there is no δ_0-approximation. In particular, for each $\delta \in \delta_0$ there would be a δ-approximation, and by the Axiom Schema of Replacement, the collection of all δ-approximations (for $\delta \in \delta_0$) is a set, where the union of this set is a δ'-approximation for some $\delta' \in \Omega$. Now, if δ_0 is a limit ordinal, then $\delta' = \delta_0$ and we get a δ_0-approximation, and if δ_0 is a successor ordinal, then $\delta_0 = \delta'+1$ and we get a δ_0-approximation by (a). So, in both cases we get a contradiction to our assumption that there is no δ_0-approximation.

Now, for each $\alpha \in \Omega$ define $G(\alpha) := g(\alpha)$, where g is the δ-approximation for any δ such that $\alpha \in \delta$. ⊣

By transfinite recursion we are able to define addition, multiplication, and exponentiation of arbitrary ordinal numbers:

Ordinal Addition: For arbitrary ordinals $\alpha \in \Omega$ we define:

(a) $\alpha + 0 := \alpha$.
(b) $\alpha + (\beta+1) := (\alpha+\beta)+1$, for all $\beta \in \Omega$.
(c) If $\beta \in \Omega$ is non-empty and a limit ordinal, then $\alpha+\beta := \bigcup_{\delta\in\beta}(\alpha+\delta)$.

Notice that addition of ordinals is in general not commutative (*e.g.*, $1+\omega = \omega \neq \omega+1$).

Ordinal Multiplication: For arbitrary ordinals $\alpha \in \Omega$ we define:

(a) $\alpha \cdot 0 := 0$.
(b) $\alpha \cdot (\beta+1) := (\alpha\cdot\beta)+\alpha$, for all $\beta \in \Omega$.
(c) If $\beta \in \Omega$ is a limit ordinal, then $\alpha\cdot\beta := \bigcup_{\delta\in\beta}(\alpha\cdot\delta)$.

Notice that multiplication of ordinals is in general not commutative (*e.g.*, $2\cdot\omega = \omega \neq \omega+\omega = \omega\cdot 2$).

Ordinal Exponentiation: For arbitrary ordinals $\alpha \in \Omega$ we define:

(a) $\alpha^0 := 1$.
(b) $\alpha^{\beta+1} := \alpha^\beta \cdot \alpha$, for all $\beta \in \Omega$.
(c) If $\beta \in \Omega$ is non-empty and a limit ordinal, then $\alpha^\beta := \bigcup_{\delta\in\beta}(\alpha^{\delta+1})$.

Notice that for example $2^\omega = \omega$, which should not be confused with cardinal exponentiation defined in Chapter 5.

THEOREM 3.20. *Addition, multiplication, and exponentiation of ordinals are proper binary operations on* Ω.

Proof. We just prove it for addition (the proof for the other operations is similar): For each $\alpha \in \Omega$ define a class function F_α by stipulating $F_\alpha(x) := \emptyset$ if x is *not* a function; and if x *is* a function, then let

$$F_\alpha(x) = \begin{cases} \alpha & \text{if } x = \emptyset, \\ x(\beta) \cup \big\{x(\beta)\big\} & \text{if } \operatorname{dom}(x) = \beta + 1 \text{ and } \beta \in \Omega, \\ \bigcup_{\delta\in\beta} x(\delta) & \text{if } \operatorname{dom}(x) = \beta \text{ and } \beta \in \Omega \setminus \{\emptyset\} \text{ is a limit ordinal,} \\ \emptyset & \text{otherwise.} \end{cases}$$

By the TRANSFINITE RECURSION THEOREM 3.19, for each $\alpha \in \Omega$ there is a unique class function G_α defined on Ω such that for each $\beta \in \Omega$ we have $G_\alpha(\beta) = F_\alpha(G_\alpha|_\beta)$, and in particular we get $G_\alpha(\beta) = \alpha + \beta$. ⊣

Even though addition and multiplication of ordinals are not commutative, they are still associative.

PROPOSITION 3.21. *Addition and multiplication of ordinals defined as above are associative operations.*

Proof. We have to show that for all $\alpha, \beta, \gamma \in \Omega$, $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ and $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$. We give the proof just for addition and leave the proof for multiplication as an exercise to the reader.

Let α and β be arbitrary ordinals. The proof is by induction on $\gamma \in \Omega$. For $\gamma = 0$ we obviously have $(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0)$. Now, let us assume that $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ for some γ. Then:

$$\begin{aligned} (\alpha + \beta) + (\gamma + 1) &= \big((\alpha + \beta) + \gamma\big) + 1 && \text{(by definition of “+”)} \\ &= \big(\alpha + (\beta + \gamma)\big) + 1 && \text{(by our assumption)} \\ &= \alpha + \big((\beta + \gamma) + 1\big) && \text{(by definition of “+”)} \\ &= \alpha + \big(\beta + (\gamma + 1)\big) && \text{(by definition of “+”)} \end{aligned}$$

Finally, let γ be a limit ordinal. Notice first that $\alpha+(\beta+\gamma) = \bigcup_{\delta\in(\beta+\gamma)} \alpha+\delta = \bigcup_{(\beta+\gamma')\in(\beta+\gamma)} \alpha+(\beta+\gamma') = \bigcup_{\gamma'\in\gamma} \alpha+(\beta+\gamma')$. Thus, if $(\alpha+\beta)+\gamma' = \alpha+(\beta+\gamma')$ for all $\gamma' \in \gamma$, then

$$(\alpha + \beta) + \gamma = \bigcup_{\gamma'\in\gamma} (\alpha + \beta) + \gamma' = \bigcup_{\gamma'\in\gamma} \alpha + (\beta + \gamma') = \alpha + (\beta + \gamma)\,.$$

⊣

8. The Axiom of Foundation

$$\forall x\big(\exists z(z \in x) \rightarrow \exists y \in x\,(y \cap x = \emptyset)\big)$$

As a consequence of the Axiom of Foundation we get that there is no infinite descending sequence $x_0 \ni x_1 \ni x_2 \ni \cdots$ since otherwise, the set $\{x_0, x_1, x_2, \dots\}$ would contradict the Axiom of Foundation. In particular, there is no set x such that $x \in x$ and there are also no cycles like $x_0 \in x_1 \in \cdots \in x_n \in x_0$. As a matter of fact we would like to mention that if one assumes the Axiom of Choice, then the non-existence of such infinite descending sequences can be proved to be equivalent to the Axiom of Foundation.

The axiom system containing the axioms 0–8 is called **Zermelo-Fraenkel Set Theory** and is denoted by ZF. In fact, ZF contains all axioms of Set Theory except the Axiom of Choice.

Even though the Axiom of Foundation is irrelevant outside Set Theory, it is extremely useful in the metamathematics of Set Theory, since it allows us to arrange all sets in a cumulative hierarchy and let us define cardinalities as sets.

Models of ZF

By induction on $\alpha \in \Omega$, define the following sets:

$$\begin{aligned} \mathrm{V}_0 &= \emptyset \\ \mathrm{V}_\alpha &= \textstyle\bigcup_{\beta\in\alpha} \mathrm{V}_\beta \qquad \textit{if } \alpha \textit{ is a limit ordinal} \\ \mathrm{V}_{\alpha+1} &= \mathscr{P}(\mathrm{V}_\alpha) \end{aligned}$$

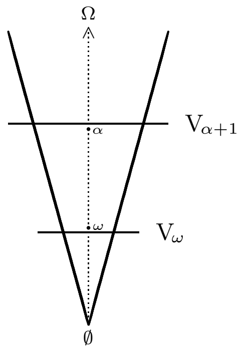
and let

$$\mathbf{V} = \bigcup_{\alpha\in\Omega} \mathrm{V}_\alpha \,.$$

Notice that by construction, for each $\alpha \in \Omega$, V_α is a *set*. Again by induction on $\alpha \in \Omega$ one can easily show that the sets V_α have the following properties:

- Each V_α is transitive.
- If $\alpha \in \beta$, then $\mathrm{V}_\alpha \subsetneq \mathrm{V}_\beta$.
- $\alpha \subseteq \mathrm{V}_\alpha$ and $\alpha \in \mathrm{V}_{\alpha+1}$.

These facts are visualised by the following figure:



Before we can prove that the class $\mathbf{V}$, called the **cumulative hierarchy**, contains *all* set, we have to introduce the notion of transitive closure: Let S be an arbitrary set. By induction on $n \in \omega$ define

$$S_0 = S\,, \qquad S_{n+1} = \bigcup S_n\,,$$

and finally

$$\mathrm{TC}(S) = \bigcup_{n\in\omega} S_n$$

where $\bigcup_{n\in\omega} S_n := \bigcup\{S_n : n \in \omega\}$. For example $x_1 \in S_1$ *iff* $\exists x_0 \in S_0(x_0 \ni x_1)$, and in general, $x_{n+1} \in S_{n+1}$ *iff* $\exists x_0 \in S_0 \cdots \exists x_n \in S_n(x_0 \ni x_1 \ni \cdots \ni x_{n+1})$. Notice that by the Axiom of Foundation, every descending sequence of the form $x_0 \ni x_1 \ni \cdots$ must be finite.

By construction, $\mathrm{TC}(S)$ is transitive, *i.e.*, $x \in \mathrm{TC}(S)$ implies $x \subseteq \mathrm{TC}(S)$, and we further have $S \subseteq \mathrm{TC}(S)$. Moreover, since every transitive set T must satisfy $\bigcup T \subseteq T$, it follows that the set $\mathrm{TC}(S)$ is the smallest transitive set which contains S. Thus,

$$\mathrm{TC}(S) = \bigcap\bigl\{T : T \supseteq S \text{ and } T \text{ is transitive}\bigr\}$$

and consequently the set $\mathrm{TC}(S)$ is called the **transitive closure** of S.

THEOREM 3.22. *For every set x there is an ordinal α such that $x \in \mathrm{V}_\alpha$. In particular, the class $\mathbf{V}$ is equal to the set-theoretic universe.*

Proof. Assume towards a contradiction that there exists a set x which does not belong to $\mathbf{V}$. Let $\bar{x} := \mathrm{TC}\bigl(\{x\}\bigr)$ and let $w := \{z \in \bar{x} : z \notin \mathbf{V}\}$, *i.e.*, $w = \bar{x} \setminus \bigl\{z' \in \bar{x} : \exists\alpha \in \Omega\,(z' \in \mathrm{V}_\alpha)\bigr\}$. Since $x \in w$ we have $w \neq \emptyset$, and by the Axiom of Foundation there is a $z_0 \in w$ such that $(z_0 \cap w) = \emptyset$. Since $z_0 \in w$ we have $z_0 \notin \mathbf{V}$, which implies that $z_0 \neq \emptyset$, but for all $u \in z_0$ there is a least ordinal α_u such that $u \in \mathrm{V}_{\alpha_u}$. By the Axiom Schema of Replacement, $\{\alpha_u : u \in z_0\}$ is a set, and moreover, $\alpha = \bigcup\{\alpha_u : u \in z_0\} \in \Omega$. This implies that $z_0 \subseteq \mathrm{V}_\alpha$ and consequently we get $z_0 \in \mathrm{V}_{\alpha+1}$, which contradicts the fact that $z_0 \notin \mathbf{V}$ and completes the proof. ⊣

It is natural to ask whether there exists some kind of upper bound or ceiling for the set-theoretic universe **V** or if there exists arbitrarily large sets. In order to address this questions we have to introduce the notion of cardinal numbers.

Cardinals in ZF

Let A be an arbitrary set. The cardinality of A, denoted $|A|$, could be defined as the class of all sets B which have the same cardinality as A (*i.e.*, for which there exists a bijection between A and B), but this would have the disadvantage that except for $A = \emptyset$, $|A|$ would not belong to the set-theoretic universe. However, with the Axiom of Foundation the cardinality of a set A can be defined as a proper set:

$$|A| = \{B \in \mathrm{V}_{\beta_0} : \textit{there exists a bijection between } B \textit{ and } A\}$$

where β_0 is the least ordinal number for which there is a $B \in \mathrm{V}_{\beta_0}$ such that B has the same cardinality as A. Notice that for example $|\emptyset| = \{\emptyset\}$, where $\{\emptyset\} \subseteq \mathrm{V}_1$ (in this case, $\beta_0 = 1$). The set $|A|$ is called a **cardinal number**, or just a **cardinal**. Notice that A is not necessarily a member of $|A|$. Further notice that $|A| = |B|$ *iff* there is a bijection between A and B, and as above we write $|A| \leq |B|$ if $|A| = |B'|$ for some $B' \subseteq B$. Cardinal numbers are usually denoted by Fraktur letters like $\mathfrak{m}$ and $\mathfrak{n}$. A cardinal number is **finite** if it is the cardinality of a natural number $n \in \omega$, otherwise it is **infinite**. Finite cardinals are usually denoted by letters like $n, m, \ldots$ An infinite cardinal which contains a well-orderable set is traditionally called an **aleph** and consequently denoted by an "$\aleph$", *e.g.*, $\aleph_0 := |\omega|$. The following fact summarises some simple properties of alephs.

FACT 3.23. *All sets which belong to an aleph can be well-ordered and the cardinality of any ordinal is an aleph. Further, for any ordinals $\alpha, \beta \in \Omega$ we have $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ or $|\alpha| > |\beta|$, and these three cases are mutually exclusive.*

A non-empty set A is called **uncountable** if there is no enumeration of the elements of A, or equivalently, no mapping from ω to A is surjective.

By the Axiom of Infinity we know that there is an infinite set and we have seen that there is even a smallest infinite ordinal, namely ω, which is of course a countable set. Now, the question arises whether every infinite set is countable. We answer this question in two steps: First we show that the set of real numbers is uncountable, and then we show that in general, for every set A there exists a set of strictly greater cardinality than A — which implies that there is no largest cardinal.

PROPOSITION 3.24. *The set of real numbers is uncountable.*

Proof. By PROPOSITION 3.18 we already know that there is a bijection between $\mathbb{R}$ and $\mathscr{P}(\omega)$. Further we have $|\mathscr{P}(\omega)| = |{}^{\omega}2|$. Indeed, for every $x \in \mathscr{P}(\omega)$ let $\chi_x \in {}^{\omega}2$ be such that

$$\chi_x(n) = \begin{cases} 1 & \text{if } n \in x, \\ 0 & \text{otherwise.} \end{cases}$$

So, it is enough to show that no mapping from ω to ${}^{\omega}2$ is surjective. Let

$$\begin{aligned} g : \omega &\longrightarrow {}^{\omega}2 \\ n &\longmapsto f_n \end{aligned}$$

be any mapping from ω to ${}^{\omega}2$. Define the function $f \in {}^{\omega}2$ by stipulating

$$f(n) = 1 - f_n(n)\,.$$

Then for each $n \in \omega$ we have $f(n) \neq f_n(n)$, so, f is distinct from every function f_n $(n \in \omega)$, which shows that g is not surjective. ⊣

For cardinals $\mathfrak{m} = |A|$ let $2^{\mathfrak{m}} := \big|\mathscr{P}(A)\big|$. By modifying the proof above we can show the following result:

THEOREM 3.25 (CANTOR'S THEOREM). *For every cardinal* $\mathfrak{m}$, $2^{\mathfrak{m}} > \mathfrak{m}$.

Proof. Let $A \in \mathfrak{m}$ be arbitrary. It is enough to show that there is an injection from A into $\mathscr{P}(A)$, but there is no surjection from A onto $\mathscr{P}(A)$.
Firstly, the function

$$\begin{aligned} f : A &\longrightarrow \mathscr{P}(A) \\ x &\longmapsto \{x\} \end{aligned}$$

is obviously injective, and therefore we get $\mathfrak{m} \leq 2^{\mathfrak{m}}$.
Secondly, let $g : A \to \mathscr{P}(A)$ be an arbitrary function. Consider the set

$$A' = \big\{x \in A : x \notin g(x)\big\}\,.$$

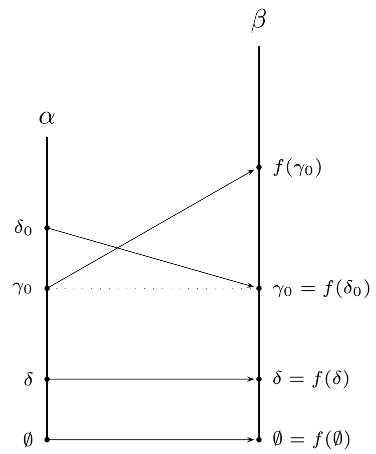
As a subset of A, the set A' is an element of $\mathscr{P}(A)$. If there would be an $x_0 \in A$ such that $g(x_0) = A'$, then $x_0 \in A' \leftrightarrow x_0 \notin g(x_0)$, but since $g(x_0) = A'$, $x_0 \notin g(x_0) \leftrightarrow x_0 \notin A'$. Thus, $x_0 \in A' \leftrightarrow x_0 \notin A'$, which is obviously a contradiction and shows that g is not surjective. ⊣

As an immediate consequence of CANTOR'S THEOREM 3.25 we get that there are arbitrarily large cardinal numbers. Before we show that there are also arbitrarily large ordinal numbers, let us summarise some basic facts about well-orderings: Recall that a binary relation $R \subseteq A \times A$ is a well-ordering of A, if there is an $\alpha \in \Omega$ and a bijection $f : A \to \alpha$ such that $R(x, y)$ *iff* $f(x) \in f(y)$.

The following proposition is crucial in order to define the *order type* of a well-ordering.

PROPOSITION 3.26. *If $\alpha, \beta \in \Omega$ and $f : \alpha \to \beta$ is a bijection such that for all $\gamma_1 \in \gamma_2 \in \alpha$ we have $f(\gamma_1) \in f(\gamma_2)$, then $\alpha = \beta$*

Proof. If $\alpha \neq \beta$, then, by THEOREM 3.12.(a), we have either $\alpha \in \beta$ or $\beta \in \alpha$. Without loss of generality we assume that $\alpha \in \beta$. Thus, there is a $\eta \in \beta \setminus \alpha$. Since f is a bijection, there is a $\gamma \in \alpha$ such that $f(\gamma) = \eta$, and since $\eta \notin \alpha$, $f(\gamma) \neq \eta$ — in fact, $f(\gamma) \in \eta$. Let γ_0 be the $\in$-minimal ordinal in α such that $f(\gamma_0) \neq \gamma_0$, in particular, $f|_{\gamma_0}$ is the identity. The situation we have is illustrated by the following figure:



Since $f(\delta) = \delta$ for all $\delta \in \gamma_0$, $\gamma_0 \in f(\gamma_0)$. Let $\delta_0 = f^{-1}(\gamma_0)$. By the definition of γ_0 we have $\gamma_0 \in \delta_0$, which implies $f(\gamma_0) \in f(\delta_0)$, or equivalently, $f(\gamma_0) \in \gamma_0$, a contradiction. ⊣

As an immediate consequence we get that each well-ordering R of A corresponds to exactly one ordinal, called the **order type** of R, denoted o.t.(R), such that there exists a bijection $f : A \to$ o.t.(R) with the property that for all $a_1, a_2 \in A$ we have $a_1 R a_2 \iff f(a_1) \in f(a_2)$. Indeed, for every $b \in A$ define $A_b = \{a \in A : aRb\}$ and let $f : A \to \Omega$ such that for each $b \in A$ there exists a unique ordinal β such that $f[A_b] = \beta$; then o.t.$(R) = f[A]$. Moreover, by THEOREM 3.12.(a), if R_1 and R_2 are well-orderings of any two subsets of A, then we have o.t.$(R_1) \in$ o.t.(R_2) or o.t.$(R_1) =$ o.t.(R_2) or o.t.$(R_1) \ni$ o.t.(R_2), where the three cases are mutually exclusive.

THEOREM 3.27 (HARTOGS' THEOREM). *For every cardinal $\mathfrak{m}$ there is a smallest aleph, denoted $\aleph(\mathfrak{m})$, such that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$.*

Proof. Let $A \in \mathfrak{m}$ be arbitrary and let $\mathscr{R} \subseteq \mathscr{P}(A \times A)$ be the set of all well-orderings of subsets of A. For every $R \in \mathscr{R}$, o.t.(R) is an ordinal, and for every

$R \in \mathscr{R}$ and any $\beta \in \text{o.t.}(R)$ there is an $R' \in \mathscr{R}$ such that $\text{o.t.}(R') = \beta$, which shows that

$$\alpha = \{\, \text{o.t.}(R) : R \in \mathscr{R} \,\}$$

is an ordinal. By definition, for every $\beta \in \alpha$ there is a well-ordering R_S of some $S \subseteq A$ such that $\text{o.t.}(R_S) = \beta$, which implies that $|\beta| \leq |A|$. On the other hand, $|\alpha| \leq |A|$ would imply that $\alpha \in \alpha$, which is obviously a contradiction. Let $\aleph(\mathfrak{m}) := |\alpha|$, then $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$ and for each $\aleph < \aleph(\mathfrak{m})$ we have $\aleph \leq \mathfrak{m}$. ⊣

COROLLARY 3.28. *For every ordinal number α and for every cardinal number $\mathfrak{m}$, there exists an ordinal number β such that $|\beta| > |\alpha|$ and $|\beta| \not\leq \mathfrak{m}$.*

Proof. For the first inequality let $\alpha \in \Omega$ and let $\mathfrak{n} = |\alpha|$. By HARTOGS' THEOREM 3.27 there is an aleph, namely $\aleph(\mathfrak{n})$, such that $\aleph(\mathfrak{n}) \not\leq \mathfrak{n}$. Now, since $\mathfrak{n}$ and $\aleph(\mathfrak{n})$ both contain well-ordered sets we have $\mathfrak{n} < \aleph(\mathfrak{n})$. Let $w \in \aleph(\mathfrak{n})$ be a well-ordered set and let β be the order type of w. Then $\aleph(\mathfrak{n}) = |\beta| > |\alpha| = \mathfrak{n}$.

For the second inequality let β be the order type of a well-ordered set which belongs to $\aleph(\mathfrak{m})$; then $|\beta| \not\leq \mathfrak{m}$. ⊣

On the Consistency of ZF

Zermelo writes in [118, p. 262] that he was not able to show that the seven axioms for Set Theory given in that article are consistent. Even though it is essential to know whether a theory is consistent or not, by GÖDEL'S SECOND INCOMPLETENESS THEOREM 3.9 we know that for a sufficiently strong consistent theory, there is no way to prove its consistency within this theory.

To apply this result for Set Theory, we first have to show that ZF is "sufficiently strong". In other words, we have to show that ZF is strong enough to define the concept of natural numbers and to prove certain basic arithmetical facts. We do this by showing that $\omega \vDash \mathsf{PA}$: Firstly, PROPOSITION 3.21 shows that addition and multiplication is associative. Secondly, by replacing Ω with ω in COROLLARY 3.15 we get the INDUCTION SCHEMA for natural numbers:

PROPOSITION 3.29 (INDUCTION SCHEMA). *If $\varphi(0)$ and $\varphi(n) \to \varphi(n+1)$ for all $n \in \omega$, then we have $\varphi(n)$ for all $n \in \omega$.*

Hence, every model of ZF contains a model of PA (*i.e.*, if ZF is consistent, then so is PA). However, by GÖDEL'S SECOND INCOMPLETENESS THEOREM 3.9, if ZF is consistent (what we believe or at least assume), then ZF cannot prove its own consistency (*i.e.*, cannot provide a model for itself). In other words, there is no mathematical proof for the consistency of ZF within ZF, which means that there is no way to construct or to define a model of ZF without the aid of some concepts that go beyond what is provided in ordinary Mathematics. More formally, any proof for Con(ZF) has to be carried out in some theory T which contains some information that is not in ZF, and whose consistency cannot be proved within T.

To sum up, either ZF is inconsistent — which is hopefully not the case — or any proof of the consistency of ZF has to be carried out in a theory whose consistency is not provable within that theory.

Notes

Some of the papers mentioned below, or at least their translation into English, can be found in the collection [109] edited by van Heijenoort (whose biography is written by Feferman [35]).

Milestones in Logic. Before we discuss the development of Set Theory, let us give a brief overview of the history of Logic (see Bocheński [11] for a comprehensive problem history of formal logic, providing also large quotes from historical texts).

Organon. Aristotle's logical treatises contain the earliest formal study of Logic (*i.e.*, of Propositional Logic, which is concerned about logical relations between propositions as wholes) and consequently he is commonly considered the first logician. Aristotle's logical works were grouped together by the ancient commentators under the title *Organon*, consisting of *Categories, On Interpretation, Prior Analytics, Posterior Analytics, Topics*, and *On Sophistical Refutations.* Aristotle's work was so outstanding and ahead of his time that nothing significant had been added to his views during the following two millennia.

The Laws of Thought. In 1854, Boole published in *An Investigation of the Laws of Thought* [15] (see also [14]) a new approach to Logic by reducing it to a kind of algebra and thereby incorporated Logic into Mathematics: Boole noticed that Aristotle's Logic was essentially dealing with classes of objects and he further observed that these classes can be denoted by symbols like x, y, z, subject to the ordinary rules of algebra, with the following interpretations.

(a) xy denotes the class of members of x which are also members of y.
(b) If x and y have no members in common, then $x+y$ denotes the class of objects which belong either to x or to y.
(c) $1-x$ denotes all the objects not belonging to the class x.
(d) $x=0$ means that the class x has no members.

However, Boole's Logic was still Propositional Logic, but just 25 years later this weakness was eliminated.

Begriffsschrift. In 1879, Frege published in his *Begriffsschrift* [42] the most important advance in Logic since Aristotle. In this work, Frege presented for the first time what we would recognise today as a logical system with negation, implication, universal quantification, logical axioms, *et cetera*. Even though Frege's achievement in Logic was a major step towards First-Order Logic, his work had led to some contradictions — discovered by Russell — and further steps had to be taken.

Peano Arithmetic. Written in Latin, [89] was Peano's first attempt at an axiomatisation of Mathematics — and in particular of Arithmetic — in a symbolic language. The initial arithmetic notions are *number*, *one*, *successor*, *is equal to*, and nine axioms are stated concerning theses notions. (Today, "=" belongs to the underlying language of Logic, and so, Peano's axioms dealing with equality become redundant; further, we start the natural numbers with *zero*, rather than *one*.) Concerning the problem whether the natural numbers can be considered as symbols without inherent meaning, we refer the reader to the discussion between Müller [83] and Bernays [6]. For Peano's work in Logic, and in particular for the development of the axioms for natural numbers, we refer the reader to Jourdain [67, pp. 270–314] (where one can also find some comments by Peano) and to Wang [111]. According to Jourdain (*cf.* [67, p. 273]), Peano [89] succeeded in writing out wholly in symbols the propositions and proofs of a complete treatise on the arithmetic of positive numbers. However, in the arithmetical demonstrations, Peano made extensive use of Grassmann's work [54], and in fundamental questions of arithmetic as well as in the theory of logical functions, he used Dedekind's work [24]. The main feature of Wang's paper [111] is the printing of a letter (mentioned by Noether on page 490 of [25]) from Dedekind to a headmaster in Hamburg, dated 27 February, 1890. In that letter, Dedekind points out the appearance of non-standard models of axioms for natural numbers (see Kaye [71]) and explains how one could avoid such unintended models by using his *Kettentheorie* (*i.e.*, concept of chains) which he developed in [24]. He also refers to Frege's works [42, 43] and notes that Frege's method of defining a kind of "successor relation" agrees in essence with his concept of chains.

Principia Mathematica. One of these steps was taken by Russell and Whitehead in their *Principia Mathematica* [113], which is a three-volume work on the foundations of Mathematics, published between 1910 and 1913. It is an attempt to derive all mathematical truths from a well-defined set of axioms and inference rules in symbolic logic. The main inspiration and motivation for the *Principia Mathematica* was Frege's earlier work on Logic, especially the contradictions discovered by Russell (as mentioned above). The questions remained whether a contradiction could also be derived from the axioms given in the *Principia Mathematica*, and whether there exists a mathematical statement which could neither be proven nor disproven in the system (for Russell's search for truth we refer the reader to Doxiadis and Papadimitriou [27]). It took another twenty odd years until these questions were answered by Gödel's Incompleteness Theorem, but before, the logical axioms had to be settled.

Grundzüge der theoretischen Logik. In 1928, Ackermann and Hilbert published in their *Grundzüge der theoretischen Logik* [66] to some extent the final version of logical axioms (for the development of these axioms see Hilbert [61, 62, 64]). Our approach to First-Order Logic is partially taken from the first few sections of the hyper-textbook for students by Detlovs and Podnieks (these sections are an extended translation of the corresponding chapters of Detlovs [26]). For other rules of inference see for example Hermes [60] or Ebbinghaus, Flum, and Thomas [28, 29].

Über die Vollständigkeit des Logikkalküls. Gödel proved the COMPLETENESS THEOREM in his doctoral dissertation *Über die Vollständigkeit des Logikkalküls* [46] which was completed in 1929. In 1930, he published the same material as in the doctoral dissertation in a rewritten and shortened form in [47]. The standard proof for GÖDEL'S COMPLETENESS THEOREM is Henkin's proof, which can be found in [58] (see also [59]) as well as in most other textbooks on Logic. A slightly different approach can be found for example in Kleene [72, §72].

Über formal unentscheidbare Sätze der Principia Mathematica. In 1930, Gödel announced in [48] his INCOMPLETENESS THEOREM (published later in [49]), which is probably the most famous theorem in Logic. The theorem as it is stated above is Satz VI of [49], and GÖDEL'S SECOND INCOMPLETENESS THEOREM 3.9, which is in fact a consequence of the proof of that theorem, is Satz XI of [49]. GÖDEL'S INCOMPLETENESS THEOREM 3.4 is discussed in great detail in Mostowski [82] (see also Goldstern and Judah [53, Chapter 4]); and for a different proof of GÖDEL'S INCOMPLETENESS THEOREM, not just a different version of Gödel's proof, see Putnam [95]. For more historical background — as well as for Gödel's platonism — we refer the reader to Goldstein [51].

Now, let us discuss the development of Set Theory: To some extent, Set Theory is the theory of infinite sets; but, what is the infinite and does it exist?

The infinite. As mentioned before, there are two different kinds of infinite, namely the *actual infinite* and the *potential infinite*. To illustrate the difference, let us consider the collection of prime numbers. Euclid proved that for any prime number p there is a prime number p' which is larger than p (see [31, Book IX]). This shows that there are arbitrarily many prime numbers, and therefore, the collection of primes is "potentially" infinite. However, he did not claim that the collection of all prime numbers as a whole "actually" exists. (The difference between actual and potential infinite is discussed in greater detail for example in Bernays [7, Teil II]).

Two quite similar attempts to prove the objective existence of the (actual) infinite are due to Bolzano [12, 13, §13] and Dedekind [24, §5, No. 66], and both are similar to the approach suggested in Plato's *Parmenides* [94, *132a-b*] (for a philosophical view to the notion of infinity we refer the reader to Mancosu [78]). However, Russell [99, Chapter XIII, p. 139 ff.] (see also [101, Chapter XLIII]) shows that these attempts must fail. Moreover, he demonstrates that the infinite is neither self-contradictory nor demonstrable logically and writes that *we must conclude that nothing can be known* a priori *as to whether the number of things in the world is finite or infinite. The conclusion is, therefore, to adopt a Leibnizian phraseology, that some of the possible worlds are finite, some infinite, and we have no means of knowing to which of these two kinds our actual world belongs. The axiom of infinity will be true in some possible worlds and false in others; whether it is true or false in this world, we cannot tell* (*cf.* [99, p. 141]).

If the infinite exists, the problem still remains how one would recognise infinite sets, or in other words, how one would define the predicate "infinite". Dedekind provided a definition in [24, §5, No. 64], which is — as Schröder [103, p. 303 f.] pointed out — equivalent to the definition given three years earlier by Peirce (*cf.* [91, p. 202] or [5, p. 51]). However, the fact that an infinite set can be mapped injectively into a proper subset of itself — which is the key idea of Dedekind's definition of infinite sets — was already discovered and clearly explained about 250 years earlier by Galilei (see [45, First Day]). Another definition of the infinite — which will be compared with Dedekind's definition in Chapter 7 — can be found in von Neumann [86, p. 736]. More definitions of finiteness, as well as their dependencies, can be found for example in Lévy [75] and in Spišiak and Vojtáš [106].

Birth of Set Theory. As mentioned above, the birth of Set Theory dates to 1873 when Cantor proved that the set of real numbers is uncountable. One could even argue that the exact birth date is 7 December 1873, the date of Cantor's letter to Dedekind informing him of his discovery.

Cantor's first proof that there is no bijection between the set of real numbers and the set of natural numbers used an argument with nested intervals (*cf.* [18, §2] or [23, p. 117]). Later, he improved the result by showing that $2^{\mathfrak{m}} > \mathfrak{m}$ for every cardinal $\mathfrak{m}$ (*cf.* [20] or [23, III. 8]), which is nowadays called CANTOR'S THEOREM. The argument used in the proof of PROPOSITION 3.24 — which is in fact just a special case of CANTOR'S THEOREM — is sometimes called *Cantor's diagonal argument*. The word "diagonal" comes from the diagonal process used in the proofs of PROPOSITION 3.24 and CANTOR'S THEOREM. The diagonal process is a technique of constructing a new member of a set of lists which is distinct from all members of a given list. This is done by arranging first the list as a matrix, whose *diagonal* gives information about the x^{th} term of the x^{th} row of the matrix. Then, by changing each term of the diagonal, we get a new list which is distinct from every row of the matrix (see also Kleene [72, §2]).

For a brief biography of Cantor and for the development of Set Theory see for example Fraenkel [41], Schoenflies [102], and Kanamori [68].

Russell's Paradox. The fact that a naïve approach to the notion of "set" leads to contradictions was discovered by Russell in June 1901 while he was working on his *Principles of Mathematics* [101] (see also Grattan-Guinness [55]). When Russell published his discovery, other mathematicians and set-theorists like Zermelo (see [115, footnote p. 118 f.] or Rang and Thomas [96]) had already been aware of this antinomy, which — according to Hilbert — *had a downright catastrophic effect when it became known throughout the world of Mathematics* (cf. [63, p. 169] or [65, p. 190]). However, Russell was the first to discuss the contradiction at length in his published works, the first to attempt to formulate solutions and the first to appreciate fully its importance. For example the entire Chapter X of [101] was dedicated to discussing this paradox (in particular see [101, Chapter X, §102]). In order to prevent the emergence of antinomies and paradoxes in Set Theory and in Logic in general, Russell developed in [101, Appendix B] (see also [98]) his theory of logical types which rules out self-reference. According to this theory, self-referential statements are neither true nor false, but meaningless.

Russell's Paradox as well as some other antinomies can also be found in Fraenkel, Bar-Hillel, and Lévy [36, Chapter I].

Axiomatisation of Set Theory. In 1908, Zermelo published in [118] his first axiomatic system consisting of seven axioms, which he called:

1. Axiom der Bestimmtheit
   which corresponds to the Axiom of Extensionality
2. Axiom der Elementarmengen
   which includes the Axiom of Empty Set as well as the Axiom of Pairing
3. Axiom der Aussonderung
   which corresponds to the Axiom Schema of Separation
4. Axiom der Potenzmenge
   which corresponds to the Axiom of Power Set
5. Axiom der Vereinigung
   which corresponds to the Axiom of Union
6. Axiom der Auswahl
   which corresponds to the Axiom of Choice
7. Axiom des Unendlichen
   which corresponds to the Axiom of Infinity

In 1930, Zermelo presented in [116] his second axiomatic system, which he called ZF-system, in which he incorporated ideas of Fraenkel [38], Skolem [104], and von Neumann [85, 86, 88]. (see also Zermelo [114]). In fact, he added the Axiom Schema of

Replacement and the Axiom of Foundation to his former system, cancelled the Axiom of Infinity (since he thought that it does not belong to the general theory of sets), and did not mention explicitly the Axiom of Choice (because of its different character and since he considered it as a general logical principle). For Zermelo's published work in Set Theory, described and analysed in its historical context, see Zermelo [117], Kanamori [70] and Ebbinghaus [30].

The need for the Axiom Schema of Replacement was first noticed by Fraenkel (see [117, p. 23]) who introduced a certain form of it in [38] (another form of it he gave in [37, Definition 2, p. 158]). However, the present form was introduced by von Neumann [87] (see the note below on the TRANSFINITE RECURSION THEOREM). As a matter of fact we would like to mention that the Axiom Schema of Replacement was already used implicitly by Cantor in 1899 (*cf.* [23, p. 444, line 3]). Beside Fraenkel, also Skolem realised that Zermelo's first axiomatic system was not sufficient to provide a complete foundation for the usual theory of sets and introduced — independently of Fraenkel — in 1922 the Axiom Schema of Replacement (see [104] or [105, p. 145 f.]). In [104], he also gave a proper definition of the notion "definite proposition" and, based on a theorem of Löwenheim [77], he discovered the following fact [105, p. 139] (stated in Chapter 15 as LÖWENHEIM-SKOLEM THEOREM 15.1): *If the axioms are consistent, there exists a domain in which the axioms hold and whose elements can all be enumerated by means of the positive finite integers* . At a first glance this looks strange, since we know for example that the set of real numbers is uncountable. However, this so-called SKOLEM PARADOX — which we will meet in a slightly different form in Chapter 15 — is not a paradox in the sense of an antinomy, it is just a somewhat unexpected feature of formal systems (see also Kleene [72, p. 426 f.] and von Plato [110]).

Concerning the terminology we would like to mention that the definition of ordered pairs given above was introduced by Kuratowski [74, Définition V, p. 171] (compare with Hausdorff [57, p. 32] and see also Kanamori [69, §5]), and that the infinite set which corresponds to $\omega = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots\}$ was introduced by von Neumann [84]. For more historical background see Bachmann [4] or Fraenkel [8, Part I], and for a brief discussion of the axiom systems of von Neumann, Bernays, and Gödel see Fraenkel [8, Part I, Section 7].

The Axiom of Foundation. As mentioned above, Zermelo introduced this axiom in his second axiomatisation of Set Theory in 1930, but it goes back to von Neumann (*cf.* [85, p. 239] and [88, p. 231]), and in fact, the idea can already be found in Mirimanoff [80, 81]: For example in [80, p. 211] he calls a set x *regular* (French "ordinaire") if every descending sequence $x \ni x_1 \ni x_2 \ni \dots$ is finite. However, he did not postulate the regularity of sets as an axiom, but if one would do so, one would get the Axiom of Regularity saying that every set is regular. Now, as a consequence of the Axiom of Foundation we got the fact that there are no infinite descending sequences of the form $x_1 \ni x_2 \ni \dots \ni x_i \dots$, which just tells us that every set is regular. Thus, the Axiom of Foundation implies the Axiom of Regularity. The converse is not true, unless we assume some non-trivial form of the Axiom of Choice (see Mendelson [79]). As a matter of fact we would like to mention that Zermelo, when he formulated the Axiom of Foundation in [116], gave both definitions and just mentioned (without proof) that they are equivalent.

Ordinal numbers. The theory of ordinals was first developed in an axiomatic way by von Neumann in [84] (see also [85, 86, 87]). For an alternative axiomatic approach to ordinals, independently of ordered sets and types, see Tarski [108] or Lindenbaum and Tarski [76]. For some more definitions of ordinals see Bachmann [4, p. 24].

The Transfinite Recursion Theorem. The TRANSFINITE RECURSION THEOREM was first formulated and proved by von Neumann [87], who also pointed out that, beside the axioms of Zermelo, also the Axiom Schema of Replacement has to be used. Even though a certain form of the Axiom Schema of Replacement was already given by Fraenkel (see above), von Neumann showed that Fraenkel's notion of function is not sufficient to prove the TRANSFINITE RECURSION THEOREM. Moreover, he showed (*cf.* [87, I.3]) that Fraenkel's version of the Axiom Schema of Replacement given in [39, §1 1] follows from the other axioms given there (see also Fraenkel's note [40]).

The Cantor-Bernstein Theorem. This theorem, unfortunately also known as SCHRÖDER-BERNSTEIN THEOREM, was first stated and proved by Cantor (*cf.* [19, VIII.4] or [23, p. 413], and [21, §2, Satz B] or [23, p. 285]). In order to prove this theorem, Cantor used the Trichotomy of Cardinals, which is — as we will see in Chapter 5 — equivalent to the Axiom of Choice (see also [23, p. 351, Anm. 2]). An alternative proof, avoiding any form of the Axiom of Choice, was found by Bernstein, who was initially a student of Cantor's. Bernstein presented his proof around Easter 1897 in one of Cantor's seminars in Halle, and the result was published in 1898 in Borel [16, p. 103–106] (see RELATED RESULT 12). About the same time, Schröder gave a similar proof in [103] (submitted May 1896), but unfortunately, Schröder's proof was flawed by an irreparable error. While other mathematicians regarded his proof as correct, Korselt wrote to Schröder about the error in 1902. In his reply, Schröder admitted his mistake which he had already found some time ago but did not have the opportunity to make public. A few weeks later, Korselt submitted the paper [73] — which appeared almost a decade later — with a proof of the CANTOR-BERNSTEIN THEOREM which is quite different from the one given by Bernstein. A proof of the CANTOR-BERNSTEIN THEOREM, similar to Korselt's proof, was found in 1906 independently by Peano [90] and Zermelo (see [118, footnote p. 272 f.]). However, they could not know that they had just rediscovered the proof that had already been obtained twice by Dedekind in 1887 and 1897, since Dedekind's proof — in our terminology given above — was not published until 1932 (see [25, LXII & Erl. p. 448] and [23, p. 449]).

Cantor products. Motivated by a result due to Euler on partition numbers (*cf.* [32, Caput XVI]), Cantor showed in [17] (see also [23, pp. 43–50]) that every real number $r > 1$ can be written in a unique way as a product of the form $\prod_{n\in\omega}\left(1+\frac{1}{q_n}\right)$, where all q_n's are positive integers and $q_{n+1} \geq q_n^2$. He also showed that $r = \prod_{n\in\omega}\left(1+\frac{1}{q_n}\right)$ is rational if and only if there is an $m \in \omega$ such that for all $n \geq m$ we have $q_{n+1} = q_n^2$, and further he gave the representation of the square roots of some small natural numbers. For example, the q_n's in the representation of $\sqrt{2}$ are $q_0 = 3$ and $q_{n+1} = 2q_n^2 - 1$. More about Cantor products can be found for example in Perron [92, §35].

Cardinal numbers. The concept of cardinal number is one of the most fundamental concepts in Set Theory. Cantor describes cardinal numbers as follows (*cf.* [21, §1] or [23, p. 282 f.]): *The general concept which with the aid of our active intelligence results from a set M, when we abstract from the nature of its various elements and from the order of their being given, we call the "power" or "cardinal number" of M.*

This double abstraction suggests his notation "$\overline{\overline{M}}$" for the cardinality of M. As mentioned above, one can define the cardinal number of a set M as an object $\overline{\overline{M}}$ which consists of all those sets (including M itself) which have the same cardinality as M. This approach, which was for example taken by Frege (*cf.* [43, 44]), and Russell (*cf.* [97, p. 378] or [98, Section IX, p. 256]), has the advantage that it can be carried out in naïve Set Theory (see also Kleene [72, p. 9]). However, it has the disadvantage that for every non-empty set M, the object $\overline{\overline{M}}$ is a proper class and therefore does not belong to the set-theoretic universe.

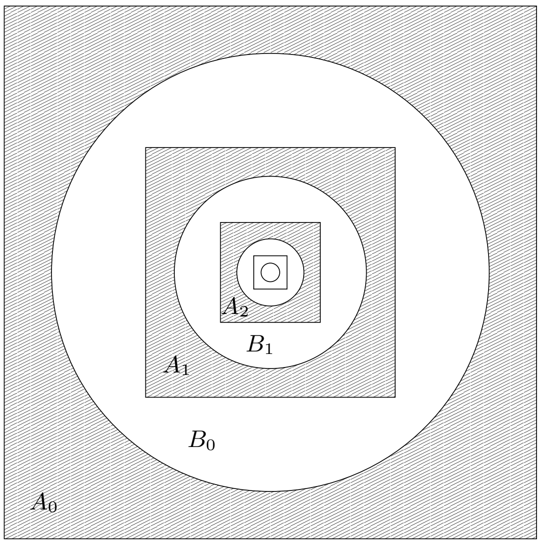
Hartogs' Theorem. The proof of HARTOGS' THEOREM is taken from Hartogs [56]. In that paper, Hartogs' main motivation was to find a proof for Zermelo's Well-Ordering Principle which does not make use of the Axiom of Choice. However, since the Well-Ordering Principle and the Axiom of Choice are equivalent, he had to assume something similar, which he had done assuming explicitly Trichotomy of Cardinals. These principles will be discussed in greater detail in Chapter 5.

In 1935, Hartogs was forced to retire from his position in Munich, where he committed suicide in August 1943 because he could not bear any longer the continuous humiliations by the Nazis.

RELATED RESULTS

12. *Bernstein's proof of the Cantor-Bernstein Theorem.* Below we sketch out Bernstein's proof of the CANTOR-BERNSTEIN THEOREM as it was published by Borel in [16, p. 104 ff.]: Let A and B be two arbitrary sets and let $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$ two injections. Further, let $A_0 := A$, $B_0 := g[B]$, and for $n \in \omega$ let $A_{n+1} := (g\circ f)[A_n]$ and $B_{n+1} := (g\circ f)[B_n]$; finally let $D := \bigcap_{n\in\omega} A_n$.

    We get the following picture:



It is not hard to verify that the sets A_n and B_n have the following properties:

(a) $A_0 = D \cup (A_0 \setminus B_0) \cup (B_0 \setminus A_1) \cup (A_1 \setminus B_1) \cup (B_1 \setminus A_2) \cup \ldots$

(b) $B_0 = D \cup (B_0 \setminus A_1) \cup (A_1 \setminus B_1) \cup (B_1 \setminus A_2) \cup (A_2 \setminus B_2) \cup \ldots$

(c) For all $n \in \omega$, $|A_n \setminus B_n| = |A_{n+1} \setminus B_{n+1}|$.

Since the sets $(A_n \setminus B_n)$, $(B_n \setminus A_{n+1})$, and D, are pairwise disjoint, by (c) and by regrouping the representation of B_0 in (b), we get $|A_0| = |B_0|$.

References

1. Aristotle, ***Organon***, Athens, *published by Andronikos of Rhodos around* 40 B.C.
2. ———, ***Topics***, Athens, *published by Andronikos of Rhodos around* 40 B.C.
3. ———, ***Physics***, Athens, *published by Andronikos of Rhodos around* 40 B.C.
4. Heinz Bachmann, ***Transfinite Zahlen***, Springer-Verlag, Berlin · Heidelberg, 1967.
5. Karel Berka and Lothar Kreiser, ***Logik-Texte.*** *Kommentierte Auswahl zur Geschichte der modernen Logik*, Akademie-Verlag, Berlin, 1971.
6. Paul Bernays, *Erwiderung auf die Note von Herrn Aloys Müller: Über Zahlen als Zeichen*, ***Mathematische Annalen***, vol. 90 (1923), 159–163.
7. ———, *Die Philosophie der Mathematik und die Hilbertsche Beweistheorie*, ***Blätter für deutsche Philosophie***, vol. 4 (1930), 326–367 (also published in [9]).
8. ———, ***Axiomatic Set Theory.*** *With a historical introduction by Abraham A. Fraenkel*, 2nd ed., [Studies in Logic and the Foundations of Mathematics], North-Holland, Amsterdam, 1968 [reprint: Dover Publications, New York, 1991].
9. ———, ***Abhandlungen zur Philosophie der Mathematik***, Wissenschaftliche Buchgesellschaft, Darmstadt, 1976.
10. Joseph M. Bocheński, ***A History of Formal Logic***, 2nd ed., [translated and edited by Ivo Thomas], Chelsea Publishing Company, New York, 1970.
11. ———, ***Formale Logik***, 4th ed., Orbis Academicus: Problemgeschichten der Wissenschaft in Dokumenten und Darstellungen, Verlag Karl Alber, Freiburg, 1978 (see [10] for a translation into English).
12. Bernard Bolzano, ***Paradoxien des Unendlichen***, Hrsg. aus dem schriftlichen Nachlasse des Verfassers von Fr. Přihonský, C. H. Reclam Sen., Leipzig, 1851.
13. ———, ***Paradoxes of the Infinite***, [translated by D. A. Steele], Routledge and Kegan Paul, London, 1950.
14. George Boole, *The calculus of logic*, ***The Cambridge and Dublin Mathematical Journal***, vol. 3 (1848), 183–198.
15. ———, ***An Investigation of the Laws of Thought, on Which are Founded the Mathematical Theories of Logic and Probabilities***, Walton and Maberley, London, 1854 [reprint: Prometheus Books, New York, 2003].
16. Émile Borel, ***Leçons sur la Théorie des Fonctions***, Gauthier-Villars et Fils, Paris, 1898.
17. Georg Cantor, *Zwei Sätze über eine gewisse Zerlegung der Zahlen in unendliche Produkte*, ***Zeitschrift für Mathematik und Physik***, vol. 14 (1869), 152–158.

18. ______, *Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen*, ***Journal für die reine und angewandte Mathematik (Crelle)***, vol. 77 (1874), 258–262.
19. ______, *Mitteilungen zur Lehre vom Transfiniten. I.&II.*, ***Zeitschrift für Philosophie und philosophische Kritik***, vol. 91/92 (1887/1888), 81–125 / 240–265.
20. ______, *Über eine elementare Frage der Mannigfaltigkeitslehre*, ***Jahresbericht der Deutschen Mathematiker-Vereinigung***, vol. 1 (1891), 75–78.
21. ______, *Beiträge zur Begründung der transfiniten Mengenlehre. I./II.*, ***Mathematische Annalen***, vol. 46/49 (1895/1897), 481–512/207–246 (see [22] for a translation into English).
22. ______, ***Contributions to the Founding of the Theory of Transfinite Numbers,*** (translation into English of [21]), [translated, and provided with an introduction and notes, by Philip E. B. Jourdain], Open Court Publishing Company, Chicago and London, 1915 [reprint: Dover Publications, New York, 1952].
23. ______, ***Gesammelte Abhandlungen mathematischen und philosophischen Inhalts***, *Mit Erläuternden Anmerkungen sowie mit Ergänzungen aus dem Briefwechsel Cantor-Dedekind*, edited by E. Zermelo, Julius Springer, Berlin, 1932.
24. Richard Dedekind, ***Was sind und was sollen die Zahlen***, Friedrich Vieweg & Sohn, Braunschweig, 1888 (see also [25, pp. 335–390]).
25. ______, ***Gesammelte mathematische Werke III***, edited by R. Fricke, E. Noether, and Ö. Ore, Friedrich Vieweg & Sohn, Braunschweig, 1932.
26. Vilnis Detlovs, ***Matemātiskā logika***, Izdevniecība "Zvaigzne", Riga, 1974.
27. Apostolos Doxiadis and Christos H. Papadimitriou, ***Logicomix: An Epic Search for Truth***, *(a graphic novel with art by Alecos Papadatos and Annie di Donna)*, Bloomsbury, New York, 2009.
28. Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas, ***Mathematical Logic***, 2nd ed., *English translation of* [29], [Undergraduate Texts in Mathematics], Springer-Verlag, New York, 1994.
29. ______, ***Einführung in die mathematische Logik***, 4th ed., Spektrum Akademischer Verlag, Heidelberg · Berlin, 1996.
30. Heinz-Dieter Ebbinghaus (in cooperation with Volker Peckhaus), ***Ernst Zermelo, An Approach to His Life and Work***, Springer-Verlag, Berlin · Heidelberg, 2007.
31. Euclid, ***"Elements"***, Alexandria, *written around* 300 B.C.
32. Leonhard Euler, ***Introductio in analysin infinitorum (Tomus Primus)***, Marcum-Michaelem Bousquet & Socios, Lausanne, 1748 (see [34]/[33] for a translation into English/German).
33. ______, ***Einleitung in die Analysis des Unendlichen***, [translated by H. Maser], Julius Springer, Berlin, 1885 [reprint with an introduction by W. Walter: Springer-Verlag, Berlin, 1983].
34. ______, ***Introduction to Analysis of the Infinite***, [translated by John D. Blanton], Springer-Verlag, Berlin · Heidelberg, 1988.
35. Anita Burdman Feferman, ***From Trotsky to Gödel: The Life of Jean Van Heijenoort***, A K Peters, Natick, Massachusetts, 1993.
36. Abraham A. Fraenkel, Yehoshua Bar-Hillel, and Azriel Levy, ***Foundations of Set Theory***, [Studies in Logic and the Foundations of Mathematics 67], North-Holland, Amsterdam, 1973.

37. Adolf Fraenkel, *Axiomatische Begründung der transfiniten Kardinalzahlen. I.*, ***Mathematische Zeitschrift***, vol. 13 (1922), 153–188.
38. ———, *Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre*, ***Mathematische Annalen***, vol. 86 (1922), 230–237.
39. ———, *Axiomatische Theorie der geordneten Mengen. (Untersuchungen über die Grundlagen der Mengenlehre. II.)*, ***Journal für die reine und angewandte Mathematik (Crelle)***, vol. 155 (1926), 129–158.
40. ———, *Zusatz zu vorstehendem Aufsatz Herrn v. Neumanns* (refers to [87]), ***Mathematische Annalen***, vol. 99 (1928), 392–393.
41. ———, *Das Leben Georg Cantors*, *in* ***Gesammelte Abhandlungen mathematischen und philosophischen Inhalts*** (E. Zermelo, ed.), Julius Springer, Berlin, 1932, pp. 452–483.
42. Gottlob Frege, ***Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens***, L. Nebert, Halle, 1879 (see [109] for a translation into English).
43. ———, ***Die Grundlagen der Arithmetik, eine logisch-mathematische Untersuchung über den Begriff der Zahl***, Verlag von Wilhelm Koebner, Breslau, 1884. [English translation (with German original): *The foundations of arithmetic. A logo-mathematical enquiry into the concept of number*, translated by J. L. Austin, Basil Blackwell, Oxford, 1950].
44. ———, *The concept of number,* (translation into English of parts of [43]), *in* ***Philosophy of Mathematics. Selected Readings*** (Paul Benacerraf and Hilary Putnam, eds.), Cambridge University Press, Cambridge, 2nd ed., 1983, pp. 130–159.
45. Galileo Galilei, ***Discorsi e Dimonstrazioni Matematiche, intorno à due nuove scienze attenenti alle Mecanica & i Moviemnti Locali***, Elzevirs, Leyden, 1638. [English translation: *Two New Sciences. Including Centers of Gravity and Force of Percussion*, translated by S. Drake, The University of Wisconsin Press, Madison, 1974; German translation: *Unterredungen und mathematische Demonstrationen über zwei neue Wissenszweige, die Mechanik und die Fallgesetze betreffend*, translated and edited by A. J. von Oettingen, Verlag Harri Deutsch, Frankfurt/M., 2004].
46. Kurt Gödel, *Über die Vollständigkeit des Logikkalküls*, Dissertation (1929), University of Vienna (Austria), (reprinted and translated into English in [50].
47. ———, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, ***Monatshefte für Mathematik und Physik***, vol. 37 (1930), 349–360 (see [109, 50] for a translation into English).
48. ———, *Einige metamathematische Resultate über Entscheidungsdefinitheit und Widerspruchsfreiheit*, ***Anzeiger der Akademie der Wissenschaften in Wien, mathematisch-naturwissenschaftliche Klasse***, vol. 67 (1930), 214–215 (see [109, 50] for a translation into English).
49. ———, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme*, ***Monatshefte für Mathematik und Physik***, vol. 38 (1931), 173–198 (see [109, 50] for a translation into English).
50. ———, ***Collected Works, Volume I: Publications 1929–1936***, edited by S. Feferman (Editor-in-chief), J. W. Dawson, Jr., S. C. Kleene, G. H. Moore, R. M. Solovay, J. van Heijenoort, Oxford University Press, New York, 1986.
51. Rebecca Goldstein, ***Incompleteness – The proof and paradox of Kurt Gödel***, Great Discoveries, Atlas Books / W. W. Norton & Company, New York and London, 2005 (see [52] for a translation into German).

52. ______, ***Kurt Gödel, Jahrhundertmathematiker und großer Entdecker***, [translated into German by Thorsten Schmidt], Piper, München and Zürich, 2006.
53. Martin Goldstern and Haim Judah, ***The incompleteness phenomenon. A new course in mathematical logic***, A.K. Peters, Wellesley, 1995.
54. Hermann Grassmann, ***Lehrbuch der Arithmetik für höhere Lehranstalten***, Th. Chr. Fr. Enslin, Berlin, 1861.
55. Ivor Grattan-Guinness, *How Bertrand Russell discovered his paradox*, ***Historia Mathematica***, vol. 5 (1978), 127–137.
56. Friedrich Hartogs, *Über das Problem der Wohlordnung*, ***Mathematische Annalen***, vol. 76 (1915), 438–443.
57. Felix Hausdorff, ***Grundzüge der Mengenlehre***, de Gruyter, Leipzig, 1914 [reprint: Chelsea, New York, 1965].
58. Leon Henkin, *The completeness of the first-order functional calculus*, ***The Journal of Symbolic Logic***, vol. 14 (1949), 159–166.
59. ______, *The discovery of my completeness proofs*, ***The Bulletin of Symbolic Logic***, vol. 2 (1996), 127–158.
60. Hans Hermes, ***Einführung in die mathematische Logik. Klassische Prädikatenlogik***, Mathematische Leitfäden, B. G. Teubner Verlagsgesellschaft, Stuttgart, 1963.
61. David Hilbert, *Neubegründung der Mathematik. Erste Mitteilung*, ***Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität***, vol. 1 (1922), 157–177.
62. ______, *Die logischen Grundlagen der Mathematik*, ***Mathematische Annalen***, vol. 88 (1923), 151–165.
63. ______, *Über das Unendliche*, ***Mathematische Annalen***, vol. 95 (1925), 161–190 (see [65] or [109] for a translation into English).
64. ______, *Die Grundlagen der Mathematik. Vortrag, gehalten auf Einladung des Mathematischen Seminars im Juli 1927 in Hamburg.*, ***Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität***, vol. 6 (1928), 65–85 (see [109] for a translation into English).
65. ______, *On the infinite*, in ***Philosophy of Mathematics. Selected Readings*** (Paul Benacerraf and Hilary Putnam, eds.), Cambridge University Press, Cambridge, 2nd ed., 1983, pp. 183–201.
66. David Hilbert and Wilhelm Ackermann, ***Grundzüge der theoretischen Logik***, [Die Grundlehren der mathematischen Wissenschaften 27], Julius Springer, Berlin, 1928 (6. Auflage, 1972).
67. Philip E. B. Jourdain, *The development of the theories of mathematical logic and the principles of mathematics*, ***The Quarterly Journal of Pure and Applied Mathematics***, vol. 43 (1912), 219–314.
68. Akihiro Kanamori, *The mathematical development of set theory from Cantor to Cohen*, ***The Bulletin of Symbolic Logic***, vol. 2 (1996), 1–71.
69. ______, *The empty set, the singleton, and the ordered pair*, ***The Bulletin of Symbolic Logic***, vol. 9 (2003), 273–298.
70. ______, *Zermelo and set theory*, ***The Bulletin of Symbolic Logic***, vol. 10 (2004), 487–553.
71. Richard Kaye, ***Models of Peano Arithmetic***, [Oxford Logic Guides 15], The Clarendon Press Oxford University Press, New York, 1991.

72. Stephen Cole Kleene, ***Introduction to Metamathematics***, [Bibliotheca Mathematica, A Series of Monographs on Pure and Applied Mathematics, Volume I], North-Holland, Amsterdam, 1959.
73. Alwin Korselt, *Über einen Beweis des Äquvialenzsatzes*, ***Mathematische Annalen***, vol. 70 (1911), 294–296.
74. Casimir Kuratowski, *Sur la notion de l'ordre dans la théorie des ensembles*, ***Fundamenta Mathematicae***, vol. 2 (1921), 161–171.
75. Azriel Lévy, *The independence of various definitions of finiteness*, ***Fundamenta Mathematicae***, vol. 46 (1958), 1–13.
76. Adolf Lindenbaum and Alfred Tarski, *Communication sur les recherches de la théorie des ensembles*, ***Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III***, vol. 19 (1926), 299–330.
77. Leopold Löwenheim, *Über Möglichkeiten im Relativkalkül*, ***Mathematische Annalen***, vol. 76 (1915), 447–470.
78. Paolo Mancosu, *Measuring the size of infinite collections of natural numbers: was Cantor's theory of infinite number inevitable?*, ***The Review of Symbolic Logic***, vol. 4 (2009), 612–646.
79. Elliott Mendelson, *The axiom of fundierung and the axiom of choice*, ***Archiv für mathematische Logik und Grundlagenforschung***, vol. 4 (1958), 67–70.
80. Dimitry Mirimanoff, *Remarques sur la théorie des ensembles et les antinomies cantoriennes. I.*, ***L'Enseignement Mathématique***, vol. 19 (1917), 209–217.
81. ______, *Remarques sur la théorie des ensembles et les antinomies cantoriennes. II.*, ***L'Enseignement Mathématique***, vol. 21 (1920), 29–52.
82. Andrzej Mostowski, ***Sentences undecidable in formalized arithmetic. An exposition of the theory of Kurt Gödel***, [Studies in logic and the foundations of mathematics], North-Holland, Amsterdam, 1952.
83. Aloys Müller, *Über Zahlen als Zeichen*, ***Mathematische Annalen***, vol. 90 (1923), 153–158.
84. John von Neumann, *Zur Einführung der transfiniten Zahlen*, ***Acta Litterarum ac Scientiarum Regiae Universitatis Hungaricae Francisco-Josephinae. Sectio Scientiarum Mathematicarum***, vol. 1 (1923), 199–208 (see [109] for a translation into English).
85. ______, *Eine Axiomatisierung der Mengenlehre*, ***Journal für die Reine und Angewandte Mathematik***, vol. 154 (1925), 219–240 (see [109] for a translation into English).
86. ______, *Die Axiomatisierung der Mengenlehre*, ***Mathematische Zeitschrift***, vol. 27 (1928), 669–752.
87. ______, *Über die Definition durch transfinite Induktion und verwandte Fragen der allgemeinen Mengenlehre*, ***Mathematische Annalen***, vol. 99 (1928), 373–391.
88. ______, *Über eine Widerspruchfreiheitsfrage in der axiomatischen Mengenlehre*, ***Journal für die Reine und Angewandte Mathematik***, vol. 160 (1929), 227–241.
89. Giuseppe Peano, ***Arithmetices principia, nova methoda exposita***, Fratres Bocca, Torino, 1889 (see [109] for a translation into English).
90. ______, *Super theorema de Cantor-Bernstein*, ***Rendiconti del Circolo Matematico di Palermo***, vol. 21 (1906), 360–366.

91. Charles S. Peirce, *On the algebra of logic*, ***American Journal of Mathematics***, vol. 7 (1885), 180–202.
92. Oskar Perron, ***Irrationalzahlen***, 2nd ed., Chelsea Publishing Company, New York, 1951.
93. Plato, ***Politeia***, Athens, Book I *written around* 390 B.C., Books II–X *written around* 375 B.C.
94. ———, ***Parmenides***, Athens, *written around* 370 B.C.
95. Hilary Putnam, *Nonstandard models and Kripke's proof of the Gödel theorem*, ***Notre Dame Journal of Formal Logic***, vol. 41 (2000), 53–58.
96. Bernhard Rang and Wolfgang Thomas, *Zermelo's discovery of the "Russell paradox"*, ***Historia Mathematica***, vol. 8 (1981), 15–22.
97. Bertrand Russell, *On finite and infinite cardinal numbers,* (Section III of Whitehead [112]), ***American Journal of Mathematics***, vol. 24 (1902), 378–383.
98. ———, *Mathematical logic as based on the theory of types*, ***American Journal of Mathematics***, vol. 30 (1908), 222–262 (also published in [109]).
99. ———, ***Introduction to Mathematical Philosophy***, 2nd ed., Georg Allen & Unwin, London, 1920 (see [100] for a translation into German).
100. ———, ***Einführung in die mathematische Philosophie***, [translated into German by E. J. Gumbel and W. Gordon], Drei Masken Verlag, München, 1923.
101. ———, ***The Principles of Mathematics***, 2nd ed., Georg Allen & Unwin, London, 1937.
102. Arthur M. Schoenflies, *Die Entwickelung der Lehre von den Punktmannigfaltigkeiten*, ***Jahresbericht der Deutschen Mathematiker-Vereinigung***, vol. 8_2 (1900), 1–250.
103. Ernst Schröder, *Über zwei Definitionen der Endlichkeit und G. Cantor'sche Sätze*, ***Nova Acta, Abhandlungen der Kaiserlich Leopoldinisch-Carolinisch Deutschen Akademie der Naturforscher***, vol. 71 (1898), 301–362.
104. Thoralf Skolem, *Einige Bemerkungen zur axiomatischen Begründung der Mengenlehre*, Matematikerkongressen i Helsingfors den 4–7 Juli 1922, Den femte skandinaviska matematikerkongressen (Helsingfors), Akademiska Bokhandeln, 1923, pp. 217–232 (see [109] for a translation into English).
105. ———, ***Selected Works in Logic***, Universitetsforlaget, Oslo-Bergen-Tromsö, 1970.
106. Ladislav Spišiak and Peter Vojtáš, *Dependences between definitions of finiteness*, ***Czechoslovak Mathematical Journal***, vol. 38(113) (1988), 389–397.
107. Fabian Stedman, ***Campanalogia: or the Art of Ringing Improved***, W. Godbid, London, 1677 [reprint: Christopher Groome 1990].
108. Alfred Tarski, *Sur les principes de l'arithmétique des nombres ordinaux (transfinis)*, ***Annales de la Société Polonaise de Mathématique***, vol. 3 (1925), 148–149.
109. Jean van Heijenoort, ***From Frege to Gödel. A Source Book in Mathematical Logic, 1879–1931***, [Source Books in the History of Science], Harvard University Press, Cambridge, Massachusetts, 1967.
110. Jan von Plato, *In the shadows of the Löwenheim-Skolem theorem: Early combinatorial analyses of mathematical proofs*, ***The Bulletin of Symbolic Logic***, vol. 13 (2007), 189–225.

111. Hao Wang, *The axiomatization of arithmetic*, ***The Journal of Symbolic Logic***, vol. 22 (1957), 145–158.
112. Alfred North Whitehead, *On cardinal numbers*, ***American Journal of Mathematics***, vol. 24 (1902), 367–394.
113. Alfred North Whitehead and Bertrand Russell, ***Principia Mathematica, Vol. I–III***, Cambridge University Press, Cambridge, 1910–1913.
114. Ernst Zermelo, *Bericht an die Notgemeinschaft der Deutschen Wissenschaft über meine Forschungen betreffend die Grundlagen der Mathematik*, typescript, 5 pp., with appendices, 2 pp., dated 3 December 1930, Universitätsarchiv Freiburg, *Zermelo Nachlass, part of C 129/140* (see [117] for a translation into English).
115. ______, *Neuer Beweis für die Möglichkeit einer Wohlordnung*, ***Mathematische Annalen***, vol. 65 (1908), 107–128 (see [109, 117] for a translation into English).
116. ______, *Über Grenzzahlen und Mengenbereiche. Neue Untersuchungen über die Grundlagen der Mengelehre*, ***Fundamenta Mathematicae***, vol. 16 (1930), 29–47 (see [117] for a translation into English).
117. ______, ***Collected Works / Gesammelte Werke***, *Volume I: Set Theory, Miscellanea / Band I: Mengenlehre, Varia*, [Schriften der Mathematisch-naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften, Nr. 21 (2010)], edited by Heinz-Dieter Ebbinghaus, Craig G. Fraser, and Akihiro Kanamori, Springer-Verlag, Berlin · Heidelberg, 2010.
118. ______, *Untersuchungen über die Grundlagen der Mengenlehre. I.*, ***Mathematische Annalen***, vol. 65 (1908), 261–281 (see [109, 117] for a translation into English).

4

Cardinal Relations in ZF only

To some it may appear novel that I include the fourth among the consonances, because practicing musicians have until now relegated it to the dissonances. Hence I must emphasise that the fourth is actually not a dissonance but a consonance.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

In the previous chapter we introduced *cardinal numbers* as certain sets, which contain only sets of the same cardinality. Cardinal numbers in Zermelo-Fraenkel Set Theory are traditionally denoted by Fraktur letters like $\mathfrak{m}$ and $\mathfrak{n}$. However, the *cardinality* of a given set A is denoted by $|A|$. If $|A| = \mathfrak{m}$, then we say that A is of cardinality $\mathfrak{m}$. Recall that for cardinals $\mathfrak{m} = |A|$, $2^{\mathfrak{m}} := |\mathscr{P}(A)|$, in particular $2^{\aleph_0} = |\mathscr{P}(\omega)|$.

Recall that a set A is finite if there exists a bijection between A and a natural number $n \in \omega$. Now, a cardinal number $\mathfrak{m}$ is **finite** if $\mathfrak{m}$ contains a finite set — recall that $|\emptyset| = \{\emptyset\}$. Finite cardinal numbers are usually denoted like elements of ω, *i.e.*, by letters like n, m, k *et cetera*. In other words, for $n \in \omega$ we usually do not distinguish between the *ordinal number* n and the *cardinal number* n. Finally, a cardinal number is **infinite** if it is not finite. Recall that an infinite cardinal which contains a well-orderable set is called an *aleph* and that alephs are denoted by $\aleph$'s, *e.g.*, $\aleph_0 := |\omega|$. A cardinal $\mathfrak{m}$ is called **transfinite** or **Dedekind-infinite** if $\aleph_0 \leq \mathfrak{m}$. Notice that transfinite cardinals are always infinite. If the cardinality of a set A is transfinite, then A is called **transfinite**. Notice that for each transfinite set A there is an injection from ω into A. Sets or cardinals which are not transfinite are called **D-finite** or **Dedekind-finite**. Notice that every finite set is D-finite, but as we will see later, D-finite sets are not necessarily finite. For other notions of finiteness see RELATED RESULT 13.

Basic Cardinal Relations

Below we show some relations between cardinals which can be proved in ZF. We start with some simple facts.

FACT 4.1. $\aleph_0 = |\mathbb{P}| = |\mathbb{Z}| = |\mathbb{Z}^2| = |\mathbb{Q}|$, *where* $\mathbb{P}$ *denotes the set of prime numbers,* $\mathbb{Z}$ *denotes the set of integers, and* $\mathbb{Q}$ *denotes the set of rational numbers.*

Proof. By definition we have $\aleph_0 = |\omega|$. Further, $|\mathbb{P}| \leq |\omega| \leq |\mathbb{Z}| \leq |Q|$, and since every reduced rational number $\frac{p}{q}$ corresponds to an ordered pair $\langle p, q\rangle$ of integers we also have $|\mathbb{Q}| \leq |\mathbb{Z}^2|$. Thus, by the CANTOR-BERNSTEIN THEOREM 3.17 it is enough to show that the set $\mathbb{P}$ is transfinite and to find an injection from $\mathbb{Z}^2$ into ω. That $\mathbb{P}$ is transfinite follows from the fact that $\mathbb{P}$ is an infinite, well-orderable set; and to construct an injection $f : \mathbb{Z}^2 \hookrightarrow \omega$ we define for example first $g : \mathbb{P} \times \mathbb{Z} \to \omega$ by stipulating $g(p, z) := \max\{1, p^z\}$ and then let $f\big(\langle x, y\rangle\big) := g(2, x) \cdot g(3, -x) \cdot g(5, y) \cdot g(7, -y)$. ⊣

For an arbitrary set A let $\operatorname{fin}(A)$ denote the set of all finite subsets of A. Notice that $\operatorname{fin}(A) = \mathscr{P}(A)$ if and only if A is finite. Further, recall that $\operatorname{seq}(A)$ denotes the set of all finite sequences which can be formed with elements of A and that $\operatorname{seq}^{1\text{-}1}(A)$ be those sequences of $\operatorname{seq}(A)$ in which no element appears twice. Further, recall that $[A]^2$ is the set of all 2-element subsets of A.

FACT 4.2. $\aleph_0 = |[\omega]^2| = |\operatorname{fin}(\omega)| = |\operatorname{seq}^{1\text{-}1}(\omega)| = |\operatorname{seq}(\omega)| = |\mathbb{A}|$, *where* $\mathbb{A}$ *denotes the set of algebraic numbers, which is the set of all real numbers which are roots of polynomials with integer coefficients.*

Proof. Since every finite subset of ω corresponds to a strictly increasing finite sequence of elements of ω we obviously have $\aleph_0 \leq |[\omega]^2| \leq |\operatorname{fin}(\omega)| \leq |\operatorname{seq}^{1\text{-}1}(\omega)| \leq |\operatorname{seq}(\omega)|$. By the CANTOR-BERNSTEIN THEOREM 3.17, in order to prove that $|\operatorname{seq}(\omega)| = \aleph_0$ it is enough to find an injection from $\operatorname{seq}(\omega)$ into ω. Let $\mathbb{P} = \{p_i : i \in \omega\}$ be such that for all $i, j \in \omega$, $i < j \to p_i < p_j$, and define $f : \operatorname{seq}(\omega) \to \omega$ by stipulating

$$f\big(\langle a_0, a_1, \ldots, a_n\rangle\big) := p_0^{a_0+1} \cdot p_1^{a_1+1} \cdot \ldots \cdot p_n^{a_n+1}.$$

Then, by unique factorisation of integers, f is injective. Now, let us consider the set $\mathbb{A}$: A polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$ with integer coefficients has at most n different real roots say $r_0 < r_1 < \ldots r_k$ where $k < n$, and since there exists a bijection g between $\mathbb{Z}$ and ω (by FACT 4.1), we can define a mapping $h_{p(x)}$ which assigns to each root r_i of $p(x)$ an element of $\operatorname{seq}(\omega)$ by stipulating

$$h_{p(x)}(r_i) = \big\langle g(a_0), \ldots, g(a_n), i\big\rangle,$$

and define $H : \mathbb{A} \to \omega$ by stipulating

$$H(r) = \min\big\{h_{p(x)}(r_i) : p(r) = 0 \wedge r = r_i\big\}.$$

This shows that $|\mathbb{A}| \leq \aleph_0$ and completes the proof. ⊣

By PROPOSITION 3.18 we know that $|\mathbb{R}| = 2^{\aleph_0}$ and by CANTOR'S THEOREM 3.25 we get that $\aleph_0 < 2^{\aleph_0}$, hence, the set of reals is uncountable (*cf.* PROPOSITION 3.24). The following result gives a few examples of sets of the same cardinality as $\mathbb{R}$.

FACT 4.3. $\big|[0,\varepsilon]\big| = \big|\mathbb{R}\big| = \big|{}^{\omega}2\big| = \big|{}^{\omega}\omega\big| = \big|\mathbb{R}\times\mathbb{R}\big| = \big|{}^{\omega}\mathbb{R}\big| = \big|C[0,1]\big| = \big|\mathbb{R}\setminus\mathbb{A}\big|$, *where for* $\varepsilon > 0$, $[0,\varepsilon] = \{r \in \mathbb{R} : 0 \leq r \leq \varepsilon\}$, *and* $C[0,1]$ *denotes the set of continuous functions from* $[0,1]$ *to* $\mathbb{R}$.

Proof. The function $\varepsilon \cdot \big(\arctan(x) + \frac{\pi}{2}\big)/\pi$ is a bijection between $\mathbb{R}$ and the open interval $(0,\varepsilon)$, thus, by the CANTOR-BERNSTEIN THEOREM 3.17 we get $\big|[0,\varepsilon]\big| = \big|\mathbb{R}\big|$.

Since the function $h : {}^{\omega}2 \to \mathscr{P}(\omega)$ defined by stipulating $h(f) := \big\{n \in \omega : f(n) = 1\big\}$ is bijective, and since $|\mathbb{R}| = |\mathscr{P}(\omega)|$, we get $|\mathbb{R}| = |{}^{\omega}2|$.

Recall that there is a bijection $g : \omega \times \omega \to \omega$, *e.g.*, let $g\big(\langle n,m\rangle\big) := m + \frac{1}{2}(n+m)(n+m+1)$. In order to show that $|{}^{\omega}\mathbb{R}| = |\mathbb{R}|$ it is enough to show that there is a bijection between ${}^{\omega}\mathscr{P}(\omega)$ and $\mathscr{P}(\omega)$. Now, there is a one-to-one correspondence between functions $h \in {}^{\omega}\mathscr{P}(\omega)$ and sets $X \in \mathscr{P}(\omega \times \omega)$ by $\langle a,b\rangle \in X \iff b \in h(a)$. Thus, the function

$$\begin{array}{ccc} \mathscr{P}(\omega \times \omega) & \longrightarrow & \mathscr{P}(\omega) \\ X & \longmapsto & g[X] \end{array}$$

induces an bijection between ${}^{\omega}\mathscr{P}(\omega)$ and $\mathscr{P}(\omega)$, hence, $|{}^{\omega}\mathbb{R}|$ and $|\mathbb{R}|$, and since $|\mathbb{R}| \leq |\mathbb{R} \times \mathbb{R}| \leq |{}^{\omega}\mathbb{R}|$ and $|\mathbb{R}| = |{}^{\omega}2| \leq |{}^{\omega}\omega| \leq |{}^{\omega}\mathbb{R}|$, we finally get $|\mathbb{R}| = |{}^{\omega}2| = |{}^{\omega}\omega| = |\mathbb{R} \times \mathbb{R}| = |{}^{\omega}\mathbb{R}|$.

To see that $\big|\mathbb{R}\big| = \big|C[0,1]\big|$, notice first that a continuous function from $[0,1]$ to $\mathbb{R}$ is defined by its values on $\mathbb{Q} \cap [0,1]$. By FACT 4.1 there is a bijection between $\mathbb{Q} \cap [0,1]$ and ω, and consequently there is a one-to-one correspondence between functions in $C[0,1]$ and some functions in ${}^{\omega}\mathbb{R}$ which shows that $\big|C[0,1]\big| \leq \big|{}^{\omega}\mathbb{R}\big|$. Since $|{}^{\omega}\mathbb{R}| = |\mathbb{R}|$ and since we obviously have $\big|\mathbb{R}\big| \leq \big|C[0,1]\big|$, by the CANTOR-BERNSTEIN THEOREM 3.17 we finally get $\big|C[0,1]\big| = \big|\mathbb{R}\big|$.

By FACT 4.2, $|\mathbb{A}| = \aleph_0$ and we leave it as an exercise to the reader to show that $|\mathbb{R} \setminus A| = |\mathbb{R}|$ for all countable sets $A \subseteq \mathbb{R}$. At this point we would like to mention that the reals $\mathbb{R} \setminus \mathbb{A}$ are called transcendental numbers; thus, all but countably many reals are transcendental. ⊣

Let us now turn our attention to arbitrary cardinalities and let us prove that whenever we can embed ω into $\mathscr{P}(A)$. Then we can also embed $\mathbb{R}$ into $\mathscr{P}(A)$.

PROPOSITION 4.4. *If* $\aleph_0 \leq 2^{\mathfrak{m}}$, *then* $2^{\aleph_0} \leq 2^{\mathfrak{m}}$.

Proof. Let A be an arbitrary set of cardinality $\mathfrak{m}$. Because $\aleph_0 \leq 2^{\mathfrak{m}}$ there is an injection $f_0 : \omega \hookrightarrow \mathscr{P}(A)$. Define an equivalence relation on A by stipulating

$$x \sim y \iff \forall n \in \omega \, \big(x \in f_0(n) \leftrightarrow y \in f_0(n)\big) \,,$$

and let $[x]^{\sim} := \{y \in A : y \sim x\}$. For $x \in A$ let $g_x := \{n \in \omega : x \in f_0(n)\}$. Then for every $x \in A$ we have $g_x \subseteq \omega$ and $g_x = g_y$ *iff* $[x]^{\sim} = [y]^{\sim}$. We can consider the set g_x as a function from ω to $\{0, 1\}$ by $g_x(n) = 0$ if $x \in f_0(n)$ and $g_x(n) = 1$ if $x \notin f_0(n)$. Now we define an ordering "$\prec$" on the set $\{g_x : x \in A\}$ by stipulating

$$g_x \prec g_y \iff \exists n \in \omega \Big(g_x(n) < g_y(n) \wedge \forall k \in n \big(g_x(k) = g_y(k) \big) \Big) .$$

Notice that for all $x, y \in A$ such that $g_x \neq g_y$ we have either $g_x \prec g_y$ or $g_y \prec g_x$. Let $P_n^0 := \{g_x : g_x(n) = 0\}$. Then for each $n \in \omega$, $P_n^0 \subseteq {}^{\omega}2$. Obviously, the relation "$\prec$" defines an ordering on each P_n^0. We consider the following two cases:

If for each $n \in \omega$, P_n^0 is well-ordered by "$\prec$", then we can easily well-order the infinite set $\bigcup_{n\in\omega} P_n^0$ and construct a countably infinite set $\{g_{x_i} : i \in \omega\}$ such that for all distinct $i, j \in \omega$, $g_{x_i} \neq g_{x_j}$. If we define $q_i = \{x \in A : g_x = g_{x_i}\}$, then the set $Q := \{q_i : i \in \omega\}$ is a countable infinite set of pairwise disjoint subsets of A.

If not every P_n^0 is well-ordered by "$\prec$", there exists a least $m \in \omega$ such that P_m^0 is not well-ordered by "$\prec$" and we can define

$$S_0 = \bigcup \big\{ S \subseteq P_m^0 : S \text{ has no } \prec\text{-minimal element} \big\} .$$

By definition of $S_0 \subseteq P_m^0$, S_0 has no $\prec$-minimal element, too. For $k \in \omega$ we define S_{k+1} as follows: If $S_k \cap P_{m+k+1}^0 = \emptyset$, then $S_{k+1} := S_k$; otherwise, $S_{k+1} := S_k \cap P_{m+k+1}^0$. By construction, for every $k \in \omega$, $S_k \neq \emptyset$ and S_k is not well-ordered by "$\prec$". This implies that for every $k \in \omega$ there exists an $l > k$ such that S_l is a proper subset of S_k. Now let $S_{k_0}, S_{k_1}, \dots$ be such that for all $i < j$ we have $S_{k_i} \setminus S_{k_j} \neq \emptyset$ and let $q_i := \big\{x \in A : g_x \in (S_{k_i} \setminus S_{k_{i+1}}\big\}$. Then the set $Q := \{q_i : i \in \omega\}$ is again a countable infinite set of pairwise disjoint subsets of A.

Thus, in both cases the cardinality of $\mathscr{P}(Q)$ is $2^{\aleph_0}$, and since the function

$$\begin{aligned} \mathscr{P}(Q) &\longrightarrow \mathscr{P}(A) \\ X \ &\longmapsto \bigcup X \end{aligned}$$

is injective we finally have $2^{\aleph_0} \leq 2^{\mathfrak{m}}$. ⊣

It is now time to define addition and multiplication of cardinals. Let $\mathfrak{m}$ and $\mathfrak{n}$ be cardinals and let A and B be disjoint sets of cardinality $\mathfrak{m}$ and $\mathfrak{n}$ respectively. Then we define the sum and product of $\mathfrak{m}$ and $\mathfrak{n}$ as follows:

$$\begin{aligned} \mathfrak{m} + \mathfrak{n} &= |A \,\dot\cup\, B| \\ \mathfrak{m} \cdot \mathfrak{n} &= |A \times B| \end{aligned}$$

Furthermore, let $2\mathfrak{m} := \mathfrak{m} + \mathfrak{m}$ and $\mathfrak{m}^2 := \mathfrak{m} \cdot \mathfrak{m}$. We leave it as an exercise to the reader to show that for any cardinals $\mathfrak{m}$, $\mathfrak{n}$ and $\mathfrak{p}$ we have for example:

$$\mathfrak{m} + \mathfrak{n} = \mathfrak{n} + \mathfrak{m}\,, \quad \mathfrak{m} \cdot \mathfrak{n} = \mathfrak{n} \cdot \mathfrak{m}$$

$$\mathfrak{m} \leq \mathfrak{n} \to \mathfrak{p} + \mathfrak{m} \leq \mathfrak{p} + \mathfrak{n}\,, \quad \mathfrak{m} \leq \mathfrak{n} \to \mathfrak{p} \cdot \mathfrak{m} \leq \mathfrak{p} \cdot \mathfrak{n}$$

$$2^{\mathfrak{m}+\mathfrak{n}} = 2^{\mathfrak{m}} \cdot 2^{\mathfrak{n}}\,, \quad 2^{\mathfrak{m}\cdot\mathfrak{n}} = \left(2^{\mathfrak{m}}\right)^{\mathfrak{n}}$$

For example to show that $2^{\mathfrak{m}+\mathfrak{n}} = 2^{\mathfrak{m}} \cdot 2^{\mathfrak{n}}$, define $f : \mathscr{P}(A \dot{\cup} B) \to \mathscr{P}(A) \times \mathscr{P}(B)$ by stipulating $f(S) := \langle S \cap A, S \cap B \rangle$.

The following fact is just an easy consequence of the definition of ordered pairs.

FACT 4.5. *For any cardinal* $\mathfrak{m}$, $\mathfrak{m}^2 \leq 2^{2^{\mathfrak{m}}}$.

Proof. Let A be a set of cardinality $\mathfrak{m}$. Any $\langle a, b \rangle \in A \times A$ can be written in the form $\{a, \{a, b\}\}$, which is obviously an element of $\mathscr{P}\big(\mathscr{P}(A)\big)$. ⊣

Let $\mathfrak{m}$ be a cardinal and let A be a set of cardinality $\mathfrak{m}$. Then we define $\operatorname{fin}(\mathfrak{m}) := |\operatorname{fin}(A)|$ and $[\mathfrak{m}]^2 := |[A]^2|$. Notice that for all cardinals $\mathfrak{m} > 2$ we have $\mathfrak{m} \leq [\mathfrak{m}]^2 \leq \operatorname{fin}(\mathfrak{m})$. We leave it as an exercise to the reader to show that $\aleph_0 \leq \mathfrak{m}^2 \to \aleph_0 \leq \mathfrak{m}$; however, $\aleph_0 \leq [\mathfrak{m}]^2 \to \aleph_0 \leq \mathfrak{m}$ is *not* provable in ZF (see THEOREM 7.6.(b)).

As mentioned above, an infinite set can be D-finite and moreover, even the power set of an infinite set can be D-finite. However, for every infinite cardinal $\mathfrak{m}$, $2^{\operatorname{fin}(\mathfrak{m})}$ is transfinite (notice that $2^{\operatorname{fin}(\mathfrak{m})} \leq 2^{2^{\mathfrak{m}}}$).

FACT 4.6. *If* $\mathfrak{m}$ *is an infinite cardinal, then* $2^{\aleph_0} \leq 2^{\operatorname{fin}(\mathfrak{m})}$, *in particular* $2^{\operatorname{fin}(\mathfrak{m})}$ *is transfinite.*

Proof. Let A be an arbitrary infinite set of cardinality $\mathfrak{m}$. For every $n \in \omega$ let $X_n := \{x \subseteq A : |x| = n\}$. Then for any $n \in \omega$, $X_n \in \mathscr{P}\big(\operatorname{fin}(A)\big)$. For any two distinct integers $n, m \in \omega$ we get $X_n \neq X_m$. This shows that $\aleph_0 \leq 2^{\operatorname{fin}(\mathfrak{m})}$, and hence, by PROPOSITION 4.4, $2^{\aleph_0} \leq 2^{\operatorname{fin}(\mathfrak{m})}$. ⊣

The following result is an immediate consequence of FACT 4.6 (see THEOREM 4.28 for a stronger result).

FACT 4.7. *If* $\mathfrak{m}$ *is an infinite cardinal, then* $2^{2^{2^{\mathfrak{m}}}} + 2^{2^{2^{\mathfrak{m}}}} = 2^{2^{2^{\mathfrak{m}}}}$.

Proof. Notice that

$$2^{2^{2^{\mathfrak{m}}}} + 2^{2^{2^{\mathfrak{m}}}} = 2 \cdot 2^{2^{2^{\mathfrak{m}}}} = 2^{(2^{2^{\mathfrak{m}}}+1)},$$

and since $2^{2^{\mathfrak{m}}}$ is transfinite, $2^{2^{\mathfrak{m}}} + 1 = 2^{2^{\mathfrak{m}}}$.

For arbitrary sets A and B we write $|A| \leq^* |B|$ if either $A = \emptyset$ or there is a surjection from B onto A. Similarly we write $\mathfrak{m} \leq^* \mathfrak{n}$ if there are sets $A \in \mathfrak{m}$ and $B \in \mathfrak{n}$ such that $|A| \leq^* |B|$. Notice that cardinal relation "$\leq$" is reflexive and transitive, and that $\mathfrak{m} \leq \mathfrak{n} \rightarrow \mathfrak{m} \leq^* \mathfrak{n}$. We leave it as an exercise to the reader to show that for all cardinals $\mathfrak{m}$, $[\mathfrak{m}]^2 \leq^* \mathfrak{m}^2$ (compare this result with PROPOSITION 7.18). However, in ZF, $|A| \leq^* |B|$ and $|B| \leq^* |A|$ does not imply $|A| = |B|$ (see Chapter 7 for counterexamples). On the other hand, we have the following

FACT 4.8. *If* $\mathfrak{m} \leq^* \mathfrak{n}$, *then* $2^{\mathfrak{m}} \leq 2^{\mathfrak{n}}$. *Moreover, if* $\mathfrak{m} \leq^* \aleph$, *then* $\mathfrak{m} \leq \aleph$.

Proof. Let the sets A and B be of cardinality $\mathfrak{m}$ and $\mathfrak{n}$ respectively. Since $\mathfrak{m} \leq^* \mathfrak{n}$ there is a surjection $g : B \twoheadrightarrow A$. Let $f : \mathscr{P}(A) \rightarrow \mathscr{P}(B)$ by stipulating $f(X) := \{y \in B : g(y) \in X\}$. Then f is injective which shows that $|\mathscr{P}(A)| \leq |\mathscr{P}(B)|$.

Now, let S be a set of cardinality $\aleph$ and let $R_S \subseteq S \times S$ be a well-ordering of S. Further, let $g : S \twoheadrightarrow A$ (where $|A| = \mathfrak{m}$) be a surjection. Then $f : A \rightarrow S$, where $f(a)$ is the R_S-minimal element of $\{s \in S : g(s) = a\}$ is obviously an injection. ⊣

Recall that by HARTOGS' THEOREM 3.27, for any cardinal $\mathfrak{m}$ there is a smallest $\aleph$, denoted $\aleph(\mathfrak{m})$, such that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$.

FACT 4.9. *If* $\mathfrak{m}$ *is an infinite cardinal, then* $\aleph(\mathfrak{m}) \leq^* 2^{\mathfrak{m}^2}$.

Proof. Let A be a set of cardinality $\mathfrak{m}$. Any binary relation R on A corresponds to a subset X_R of $A \times A$ by stipulating $\langle a_0, a_1 \rangle \in X_R \iff R(a_0, a_1)$. Thus, we get that the cardinality of the set of binary relations on A is less than or equal to $2^{\mathfrak{m}^2}$. Further, let S be a well-orderable set of cardinality $\aleph(\mathfrak{m})$, let R be a well-ordering of S, and let $\alpha = \text{o.t.}(R)$ be the order type of R. Then $|\alpha| = |S| = \alpha(\mathfrak{m})$. Define $f : \mathscr{P}(A \times A) \rightarrow \alpha$ by stipulating

$$f(X) = \begin{cases} \emptyset & \text{if } X \text{ is not a well-ordering of a subset of } A, \\ \text{o.t.}(X) & \text{otherwise.} \end{cases}$$

By the proof of HARTOGS' THEOREM 3.27, for every $\beta \in \alpha$ there is a well-ordering R of a subset of A such that $\text{o.t.}(R) = \beta$, hence, f is surjective. ⊣

In the proof of CANTOR'S THEOREM 3.25 it is in fact shown that for all cardinals $\mathfrak{m}$, $2^{\mathfrak{m}} \not\leq^* \mathfrak{m}$. On the other hand, we obviously have $2^{\mathfrak{m}} \leq^* \mathfrak{m}^2$ in the case when $\mathfrak{m} \leq 4$; however, it is not known whether $2^{\mathfrak{m}} \leq^* \mathfrak{m}^2 \rightarrow \mathfrak{m} \leq 4$ is provable in ZF (see RELATED RESULT 21).

The situation is different when we replace "$\leq^*$" by "$\leq$". By CANTOR'S THEOREM 3.25 we know that $\mathfrak{m} < 2^{\mathfrak{m}}$, thus, $2^{\mathfrak{m}} \not\leq \mathfrak{m}$. Moreover, $2^{\mathfrak{m}} \leq \mathfrak{m}^2 \rightarrow \mathfrak{m} \leq 4$ (see THEOREM 4.20), but we have to postpone the proof until we can compute the cardinality of products of infinite ordinal numbers. However, let us first investigate the cardinality of the *continuum* $\mathbb{R}$.

On the Cardinals $2^{\aleph_0}$ and $\aleph_1$

By HARTOGS' THEOREM 3.27 we know that for any cardinal $\mathfrak{m}$ (*e.g.*, $\mathfrak{m} = \aleph_0$) there is a smallest $\aleph$, denoted $\aleph(\mathfrak{m})$, such that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$. Now let $\aleph_1 := \aleph(\aleph_0)$. Then $\aleph_1$ contains an uncountable well-orderable set, say A, such that every subset of A of cardinality strictly less than A is countable. Let α be the order type of a well-ordering of A. Then, since $|\alpha| = \aleph_1$, α is an uncountable ordinal. Now, if $\alpha \setminus \{\beta \in \alpha : |\beta| = \aleph_0\} = \emptyset$, then α is the least uncountable ordinal which is usually denoted ω_1. Otherwise, the non-empty set $\alpha \setminus \{\beta \in \alpha : |\beta| = \aleph_0\}$, as a set of ordinals, has an $\in$-minimal element, say γ. Then γ is the least uncountable ordinal, *i.e.*, $\gamma = \omega_1$. In particular we get $|\omega_1| = \aleph_1$, and for all $\beta \in \omega_1$ we have $|\beta| = \aleph_0$.

If $2^{\aleph_0}$ would be an aleph, then we would have $\aleph_1 \leq 2^{\aleph_0}$, (notice that $\aleph_0 < 2^{\aleph_0}$ and that $\aleph_0 < \aleph_1$). Now, the Continuum Hypothesis, denoted CH, states that $2^{\aleph_0} = \aleph_1$. In particular, if $2^{\aleph_0}$ is an aleph then CH is equivalent to saying that every subset of $\mathbb{R}$ is either countable or of cardinality $2^{\aleph_0}$.

In Chapter 16 we shall see that CH is independent of ZF, thus, neither ZF $\vdash$ CH nor ZF $\vdash \neg$CH. Below we investigate the relationship between the cardinals $2^{\aleph_0}$ and $\aleph_1$. In order to construct a surjection from $\mathbb{R}$ onto ω_1 — even though there might be no injection from ω_1 into $\mathbb{R}$ — we prove first the following result:

LEMMA 4.10. *For every ordinal $\alpha \in \omega_1$ there is a set of rationals $Q_\alpha \subseteq \mathbb{Q} \cap (0,1)$ and a bijection $h_\alpha : \alpha \to Q_\alpha$ such that for all $\beta, \beta' \in \alpha$, $\beta \in \beta' \iff h_\alpha(\beta) < h_\alpha(\beta')$.*

Proof. Let α be an arbitrary but fixed ordinal in ω_1. For $\alpha = 0$ let $Q_0 := \emptyset$ and we are done; and if $0 \neq \alpha \in \omega$ (*i.e.*, if α is finite), then for $n \in \alpha$ we define $h_\alpha(n) := 1 - 1/(n+2)$. If α is infinite we proceed as follows. Firstly let

$$\begin{aligned} \omega &\longrightarrow \alpha \\ n &\longmapsto \beta_n \end{aligned}$$

and

$$\begin{aligned} \omega &\longrightarrow \mathbb{Q} \cap (0,1) \\ n &\longmapsto \quad q_n \end{aligned}$$

be two bijections (notice that the sets α and $\mathbb{Q} \cap (0,1)$ are both countably infinite). Since $\{\beta_n : n \in \omega\} = \alpha$, it is enough to define $h_\alpha(\beta_n)$ for all $n \in \omega$ which is done by induction: $h_\alpha(\beta_0) := q_0$ and if $h_\alpha(\beta_k)$ is defined for all $k \in n$, then

$$h_\alpha(\beta_n) = q_{\mu(n)}$$

where

$$\mu(n) = \min\left\{m \in \omega : \forall k \in n \, (q_m \leq h_\alpha(\beta_k) \leftrightarrow \beta_n \in \beta_k)\right\}.$$

Further, let $Q_\alpha := h_\alpha[\alpha]$. Then by induction one can show that h_α and Q_α have the required properties (the details are left to the reader). ⊣

THEOREM 4.11. $\aleph_1 \leq^* 2^{\aleph_0}$.

Proof. It is enough to construct a surjection from the open interval $(0,1)$ onto ω_1. Firstly notice that every real $r \in (0,1)$ can be written uniquely as

$$r = \sum_{n\in\omega} r_n \cdot 2^{-(n+1)}$$

where for all $n \in \omega$, $r_n \in \{0,1\}$, and infinitely many r_n's are equal to 0. On the other hand, for every function $f \in {}^{\omega}2$ such that $\{n \in \omega : f(n) = 0\}$ is infinite there exists a unique real $r = \sum_{n\in\omega} f(n) \cdot 2^{-(n+1)}$ in $(0,1)$. Secondly, for $r \in (0,1)$ let $Q_r = \{q_n : r_{2n} = 1\}$ where the function which maps n to q_n is a bijection between ω and $\mathbb{Q} \cap (0,1)$. If Q_r is well-ordered by "$<$", then let $\eta(r)$ be the order type of $(Q_r, <)$; otherwise, let $\eta(r) = \emptyset$. Since the set of rational numbers is countable, η is a function from $(0,1)$ to ω_1. Moreover, the function η is even surjective. Indeed, by LEMMA 4.10 we know that for any $\alpha \in \omega_1$ there is a set of rational numbers $Q_\alpha \subseteq \mathbb{Q} \cap (0,1)$ such that the order type of $(Q_\alpha, <)$ is equal to α. Thus, for

$$r = \sum_{n\in N(Q_\alpha)} 2^{-(2n+1)} \quad \text{where } N(Q_\alpha) = \{k \in \omega : q_k \in Q_\alpha\}$$

we have $r \in (0,1)$ and $\eta(r) = \alpha$, and since $\alpha \in \omega_1$ was arbitrary this shows that η is surjective. ⊣

In contrast to THEOREM 4.11 the existence of an injection from ω_1 into $\mathbb{R}$ is not provable in ZF, *i.e.*, $\aleph_1 \nleq 2^{\aleph_0}$ is consistent with ZF. For example there is no such injection in the case when the reals can be written as a countable union of countable sets (for the consistency of this statement with ZF see Chapter 17).

PROPOSITION 4.12. *If the set of real numbers is a countable union of countable sets, then* $\aleph_1 \nleq 2^{\aleph_0}$.

Proof. By FACT 4.3, $|\mathbb{R}| = |{}^{\omega}\mathbb{R}|$. Thus, if $\mathbb{R}$ is a countable union of countable sets, then we also have ${}^{\omega}\mathbb{R} = \bigcup_{n\in\omega} F_n$ where each F_n is countable. The proof is by contraposition: Under the assumption that there is an injection $j : \omega_1 \hookrightarrow \mathbb{R}$ we show that ${}^{\omega}\mathbb{R} \neq \bigcup_{n\in\omega} F_n$. Consider the function

$$\begin{aligned} G : \omega &\longrightarrow \mathscr{P}(\mathbb{R}) \\ n &\longmapsto \big\{r \in \mathbb{R} : \exists f \in F_n \, \exists k \in \omega \, \big(f(k) = r\big)\big\}. \end{aligned}$$

For each $n \in \omega$ we have $|G(n)| \leq \aleph_0$ and we can define $h : \omega \to \mathbb{R}$ by stipulating

$$h(n) := j(\alpha_n) \quad \text{where } \alpha_n = \min\big\{\beta \in \omega_1 : j(\beta) \notin G(n)\big\}.$$

By definition $h \in {}^{\omega}\mathbb{R}$, but on the other hand, h does not belong to any set F_n (for $n \in \omega$); since otherwise we would have $h(n) \in G(n)$ which contradicts the definition of $h(n)$. Thus, $h \notin \bigcup_{n\in\omega} F_n$ which shows that ${}^{\omega}\mathbb{R}$ — and consequently $\mathbb{R}$ — cannot be covered by countably many countable sets. $\dashv$

As a consequence of PROPOSITION 4.12 one can show that if $\mathbb{R}$ is a countable union of countable sets, then $\mathbb{R}$ can be partitioned into strictly more parts than real numbers exist, where a **partition** of $\mathbb{R}$ is a set $\mathscr{R} \subseteq \mathscr{P}(\mathbb{R})$ such that $\bigcup \mathscr{R} = \mathbb{R}$ and for any distinct $x, y \in \mathscr{R}$, $x \cap y = \emptyset$.

COROLLARY 4.13. *If the set of real numbers is a countable union of countable sets, then there exists a partition $\mathscr{R}$ of $\mathbb{R}$ such that $|\mathscr{R}| > |\mathbb{R}|$.*

Proof. By FACT 4.3 and the CANTOR-BERNSTEIN THEOREM 3.17 there exists a bijection between $\mathbb{R} \setminus (0,1)$ and $\mathbb{R}$, and by THEOREM 4.11 there exists a surjection from $(0,1)$ onto ω_1. Thus, there is a surjection $f : \mathbb{R} \twoheadrightarrow \mathbb{R}\dot{\cup}\omega_1$ and with f we can define an equivalence relation "$\sim$" on $\mathbb{R}$ by stipulating $x \sim y \iff f(x) = f(y)$. Let $\mathscr{R} = \{[x]^{\tilde{}} : x \in \mathbb{R}\}$. Then $\mathscr{R}$ is a partition of $\mathbb{R}$ and we have $|\mathscr{R}| = \aleph_1 + 2^{\aleph_0}$. By PROPOSITION 4.12, $\aleph_1 \not\leq 2^{\aleph_0}$ and consequently $\aleph_1 + 2^{\aleph_0} \not\leq 2^{\aleph_0}$, and since $2^{\aleph_0} \leq \aleph_1 + 2^{\aleph_0}$ we have $2^{\aleph_0} < \aleph_1 + 2^{\aleph_0}$, in particular, $|\mathbb{R}| < |\mathscr{R}|$. $\dashv$

Ordinal Numbers revisited

In the previous chapter we have defined addition, multiplication, and exponentiation of ordinal numbers. Using these arithmetical operations we can show that every ordinal number can be uniquely represented in a standardised form, but first let us introduce some terminology: For ordinals $\alpha, \beta \in \Omega$ we will write $\beta < \alpha$ instead of $\beta \in \alpha$ and consequently we define $\beta \leq \alpha \iff \beta \in \alpha \vee \beta = \alpha$. Further notice that if $\beta \leq \alpha$, then there is a unique ordinal, denoted $\alpha - \beta$, such that $\beta + (\alpha - \beta) = \alpha$.

LEMMA 4.14. *For every ordinal $\alpha > 0$ there exists a unique ordinal α_0 such that $\omega^{\alpha_0} \leq \alpha$ and $\omega^{\alpha_0+1} > \alpha$.*

Proof. Firstly notice that by the rules of ordinal exponentiation, for $\gamma < \gamma'$ we have $\omega^{\gamma} < \omega^{\gamma} \cdot \omega \leq \omega^{\gamma} \cdot \omega^{\gamma'-\gamma} = \omega^{\gamma'}$. In particular, for any ordinal α_0 we have $\omega^{\alpha_0} < \omega^{\alpha_0+1}$. Secondly notice that for all ordinals α we have $\omega^{\alpha} \geq \alpha$, hence, $\omega^{\alpha+1} > \omega^{\alpha} \geq \alpha$. Now, since $\alpha+1$ is well-ordered by "$<$" and $\omega^{\alpha+1} > \alpha \geq \omega^0$, there is a unique least ordinal $\beta \leq \alpha+1$ such that $\omega^{\beta} > \alpha$. It remains to show that β is a successor ordinal, *i.e.*, $\beta = \alpha_0 + 1$ for some α_0. Indeed, if β would be a limit ordinal, then $\omega^{\beta} = \bigcup_{\gamma\in\beta} \omega^{\gamma}$, and by definition of β we would have $\omega^{\gamma} \leq \alpha$ (for all $\gamma \in \beta$). Since $\omega^{\gamma+1} > \omega^{\gamma}$ and since β is a limit ordinal, this would imply that $\omega^{\gamma} \in \alpha$ whenever $\gamma \in \beta$ and consequently $\omega^{\beta} \leq \alpha$, whereas $\omega^{\beta} > \alpha$, a contradiction. $\dashv$

LEMMA 4.15. *Let $\alpha \geq \omega$ be an infinite ordinal. Then there exist a positive integer k_0 and ordinals α' and α_0 where $\alpha' < \omega^{\alpha_0}$ such that $\alpha = \omega^{\alpha_0} \cdot k_0 + \alpha'$. Moreover, the ordinals k_0, α_0, and α' are uniquely determined by α.*

Proof. Let α_0 be as in LEMMA 4.14. Then $\omega^{\alpha_0} \leq \alpha$ and $\omega^{\alpha_0+1} > \alpha$. By a similar argument as in the proof of LEMMA 4.14, this implies that there are positive integers k such that $\omega^{\alpha_0} \cdot k > \alpha$. Let k_0 be the least integer such that $\omega^{\alpha_0} \cdot (k_0 + 1) > \alpha$; then $1 \leq k_0 < \omega$ (notice that $\omega^{\alpha_0} = \omega^{\alpha_0} \cdot 1 \leq \alpha$). Finally, let $\alpha' = \big(\alpha - \omega^{\alpha_0} \cdot k_0\big)$. Then $\omega^{\alpha_0} \cdot k_0 + \alpha' = \alpha$ and since $\omega^{\alpha_0} \cdot (k_0 + 1) = \omega^{\alpha_0} \cdot k_0 + \omega^{\alpha_0} > \alpha$, $\alpha' < \omega^{\alpha_0}$. We leave it as an exercise to the reader to show that k_0, α_0, and α' are uniquely determined by α. ⊣

Now we are ready to prove the following result:

THEOREM 4.16 (CANTOR'S NORMAL FORM THEOREM). *Every ordinal number $\alpha > 0$ can be uniquely represented in the form*

$$\alpha = \omega^{\alpha_0} \cdot k_0 + \omega^{\alpha_1} \cdot k_1 + \ldots + \omega^{\alpha_n} \cdot k_n$$

where $n+1$ and $k_0, k_1, \ldots, k_n$ are positive integers and the ordinal exponents satisfy $\alpha \geq \alpha_0 > \alpha_1 > \alpha_2 > \ldots > \alpha_n \geq 0$.

Proof. By an iterative application of LEMMA 4.15 we get

$$\begin{aligned} \alpha &= \omega^{\alpha_0} \cdot k_0 + \alpha' \\ \alpha' &= \omega^{\alpha_1} \cdot k_1 + \alpha'' \\ \alpha'' &= \omega^{\alpha_2} \cdot k_2 + \alpha''' \\ &\vdots \end{aligned}$$

where $\alpha' < \omega^{\alpha_0}$, $\alpha'' < \omega^{\alpha_1}$, $\alpha''' < \omega^{\alpha_2}$, *et cetera*, and $k_0, k_1, k_2, \ldots$ are positive integers. Now, $\alpha' < \omega^{\alpha_0}$ implies that $\alpha_1 < \alpha_0$, and $\alpha'' < \omega^{\alpha_1}$ implies that $\alpha_2 < \alpha_1$, and so on. Thus, we get a descending sequence $\alpha \geq \alpha_0 > \alpha_1 > \alpha_2 > \ldots$, and since by the Axiom of Foundation every such sequence is finite, there exists an $n \in \omega$ such that $\alpha_{n+1} = 0$, and since $\omega^0 = 1$ this implies that $\alpha = \omega^{\alpha_0} \cdot k_0 + \ldots + \omega^{\alpha_n} \cdot k_n$. ⊣

The form $\alpha = \omega^{\alpha_0} \cdot k_0 + \ldots + \omega^{\alpha_n} \cdot k_n$ is called the **Cantor normal form** of α, denoted $\operatorname{cnf}(\alpha)$. Notice that by CANTOR'S NORMAL FORM THEOREM 4.16, every ordinal number can be written in a unique way in Cantor normal form.

For $\alpha = \omega^{\alpha_0} \cdot k_0 + \ldots + \omega^{\alpha_n} \cdot k_n$ let $\operatorname{cnf}_0(\alpha) := \omega^{\alpha_0} \cdot k_0$. The next lemma will be used to show that for every infinite ordinal α, there is a bijection between α and $\operatorname{cnf}_0(\alpha)$.

LEMMA 4.17. *If $\alpha_0, \alpha_1, k_0, k_1$ are ordinals, where $\alpha_0 > \alpha_1$ and $0 < k_0, k_1 < \omega$, then*

$$\omega^{\alpha_1} \cdot k_1 + \omega^{\alpha_0} \cdot k_0 = \omega^{\alpha_0} \cdot k_0 \,.$$

Proof. By distributivity we get $\omega^{\alpha_1}\cdot k_1+\omega^{\alpha_0}\cdot k_0=\omega^{\alpha_1}\cdot\big(k_1+\omega^{\alpha_0-\alpha_1}\cdot k_0\big)$, and since $k_1+\omega=\omega$ we get $k_1+\omega^{\alpha_0-\alpha_1}\cdot k_0=\omega^{\alpha_0-\alpha_1}\cdot k_0$. Thus, $\omega^{\alpha_1}\cdot k_1+\omega^{\alpha_0}\cdot k_0=\omega^{\alpha_1}\cdot\big(k_1+\omega^{\alpha_0-\alpha_1}\cdot k_0\big)=\omega^{\alpha_0}\cdot k_0$. ⊣

LEMMA 4.18. *For each ordinal $\alpha>0$ there exists a bijection between α and $\mathrm{cnf}_0(\alpha)$.*

Proof. Let $\mathrm{cnf}(\alpha)=\omega^{\alpha_0}\cdot k_0+\omega^{\alpha_1}\cdot k_1+\ldots+\omega^{\alpha_n}\cdot k_n$ and define the "reverse Cantor normal form" of α, denoted $\overleftarrow{\mathrm{cnf}}(\alpha)$, by

$$\overleftarrow{\mathrm{cnf}}(\alpha)=\omega^{\alpha_n}\cdot k_n+\omega^{\alpha_{n-1}}\cdot k_{n-1}+\ldots+\omega^{\alpha_0}\cdot k_0\,.$$

If $\alpha<\omega$, then $\alpha_0=0$, hence, $\alpha=\omega^{\alpha_0}\cdot k_0=k_0$ and therefore $\alpha=\mathrm{cnf}_0(\alpha)$. If $\alpha\geq\omega$, then by an iterative application of LEMMA 4.17 we get $\overleftarrow{\mathrm{cnf}}(\alpha)=\omega^{\alpha_0}\cdot k_0=\mathrm{cnf}_0(\alpha)$, and since there is obviously a bijection between α and $\overleftarrow{\mathrm{cnf}}(\alpha)$, there exists a bijection between α and $\mathrm{cnf}_0(\alpha)$. ⊣

Now we are ready to show that for each infinite ordinal α, the cardinality of the set of all finite sequences which can be formed with elements of α is the same as the cardinality of α. Moreover, we can show the following result:

THEOREM 4.19. *For each infinite ordinal α we have*

$$|\alpha|=|\operatorname{fin}(\alpha)|=|\operatorname{seq}^{1\text{-}1}(\alpha)|=|\operatorname{seq}(\alpha)|\,.$$

Moreover, there exists a class function F such that for each infinite ordinal $\alpha\geq\omega$, $\{\alpha\}\times\operatorname{seq}(\alpha)\subseteq\operatorname{dom}(F)$ and $F|_{\{\alpha\}\times\operatorname{seq}(\alpha)}$ induces an injection from $\operatorname{seq}(\alpha)$ into α.

Proof. Firstly notice that for every ordinal α, $|\alpha|\leq|\operatorname{fin}(\alpha)|\leq|\operatorname{seq}^{1\text{-}1}(\alpha)|\leq|\operatorname{seq}(\alpha)|$. In fact, there is a class function assigning to each ordinal α some appropriate functions to witness these inequalities. Thus, it is enough to prove that for every infinite ordinal α, $|\operatorname{seq}(\alpha)|\leq|\alpha|$ uniformly; *i.e.*, it is enough to show the existence of a class function F such that for every infinite ordinal α and any distinct finite sequences $s,t\in\operatorname{seq}(\alpha)$ we have $F\big(\langle\alpha,s\rangle\big)\in\alpha$ and $F\big(\langle\alpha,s\rangle\big)\neq F\big(\langle\alpha,t\rangle\big)$. Let α be an arbitrary but fixed infinite ordinal. In the following steps we will construct an injection $F_\alpha:\operatorname{seq}(\alpha)\hookrightarrow\alpha$ such that the class function F defined by $F\big(\langle\alpha,s\rangle\big):=F_\alpha(s)$ has the desired properties (notice that this requires that the function F_α is fully determined by α).

First we give a detailed construction of an injection $g_\alpha:\alpha\hookrightarrow\omega^{\alpha_0}$, where $\omega^{\alpha_0}\cdot k_0=\mathrm{cnf}_0(\alpha)$. By LEMMA 4.18 there is a bijection between α and $\omega^{\alpha_0}\cdot k_0$. Further, there is a bijection between the ordinal $\omega^{\alpha_0}\cdot k_0$ and the set $\omega^{\alpha_0}\times k_0$. Indeed, if $\beta\in\omega^{\alpha_0}\cdot k_0$, then there is a $\beta'\in\omega^{\alpha_0}$ and an $j\in k_0$ such that $\beta=\omega^{\alpha_0}\cdot j+\beta'$; let the image of β be $\langle\beta',j\rangle$. Similarly, there is a bijection between the set $k_0\times\omega^{\alpha_0}$ and the ordinal $k_0\cdot\omega^{\alpha_0}$, and since there is obviously a bijection between $\omega^{\alpha_0}\times k_0$ and $k_0\times\omega^{\alpha_0}$, there is a bijection between α and

$k_0 \cdot \omega^{\alpha_0}$. Further, since $1 \leq k_0 < \omega$, there is an injection from $k_0 \cdot \omega^{\alpha_0}$ into $\omega \cdot \omega^{\alpha_0} = \omega^{1+\alpha_0}$, thus, there is an injection

$$g : \alpha \hookrightarrow \omega^{1+\alpha_0}.$$

Notice that because $\alpha \geq \omega$, $\alpha_0 \geq 1$. Now we consider the following two cases:

If $\alpha_0 \geq \omega$, then $1 + \alpha_0 = \alpha_0$, thus, g is an injection from α into ω^{α_0}; in this case let $g_\alpha := g$.

If $\alpha_0 < \omega$, then $1+\alpha_0 = \alpha_0+1$ and there is a bijection between the ordinal ω^{α_0+1} and the set of functions from α_0+1 to ω, denoted ${}^{\alpha_0+1}\omega$. Similar to the proof of FACT 4.2 let $p_0 < p_1 < \ldots < p_{\alpha_0}$ be the least $\alpha_0 + 1$ prime numbers and define $h : {}^{\alpha_0+1}\omega \to \omega$ by stipulating $h(s) = \prod_{i\leq\alpha_0} p_i^{s(i)+1}$. Then h is injective and since $\alpha_0 \geq 1$ (notice that $\alpha \geq \omega$), there is an injection from α into ω^{α_0}; in this case let g_α be that injection.

Similarly, for each $n \in \omega$ we can construct an injection $f_{\alpha,n} : {}^n\alpha \hookrightarrow \alpha$. For $n = 0$ let $f_{\alpha,0}(\emptyset) := \emptyset$; and for $n > 0$ let $f_{\alpha,n}$ be defined by the following sequence of injections:

$$f_{\alpha,n} :\ {}^n\alpha \xrightarrow[\text{by } g_\alpha]{} {}^n\big(\omega^{\alpha_0}\big) \longrightarrow \big(\omega^{\alpha_0}\big)^n \longrightarrow \omega^{\alpha_0\cdot n} \longrightarrow \omega^{n\cdot\alpha_0} \dashrightarrow$$

$$\begin{tikzcd}
& & \omega^{n\cdot d_0} \arrow[r] & \omega \arrow[r] & \alpha & \\
{} \arrow[r, dotted, "\substack{\text{by } g_{\alpha_0}\text{, where}\\ \omega^{\delta_0}\cdot d_0 = \mathrm{cnf}_0(\alpha_0)}"'] & \omega^{n\cdot\omega^{\delta_0}\cdot d_0} \arrow[r] & \omega^{n\cdot d_0\cdot\omega^{\delta_0}} \arrow[u, "\delta_0=0"] \arrow[d, "\delta_0>0"'] & & \omega^{\omega} \arrow[r] & \alpha \\
& & \omega^{\omega\cdot\omega^{\delta_0}} \arrow[r] & \omega^{\omega^{1+\delta_0}} \arrow[ur, "\delta_0<\omega"] \arrow[dr, "\delta_0\geq\omega"'] & & \\
& & & & \omega^{\omega^{\delta_0}} \arrow[r] & \alpha
\end{tikzcd}$$

Now we can construct an injection from $\mathrm{seq}(\alpha)$ into α: Firstly notice that there is a natural bijection between $\mathrm{seq}(\alpha)$ and $\bigcup_{n\in\omega} {}^n\alpha$, thus, it is enough to construct an injection F_α from $\bigcup_{n\in\omega} {}^n\alpha$ into α. If $s \in \bigcup_{n\in\omega} {}^n\alpha$, then s is a finite set of ordered pairs (*i.e.*, $|s| \in \omega$) and $f_{\alpha,|s|}$ is an injection from ${}^{|s|}\alpha$ into α, in particular, $f_{\alpha,|s|}(s) \in \alpha$. Finally let us define $F_\alpha : \bigcup_{n\in\omega} {}^n\alpha \to \alpha$ by stipulating

$$F(s) := f_{\alpha,2}\big(\big\{\langle 0, |s|\rangle, \langle 1, f_{\alpha,|s|}(s)\rangle\big\}\big).$$

Then, since α is infinite, $|s| \in \alpha$, and since $f_{\alpha,2}$ is an injection from ${}^2\alpha$ into α, F_α is injective. $\dashv$

As an application of THEOREM 4.19 let us prove that whenever we have an injection from $\mathscr{P}(A)$ into $A \times A$, then A has at most four elements.

THEOREM 4.20. $2^{\mathfrak{m}} \leq \mathfrak{m}^2 \to \mathfrak{m} \leq 4$.

Proof. If $\mathfrak{m}$ is finite, an easy calculation shows that $2^{\mathfrak{m}} \leq \mathfrak{m}^2$ implies that $\mathfrak{m} \in \{2,3,4\}$. Thus, let $\mathfrak{m}$ be infinite and assume towards a contradiction that $2^{\mathfrak{m}} \leq \mathfrak{m}^2$. Let A be a set of cardinality $\mathfrak{m}$ and let $f_0 : \mathscr{P}(A) \hookrightarrow A \times A$. With the function f_0 we can construct an *injective* class function from Ω into A, which is obviously a contradiction to the Axiom Schema of Replacement — which implies that there is no injection from a proper class (like Ω) into a set.

Firstly we construct an injection $F_\omega : \omega \hookrightarrow A$. Let a_0, a_1, a_2, a_3, a_4 be five distinct elements of A and define $F_5 : 5 \to A$ by stipulating $F_5(i) := a_i$ (for all $i \in 5$); further let $S_5 := F_5[5]$ (*i.e.*, $S_5 = \{F_5(i) : i \in 5\}$). Assume that for some $n \geq 5$ we have already constructed an injection $F_n : n \hookrightarrow A$. For any distinct sets $x, y \in \mathscr{P}(S_n)$, where $S_n := F_n[n]$, let

$$x \prec y \iff |x| < |y| \vee \exists i \in n\Big(F(i) \in (x \backslash y) \wedge \forall j \in i\,\big(F(j) \in x \leftrightarrow F(j) \in y\big)\Big)\,.$$

Since S_n is finite, the relation "$\prec$" is a well-ordering, and since $n \geq 5$, $|\mathscr{P}(S_n)| = 2^n > n^2 = |S_n \times S_n|$. Thus, there exists a $\prec$-minimal set $x \subseteq S_n$ such that $f_0(x) \notin S_n \times S_n$. Let $f_0(x) = \langle b_0, b_1\rangle$ and let

$$a_n = \begin{cases} b_0 & \text{if } b_0 \notin S_n, \\ b_1 & \text{otherwise.} \end{cases}$$

Define $F_{n+1} := F_n \cup \{\langle n, a_n\rangle\}$ and let $S_{n+1} := S_n \cup \big\{F_{n+1}(n)\big\}$. Then F_{n+1} is an injection from $n+1$ into A, and $S_{n+1} = F_{n+1}[n+1]$. Proceeding this way we finally get an injection $F_\omega : \omega \hookrightarrow A$ as well as a countably infinite set $S_\omega = F_\omega[\omega] \subseteq A$.

Assume now that we have already constructed an injection $F_\alpha : \alpha \hookrightarrow A$ for some infinite ordinal $\alpha \geq \omega$ and let $S_\alpha := F_\alpha[\alpha]$. By THEOREM 4.19 there is a canonical bijection $g : \alpha \to \alpha \times \alpha$. With g we can define a bijection $\bar{g} : S_\alpha \to S_\alpha \times S_\alpha$ by stipulating

$$\bar{g}\big(F_\alpha(\beta)\big) = \big\langle F_\alpha(\beta_0), F_\alpha(\beta_1)\big\rangle \quad \text{where } \beta = g^{-1}\big(\langle \beta_0, \beta_1\rangle\big)\,.$$

Further, define a mapping $\Gamma : S_\alpha \to \mathscr{P}(S_\alpha)$ by stipulating

$$\Gamma(a) = \begin{cases} x \subseteq S_\alpha & \text{if } f_0(x) = \bar{g}(a), \\ \emptyset & \text{otherwise.} \end{cases}$$

and let

$$M = \big\{a \in S_\alpha : a \notin \Gamma(a)\big\}\,.$$

Then $M \in \mathscr{P}(S_\alpha)$ and let $f_0(M) = \langle b_0, b_1\rangle \in A \times A$. If $\langle b_0, b_1\rangle \in S_\alpha \times S_\alpha$, then $f_0(M) = \bar{g}(a)$ for some $a \in S_\alpha$, and hence $\Gamma(a) = M$; but $a \in \Gamma(a) \leftrightarrow a \in M \leftrightarrow a \notin \Gamma(a)$, which is obviously impossible. Thus, $\langle b_0, b_1\rangle \notin S_\alpha \times S_\alpha$ and we let

$$a_\alpha = \begin{cases} b_0 & \text{if } b_0 \notin S_\alpha, \\ b_1 & \text{otherwise.} \end{cases}$$

Further, define $F_{\alpha+1} := F_\alpha \cup \{\langle \alpha, a_\alpha \rangle\}$ and let $S_{\alpha+1} := S_\alpha \cup \{a_\alpha\}$. Then $F_{\alpha+1}$ is an injection from $\alpha + 1$ into A, and $S_{\alpha+1} = F_{\alpha+1}[\alpha + 1]$. Finally, if λ is a limit ordinal and F_β is defined for each $\beta \in \lambda$ we define $F_\lambda := \bigcup_{\beta \in \lambda} F_\beta$.

Now, by the TRANSFINITE RECURSION THEOREM 3.19, $\bigcup_{\alpha \in \Omega} F_\alpha$ is an injective class function which maps Ω into A; a contradiction to HARTOGS' THEOREM. ⊣

The idea of the previous proof — getting a contradiction by constructing an injective class function from Ω into a given set — is used again in the proofs of THEOREM 4.21, PROPOSITION 4.22, and LEMMA 4.23.

More Cardinal Relations

$\mathrm{fin}(\mathfrak{m}) < 2^{\mathfrak{m}}$ whenever $\mathfrak{m}$ is infinite

THEOREM 4.21. *If* $\mathfrak{m}$ *is an infinite cardinal, then* $\mathrm{fin}(\mathfrak{m}) < 2^{\mathfrak{m}}$.

Proof. Let A be an arbitrary but fixed infinite set of cardinality $\mathfrak{m}$. Obviously, the identity mapping is an injection from $\mathrm{fin}(A)$ into $\mathscr{P}(A)$, hence, $\mathrm{fin}(\mathfrak{m}) \leq 2^{\mathfrak{m}}$. Now, assume towards a contradiction that $\left|\mathscr{P}(A)\right| = \left|\mathrm{fin}(A)\right|$ and let

$$f_0 : \mathscr{P}(A) \to \mathrm{fin}(A)$$

be a bijection. The mapping will be used in order to construct an injective class function $F : \Omega \hookrightarrow \mathrm{fin}(A)$. First we define an injection $F_\omega : \omega \hookrightarrow \mathrm{fin}(A)$ by stipulating

$$F_\omega(n) = f_0^{n+1}(A)$$

where $f_0^1(A) := f_0(A)$ and for positive integers k, $f_0^{k+1}(A) := f_0\big(f_0^k(A)\big)$. Then, since A is infinite, F_ω is indeed an injection.

Assume that we have already constructed an injection $F_\alpha : \alpha \hookrightarrow \mathrm{fin}(A)$ for some infinite ordinal $\alpha \geq \omega$ and for $\iota \in \alpha$ let $s_\iota := F(\iota)$. Notice that $s_\iota \neq s_{\iota'}$ whenever $\iota \neq \iota'$. Define an equivalence relation on A by

$$x \sim y \iff \forall \iota \in \alpha (x \in s_\iota \leftrightarrow y \in s_\iota)\,.$$

For $x \in A$ and $\mu \in \alpha$ define

$$D_{x,\mu} = \bigcap \big\{ s_\iota : \iota \in \mu \wedge x \in s_\iota \big\}$$

where we define for the moment $\bigcap \emptyset := A$, and let

$$g_x = \big\{ \mu \in \alpha : x \in s_\mu \wedge (s_\mu \cap D_{x,\mu} \neq D_{x,\mu}) \big\}\,.$$

We leave it as an exercise to the reader to show that for any $x, y \in A$, $g_x = g_y$ *iff* $x \sim y$. Hence, there is a bijection between $\{[x]^{\tilde{}} : x \in A\}$ and $\{g_x : x \in A\}$. Further, for each $x \in A$, $g_x \in \operatorname{fin}(\alpha)$. To see this, let $\mu_0 < \mu_1 < \mu_2 < \dots$ be the ordinals in g_x in increasing order. By definition we have:

(1) $x \notin s_\iota$ whenever $\iota \in \mu_0$

(2) $x \in s_{\mu_0}$ and $s_{\mu_0} = D_{x,\mu_0+1}$

(3) $D_{x,\mu_0+1} \supsetneq D_{x,\mu_1+1} \supsetneq D_{x,\mu_2+1} \supsetneq \dots$

By (2), D_{x,μ_0+1} is finite, and therefore the decreasing sequence (3) must be finite too, which implies that also g_x is finite.

Since $\{g_x : x \in A\} \subseteq \operatorname{fin}(\alpha)$ we can apply THEOREM 4.19 to obtain an injection $h : \{g_x : x \in A\} \hookrightarrow \alpha$. The set $h[\{g_x : x \in A\}]$, as a subset of α, is well-ordered by "$\in$". Let γ be the order type of $h[\{g_x : x \in A\}]$. Then $\gamma \leq \alpha$ and for each g_x assign an ordinal number $\eta(g_x) \in \gamma$ such that the mapping $\eta : \{g_x : x \in A\} \to \gamma$ is bijective. For each $\iota \in \alpha$, s_ι is the union of at most finitely many equivalence classes. Thus, we can construct an injection from α into $\operatorname{fin}(\gamma)$ by stipulating

$$\iota \longmapsto \{\xi \in \gamma : \exists x \in s_\iota (\eta(g_x) = \xi)\}.$$

Because by THEOREM 4.19 we can construct a bijection between $\operatorname{fin}(\gamma)$ and γ, we can also construct an injection from α into γ, and because $\gamma \leq \alpha$, by the CANTOR-BERNSTEIN THEOREM 3.17 we finally get a bijection $H : \gamma \to \alpha$ between γ and α. Define the function $\Gamma : A \to \mathscr{P}(A)$ by stipulating

$$\Gamma(x) = {f_0}^{-1}\big(s_{H(\eta(g_x))}\big)$$

and consider the set

$$M = \{x \in A : x \notin \Gamma(x)\}.$$

We claim that the set M does not belong to $\{{f_0}^{-1}(s_\iota) : \iota \in \alpha\}$. Indeed, if there would be a $\beta \in \alpha$ such that ${f_0}^{-1}(s_\beta) = M$, then there would also be an equivalence class $[x]^{\tilde{}}$, which corresponds to g_x, such that

$$\beta = H\big(\eta(g_x)\big).$$

For each $y \in [x]^{\tilde{}}$ we have $\Gamma(y) = M$, and $y \in \Gamma(y) \leftrightarrow y \in M \leftrightarrow y \notin \Gamma(y)$, which is obviously impossible.

Now, let $s_\alpha := {f_0}^{-1}(M)$ and define $F_{\alpha+1} := F_\alpha \cup \{s_\alpha\}$. Then $F_{\alpha+1}$ is an injection from $\alpha + 1$ into $\operatorname{fin}(A)$. Finally, if λ is a limit ordinal and F_β is defined for each $\beta \in \lambda$, then define $F_\lambda := \bigcup_{\beta\in\lambda} F_\beta$. Thus, by the TRANSFINITE RECURSION THEOREM 3.19, $\bigcup_{\alpha\in\Omega} F_\alpha$ is an injective class function which maps Ω into $\operatorname{fin}(A)$; a contradiction to HARTOGS' THEOREM. ⊣

Even though $\operatorname{fin}(\mathfrak{m}) < 2^{\mathfrak{m}}$ (for all infinite cardinals $\mathfrak{m}$), it might be possible that for some natural number n, $n \cdot \operatorname{fin}(\mathfrak{m}) = 2^{\mathfrak{m}}$. The next result shows that in that case, n must be a power of 2.

PROPOSITION 4.22. *If* $2^{\mathfrak{m}} = n \cdot \operatorname{fin}(\mathfrak{m})$ *for some natural number* n*, then* $n = 2^k$ *for some* $k \in \omega$.

Proof. If the cardinal $\mathfrak{m}$ is finite, then $2^{\mathfrak{m}} = \operatorname{fin}(\mathfrak{m}) = 1 \cdot \operatorname{fin}(\mathfrak{m}) = 2^0 \cdot \operatorname{fin}(\mathfrak{m})$. So, let $\mathfrak{m}$ be an infinite cardinal and let A be an arbitrary but fixed set of cardinality $\mathfrak{m}$. Further, let n be a natural number which is not a power of 2. Assume towards a contradiction that $|\mathscr{P}(A)| = |n \times \operatorname{fin}(A)|$. Let

$$f_0 : n \times \operatorname{fin}(A) \to \mathscr{P}(A)$$

be a bijection which will be used to construct an injective class function from Ω into $\operatorname{fin}(A)$. Let $\langle m_0, x_0 \rangle := {f_0}^{-1}(A)$. Assume that for some $\ell \in \omega$, $x_0, x_1, \ldots, x_\ell$ are pairwise distinct finite subsets of A. For each $i \in n$ and $j \leq \ell$ let

$$X_{i,j} = f_0\big(\langle i, x_j \rangle\big) .$$

On A define an equivalence relation by stipulating

$$a \sim b \iff \forall i \in n \, \forall j \leq \ell \, (a \in X_{i,j} \leftrightarrow b \in X_{i,j}) .$$

Further, let $\mathrm{Eq} := \big\{[a]^{\sim} : a \in A\big\}$ be the set of all equivalence classes and let $k_0 := |\,\mathrm{Eq}\,|$. Now define an ordering "$\prec$" on the set $\{X_{i,j} : i \in n \wedge j \leq \ell\}$, for example define

$$X_{i,j} \prec X_{i',j'} \iff j < j' \vee (j = j' \wedge i < i') .$$

The ordering "$\prec$" induces in a natural way an ordering on the set Eq, and consequently of the set $E = \big\{ \bigcup Y : Y \subseteq \mathrm{Eq} \big\}$. Since the equivalence classes in Eq are pairwise disjoint, $|E| = 2^{k_0}$. Notice that $2^{k_0} \geq n \cdot (\ell + 1)$, and since n is not a power of 2, there is a least set $\bigcup Y_0 \in E$ (least with respect to the ordering on E induced by "$\prec$") such that ${f_0}^{-1}\big(\bigcup Y_0\big) = \langle m_{\ell+1}, x_{\ell+1} \rangle$ and $x_{\ell+1} \notin \{x_j : j \leq \ell\}$. For $i \in n$ define $X_{i,\ell+1} := f_0\big(\langle i, x_{\ell+1} \rangle\big)$ and proceed as before. Finally we get an infinite sequence $x_0, x_1, \ldots$ of pairwise distinct finite subsets of A which shows that $\operatorname{fin}(A)$ is transfinite, *i.e.*, there exists a injection $F_\omega : \omega \hookrightarrow \operatorname{fin}(A)$.

Assume that we have already constructed an injection $F_\alpha : \alpha \hookrightarrow \operatorname{fin}(A)$ for some infinite ordinal $\alpha \geq \omega$. Using the fact that there is a bijection between $n \cdot \alpha$ and α, by the same arguments as in the proof of THEOREM 4.21 we can construct an injection $F_{\alpha+1} : \alpha + 1 \hookrightarrow \operatorname{fin}(A)$ and finally obtain an injective class function from Ω into $\operatorname{fin}(A)$; a contradiction to HARTOGS' THEOREM. ⊣

Even though PROPOSITION 4.22 looks a little bland, one cannot do better in ZF, *i.e.*, for all $k \in \omega$, the statement "$\exists \mathfrak{m}\big(2^{\mathfrak{m}} = 2^k \cdot \operatorname{fin}(\mathfrak{m})\big)$" is consistent with ZF (*cf.* PROPOSITION 7.5).

$\text{seq}^{1\text{-}1}(\mathfrak{m}) \neq 2^{\mathfrak{m}} \neq \text{seq}(\mathfrak{m})$ whenever $\mathfrak{m} \geq 2$

First we prove that the inequality $\text{seq}^{1\text{-}1}(\mathfrak{m}) \neq 2^{\mathfrak{m}} \neq \text{seq}(\mathfrak{m})$ whenever $\mathfrak{m}$ is transfinite.

LEMMA 4.23. *Let $\mathfrak{m}$ be a transfinite cardinal number. Then $2^{\mathfrak{m}} \nleq \text{seq}(\mathfrak{m})$ and consequently also $2^{\mathfrak{m}} \nleq \text{seq}^{1\text{-}1}(\mathfrak{m})$.*

Proof. Let A be a set of cardinality $\mathfrak{m}$ and assume towards a contradiction that there exists an injection $f_0 : \mathscr{P}(A) \hookrightarrow \text{seq}(A)$. Since A is transfinite there is an injection $F_\omega : \omega \hookrightarrow A$ and let $S_\omega := F_\omega[\omega]$. Assume that we have already constructed an injection $F_\alpha : \alpha \hookrightarrow A$ for some infinite ordinal $\alpha \geq \omega$ and let $S_\alpha := F_\alpha[\alpha]$. By THEOREM 4.19 there is a bijection between α and $\text{seq}(\alpha)$, and consequently we can define a bijection $\bar{g} : S_\alpha \to \text{seq}(S_\alpha)$. Further, define $\Gamma : S_\alpha \to \mathscr{P}(S_\alpha)$ by stipulating

$$\Gamma(a) = \begin{cases} x \subseteq S_\alpha & \text{if } f_0(x) = \bar{g}(a), \\ \emptyset & \text{otherwise,} \end{cases}$$

and let

$$M = \left\{a \in S_\alpha : a \notin \Gamma(a)\right\}.$$

Then $M \in \mathscr{P}(S_\alpha)$ and $f_0(M) = \langle b_0, b_1, \dots, b_n \rangle \in \text{seq}(A) \setminus \text{seq}(S_\alpha)$. Now, let $a_\alpha := b_i$, where $i \leq n$ is the least number such that $b_i \notin S_\alpha$ and define $F_{\alpha+1} := F_\alpha \cup \{\langle \alpha, a_\alpha \rangle\}$ and $S_{\alpha+1} := S_\alpha \cup \left\{F_{\alpha+1}(\alpha)\right\}$. Then $F_{\alpha+1}$ is an injection from $\alpha + 1$ into A, and $S_{\alpha+1} = F_{\alpha+1}[\alpha + 1]$. Finally, if λ is a limit ordinal and F_β is defined for each $\beta \in \lambda$ we define $F_\lambda := \bigcup_{\beta \in \lambda} F_\beta$ and finally get that $\bigcup_{\alpha \in \Omega} F_\alpha$ is an injective class function; a contradiction to HARTOGS' THEOREM. ⊣

To prove that $\text{seq}(\mathfrak{m}) \neq 2^{\mathfrak{m}}$ whenever $\mathfrak{m} \geq 1$ one could for example show that $\text{seq}(\mathfrak{m}) = 2^{\mathfrak{m}}$ implies that $\mathfrak{m}$ is transfinite by using similar ideas as above, but we get a slightly more elegant proof by showing that $\text{seq}(\mathfrak{m}) = 2^{\mathfrak{m}}$ implies that $\text{seq}(\mathfrak{m} + \aleph_0) = 2^{\mathfrak{m} + \aleph_0}$.

THEOREM 4.24. *For all cardinals $\mathfrak{m} \geq 1$, $\text{seq}(\mathfrak{m}) \neq 2^{\mathfrak{m}}$.*

Proof. We will show that whenever $\mathfrak{m} \geq 1$ is a cardinal such that $2^{\mathfrak{m}} = \text{seq}(\mathfrak{m})$, then $2^{\mathfrak{m}+\aleph_0} = \text{seq}(\mathfrak{m} + \aleph_0)$ which is a contradiction to LEMMA 4.23. Let the set A be such $|A| = \mathfrak{m}$ and $A \cap \omega = \emptyset$. Further, let $f_0 : \mathscr{P}(A) \to \text{seq}(A)$ be a bijection. For a fixed element $a_0 \in A$ and $n \in \omega$ let

$$s_n = \langle \underbrace{a_0, \dots, a_0}_{n\text{-times}} \rangle.$$

With the sequences s_n we can define an injection $g : \omega \hookrightarrow \mathscr{P}(A)$ by stipulating $g(n) := {f_0}^{-1}(s_n)$, which shows that $\mathscr{P}(A)$ is transfinite, *i.e.*, $\aleph_0 \leq 2^{\mathfrak{m}}$. Thus, by PROPOSITION 4.4 we have $2^{\aleph_0} \leq 2^{\mathfrak{m}}$ which implies that there exists an injection $h : \mathscr{P}(\omega) \hookrightarrow \mathscr{P}(A)$. Finally let

$$\begin{aligned} F : \mathscr{P}(A) \times \mathscr{P}(\omega) &\longrightarrow \qquad \operatorname{seq}(A \cup \omega) \\ \langle x, y \rangle \qquad &\longmapsto f_0(x)^\frown 0^\frown f_0\big(h(y)\big) \end{aligned}$$

where $s^\frown t$ denotes the concatenation of the sequences s and t. Then F is injective and we consequently get $2^{\mathfrak{m}+\aleph_0} = 2^{\mathfrak{m}} \cdot 2^{\aleph_0} = \operatorname{seq}(\mathfrak{m} + \aleph_0)$. ⊣

In order to prove that $\operatorname{seq}^{1\text{-}1}(\mathfrak{m}) \neq 2^{\mathfrak{m}}$ whenever $\mathfrak{m} \geq 2$ we show that $\operatorname{seq}^{1\text{-}1}(\mathfrak{m}) = 2^{\mathfrak{m}}$ would imply that $\mathfrak{m}$ is transfinite, which is a contradiction to LEMMA 4.23. However, before we have to introduce some notation concerning finite sequences of natural numbers.

For $n \in \omega$ let $n^\star := |\operatorname{seq}^{1\text{-}1}(n)|$ be the number of non-repetitive sequences (*i.e.*, sequences without repetitions) we can build with n distinct objects (*e.g.*, with $\{0, \ldots, n-1\} = n$). It is not hard to verify that

$$n^\star = \sum_{k=0}^{n} \binom{n}{k} k! = \sum_{j=0}^{n} \frac{n!}{j!}\,,$$

and that for all positive integers n we have $n^\star = \lfloor en! \rfloor$, where $\lfloor x \rfloor$ denotes the integer part of a real number x and $e$is the Euler number. Obviously, $0^\star = 1$ and $n^\star = n \cdot (n-1)^\star + 1$, which implies that

$$n^\star = e \int_1^\infty t^n e^{-t} dt\,.$$

The number $n^\star$ is also the number of paths (without loops) in the complete graph on $n+2$ vertices starting in one vertex and ending in another.

The first few numbers of the integer sequence $n^\star$ are $0^\star = 1$, $1^\star = 2$, $2^\star = 5$, $3^\star = 16$, $4^\star = 65$, $5^\star = 326$, and further we get *e.g.*, $100^\star \approx 2.53687 \cdot 10^{158}$ and $256^\star \approx 2.33179 \cdot 10^{507}$.

For each positive integer q, an easy calculation modulo q shows that for all $n \in \omega$ we have $n^\star \equiv (n+q)^\star \mod q$. In particular, if $q \mid n^\star$, then $q \mid (n+q)^\star$. Now we can ask whether there is a positive integer $t < q$ such that $q \mid (n+t)^\star$ and $q \mid n^\star$. The following lemma shows that this is not the case whenever q is a power of 2.

LEMMA 4.25. *If* $2^k \mid n^\star$ *and* $2^k \mid (n+t)^\star$ *for some* $t \in \omega$, *then* $2^k \mid t$.

Proof. For $k \leq 3$, an easy calculation modulo 2^k shows that for each n, if $2^k | n^\star$, then $2^k \nmid (n+t)^\star$ whenever $0 < t < 2^k$.

Assume towards a contradiction that there is a smallest $k \geq 3$ such that $2^{k+1} \mid n^\star$ and $2^{k+1} \mid (n+t)^\star$ for some integer t with $0 < t < 2^{k+1}$. Notice that since $k \geq 3$, $n \geq 3$. Then, because $2^k \mid 2^{k+1}$, we have $2^k \mid n^\star$ and $2^k \mid (n+t)^\star$, and by the choice of k we get $t = 2^k$. Let us now compute $\left(n+2^k\right)^\star$ by writing down $\sum_{i=0}^{n+2^k} \frac{(n+2^k)!}{i!}$ explicitly:

$$
\begin{array}{rlr}
\left(n+2^k\right)^\star = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2^k \cdot (2^k+1) \cdot \ldots \cdot (2^k+n) & + & [1] \\
2 \cdot 3 \cdot \ldots \cdot 2^k \cdot (2^k+1) \cdot \ldots \cdot (2^k+n) & + & [2] \\
3 \cdot \ldots \cdot 2^k \cdot (2^k+1) \cdot \ldots \cdot (2^k+n) & + & [3] \\
\ddots & \vdots & \vdots \\
2^k \cdot (2^k+1) \cdot \ldots \cdot (2^k+n) & + & [2^k] \\
(2^k+1) \cdot \ldots \cdot (2^k+n) & + & [2^k+1] \\
\ddots & \vdots & \vdots \\
(2^k+n) & + & [2^k+n] \\
1 & & [2^k+n+1]
\end{array}
$$

Since $k \geq 4$ and $n \geq 3$, 2^{k+1} divides rows $[1] - [2^k]$. In order to calculate the products in rows $[2^k+1] - [2^k+n+1]$ (modulo 2^{k+1}), we only have to consider products which are not obviously divisible by 2^{k+1}. So, since $2^{k+1} \mid (n+2^k)^\star$, for a suitable natural number r we have

$$(n+2^k)^\star = 2^k \cdot \Big(\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!} \Big) + n^\star + 2^{k+1} \cdot r\,.$$

We know that $2^{k+1} | n^\star$ where $n \geq 3$ and $k \geq 4$, and because $n^\star$ is even, n has to be odd. If j is equal to $n-1$, $n-2$, or $n-3$, then $\sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd, and if $0 \leq j \leq (n-4)$, then $\sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is even. So,

$$\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!}$$

is odd, and since $2^{k+1} \mid n^\star$, $2^{k+1} \nmid (n+2^k)^\star$. $\dashv$

Now we are ready to prove the following result:

THEOREM 4.26. *For all cardinals* $\mathfrak{m} \geq 2$, $\text{seq}^{1\text{-}1}(\mathfrak{m}) \neq 2^{\mathfrak{m}}$.

Proof. By LEMMA 4.23 it is enough to prove that for $\mathfrak{m} \geq 2$, $\text{seq}^{1\text{-}1}(\mathfrak{m}) = 2^{\mathfrak{m}} \rightarrow \aleph_0 \leq \mathfrak{m}$. Let A be an arbitrary set of cardinality $\mathfrak{m}$ and assume that

$$f_0 : \mathscr{P}(A) \longrightarrow \text{seq}^{1\text{-}1}(A)$$

is a bijection between $\mathscr{P}(A)$ and $\text{seq}^{1\text{-}1}(A)$. We shall use this bijection to show that A is transfinite. In fact it is enough to show that every finite sequence

$s_n = \langle a_0, \dots, a_{n-1}\rangle \in \mathrm{seq}^{1\text{-}1}(A)$ of length n can be extended canonically to a sequence $s_{n+1} = s_n^\frown\langle a_n\rangle \in \mathrm{seq}^{1\text{-}1}(A)$ of length $n+1$.

Let a_0 and a_1 be two distinct elements of A and assume that for some $n \geq 2$ we already have constructed a sequence $s_n = \langle a_0, a_1, \dots, a_{n-1}\rangle$ of distinct elements of A and let $S_n = \{a_i : i \in n\}$. The sequence s_n induces in a natural way an ordering on the set $\mathrm{seq}^{1\text{-}1}(S_n)$, e.g., order $\mathrm{seq}^{1\text{-}1}(S_n)$ by length and lexicographically. Let us define an equivalence relation on A by stipulating

$$a \sim b \iff \forall s \in \mathrm{seq}^{1\text{-}1}(S_n)\big(a \in {f_0}^{-1}(s) \leftrightarrow b \in {f_0}^{-1}(s)\big).$$

Let $\mathrm{Eq}(n) := \big\{[a]^{\tilde{}} : a \in A\big\}$ be the set of all equivalence classes. The ordering on $\mathrm{seq}^{1\text{-}1}(S_n)$ induces an ordering on $\mathrm{Eq}(n)$. Let

$$k_0 = |\,\mathrm{Eq}(n)|\,.$$

Then 2^{k_0} is equal to the cardinality of $\mathscr{P}\big(\mathrm{Eq}(n)\big)$. Identify $\big\{\bigcup Y : Y \subseteq \mathrm{Eq}(n)\big\}$ with the set of all functions $\bar{g} \in {}^{\mathrm{Eq}(n)}2$. Now, the ordering on $\mathrm{Eq}(n)$ induces in a natural way an ordering on the set of functions ${}^{\mathrm{Eq}(n)}2$. By construction we have $n^\star = |\,\mathrm{seq}^{1\text{-}1}(S_n)| \leq 2^{k_0}$, i.e., we have either $n^\star < 2^{k_0}$ or $n^\star = 2^{k_0}$:

Case 1: If $n^\star < 2^{k_0}$, then there exists a least function $\bar{g}_0 \in {}^{\mathrm{Eq}(n)}2$ (least with respect to the ordering on ${}^{\mathrm{Eq}(n)}2$) such that $\bar{g}_0 \notin \big\{x_s : s \in \mathrm{seq}^{1\text{-}1}(S_n)\big\}$, where x_s is the characteristic function of the set of equivalence classes included in ${f_0}^{-1}(s)$. In particular we get $f_0(\bar{g}_0) \notin \mathrm{seq}^{1\text{-}1}(S_n)$. Let $a_n \in A$ be the first element in the sequence $f_0(\bar{g}_0)$ which does not belong to S_n. Now, $s_n^\frown\langle a_n\rangle \in \mathrm{seq}^{1\text{-}1}(A)$ is a sequence of length $n+1$ and we are done.

Case 2: Suppose that $n^\star = 2^{k_0}$. For arbitrary elements $a \in A\backslash S_n$ let us resume the construction with the sequence $s_n^\frown\langle a\rangle$. By a parity argument one easily verifies that $(n+1)^\star$ is not an integer power of 2, and thus, we are in Case 1. We proceed as long as we are in Case 1. If there is an element $a \in A \setminus S_n$ such that we are always in Case 1, then we can construct an infinite non-repetitive sequence of elements of A and we are done.

Assume now that no matter with which element $a \in A \setminus S_n$ we resume our construction, we always get back to Case 2. We then have the following situation: Starting with any element $a \in A \setminus S_n$ we get a non-repetitive sequence of elements of A of length $n+\ell+1$ (for some positive integer ℓ) where $(n+\ell+1)^\star$ is an integer power of 2. Let $s^a_{n+\ell} = \langle a_0, a_1, \dots, a_{n+\ell}\rangle$ be that sequence and let $\bar{S}^a_n = \{a_0, a_1, \dots, a_{n+\ell}\}$. By construction we have $a \in \bar{S}^a_n$, i.e., a belongs to the corresponding sequence $s^a_{n+\ell}$. However, $\bar{S}^a_n$ is not necessarily the union of elements of $\mathrm{Eq}(n)$, which leads to the following definition:

A subset of A is called ***good*** *if it is* not *the union of elements of* $\mathrm{Eq}(n)$.

For every set $X \subseteq A$ which is good we have $f_0(X) \notin \operatorname{seq}^{1\text{-}1}(S_n)$, which implies that there is a first element in the sequence $f_0(X)$ which does not belong to the set S_n. Thus, it is enough to determine a good subset of A. For this, consider the set

$$T_{\min} := \left\{a \in A \setminus S_n : \bar{S}_n^a \textit{ is good and of least cardinality}\right\}.$$

Notice that for every $a \in A \setminus S_n$, $\bar{S}_n^a$ is finite and contains a, and since $A \setminus S_n$ is infinite, there is an $\bar{S}_n^a$ (for some $a \in A \setminus S_n$) which is good, thus, $T_{\min} \neq \emptyset$. If $T_{\min}$ is good, use $f_0(T_{\min})$ to construct a non-repetitive sequence in A of length $(n+1)$, and we are done. Otherwise, let $m_T := \left|\bar{S}_n^a\right|$ for some a in $T_{\min}$ (notice that by our assumptions, m_T is a positive integer). For each $a \in T_{\min}$ let us construct a non-repetitive sequence SEQ^a of elements of $\bar{S}_n^a$ of length m_T in such a way that for all $a, b \in T_{\min}$:

$$\bar{S}_n^a = \bar{S}_n^b \implies \mathrm{SEQ}^a = \mathrm{SEQ}^b$$

In order to do so, let $a \in T_{\min}$ be arbitrary. Because $\bar{S}_n^a \in T_{\min}$, $\bar{S}_n^a$ is good, thus

$$f_0(\bar{S}_n^a) \notin \operatorname{seq}^{1\text{-}1}(S_n),$$

hence, there is a first element a_n in the sequence $f_0(\bar{S}_n^a)$ which does not belong to S_n. Repeat the construction starting with the sequence $s_{n+1} = s_n{}^\frown\langle a_n\rangle$ and consider the set $\bar{S}_n^{a_n}$. If $\bar{S}_n^{a_n} = \bar{S}_n^a$, then the corresponding sequence $s^{a_n} \in \operatorname{seq}^{1\text{-}1}(\bar{S}_n^{a_n})$ is of length m_T and we define $\mathrm{SEQ}^a := s^{a_n}$. On the other hand, if $\bar{S}_n^{a_n} \subsetneq \bar{S}_n^a$, then $\bar{S}_n^{a_n}$ is not good (since $\bar{S}_n^a$ is a good set of *least* cardinality), *i.e.*, $\bar{S}_n^{a_n}$ is the union of elements of $\mathrm{Eq}(n)$. Let $S' = \bar{S}_n^a \setminus \bar{S}_n^{a_n}$ and let $s' \in \operatorname{seq}^{1\text{-}1}(S')$ be the corresponding sequence. Then S' is good, which implies that $f_0(S') \notin \operatorname{seq}^{1\text{-}1}(\bar{S}^{a_n})$, and let a' be the first element in the sequence $f_0(S')$ which does not belong to $\bar{S}^{a_n}$. Now proceed building the sequence SEQ^a by starting with the sequence $s'{}^\frown\langle a'\rangle$. Notice that by construction the sequence SEQ^a depends only on the set $\bar{S}_n^a$, thus, for all $a, b \in T_{\min}$, $\mathrm{SEQ}^a = \mathrm{SEQ}^b$ whenever $\bar{S}_n^a = \bar{S}_n^b$.

So far, for each $a \in T_{\min}$ with $\left|\bar{S}_n^a\right| = m_T$ we can construct a non-repetitive sequence $\mathrm{SEQ}^a \in \operatorname{seq}^{1\text{-}1}(\bar{S}_n^a)$ of length $m_T > n$. On the other hand, we still have to determine in a constructive way a good subset of A which contains S_n — even though $\bar{S}_n^a$ is good for each $a \in T_{\min}$, it is not clear which set $\bar{S}_n^a$ we should choose. Now, for $i < m_T$ define

$$Q_i := \{b \in A : \ b \textit{ is the } i^{th} \textit{ element in } \mathrm{SEQ}^a \textit{ for some } a \in T_{\min}\}.$$

Claim. *There is a smallest $j_0 < m_T$ such that Q_{j_0} is good.*

Proof of Claim. For any $a \in T_{\min}$ let

$$a^{=} := \{a' \in A : \bar{S}^{a'} = \bar{S}^a\},$$

which are the elements of the finite set $\bar{S}^a$ which are to some extent indistinguishable, and further let t_0 denote the least cardinality of the sets $a^=$, where $a \in T_{\min}$. Note that if for some $i \neq j_0$, $a \in Q_i \cap Q_j$, then $\bar{S}^a_n$ cannot be good (otherwise, SEQ^a would not be unique). Consequently, for each $a \in T_{\min}$ there is exactly one i_a such that $a \in Q_{i_a}$ and for all $b, b' \in a^=$ with $b \neq b'$ we have $i_b \neq i_{b'}$. Hence, if there are no good Q_i's, then t_0 cannot exceed $k_0 = |\,\mathrm{Eq}(n)|$. Let us now show that indeed, t_0 *must* exceed k_0: Recall that $n^\star = 2^{k_0}$ and that $(n+\ell+1)^\star$ is an integer power of 2, where $\ell+1 = m_T - n$. As a consequence of LEMMA 4.25, for any positive integer t we get:

$$\textit{If } n^\star = 2^k \textit{ and } (n+t)^\star = 2^{k'} \textit{ then } t \geq 2^k, \textit{ in particular } t > k\,. \qquad (\star)$$

For every $a \in T_{\min}$ with $|a^=| = t_0$, and for any $b \in \bar{S}^a \setminus S_n$, where $\bar{S}^b$ is not necessarily good, we have the following situation:

- $|\bar{S}^b| = n + t$ where $(n+t)^\star = 2^k$ for some $k > k_0$, and
- either $b \in a^=$ or $\bar{S}^b$ is not good.

Hence, for some integer $t' \geq 0$ we have

$$m_T = n + \ell + 1 = n + t' + t_0 = |\bar{S}^a|\,,$$

where $(n+t')^\star$ and $(n+t'+t_0)^\star$ are both integer powers of 2. Say $(n+t')^\star = 2^k$ and $(n+t'+t_0)^\star = 2^{k'}$ where $k' > k \geq k_0$. Then, by $(\star)$, $t_0 > k \geq k_0$ which completes the proof of the claim. $\dashv_{\text{Claim}}$

Since $f_0(Q_{j_0}) \notin \mathrm{seq}^{1\text{-}1}(S_n)$ there exists a first element a_n in the sequence $f_0(Q_{j_0})$ which does not belong to S_n. Let $s_{n+1} = s_n{}^\frown\langle a_n\rangle$. Then s_{n+1} is a non-repetitive sequence in A of length $n+1$, which is what we were aiming for. $\dashv$

To some extent, THEOREM 4.24 and THEOREM;4.26 are optimal, *i.e.*, there are no other relations between $\mathrm{seq}^{1\text{-}1}(\mathfrak{m})$, $\mathrm{seq}(\mathfrak{m})$, and $2^{\mathfrak{m}}$ which are provable in ZF (see Chapter 7 | RELATED RESULT 49). It might be tempting to prove that for all cardinals $\mathfrak{m}$, $\mathrm{seq}(\mathfrak{m}) \not< \mathrm{fin}(\mathfrak{m})$, however, such a proof cannot be carried out in ZF (*cf.* PROPOSITION 7.17).

$2^{2^{\mathfrak{m}}} + 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$ whenever $\mathfrak{m}$ is infinite

The fact that $2^{2^{\mathfrak{m}}} + 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$ whenever $\mathfrak{m}$ is infinite will turn out as a consequence of the following result:

LEMMA 4.27 (LÄUCHLI'S LEMMA). *If $\mathfrak{m}$ is an infinite cardinal, then*

$$\left(2^{\mathrm{fin}(\mathfrak{m})}\right)^{\aleph_0} = 2^{\mathrm{fin}(\mathfrak{m})}\,.$$

Proof. Let A be an arbitrary but fixed set of cardinality $\mathfrak{m}$. Recall that for $n \in \omega$, $[A]^n$ denotes the set of all n-element subsets of A. For natural numbers

$n, k \in \omega$, where $k \geq n$, we define two mappings $g_{n,k}$ and $d_{n,k}$ from $\mathscr{P}\big([A]^n\big)$ into itself as follows: For $X \subseteq [A]^n$ define

$$g_{n,k}(X) = \big\{y \in [A]^n : \forall z \in [A]^k\, \big(y \subseteq z \to \exists x \in X\, (x \subseteq z)\big)\big\}$$

and let $d_{n,k}(X) := g_{n,k}(X) \setminus X$. To get familiar with the functions $g_{n,k}$ and $d_{n,k}$ respectively, consider the following example: Let $n = 2$, $k = 4$, take $\{a_0, a_1\} \in [A]^2$, and let $X_0 = \big\{x \in [A]^2 : x \cap \{a_0, a_1\} = \emptyset\big\}$. Then $g_{2,4}(X_0) = [A]^2$ and $Y := d_{2,4}(X_0) = \big\{y \in [A]^2 : y \cap \{a_0, a_1\} \neq \emptyset\big\}$. Further, $g_{2,4}(Y) = Y$ and $d_{2,4}(Y) = d_{2,4}\big(d_{2,4}(X_0)\big) = \emptyset$. We leave it as an exercise to the reader to show that the mapping $g_{n,k}$ has the following properties:

(1) For all $X \subseteq [A]^n$, $X \subseteq g_{n,k}(X)$.

(2) $g_{n,k} \circ g_{n,k} = g_{n,k}$, i.e., for all $X \subseteq [A]^n$, $g_{n,k}\big(g_{n,k}(X)\big) = g_{n,k}(X)$.

(3) For all $X \subseteq [A]^n$, $g_{n,k}(X) \subseteq g_{n,k'}(X)$ whenever $k' \geq k$.

By induction on j we define $d^{j+1}_{n,k} := d_{n,k} \circ d^j_{n,k}$, where $d^0_{n,k}$ denotes the identity. Then, we have $d^{j+1}_{n,k} = \big(g_{n,k} \circ d^j_{n,k}\big) \setminus d^j_{n,k}$, and therefore by (1) we get

(4) $d^j_{n,k} = \big(g_{n,k} \circ d^j_{n,k}\big) \setminus d^{j+1}_{n,k}$.

In order to show that $d^n_{n,k} = g_{n,k} \circ d^n_{n,k}$ we first prove a combinatorial result by applying the Finite Ramsey Theorem 2.3.

For any fixed integers $n, k \in \omega$ where $k \geq n$, for $U \subseteq A$ with $|U| \leq n$, and for any $X \subseteq [A]^n$, let $\psi(U, X, W)$ and $\varphi(U, X)$ be the following statements:

$$\psi(U, X, W) \equiv W \subseteq A \setminus U \wedge \forall V \in [W]^{n-|U|}\, (U \cup V \in X)$$

and

$$\varphi(U, X) \equiv \forall m \in \omega\, \exists W \subseteq A\, \big(|W| \geq m \wedge \psi(U, X, W)\big)\,.$$

Notice that if $U \in X \subseteq [A]^n$, then we have $\psi(U, X, W)$ for every $W \subseteq A \setminus U$, and consequently we have $\varphi(U, X)$ for all $U \in X$. To get familiar with the statements ψ and φ respectively consider again the example given above: Let $b \in A \setminus \{a_0, a_1\}$ and let $U = \{a_0, b\}$. Then we have $\varphi\big(U, d_{2,4}(X_0)\big)$, since for any $m \in \omega$ we have $\psi\big(U, d_{2,4}(X_0), [A \setminus \{a_0, a_1, b\}]^m\big)$. Further, for $U' = \{b\} \subseteq U$ we have $\varphi(U', X_0)$, since for any positive $m \in \omega$ we have $\psi\big(U', X_0, [A \setminus \{a_0, a_1, b\}]^m\big)$.

Claim 1. *If we have $\varphi\big(U, d_{n,k}(X)\big)$, then there is a set U' with $|U'| < |U|$ such that we have $\varphi(U', X)$. In particular we get that $\varphi\big(\emptyset, d_{n,k}(X)\big)$ fails — a fact which can be easily verified directly.*

Proof of Claim 1. Let us assume that $\varphi\big(U, d_{n,k}(X)\big)$ holds for $U \subseteq A$ with $|U| \leq n$ and some set $X \subseteq [A]^n$. It is enough to show that for any integer $m \geq k$ there is a proper subset U' of U and a $W \in [A]^m$ such that $\psi(U', X, W)$ holds. Indeed, since there are just finitely many proper subsets of U, there must be a proper subset U' of U such that for arbitrarily large integers m there is a set $W_m \in [A]^m$ such that $\psi(U', X, W_m)$ holds, we get that $\varphi(U', X)$ holds.

Recall that by the FINITE RAMSEY THEOREM 2.3, for all $m, i, j \in \omega$, where $j \geq 1$ and $i \leq m$, there exists a smallest integer $N_{m,i,j} \geq m$ such that for each j-colouring of $[N]^i$ there is an m-element subset of N, all whose i-element subsets have the same colour. Let $m \geq k$, let $m' := \max\{N_{m,i,2} : 0 \leq i \leq n\}$, and let $m'' = N_{m',k-r,2^r}$ where $r = |U|$. By $\varphi\big(U, d_{n,k}(X)\big)$ there is a set S with $|S| = m''$ such that $\psi\big(U, d_{n,k}(X), S\big)$. To each subset U' of U we assign the set $X(U')$ by stipulating

$$X(U') = \big\{Y \in [S]^{k-r} : \exists V' \subseteq Y(U' \cup V' \in X)\big\}.$$

Now we show that $\bigcup_{U' \subseteq U} X(U') = [S]^{k-r}$: Let $V \in [S]^{k-r}$. By definition of $\psi\big(U, d_{n,k}(X), S\big)$, $S \subseteq A \setminus U$, and since $|U| = r$ we have $|U \cup V| = k$. Since $k - r \geq n - r$ there is a set $Q \in [V]^{n-r}$, and since $\psi\big(U, d_{n,k}(X), S\big)$ we get $U \cup Q \in d_{n,k}(X)$. Hence, by definition of $d_{n,k}$ and $g_{n,k}$ respectively, there is a set $x \in X$ such that $x \subseteq U \cup V$. If we let $U' = U \cap x$ and $V' = V \cap x$, then $U' \cup V' \in X$ and consequently $V \in X(U')$.

Because $|S| = m'' = N_{m',k-r,2^r}$, there is a set $T \in [S]^{m'}$ and a set $U' \subseteq U$ such that $[T]^{k-r} \subseteq X(U')$. Let $s = |U'|$, let

$$Z = \big\{V' \in [T]^{n-s} : U' \cup V' \in X\big\},$$

and let $Z' = [T]^{n-s} \setminus Z$. Since $|T| = m' \geq N_{m,n-s,2}$, there exists a set $W \in [T]^m$ such that either $[W]^{n-s} \subseteq Z$ or $[W]^{n-s} \subseteq Z'$. The latter case can be excluded. Indeed, since $m \geq k \geq k - r$, $[W]^{k-r} \neq \emptyset$. Now, each element w of $[W]^{k-r}$ is a subset of T and consequently an element of $X(U')$. Thus, there is a $V' \subseteq w$ such that $U' \cup V' \in X$ which implies that $V' \in Z$, in particular, $[W]^{n-s} \cap Z \neq \emptyset$. Hence, $[W]^{n-s} \subseteq Z$ and we finally have $\psi(U', X, W)$ where $|W| = m$.

It remains to show that $U' \neq U$: Since we have $\psi\big(U, d_{n,k}(X), S\big)$ and $W \subseteq S$, we also have $\psi\big(U, d_{n,k}(X), W\big)$. Now, if $U' = U$, then we would also have $\psi(U, X, W)$, but since $d_{n,k}(X) = g_{n,k}(X) \setminus X$, $d_{n,k}(X) \cap X = \emptyset$ which implies that the set $[W]^{n-r}$ is empty which is only the case when $|W| < n-r$; however, $|W| = m \geq k \geq n \geq n - r$. $\dashv_{\text{Claim 1}}$

Now we turn back to the sets $d^j_{n,k}(X)$ and show that $d^{n+1}_{n,k}(X) = \emptyset$. In fact we show a slightly stronger result:

CLAIM 2. *If $d^l_{n,k}(X) \neq \emptyset$ for some set $X \subseteq [A]^n$, then $l \leq n$.*

Proof of Claim 2. Take any $U \in d^l_{n,k}(X)$. Since $|U| = n$, for each set $W \subseteq A \setminus U$ we have $\psi\big(U, d^l_{n,k}(X), W\big)$, and since A is not finite we have $\varphi\big(U, d^l_{n,k}(X)\big)$. By applying CLAIM 1 l times we get a sequence $U = U_l, U_{l-1}, \ldots, U_0$ such that $|U_{j+1}| > |U_j|$ for all $j \in l$, which implies that $|U_j| \geq j$ (for all j's). In particular $|U| = |U_l| \geq l$, and since $|U| = n$ this implies that $l \leq n$. $\dashv_{\text{Claim 2}}$

As a consequence of CLAIM 2 we get

(5) $d^n_{n,k} = g_{n,k} \circ d^n_{n,k}$.

Define now a mapping $f_{n,k}$ from $\mathscr{P}\big([A]^n\big)$ to $\mathscr{P}\big([A]^k\big)$ by stipulating

$$f_{n,k}(X) = \big\{z \in [A]^k : \exists x \in X\,(x \subseteq z)\big\}\,.$$

Further, let

$$I_{n,k}(X) = \big\{X \subseteq [A]^n : g_{n,k}(X) = X\big\}\,.$$

Then, by (1) and (3) we get

(6) $I_{n,k'} \subseteq I_{n,k}$ whenever $k' \geq k$.

Consider now $\bar{f}_{n,k} := f_{n,k}|_{I_{n,k}}$. By definition of $g_{n,k}$ and $d_{n,k}$ respectively we have that $\bar{f}_{n,k}$ is injective. Indeed, if $X, X' \in I_{n,k}$ (*i.e.*, $g_{n,k}(X) = X$ and $g_{n,k}(X') = X'$) and $\bar{f}_{n,k}(X) = \bar{f}_{n,k}(X')$, then $X \subseteq g_{n,k}(X') = X'$ and $X' \subseteq g_{n,k}(X) = X$, and therefore $X = X'$. So, for sets in $\operatorname{dom}(\bar{f}_{n,k})$ we can define the inverse of $\bar{f}_{n,k}$ by stipulating

$$\bar{f}^{-1}_{n,k}\big(\bar{f}_{n,k}(X)\big) = X\,.$$

Now we are ready to construct a one-to-one mapping F from $\mathscr{P}\big(\operatorname{fin}(A)\big)^{\omega}$ into $\mathscr{P}\big(\operatorname{fin}(A)\big)$: Let $X \in \mathscr{P}\big(\operatorname{fin}(A)\big)^{\omega}$, *i.e.*, $X = \{X_s : s \in \omega\}$ where for each $s \in \omega$, $X_s \in \mathscr{P}\big(\operatorname{fin}(A)\big)$. Define the function F by stipulating

$$F(X) = \bigcup_{s\in\omega}\bigcup_{n\in\omega}\Big(\bigcup_{0\leq j\leq n} f_{n,k(s,n,j)} \circ g_{n,k(s,n,n)} \circ d^j_{n,k(s,n,n)}\big(X_s \cap [A]^n\big)\Big)$$

where $k(s,n,j) := 2^s \cdot 3^n \cdot 5^j$. By definition we get that F is a function from $\mathscr{P}\big(\operatorname{fin}(A)\big)^{\omega}$ to $\mathscr{P}\big(\operatorname{fin}(A)\big)$. So, it remains to show that F is injective. To keep the notation short let

$$\begin{aligned} X_{s,n} &= X_s \cap [A]^n\,, \\ X_{s,n,j} &= g_{n,k(s,n,n)} \circ d^j_{n,k(s,n,n)}(X_{s,n})\,, \\ Y_{s,n,j} &= f_{n,k(s,n,j)}(X_{s,n,j})\,. \end{aligned}$$

Then

$$F(X) = \bigcup_{s\in\omega}\bigcup_{n\in\omega}\Big(\bigcup_{0\leq j\leq n} Y_{s,n,j}\Big)\,.$$

Since $Y_{s,n,j} \in \mathscr{P}\big([A]^{k(s,n,j)}\big)$ and since the mapping $\langle s,n,j\rangle \mapsto k(s,n,j)$ is injective we get

$$Y_{s,n,j} = F(X) \cap [A]^{k(s,n,j)}\,.$$

By (2) we have $X_{s,n,j} \in I_{n,k(s,n,n)}$. Moreover, since $j \leq n$ we have $k(s,n,j) \leq k(s,n,n)$ and by (6) we get $X_{s,n,j} \in I_{n,k(s,n,j)}$. Thus, $Y_{s,n,j} = \bar{f}_{n,k(s,n,j)}(X_{s,n,j})$ and therefore

$$X_{s,n,j} = \bar{f}^{-1}_{n,k(s,n,j)}(Y_{s,n,j}) .$$

By (4) and (5) we get

$$X_{s,n} = X_{s,n,0} \setminus \Big(X_{s,n,1} \setminus \big(\cdots (X_{s,n,n-1} \setminus X_{s,n,n}) \cdots \big) \Big) ,$$

and since

$$X_s = \bigcup_{n\in\omega} X_{s,n}$$

we get that F is injective. This shows that $\big(2^{\mathrm{fin}(\mathfrak{m})}\big)^{\aleph_0} \leq 2^{\mathrm{fin}(\mathfrak{m})}$, and since we obviously have $2^{\mathrm{fin}(\mathfrak{m})} \leq \big(2^{\mathrm{fin}(\mathfrak{m})}\big)^{\aleph_0}$, by the CANTOR-BERNSTEIN THEOREM 3.17 we finally get $\big(2^{\mathrm{fin}(\mathfrak{m})}\big)^{\aleph_0} = 2^{\mathrm{fin}(\mathfrak{m})}$. ⊣

As a consequence of LÄUCHLI'S LEMMA 4.27 we get the following equality:

THEOREM 4.28. *If $\mathfrak{m}$ is an infinite cardinal, then $2^{\aleph_0} \cdot 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$, in particular we get $2^{2^{\mathfrak{m}}} + 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$.*

Proof. Let A be a set of cardinality $\mathfrak{m}$. Further, let $\mathrm{inf}(A) := \mathscr{P}(A) \setminus \mathrm{fin}(A)$ and let $\mathrm{inf}(\mathfrak{m}) := |\,\mathrm{inf}(A)|$. Then $2^{\mathfrak{m}} = \mathrm{fin}(\mathfrak{m}) + \mathrm{inf}(\mathfrak{m})$ and consequently

$$2^{2^{\mathfrak{m}}} = 2^{\mathrm{fin}(\mathfrak{m})+\mathrm{inf}(\mathfrak{m})} = 2^{\mathrm{fin}(\mathfrak{m})} \cdot 2^{\mathrm{inf}(\mathfrak{m})}.$$

Since by LÄUCHLI'S LEMMA 4.27, $2^{\mathrm{fin}(\mathfrak{m})} = \big(2^{\mathrm{fin}(\mathfrak{m})}\big)^2$, and by FACT 4.6, $2^{\mathrm{fin}(\mathfrak{m})} \geq 2^{\aleph_0}$, we have

$$2^{\mathrm{fin}(\mathfrak{m})} \cdot 2^{\mathrm{inf}(\mathfrak{m})} = \big(2^{\mathrm{fin}(\mathfrak{m})}\big)^2 \cdot 2^{\mathrm{inf}(\mathfrak{m})} = 2^{\mathrm{fin}(\mathfrak{m})} \cdot 2^{2^{\mathfrak{m}}} \geq 2^{\aleph_0} \cdot 2^{2^{\mathfrak{m}}},$$

and since $2^{2^{\mathfrak{m}}} \leq 2^{\aleph_0} \cdot 2^{2^{\mathfrak{m}}}$, by the CANTOR-BERNSTEIN THEOREM 3.17 we finally get $2^{\aleph_0} \cdot 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$. ⊣

NOTES

D-finite and transfinite sets. In [8, §5], Dedekind defined infinite and finite sets as follows: *A set S is called* infinite *when it is similar to a proper subset of itself; otherwise, S is said to be* finite. It is not hard to verify that Dedekind's definition of finite and infinite sets correspond to our definition of D-finite and transfinite sets respectively. In the footnote to his definition Dedekind writes: *In this form I communicated the definition of the infinite, which forms the core of my whole investigation, in September, 1882, to G. Cantor, and several years earlier to Schwarz and Weber.* More historical background can be found in Fraenkel [12, Ch. I., §2, 5.].

$\boldsymbol{\aleph_0 \leq 2^{\mathfrak{m}} \to 2^{\aleph_0} \leq 2^{\mathfrak{m}}}$. The proof of PROPOSITION 4.4 — which is Theorem 68 of Lindenbaum and Tarski [24] — is taken from Halbeisen [14, VIII] (see also Halbeisen and Shelah [17, Fact 8.1]); and for another proof see for example Sierpiński [34, VIII §2, Ex. 9].

$\aleph_1 \leq^* 2^{\aleph_0}$. The relation symbol "$\leq^*$" was introduced by Tarski (*cf.* Lindenbaum and Tarski [24, p. 301]). The proof of THEOREM 4.11 is essentially taken from Sierpiński [34, XV §2], and an alternative proof is given by Sierpiński [29]. LEMMA 4.10 is due to Lebesgue [22, p. 213 f.], and Church [7, Corollary 2, p. 183] showed that the set of all non-repetitive well-ordered sequences of natural numbers is of cardinality $2^{\aleph_0}$.

If the reals are a countable union of countable sets. PROPOSITION 4.12 is taken from Specker [36, III. §3], where one can find also some other implications like $\aleph_1 < \aleph_1^{\aleph_0}$, or that every subset of $\mathbb{R}$ is either finite or transfinite. COROLLARY 4.13 (*i.e.*, the paradoxical decomposition of $\mathbb{R}$) can also be found in Halbeisen and Shelah [18, Fact 8.6].

Cantor's Normal Form Theorem. The proof of CANTOR'S NORMAL FORM THEOREM 4.16 is taken from Cantor [4, §19, Satz B] (see also Cantor [6, p. 333 ff.]), but can also be found for example in Fraenkel [12, Ch. III, §11,Thm. 11]. For a slightly more general result see Bachmann [1, III. §12]. The proof of THEOREM 4.19 is taken from Halbeisen [14, VII] (*cf.* Specker [35]).

Other cardinal relations. THEOREM 4.20 — as well as the idea of getting a contradiction by constructing an injective class function from Ω into a given set — is due to Specker [35, p. 334 ff.] (*cf.* RELATED RESULT 21). THEOREM 4.21 and PROPOSITION 4.22 are due to Halbeisen [14, IX] (see also Halbeisen and Shelah [17, §2, Theorem 3 and p. 36]). LEMMA 4.23 and THEOREM 4.24 are due to Halbeisen [14, IX] (see also Halbeisen and Shelah [17, §3, Theorem 5]). The proof of THEOREM 4.26 is due to Shelah (see Halbeisen and Shelah [17, §3 Theorem 4]). LEMMA 4.25 is due to Halbeisen, who proved that number-theoretic result when THEOREM 4.26 was still a conjecture. For a generalisation of THEOREM 4.26 see RELATED RESULT 20. LÄUCHLI'S LEMMA 4.27 as well as THEOREM 4.28 is taken from Läuchli [21].

RELATED RESULTS

13. *Other definitions of finiteness.* Among the many definitions of finiteness we would like to mention just one by von Neumann who defined in [25, p. 736] finite sets as follows: *A set E is finite, if there is no non-empty set $K \subseteq \mathscr{P}(E)$ such that for each $x \in K$ there is a $y \in K$ with $|x| < |y|$.* With respect to this definition of finiteness, a set I is infinite *iff* for each natural number n there exists an n-element subset of I, or equivalently, a set E is finite *iff* there exists a bijection between E and a natural number n. However, notice that von Neumann does not use the notion of natural numbers in his definition. In [25, VIII. 2.], von Neumann investigated that notion of finiteness and showed for example that power sets of finite sets are finite. For some other definitions of finiteness and their dependencies we refer the reader to Kurepa [20], Lêvy [23], Schröder [27], Spišiak and Vojtáš [37], Tarski [38], and Truss [41].

14. *The countability of the rationals.* We have seen that the set of rational numbers is countable, but since we used the CANTOR-BERNSTEIN THEOREM 3.17 to construct a bijection between $\mathbb{Q}$ and ω, it is quite difficult to determine the image of a given rational number. However, there exists also a "computable" bijection

$f : \mathbb{Q} \to \omega$ due to Faber [10]: The image of a rational number q, written in the form

$$q = \frac{a_1}{2!} + \frac{a_2}{3!} + \cdots + \frac{a_n}{(n+1)!},$$

where the a_i's are computed by trigonometric series and for all $1 \leq i \leq n$ we have $0 \leq a_i < (i+1)!$, is defined by

$$f(q) = a_1 \cdot 1! + a_2 \cdot 2! + a_3 \cdot 3! + \ldots + a_n \cdot n!.$$

15. *Goodstein sequences.* For positive integers m and n, where $n > 1$, define the *hereditary base* n representation of m as follows. First write m as the sum of powers of n, *e.g.*, if $m = 265$ and $n = 2$ write $265 = 2^8 + 2^3 + 1$. Then write each exponent as the sum of powers of n and repeat with exponents of exponents and so on until the representation stabilises, *e.g.*, 265 stabilises at the representation $2^{2^{2+1}} + 2^{2+1} + 1$. Now define the number $G_n(m)$ as follows. If $m = 0$ let $G_n(0) := 0$; otherwise, let $G_n(m)$ be the number produced by replacing every occurrence of n in the hereditarily base n representation of m by the number $n+1$ and then subtracting 1, *e.g.*, $G_2(265) = 3^{3^{3+1}} + 3^{3+1}$. The *Goodstein sequence* $m_0, m_1, \ldots$ for m starting at 2 is defined as follows: $m_0 = m$, $m_1 = G_2(m_0)$, $m_2 = G_3(m_1)$, $m_3 = G_4(m_2)$, and so on; for example we get:

$$\begin{aligned}
265_0 &= 265 \\
&= 2^{2^{2+1}} + 2^{2+1} + 1 \\
265_1 &= 3^{3^{3+1}} + 3^{3+1} \\
265_2 &= 4^{4^{4+1}} + 4^{4+1} - 1 \\
&= 4^{4^{4+1}} + 4^4 \cdot 3 + 4^3 \cdot 3 + 4^2 \cdot 3 + 4 \cdot 3 + 3 \\
265_3 &= 5^{5^{5+1}} + 5^5 \cdot 3 + 5^3 \cdot 3 + 5^2 \cdot 3 + 5 \cdot 3 + 2 \\
265_4 &= 6^{6^{6+1}} + 6^6 \cdot 3 + 6^3 \cdot 3 + 6^2 \cdot 3 + 6 \cdot 3 + 1 \\
265_5 &= 7^{7^{7+1}} + 7^7 \cdot 3 + 7^3 \cdot 3 + 7^2 \cdot 3 + 7 \cdot 3 \\
265_6 &= 8^{8^{8+1}} + 8^8 \cdot 3 + 8^3 \cdot 3 + 8^2 \cdot 3 + 8 \cdot 3 - 1 \\
&= 8^{8^{8+1}} + 8^8 \cdot 3 + 8^3 \cdot 3 + 8^2 \cdot 3 + 8 \cdot 2 + 7 \\
265_7 &= \ \ldots
\end{aligned}$$

Computing a few of the numbers 265_k, one notices that the sequence 265_0, 265_1, $265_2, \ldots$ grows extremely fast and one would probably guess that it tends to infinity. Amazingly, Goodstein [13] showed that for every integer m there is a $k \in \omega$ such that $m_k = 0$. Indeed, if we replace in the hereditarily base n representation of m_{n-2} each n by ω, we get an ordinal number, say $\alpha_{n-2}(m)$; in fact we get $\operatorname{cnf}\big(\alpha_{n-2}(m)\big)$, *e.g.*, $\alpha_3(265) = \omega^{\omega^{\omega+1}} + \omega^\omega \cdot 3 + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 2$. We leave it as an exercise to the reader to show that the sequence of ordinal numbers $\alpha_0(m), \alpha_1(m), \alpha_2(m), \ldots$ is strictly decreasing. In other words, $\alpha_0(m) \ni \alpha_1(m) \ni \alpha_2(m) \ni \ldots$, thus, by the Axiom of Foundation, the sequence of ordinals must be finite which implies that the Goodstein sequence $m_0, m_1, \ldots$ is eventually zero. However, Kirby and Paris [19] showed that Goodstein's result is not provable in Peano Arithmetic (*cf.* also Paris [26]).

16. *Ordinal arithmetic.* As we have seen, one can define various arithmetical operations on ordinals like addition, multiplication and exponentiation, and even subtraction. Moreover, one can also define division (*cf.* Fraenkel [12, Ch. III., §11, 4.], Bachmann [1, III. §17], or Sierpiński [31]): For any given ordinals α and δ ($\delta \neq 0$) there is a single pair of ordinals β, ρ such that

$$\alpha = \delta \cdot \beta + \rho \quad \text{where } \rho < \delta .$$

For the theory of ordinal arithmetic we refer the reader to Bachmann [1, III.] (*cf.* also Sierpiński [32, 33]).

17. *Cancellation laws.* Bernstein showed in his dissertation [2] (see [3, §2, Satz 3]) that for any finite cardinal $\mathfrak{a} \geq 1$ and arbitrary cardinals $\mathfrak{m}$ and $\mathfrak{n}$ we have

$$\mathfrak{a} \cdot \mathfrak{m} = \mathfrak{a} \cdot \mathfrak{n} \rightarrow \mathfrak{m} = \mathfrak{n} .$$

In fact, Bernstein gave a quite involved proof for the case $\mathfrak{a} = 2$ ([3, §2, Satz 2]) and just outlined the proof for the general case. Later, Sierpiński [28] found a simpler proof for the case $\mathfrak{a} = 2$ and generalised the result in [30] to $(2 \cdot \mathfrak{m} \leq 2 \cdot \mathfrak{n}) \rightarrow (\mathfrak{m} \leq \mathfrak{n})$. Slightly later, Tarski showed in [39] that for any finite cardinal $\mathfrak{a} \geq 1$ and arbitrary cardinals $\mathfrak{m}$ and $\mathfrak{n}$ we have

$$\mathfrak{a} \cdot \mathfrak{m} \leq \mathfrak{a} \cdot \mathfrak{n} \rightarrow \mathfrak{m} \leq \mathfrak{n} .$$

18. *On the cardinality of power sets of power sets**. As a consequence of THEOREM 4.28 we get

$$2^{2^{2^{\mathfrak{m}}}} \times 2^{2^{2^{\mathfrak{m}}}} = 2^{2^{2^{\mathfrak{m}}}} .$$

However, it is open if also $2^{2^{\mathfrak{m}}} \times 2^{2^{\mathfrak{m}}} = 2^{2^{\mathfrak{m}}}$ is provable in ZF.

19. *The hierarchy of* $\aleph$*'s.* By induction on Ω we define

$$\begin{aligned} \aleph_0 &= |\omega| , \\ \aleph_{\alpha+1} &= \aleph(\aleph_\alpha) , \\ \aleph_\lambda &= \bigcup_{\alpha \in \lambda} \aleph_\alpha \quad \textit{for infinite limit ordinals } \lambda. \end{aligned}$$

For an ordinal α, let A be a set of cardinality $\aleph_\alpha$ and let γ_0 be the order type of a well-ordering of A. Then, since $|\gamma_0| = \aleph_\alpha$, γ_0 is an ordinal of cardinality $\aleph_\alpha$, and we define

$$\omega_\alpha = \bigcap \{\gamma \in \gamma_0 + 1 : |\gamma| = \aleph_\alpha\} .$$

20. *On the cardinality of the set of non-repetitive sequences**. Let $\mathfrak{m}$ be an infinite cardinal an let S be a set of cardinality $\mathfrak{m}$. We defined $2^{\mathfrak{m}} = |\mathscr{P}(S)|$, however, $2^{\mathfrak{m}}$ can also be considered as the cardinality of the set of functions from S to $\{0, 1\}$. Similarly, for natural numbers $a \geq 2$ let $\mathfrak{a}^{\mathfrak{m}}$ denote the cardinality of the set of functions from S to $\{0, 1, \dots a - 1\}$. By THEOREM 4.26 we have $2^{\mathfrak{m}} \neq \operatorname{seq}^{1\text{-}1}(\mathfrak{m})$ and it is natural to ask whether the following statement is provable in ZF:

For all finite cardinals $\mathfrak{a}$ *and all infinite cardinals* $\mathfrak{m}$, $\mathfrak{a}^{\mathfrak{m}} \neq \operatorname{seq}^{1\text{-}1}(\mathfrak{m})$. (❁)

Obviously, if we would have a suitable generalisation of LEMMA 4.25 at hand, then the proof of THEOREM 4.26 would work for all natural numbers $a \geq 2$.

Halbeisen and Hungerbühler investigated in [16] the function $n^{\star}$ and generalised LEMMA 4.25 to numbers different from 2, and this generalisation was later used by Halbeisen [15] who showed that (❀) holds for a large class of finite cardinals, *e.g.*, for $\mathfrak{a} \in \{2,3,4,6,7,8,9,11,12,14,15,\dots\}$; it is conjectured that (❀) holds for all finite cardinals $\mathfrak{a} \geq 2$.

21. *On the cardinality of the set of ordered pairs**. By CANTOR'S THEOREM 3.25 we always have $2^{\mathfrak{m}} \not\leq^* \mathfrak{m}$. Furthermore, one can show that if there is a finite-to-one map from $2^{\mathfrak{m}}$ onto $\mathfrak{m}$, then $\mathfrak{m}$ is finite (see Forster [11]). Now, having THEOREM 4.20 in mind, one could ask whether $2^{\mathfrak{m}} \leq^* \mathfrak{m}^2 \to \mathfrak{m} \leq 4$. This question is still open and is asked in Truss [40], where a dualisation of THEOREM 4.20 is investigated.

References

1. HEINZ BACHMANN, ***Transfinite Zahlen***, Springer-Verlag, Berlin · Heidelberg, 1967.
2. FELIX BERNSTEIN, *Untersuchungen aus der Mengelehre*, Dissertation (1901), University of Göttingen (Germany).
3. ———, *Untersuchungen aus der Mengelehre*, ***Mathematische Annalen***, vol. 61 (1905), 117–155.
4. GEORG CANTOR, *Beiträge zur Begründung der transfiniten Mengenlehre. I./ II.*, ***Mathematische Annalen***, vol. 46/49 (1895/1897), 481–512/207–246 (see [5] for a translation into English).
5. ———, ***Contributions to the Founding of the Theory of Transfinite Numbers,*** (translation into English of [4]), [translated, and provided with an introduction and notes, by Philip E. B. Jourdain], Open Court Publishing Company, Chicago and London, 1915 [reprint: Dover Publications, New York, 1952].
6. ———, ***Gesammelte Abhandlungen mathematischen und philosophischen Inhalts***, *Mit Erläuternden Anmerkungen sowie mit Ergänzungen aus dem Briefwechsel Cantor-Dedekind*, edited by E. Zermelo, Julius Springer, Berlin, 1932.
7. ALONZO CHURCH, *Alternatives to Zermelo's assumption*, ***Transactions of the American Mathematical Society***, vol. 29 (1927), 178–208.
8. RICHARD DEDEKIND, ***Was sind und was sollen die Zahlen***, Friedrich Vieweg & Sohn, Braunschweig, 1888 (see also [9, pp. 335–390]).
9. ———, ***Gesammelte mathematische Werke III***, edited by R. Fricke, E. Noether, and Ö. Ore, Friedrich Vieweg & Sohn, Braunschweig, 1932.
10. GEORG FABER, *Über die Abzählbarkeit der rationalen Zahlen*, ***Mathematische Annalen***, vol. 60 (1905), 196–203.
11. THOMAS E. FORSTER, *Finite-to-one maps*, ***The Journal of Symbolic Logic***, vol. 68 (2003), 1251–1253.
12. ABRAHAM A. FRAENKEL, ***Abstract Set Theory***, [Studies in Logic and the Foundations of Mathematics], North-Holland, Amsterdam, 1961.
13. REUBEN L. GOODSTEIN, *On the restricted ordinal theorem*, ***The Journal of Symbolic Logic***, vol. 9 (1944), 33–41.
14. LORENZ HALBEISEN, *Vergleiche zwischen unendlichen Kardinalzahlen in einer Mengenlehre ohne Auswahlaxiom*, Diplomarbeit (1990), University of Zürich (Switzerland).

15. ———, *A number-theoretic conjecture and its implication for set theory*, ***Acta Mathematica Universitatis Comenianae***, vol. 74 (2005), 243–254.
16. Lorenz Halbeisen and Norbert Hungerbühler, *Number theoretic aspects of a combinatorial function*, ***Notes on Number Theory and Discrete Mathematics***, vol. 5 (1999), 138–150.
17. Lorenz Halbeisen and Saharon Shelah, *Consequences of arithmetic for set theory*, ***The Journal of Symbolic Logic***, vol. 59 (1994), 30–40.
18. ———, *Relations between some cardinals in the absence of the axiom of choice*, ***The Bulletin of Symbolic Logic***, vol. 7 (2001), 237–261.
19. Lauri Kirby and Jeff B. Paris, *Accessible independence results for Peano arithmetic*, ***Bulletin of the London Mathematical Society***, vol. 14 (1982), 285–293.
20. Djuro (George) Kurepa, *On a characteristic property of finite sets*, ***Pacific Journal of Mathematics***, vol. 2 (1952), 323–326.
21. Hans Läuchli, *Ein Beitrag zur Kardinalzahlarithmetik ohne Auswahlaxiom*, ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik***, vol. 7 (1961), 141–145.
22. Henri Lebesgue, *Sur les fonctions représentables analytiquement*, ***Journal de Mathématiques Pures et Appliquées (6ème série)***, vol. 1 (1905), 139–216.
23. Azriel Lévy, *The independence of various definitions of finiteness*, ***Fundamenta Mathematicae***, vol. 46 (1958), 1–13.
24. Adolf Lindenbaum and Alfred Tarski, *Communication sur les recherches de la théorie des ensembles*, ***Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III***, vol. 19 (1926), 299–330.
25. John von Neumann, *Die Axiomatisierung der Mengenlehre*, ***Mathematische Zeitschrift***, vol. 27 (1928), 669–752.
26. Jeff B. Paris, *Combinatorial statements independent of arithmetic*, in ***Mathematics of Ramsey Theory*** (J. Nešetřil and V. Rödl, eds.), Springer-Verlag, Berlin, 1990, pp. 232–245.
27. Ernst Schröder, *Über zwei Definitionen der Endlichkeit und G. Cantor'sche Sätze*, ***Nova Acta, Abhandlungen der Kaiserlich Leopoldinisch-Carolinisch Deutschen Akademie der Naturforscher***, vol. 71 (1898), 301–362.
28. Wacław Sierpiński, *Sur l'égalité $2\mathfrak{m} = 2\mathfrak{n}$ pour les nombres cardinaux*, ***Fundamenta Mathematicae***, vol. 3 (1922), 1–6.
29. ———, *Sur une décomposition effective d'ensembles*, ***Fundamenta Mathematicae***, vol. 29 (1937), 1–4.
30. ———, *Sur l'implication $(2\mathfrak{m} \leq 2\mathfrak{n}) \rightarrow (\mathfrak{m} \leq \mathfrak{n})$ pour les nombres cardinaux*, ***Fundamenta Mathematicae***, vol. 34 (1946), 148–154.
31. ———, *Sur la division des types ordinaux*, ***Fundamenta Mathematicae***, vol. 35 (1948), 1–12.
32. ———, *Sur les types d'ordre des ensembles linéaires*, ***Fundamenta Mathematicae***, vol. 37 (1950), 253–264.
33. ———, *Sur un type ordinal dénombrable qui a une infinite indénombrable de divisenrs gauches*, ***Fundamenta Mathematicae***, vol. 37 (1950), 206–208.
34. ———, ***Cardinal and Ordinal Numbers***, Państwowe Wydawnictwo Naukowe, Warszawa, 1958.
35. Ernst Specker, *Verallgemeinerte Kontinuumshypothese und Auswahlaxiom*, ***Archiv der Mathematik***, vol. 5 (1954), 332–337.

36. ———, *Zur Axiomatik der Mengenlehre (Fundierungs- und Auswahlaxiom)*, ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik***, vol. 3 (1957), 173–210.
37. Ladislav Spišiak and Peter Vojtáš, *Dependences between definitions of finiteness*, ***Czechoslovak Mathematical Journal***, vol. 38(113) (1988), 389–397.
38. Alfred Tarski, *Sur les ensembles finis*, ***Fundamenta Mathematicae***, vol. 6 (1924), 45–95.
39. ———, *Cancellation laws in the arithmetic of cardinals*, ***Fundamenta Mathematicae***, vol. 36 (1949), 77–92.
40. John K. Truss, *Dualisation of a result of Specker's*, ***Journal of the London Mathematical Society (2)***, vol. 6 (1973), 286–288.
41. ———, *Classes of Dedekind finite cardinals*, ***Fundamenta Mathematicae***, vol. 84 (1974), 187–208.

5

The Axiom of Choice

Two terms occasionally used by musicians are "full" consonance and "pleasing" consonance.
An interval is said to be "fuller" than another when it has greater power to satisfy the ear.
Consonances are the more "pleasing" as they depart from simplicity, which does not delight our senses much.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

Zermelo's Axiom of Choice and its Consistency with ZF

In 1904, Zermelo published his first proof that every set can be well-ordered. The proof is based on the so-called Axiom of Choice, denoted AC, which, in Zermelo's words, states that *the product of an infinite totality of sets, each containing at least one element, itself differs from zero* (*i.e.*, the empty set). The full theory $\mathsf{ZF} + \mathsf{AC}$, denoted ZFC, is called *Set Theory*.

In order to state the Axiom of Choice we first define the notion of a choice function: If $\mathscr{F}$ is a family of non-empty sets (*i.e.*, $\emptyset \notin \mathscr{F}$), then a **choice function** for $\mathscr{F}$ is a function $f : \mathscr{F} \to \bigcup \mathscr{F}$ such that for each $x \in \mathscr{F}$, $f(x) \in x$.

The Axiom of Choice — which completes the axiom system of Set Theory and which is in our counting the ninth axiom of ZFC — states as follows:

9. The Axiom of Choice

$$\forall \mathscr{F} \Big(\emptyset \notin \mathscr{F} \to \exists f \big(f \in {}^{\mathscr{F}}\bigcup \mathscr{F} \wedge \forall x \in \mathscr{F} \left(f(x) \in x \right) \big) \Big)$$

Informally, every family of non-empty sets has a choice function, or equivalently, every Cartesian product of non-empty sets is non-empty.

Before we give some reformulations of the Axiom of Choice and show some of its consequences, we should address the question whether AC is consistent relative to the other axioms of Set Theory (*i.e.*, relative to ZF), which is indeed the case.

Assume that ZF is consistent, then, by PROPOSITION 3.5, ZF has a model, say $\mathbf{V}$. To obtain the relative consistency of AC with ZF, we have to show that also ZF + AC has a model. In 1935, Gödel informed von Neumann at the Institute for Advanced Study in Princeton that he had found such a model. In fact he showed that there exists a smallest transitive subclass of $\mathbf{V}$ which contains all ordinals (*i.e.*, contains Ω as a subclass) in which AC as well as ZF holds. This unique submodel of $\mathbf{V}$ is called the **constructible universe** and is denoted by $\mathbf{L}$, where "L" stands for the following "law" by which the constructible universe is built. Roughly speaking, the model $\mathbf{L}$ consists of all "mathematically constructible" sets, or in other words, all sets which are "constructible" or "describable", but nothing else. To be more precise, let us give the following definitions:

Let M be a set and $\varphi(x_0,\dots,x_n)$ be a first-order formula in the language $\{\in\}$. Then φ^M denotes the formula we obtain by replacing all occurrences of "$\exists x$" and "$\forall x$" by "$\exists x \in M$" and "$\forall x \in M$" respectively. A subset $y \subseteq M$ is **definable over** M if there is a first-order formula $\varphi(x_0,\dots,x_n)$ in the language $\{\in\}$, and parameters $a_1,\dots,a_n$ in M, such that $\{z : \varphi^M(z,a_1,\dots,a_n)\} = y$. Finally, for any set M:

$$\operatorname{def}(M) = \{y \subseteq M : y \text{ is definable over } M\}$$

Notice that for any set M, $\operatorname{def}(M)$ is a set being itself a subset of $\mathscr{P}(M)$. Now, by induction on $\alpha \in \Omega$, define the following sets (compare with the cumulative hierarchy defined in Chapter 3):

$$\begin{aligned} \mathrm{L}_0 &= \emptyset \\ \mathrm{L}_\alpha &= \textstyle\bigcup_{\beta\in\alpha}\mathrm{L}_\beta \qquad \text{if } \alpha \text{ is a limit ordinal} \\ \mathrm{L}_{\alpha+1} &= \operatorname{def}(\mathrm{L}_\alpha) \end{aligned}$$

and let

$$\mathbf{L} = \bigcup_{\alpha\in\Omega} \mathrm{L}_\alpha \,.$$

Like for the cumulative hierarchy one can show that for each $\alpha \in \Omega$, L_α is a transitive set, $\alpha \subseteq \mathrm{L}_\alpha$ and $\alpha \in \mathrm{L}_{\alpha+1}$, and that $\alpha \in \beta$ implies $\mathrm{L}_\alpha \subsetneq \mathrm{L}_\beta$.

Moreover, Gödel showed that $\mathbf{L} \vDash$ ZF + AC, and that $\mathbf{L}$ is the smallest transitive class containing Ω as a subclass such that $\mathbf{L} \vDash$ ZFC. Thus, by starting with any model $\mathbf{V}$ of ZF we find a subclass $\mathbf{L}$ of $\mathbf{V}$ such that $\mathbf{L} \vDash$ ZFC. In other words we get that if ZF is consistent then so is ZFC (roughly speaking, if ZFC is inconsistent, then AC cannot be blamed for it).

Equivalent Forms of the Axiom of Choice

There are dozens of hypotheses which are equivalent to the Axiom of Choice, but among the best known and most popular ones are surely the Well-Ordering Principle, the Kuratowski-Zorn Lemma, Kurepa's Principle, and Teichmüller's Principle — sometimes called Tukey's Lemma. Since the first three deal with orderings, we have to introduce first the corresponding definitions before we can state these — and some other — so-called *choice principles*.

A binary relation "$\leq$" on a set P is a **partial ordering** of P if it is transitive (*i.e.*, $p \leq q$ and $q \leq r$ implies $p \leq r$), reflexive (*i.e.*, $p \leq p$ for every $p \in P$), and anti-symmetric (*i.e.*, $p \leq q$ and $q \leq p$ implies $p = q$). If "$\leq$" is a partial ordering on P, then $(P, \leq)$ is called a **partially ordered set**.

If $(P, \leq)$ is a partially ordered set, then we define

$$p < q \iff p \leq q \wedge p \neq q\,,$$

and call $(P, <)$ a partially ordered in the **strict sense**, (replacing reflexivity by $p \not< p$ for every $p \in P$).

Two distinct elements $p, q \in P$, where $(P, <)$ is a partially ordered set, are said to be **comparable** if either $p < q$ or $q < p$; otherwise, they are called **incomparable**. Notice that for $p, q \in P$ we could have $p \not\leq q$ as well as $p \not\geq q$. However, if for any elements p and q of a partially ordered set $(P, <)$ we have $p < q$ or $p = q$ or $p > q$ (where these three cases are mutually exclusive), then P is said to be **linearly ordered** by the **linear ordering** "$<$". Two elements p_1 and p_2 of P are called **compatible** if there exists a $q \in P$ such that $p_1 \leq q \geq p_2$; otherwise they are called **incompatible**, denoted $p_1 \perp p_2$.

We would like to mention that in the context of forcing, elements of partially ordered sets are called *conditions*. Furthermore, it is worth mentioning that the definition of "compatible" given above incorporates a convention, namely the so-called *Jerusalem convention for forcing* — with respect to the American convention of forcing, p_1 and p_2 are compatible if there exists a q such that $p_1 \geq q \leq p_2$.

Let $(P, <)$ be a partially ordered set. Then $p \in P$ is called **maximal** (or more precisely $<$-maximal) in P if there is no $x \in P$ such that $p < x$. Similarly, $q \in P$ is called **minimal** (or more precisely $<$-minimal) in P if there is no $x \in P$ such that $x < q$. Furthermore, for a non-empty subset $C \subseteq P$, an element $p' \in P$ is said to be an **upper bound** of C if for all $x \in C$, $x \leq p'$.

A non-empty set $C \subseteq P$, where $(P, <)$ is a partially ordered set, is a **chain** in P if C is linearly ordered by "$<$" (*i.e.*, for any distinct members $p, q \in C$ we have either $p < q$ or $p > q$). Conversely, if $A \subseteq P$ is such that any two distinct elements of A are incomparable (*i.e.*, neither $p < q$ nor $p > q$), then in Order Theory, A is called an anti-chain. However, in the context of forcing we say that a subset $A \subseteq P$ is an **anti-chain** in P if any two distinct elements of A are *incompatible*. Furthermore, $A \subseteq P$ is a **maximal anti-chain** in P if A is an anti-chain in P and A is maximal with this property. Notice that if $A \subseteq P$

is a maximal anti-chain, then for every $p \in P \setminus A$ there is a $q \in A$ such p and q are compatible.

Recall that a binary relation R on a set P is a *well-ordering* on P, if there is an ordinal $\alpha \in \Omega$ and a bijection $f : P \to \alpha$ such that $R(x, y)$ *iff* $f(x) \in f(y)$. This leads to the following equivalent definition of a well-ordering, where the equivalence follows from the proof of THEOREM 5.1 (the details are left to the reader): Let $(P, <)$ be a linearly ordered set. Then "$<$" is a **well-ordering** on P if every non-empty subset of P has a $<$-minimal element. Furthermore, a set P is said to be **well-orderable** (or equivalently, P can be well-ordered) if there exists a well-ordering on P.

In general, it is not possible to define a well-ordering by a first-order formula on a given set (*e.g.*, on $\mathbb{R}$). However, the existence of well-ordering is guaranteed by the following principle:

Well-Ordering Principle: Every set can be well-ordered.

To some extent, the Well-Ordering Principle (like the Axiom of Choice) postulates the existence of certain sets whose existence in general (*i.e.*, without any further assumptions like $\mathbf{V} = \mathbf{L}$), cannot be proved within ZF.

In particular, the Well-Ordering Principle postulates the existence of well-orderings of $\mathbb{Q}$ and of $\mathbb{R}$. Obviously, both sets are linearly ordered by "$<$". However, since for any elements x and y with $x < y$ there exists a z such that $x < z < y$, the ordering '$<$" is far away from being a well-ordering — consider for example the set of all positive elements. Even though $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ have similar properties (at least from an order-theoretical point of view), when we try to well-order these sets they behave very differently. Firstly, by FACT 4.1 we know that $\mathbb{Q}$ is countable and the bijection $f : \mathbb{Q} \to \omega$ allows us to define a well-ordering "$\prec$" on $\mathbb{Q}$ by stipulating $q \prec p \iff f(q) < f(p)$. Now, let us consider the set $\mathbb{R}$. For example we could first well-order the rational numbers, or even the algebraic numbers, and then try to extend this well-ordering to all real numbers. However, this attempt — as well as all other attempts — to construct explicitly a well-ordering of the reals will end in failure (the reader is invited to verify this claim by writing down explicitly some orderings of $\mathbb{R}$).

As mentioned above, Zermelo proved in 1904 that the Axiom of Choice implies the Well-Ordering Principle. In the proof of this result presented here we shall use the ideas of Zermelo's original proof.

THEOREM 5.1. *The* Well-Ordering Principle *is equivalent to the* Axiom of Choice.

Proof. ($\Leftarrow$) Let M be a set. If $M = \emptyset$, then M is already well-ordered. So, assume that $M \neq \emptyset$ and let $\mathscr{P}^*(M) := \mathscr{P}(M) \setminus \{\emptyset\}$. Further, let $f : \mathscr{P}^*(M) \to M$ be an arbitrary but fixed choice function for $\mathscr{P}^*(M)$ (which exists by AC).

A one-to-one function $w_\alpha : \alpha \hookrightarrow M$, where $\alpha \in \Omega$, is an f-set if for all $\gamma \in \alpha$:

$$w_\alpha(\gamma) = f\big(M \setminus \{w_\alpha(\delta) : \delta \in \gamma\}\big)$$

For example $w_1(0) = f(M)$ is an f-set, in fact, w_1 is the unique f-set with domain $\{0\}$. Further, by HARTOGS' THEOREM 3.27, the collection of all f-sets is a *set*, say S. Define the ordering "$\prec$" on S as follows: For two distinct f-sets w_α and w_β let $w_\alpha \prec w_\beta$ if $\alpha \neq \beta$ and $w_\beta|_\alpha = w_\alpha$. Notice that $w_\alpha \prec w_\beta$ implies $\alpha \in \beta$.

CLAIM. *The set S of all f-sets is well-ordered by "$\prec$".*

Proof of Claim. Let w_α and w_β be any two f-sets and let

$$\Gamma = \big\{\gamma \in (\alpha \cap \beta) : w_\alpha(\gamma) \neq w_\beta(\gamma)\big\}.$$

If $\Gamma \neq \emptyset$, then, for $\gamma_0 = \bigcap \Gamma$, we have $w_\alpha(\gamma_0) \neq w_\beta(\gamma_0)$. On the other hand, for all $\delta \in \gamma_0$ we have $w_\alpha(\delta) = w_\beta(\delta)$, thus, by the definition of f-sets, we get $w_\alpha(\gamma_0) = w_\beta(\gamma_0)$. Hence, $\Gamma = \emptyset$, and consequently we are in exactly one of the following three cases:

- $w_\alpha \prec w_\beta$ *iff* $\alpha \in \beta$.
- $w_\alpha = w_\beta$ *iff* $\alpha = \beta$.
- $w_\beta \prec w_\alpha$ *iff* $\beta \in \alpha$.

Thus, the ordering "$\prec$" on S corresponds to the ordering of the ordinals by "$\in$", and since the latter relation is a well-ordering on Ω, the ordering "$\prec$" is a well-ordering, too. $\dashv_{\text{Claim}}$

Now, let $w := \bigcup S$ and let $M' := \big\{x \in M : \exists \gamma \in \operatorname{dom}(w)\,\big(w(\gamma) = x\big)\big\}$. Then $w \in S$ and $M' = M$; otherwise, w can be extended to the f-set $w \cup \big\{\langle \operatorname{dom}(w), f(M \setminus M')\rangle\big\}$.

Thus, the one-to-one function $w : \operatorname{dom}(w) \to M$ is onto, or in other words, M is well-orderable.

($\Rightarrow$) Let $\mathscr{F}$ be any family of non-empty sets and let "$<$" be any well-ordering on $\bigcup \mathscr{F}$. Define $f : \mathscr{F} \to \bigcup \mathscr{F}$ by stipulating $f(x)$ being the $<$-minimal element of x. $\dashv$

It turns out that in many cases, the Well-Ordering Principle — mostly in combination with transfinite induction — is easier to apply than the Axiom of Choice. For example in order to prove that every vector space has an algebraic basis, we would first well-order the set of vectors and then build a basis by transfinite induction (*i.e.*, for every vector v_α we check whether it is in the linear span of the vectors $\{v_\beta : \beta \in \alpha\}$, and if it is not, we mark it as a vector of the basis). However, similarly to the well-ordering of $\mathbb{R}$, in many cases it is not possible to write down explicitly an algebraic basis of a vector space. For example consider the real vector space of all countably infinite sequences of real numbers, or any infinite dimensional Banach space.

The following three principles, which will be shown to be equivalent to the Axiom of Choice, are quite popular in Algebra and Topology. Even though these principles look rather different, all state that certain sets have maximal elements or subsets (with respect to some partial ordering), and so they are usually called *maximality principles*. Let us first state the Kuratowski-Zorn Lemma and Kurepa's Principle.

> Kuratowski-Zorn Lemma: If $(P, \leq)$ is a non-empty partially ordered set such that every chain in P has an upper bound, then P has a maximal element.

> Kurepa's Principle: Each partially ordered set has a maximal subset of pairwise incomparable elements.

In order to state Teichmüller's Principle we have to introduce one more notion: A family $\mathscr{F}$ of sets is said to have **finite character** if for each set x, $x \in \mathscr{F}$ *iff* $\operatorname{fin}(x) \subseteq \mathscr{F}$ (*i.e.*, every finite subset of x belongs to $\mathscr{F}$).

> Teichmüller's Principle: Let $\mathscr{F}$ be a non-empty family of sets. If $\mathscr{F}$ has finite character, then $\mathscr{F}$ has a maximal element (maximal with respect to inclusion "$\subseteq$").

Below we shall see that the three maximality principles are all equivalent to the Axiom of Choice. However, in order to prove directly that the Axiom of Choice implies the Kuratowski-Zorn Lemma (*i.e.*, without using the Well-Ordering Principle), we have to show first the following interesting lemma — which is the main reason why we do not want to derive the Kuratowski-Zorn Lemma from the Well-Ordering Principle, even though this would be much easier.

LEMMA 5.2. *Let $(P, \leq)$ be a non-empty partially ordered set. If there is a function $b : \mathscr{P}(P) \to P$ which assigns to every chain C an upper bound $b(C)$, and if $f : P \to P$ is a function such that for all $x \in P$ we have $x \leq f(x)$, then there is a $p_0 \in P$ such that $p_0 = f(p_0)$.*

Proof. Notice that because every well-ordered set is a chain, it is enough to require the existence of an upper bound $b(W)$ just for every set $W \subseteq P$ which is *well-ordered* by "$<$". If $W \subseteq P$ is a well-ordered subset of P and $x \in W$, then $W_x := \{y \in W : y < x\}$. A well-ordered set $W \subseteq P$ is called an f-chain, if for all $x \in W$ we have $x = f\bigl(b(W_x)\bigr)$. Notice that since $\emptyset \subseteq P$ is well-ordered by "$<$", the set $\bigl\{f\bigl(b(\emptyset)\bigr)\bigr\}$ is an f-chain.

We leave it as an exercise to the reader to verify that the set of f-chains is well-ordered by proper inclusion "$\subsetneq$". Hence, the set

$$U = \bigcup \bigl\{W \subseteq P : W \textit{ is an } f\textit{-chain}\bigr\}$$

is itself an f-chain. Consider $p_0 := f\bigl(b(U)\bigr)$ and notice that $U \cup \{p_0\}$ is an f-chain. By the definition of U we get that $p_0 \in U$, and consequently we have $f\bigl(b(U_{p_0})\bigr) = p_0$. Now, since $f\bigl(b(U_{p_0})\bigr) \geq b(U_{p_0}) \geq p_0$, we must have $b(U_{p_0}) = p_0$, and therefore $f(p_0) = p_0$. $\dashv$

Notice that the proof of LEMMA 5.2 does not rely on any choice principles.

Now we are ready to prove that the Kuratowski-Zorn Lemma and Teichmüller's Principle are both equivalent to the Axiom of Choice.

THEOREM 5.3. *The following statements are equivalent:*

(a) Axiom of Choice.

(b) Kuratowski-Zorn Lemma.

(c) Teichmüller's Principle.

Proof. (a)⇒(b) Let $(P, \leq)$ be a non-empty partially ordered set such that every chain in P, (in particular every well-ordered chain), has an upper bound. Then, for every non-empty well-ordered subset $W \subseteq P$, the set of upper bounds $B_W := \{p \in P : \forall x \in W(x \leq p)\}$ is non-empty. Thus, the family

$$\mathscr{F} = \{B_W : W \textit{ is a well-ordered, non-empty subset of } P\}$$

is a family of non-empty sets and therefore, by the Axiom of Choice, for each $W \in \mathscr{F}$ we can pick an element $b(W) \in B_W$. Now, for every $x \in P$ let

$$M_x = \begin{cases} \{x\} & \text{if } x \text{ is maximal in } P, \\ \{y \in P : y > x\} & \text{otherwise.} \end{cases}$$

Then $\{M_x : x \in P\}$ is a family of non-empty sets and again by the Axiom of Choice, there is a function $f : P \to P$ such that

$$f(x) = \begin{cases} x & \text{if } x \text{ is maximal in } P, \\ y & \text{where } y > x. \end{cases}$$

Since $f(x) \geq x$ (for all $x \in P$) and every non-empty well-ordered subset $W \subseteq P$ has an upper bound $b(W)$, we can apply LEMMA 5.2 and get an element $p_0 \in P$ such that $f(p_0) = p_0$, hence, P has a maximal element.

(b)⇒(c) Let $\mathscr{F}$ be a non-empty family of sets and assume that $\mathscr{F}$ has finite character. Obviously, $\mathscr{F}$ is partially ordered by inclusion "$\subseteq$". For every chain $\mathscr{C}$ in $\mathscr{F}$ let $U_{\mathscr{C}} = \bigcup \mathscr{C}$. Then every finite subset of $U_{\mathscr{C}}$ belongs to $\mathscr{F}$, thus, $U_{\mathscr{C}}$ belongs to $\mathscr{F}$. On the other hand, $U_{\mathscr{C}}$ is obviously an upper bound of $\mathscr{C}$. Hence, every chain has an upper bound and we may apply the Kuratowski-Zorn Lemma and get a maximal element of the family $\mathscr{F}$.

(c)⇒(a) Given a family $\mathscr{F}$ of non-empty sets. We have to find a choice function for $\mathscr{F}$. Consider the family

$$\mathscr{E} = \{f : f \textit{ is a choice function for some subfamily } \mathscr{F}' \subseteq \mathscr{F}\}.$$

Notice that f is a choice function if and only if every finite subfunction of f is a choice function. Hence, $\mathscr{E}$ has finite character. Thus, by Teichmüller's Principle, the family $\mathscr{E}$ has a maximal element, say f_0. Since f_0 is maximal, $\operatorname{dom}(f_0) = \mathscr{F}$, and therefore f_0 is a choice function for $\mathscr{F}$. ⊣

In order to prove that also Kurepa's Principle is equivalent to the Axiom of Choice, we have to change the setting a little bit: In the proof of THEOREM 5.3, as well as in Zermelo's proof of THEOREM 5.1, the Axiom of Foundation was not involved (in fact, the proofs can be carried out in Cantor's Set Theory). However, without the aid of the Axiom of Foundation it is not possible to prove that Kurepa's Principle implies the Axiom of Choice, whereas the converse implication is evident (compare the following theorem with Chapter 7 | RELATED RESULT 46).

THEOREM 5.4. *The following statements are equivalent in* ZF*:*

(a) Axiom of Choice.

(b) Every vector space has an algebraic basis.

(c) Multiple Choice*: For every family $\mathscr{F}$ of non-empty sets, there exists a function $f : \mathscr{F} \to \mathscr{P}\big(\bigcup \mathscr{F}\big)$ such that for each $X \in \mathscr{F}$, $f(X)$ is a non-empty finite subset of X.*

(d) Kurepa's Principle.

Proof. (a)⇒(b) Let V be a vector space and let $\mathscr{F}$ be the family of all sets of linearly independent vectors of V. Obviously, $\mathscr{F}$ has finite character. So, by Teichmüller's Principle, which is, as we have seen in THEOREM 5.3 equivalent to the Axiom of Choice, $\mathscr{F}$ has a maximal element. In other words, there is a maximal set of linearly independent vectors, which must be of course a basis of V.

(b)⇒(c) Let $\mathscr{F} = \{X_\iota : \iota \in I\}$ be a family of non-empty sets. We have to construct a function $f : \mathscr{F} \to \mathscr{P}\big(\bigcup \mathscr{F}\big)$ such that for each $X_\iota \in \mathscr{F}$, $f(X_\iota)$ is a non-empty finite subset of X_ι. Without loss of generality we may assume that the members of $\mathscr{F}$ are pairwise disjoint (if necessary, consider the family $\big\{X_\iota \times \{X_\iota\} : \iota \in I\big\}$ instead of $\mathscr{F}$). Adjoin all the elements of $X := \bigcup \mathscr{F}$ as indeterminates to some arbitrary but fixed field $\mathbb{F}$ (*e.g.*, $\mathbb{F} = \mathbb{Q}$) and consider the field $\mathbb{F}(X)$ consisting of all rational functions of the "variables" in X with coefficients in $\mathbb{F}$. For each $\iota \in I$, we define the *ι-degree* of a monomial — *i.e.*, a term of the form $ax_1^{k_1} \cdots x_l^{k_l}$ where $a \in \mathbb{F}$ and $x_1, \dots, x_l \in X$ — to be the sum of the exponents of members of X_ι in that monomial. A rational function $q \in \mathbb{F}(X)$ is called *ι-homogeneous of degree d* if it is the quotient of two polynomials such that all monomials in the denominator have the same ι-degree n, while all those in the numerator have ι-degree $n + d$. The rational functions that are ι-homogeneous of degree 0 for all $\iota \in I$ form a subfield $\mathbb{F}_0$ of $\mathbb{F}(X)$. Thus, $\mathbb{F}(X)$ is a vector space over $\mathbb{F}_0$, and we let V be the subspace spanned by the set X.

By assumption, the $\mathbb{F}_0$-vector space V has an algebraic basis, say B. Below we use this basis B to explicitly define the desired function $f : \mathscr{F} \to \mathscr{P}\big(\bigcup \mathscr{F}\big)$. For each $\iota \in I$ and each $x \in X_\iota$ we can express x as a finite linear combination of elements of B. Thus, every $x \in X_\iota$ can be written in the form

$$x = \sum_{b \in B(x)} a_b^x \cdot b \,,$$

where $B(x) \in \mathit{fin}(B)$ and for all $b \in B(x)$, $a_b^x \in \mathbb{F}_0 \setminus \{0\}$. If y is another element of the same X_ι as x, then we have on the one hand

$$y = \sum_{b' \in B(y)} a_{b'}^y \cdot b' \,,$$

and on the other hand, after multiplying the above representation of x by the element $\frac{y}{x} \in \mathbb{F}_0$, we get

$$y = \sum_{b \in B(x)} \left(\tfrac{y}{x} \cdot a_b^x\right) \cdot b \,.$$

Comparing these two expressions for y and using the fact that B is a basis, *i.e.*, that the representation of y is unique, we must have

$$B(x) = B(y) \quad \text{and} \quad a_b^y = \frac{y}{x} \cdot a_b^x \ \text{ for all } b \in B(x).$$

Hence, the *finite* subset $B(x)$ of B as well as the elements $\frac{a_b^x}{x}$ of $\mathbb{F}(X)$ depend only on ι, not on the particular $x \in X_\iota$, and we therefore call them B_ι and a_b^ι respectively. Notice that, since $a_b^x \in \mathbb{F}_0$, a_b^ι is ι-homogeneous of degree -1 (and ι'-homogeneous of degree 0 for $\iota' \neq \iota$). So, when a_b^ι is written as a quotient of polynomials in reduced form, some variables from X_ι must occur in the denominator. Define $f(X_\iota)$ to be the set of all those members of X_ι that occur in the denominator of a_b^ι (in reduced form) for some $b \in B_\iota$. Then $f(X_\iota)$ is a non-empty finite subset of X_ι, as required.

(c)⇒(d) Let $(P, <)$ be a partially ordered set. By Multiple Choice, there is a function f such that for each non-empty set $X \subseteq P$, $f(X)$ is a non-empty finite subset of X. Let $g : \mathscr{P}(P) \to \mathit{fin}(P)$ be such that $g(\emptyset) := \emptyset$ and for each non-empty $X \subseteq P$, $g(X) := \big\{y \in f(X) : y \text{ is } {<}\text{-minimal in } f(X)\big\}$. Obviously, for every non-empty $X \subseteq P$, $g(X)$ is a non-empty finite set of pairwise incomparable elements. Using the function g we construct by transfinite induction a maximal subset of pairwise incomparable elements: Let $\mathscr{A}_0 := g(P)$, and for $\alpha \in \Omega$ let $\mathscr{A}_\alpha := g(X_\alpha)$, where

$$X_\alpha := \big\{x \in P : x \textit{ is incomparable with each } a \in \textstyle\bigcup\{\mathscr{A}_\beta : \beta \in \alpha\}\big\}\,.$$

By construction, the $\mathscr{A}_\alpha$'s are pairwise disjoint and any union of $\mathscr{A}_\alpha$'s is a set of pairwise incomparable elements. Again by construction there must be an $\alpha_0 \in \Omega$ such that $X_{\alpha_0} = \emptyset$. Thus, $\bigcup\{\mathscr{A}_\beta : \beta \in \alpha_0\} \subseteq P$ is a maximal set of pairwise incomparable elements.

(d)⇒(a) By the Axiom of Foundation, for every set x there exists an ordinal $\alpha \in \Omega$ such that $x \subseteq \mathrm{V}_\alpha$. Thus, since the Axiom of Choice is equivalent to the Well-Ordering Principle (see THEOREM 5.1), it is enough to show that Kurepa's Principle implies that for every $\alpha \in \Omega$, V_α can be well-ordered. The crucial point in that proof is to show that power sets of well-orderable sets are well-orderable.

The first step is quite straightforward: Let Q be a well-orderable set and let "$<_Q$" be a well-ordering on Q. We define a linear ordering "$\prec$" on $\mathscr{P}(Q)$ by stipulating $x \prec y$ *iff* the $<_Q$-minimal element of the symmetric difference $x \triangle y$ belongs to x. To see that "$\prec$" is a linear ordering, notice that "$\prec$" is just the lexicographic ordering on $\mathscr{P}(Q)$ induced by "$<_Q$". The following claim is where Kurepa's Principle comes in.

CLAIM. Kurepa's Principle *implies that every linearly orderable set is well-orderable.*

Proof of Claim. Let $(P, \prec)$ be a linearly ordered set. Consider the set W of all pairs (X, x) where $X \subseteq P$ and $x \in X$. On W we define a partial ordering "$<$" by stipulating

$$(X, x) < (Y, y) \iff X = Y \wedge x \prec y .$$

By Kurepa's Principle, $(W, <)$ has a maximal set of pairwise incomparable elements, say $\mathscr{A} \subseteq W$. For every non-empty set $X \subseteq P$ let $f(X)$ be the unique element of X such that $\big(X, f(X)\big) \in \mathscr{A}$. It is not hard to verify that f is a choice function for $\mathscr{P}(P) \setminus \{\emptyset\}$, and consequently, P can be well-ordered. $\dashv_{\text{Claim}}$

Now we are ready to show that Kurepa's Principle implies that every set V_α $(\alpha \in \Omega)$ can be well-ordered. We consider the following two cases:

α successor ordinal: Let $\alpha = \beta_0 + 1$ and assume that V_{β_0} is well-orderable. Then $\mathrm{V}_\alpha = \mathscr{P}(\mathrm{V}_{\beta_0})$, and as the power set of a well-orderable set, V_α is well-orderable.

α limit ordinal: Assume that for each $\beta \in \alpha$, V_β is well-orderable, *i.e.*, for each $\beta \in \alpha$ there exists a well-ordering "$<_\beta$" on V_β. Let ξ be the least ordinal such that there is no injection from ξ into V_α. The ordinal ξ exists by HARTOGS' THEOREM 3.27 and since every V_β can be well-ordered. Since ξ is well-ordered by $\in$, $\mathscr{P}(\xi)$ can be well-ordered; let us fix a well-ordering $\prec_\xi \subseteq \big(\mathscr{P}(\xi) \times \mathscr{P}(\xi)\big)$. For every $\beta \in \alpha$ we choose a well-ordering "$<_\beta$" on V_β as follows:

- If $\beta = 0$, then $<_0 = \emptyset$.
- If $\beta = \bigcup_{\delta \in \beta} \delta$ is a limit ordinal, then, for $x, y \in \mathrm{V}_\beta$, let

  $$x <_\beta y \iff \rho(x) \in \rho(y) \vee \big(\rho(x) = \rho(y) \wedge x <_{\rho(x)} y\big) ,$$

  where for any z, $\rho(z) := \bigcap\{\gamma \in \Omega : x \in \mathrm{V}_\gamma\}$.
- If $\beta = \delta + 1$ is a successor ordinal, then, by the choice of ξ, there is an injection $f : \mathrm{V}_\delta \hookrightarrow \xi$. Let $x = \operatorname{ran}(f)$; then $x \subseteq \xi$. Further, there exists a bijection between $\mathscr{P}(\mathrm{V}_\delta) = \mathrm{V}_\beta$ and $\mathscr{P}(x)$, and since $\mathscr{P}(x) \subseteq \mathscr{P}(\xi)$ and $\mathscr{P}(\xi)$ is well-ordered by "$\prec_\xi$", the restriction of "$\prec_\xi$" to $\mathscr{P}(x)$ induces a well-ordering on V_β.

Thus, for every $\beta \in \alpha$ we have a well-ordering "$<_\beta$" on V_β. Now, for $x, y \in \mathrm{V}_\alpha$ define

$$x <_\alpha y \iff \rho(x) \in \rho(y) \vee \big(\rho(x) = \rho(y) \wedge x <_{\rho(x)} y\big)\,.$$

Then, by construction, "$<_\alpha$" is a well-ordering on V_α. $\dashv$

We conclude this section on equivalent forms of AC by giving three cardinal relations which are equivalent to the Well-Ordering Principle.

THEOREM 5.5. *Each of the following statements is equivalent to the* Well-Ordering Principle, *and consequently to the* Axiom of Choice*:*

(a) Every cardinal $\mathfrak{m}$ *is an aleph, i.e., contains a well-orderable set.*

(b) Trichotomy of Cardinals*: If* $\mathfrak{n}$ *and* $\mathfrak{m}$ *are any cardinals, then* $\mathfrak{n} < \mathfrak{m}$ *or* $\mathfrak{n} = \mathfrak{m}$ *or* $\mathfrak{n} > \mathfrak{m}$*, where these three cases are mutually exclusive.*

(c) If $\mathfrak{n}$ *and* $\mathfrak{m}$ *are any cardinals, then* $\mathfrak{n} \leq^* \mathfrak{m}$ *or* $\mathfrak{m} \leq^* \mathfrak{n}$*.*

(d) If $\mathfrak{m}$ *is any infinite cardinal, then* $\mathfrak{m}^2 = \mathfrak{m}$*.*

Proof. (a) If every set is well-orderable, then obviously every cardinal contains an well-orderable set and is therefore an aleph. On the other hand, for an arbitrary set x let $\mathfrak{m} = |x|$ and let $y_0 \in \mathfrak{m}$ be well-orderable. By definition of $\mathfrak{m}$ there exists a bijection between y_0 and x, and therefore, x is well-orderable as well.

(b) Firstly notice that any two alephs are comparable. Thus, by (a) we get that the Well-Ordering Principle implies the Trichotomy of Cardinals and consequently so does AC. On the other hand, by HARTOGS' THEOREM 3.27 we know that for every cardinal $\mathfrak{m}$ there is a smallest aleph, denoted $\aleph(\mathfrak{m})$, such that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$. Now, if any two cardinals are comparable we must have $\mathfrak{m} < \aleph(\mathfrak{m})$, which implies that $\mathfrak{m}$ is an aleph.

(c) Notice that if every set can be well-ordered, then for any cardinals $\mathfrak{n}$ and $\mathfrak{m}$ we have $\mathfrak{n} \leq^* \mathfrak{m}$ *iff* $\mathfrak{n} \leq \mathfrak{m}$. For the other direction we first prove that for any cardinal $\mathfrak{m}$ there exists an aleph $\aleph'(\mathfrak{m})$ such that $\aleph'(\mathfrak{m}) \not\leq^* \mathfrak{m}$: Notice that if there exists a surjection from a set A onto a set B, then there exist an injection from B into $\mathscr{P}(A)$. So, by definition of $\aleph(2^{\mathfrak{m}})$ we have $\aleph(2^{\mathfrak{m}}) \not\leq^* \mathfrak{m}$. Let now $\mathfrak{m}$ be an arbitrary cardinal and let $\mathfrak{n} = \aleph(2^{\mathfrak{m}})$. If $\mathfrak{n} \leq^* \mathfrak{m}$ or $\mathfrak{n} \geq^* \mathfrak{m}$, then we must have $\mathfrak{n} \geq^* \mathfrak{m}$ (since $\mathfrak{n} \not\leq^* \mathfrak{m}$), which implies that $\mathfrak{m}$ is an aleph and completes the proof.

(d) Assume that for any infinite cardinal $\mathfrak{n}$ we have $\mathfrak{n}^2 = \mathfrak{n}$. Hence, we get $\mathfrak{m}+\aleph(\mathfrak{m}) = (\mathfrak{m}+\aleph(\mathfrak{m}))^2 = \mathfrak{m}^2+(\mathfrak{m}+\mathfrak{m})\cdot\aleph(\mathfrak{m})+\aleph(\mathfrak{m})^2 = \mathfrak{m}+\aleph(\mathfrak{m})+\mathfrak{m}\cdot\aleph(\mathfrak{m})$, and since $\mathfrak{m} + \aleph(\mathfrak{m}) \leq \mathfrak{m} \cdot \aleph(\mathfrak{m})$ we have

$$\mathfrak{m} + \aleph(\mathfrak{m}) = \mathfrak{m} \cdot \aleph(\mathfrak{m})\,.$$

Now, let $x \in \mathfrak{m}$ and let $y_0 \in \aleph(\mathfrak{m})$ be a set which is well-ordered by "$<_{y_0}$". Without loss of generality we may assume that x and y_0 are disjoint. Since $|x \cup y_0| = |x \times y_0|$, there exists a bijection $f : x \cup y_0 \to x \times y_0$. Using the bijection f we define $\tilde{x} := \big\{a \in x : \exists b \in y_0\, (\langle a, b\rangle \in f[y_0])\big\} \subseteq x$. Firstly notice that $\tilde{x} = x$. Indeed, if there would be an $a_0 \in x \setminus \tilde{x}$, then for all $b \in y_0$

we have $f^{-1}\big(\langle a_0, b\rangle\big) \notin y_0$, i.e., $f^{-1}\big(\langle a_0, b\rangle\big) \in x$. Thus, since f is bijective, $f^{-1}\big[\{a_0\} \times y_0\big] \subseteq x$ is a set of cardinality $\aleph(\mathfrak{m})$, contradicting the fact that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$. So, for every $a \in x$, the set

$$u_a := \{b \in y_0 : \exists b' \in y_0\,(f(b) = \langle a, b'\rangle)\}$$

is a non-empty subset of y_0, and — since y_0 is well-ordered by "$<_{y_0}$" — has a $<_{y_0}$-minimal element, say μ_a. Finally, define an ordering "$<$" on x by stipulating $a < a'$ *iff* $\mu_a <_{y_0} \mu_{a'}$. It is easily checked that "$<$" is a well-ordering on x, and therefore, $\mathfrak{m}$ is an aleph.

The converse implication — namely that the Well-Ordering Principle implies that $\mathfrak{m}^2 = \mathfrak{m}$ for every infinite cardinal $\mathfrak{m}$ — is postponed to the next section (see THEOREM 5.7). ⊣

Cardinal Arithmetic in the Presence of AC

In the presence of AC we are able to define cardinal numbers as ordinals: For any set A we define

$$|A| = \bigcap\big\{\alpha \in \Omega : \textit{there is a bijection between } \alpha \textit{ and } A\big\}.$$

Recall that AC implies that every set A is well-orderable and that every well-ordering of A corresponds to exactly one ordinal (which is the order type of the well-ordering).

For example we have $|n| = n$ for every $n \in \omega$, and $|\omega| = \omega$. However, for $\alpha \in \Omega$ we have in general $|\alpha| \neq \alpha$, e.g., $|\omega + 1| = \omega$.

Ordinal numbers $\kappa \in \Omega$ such that $|\kappa| = \kappa$ are called **cardinal numbers**, or just **cardinals**, and are usually denoted by Greek letters like κ, λ, μ, *et cetera*.

A cardinal κ is infinite if $\kappa \notin \omega$, otherwise, it is finite. In other words, a cardinal is finite if and only if it is a natural number.

Since cardinal numbers are just a special kind of ordinals, they are well-ordered by "$\in$". However, for cardinal numbers κ and λ we usually write $\kappa < \lambda$ instead of $\kappa \in \lambda$, thus,

$$\kappa < \lambda \iff \kappa \in \lambda\,.$$

Let κ be a cardinal. The smallest cardinal number which is greater than κ is denoted by κ^+, thus,

$$\kappa^+ = \bigcap\big\{\alpha \in \Omega : \kappa < |\alpha|\big\}.$$

Notice that by CANTOR'S THEOREM 3.25, for every cardinal κ there is a cardinal $\lambda > \kappa$, in particular, for every cardinal κ, $\bigcap\big\{\alpha \in \Omega : \kappa < |\alpha|\big\}$ is non-empty and therefore κ^+ exists.

A cardinal μ is called a **successor cardinal** if there exists a cardinal κ such that $\mu = \kappa^+$; otherwise, it is called a **limit cardinal**. In particular, every positive number $n \in \omega$ is a successor cardinal and ω is the smallest non-zero limit cardinal. By induction on $\alpha \in \Omega$ we define $\omega_{\alpha+1} := \omega_\alpha^+$, where $\omega_0 := \omega$, and $\omega_\alpha := \bigcup_{\delta\in\alpha} \omega_\delta$ for limit ordinals α; notice that $\bigcup_{\delta\in\alpha} \omega_\delta$ is a cardinal. In particular, ω_ω is the smallest uncountable limit cardinal and $\omega_1 = \omega_0^+$ is the smallest uncountable cardinal. Further, the collection $\{\omega_\alpha : \alpha \in \Omega\}$ is the class of all infinite cardinals, *i.e.*, for every infinite cardinal κ there is an $\alpha \in \Omega$ such that $\kappa = \omega_\alpha$. Notice that the collection of cardinals is — like the collection of ordinals — a proper *class* and not a *set*.

Cardinal addition, multiplication, and exponentiation is defined as follows:

Cardinal addition: For cardinals κ and μ let $\kappa + \mu := \big|(\kappa \times \{0\}) \,\dot\cup\, (\mu \times \{1\})\big|$.

Cardinal multiplication: For cardinals κ and μ let $\kappa \cdot \mu := |\kappa \times \mu|$.

Cardinal exponentiation: For cardinals κ and μ let $\kappa^\mu := \big|{}^\mu\kappa\big|$.

Since for any set A, $\big|{}^A 2\big| = \big|\mathscr{P}(A)\big|$, the cardinality of the power set of a cardinal κ is usually denoted by 2^κ. However, because 2^ω is the cardinality of the so-called *continuum* $\mathbb{R}$, it is usually denoted by $\mathfrak{c}$. Notice that by CANTOR'S THEOREM 3.25 for all cardinals κ we have $\kappa < 2^\kappa$.

As a consequence of the definition we get the following

FACT 5.6. *Addition and multiplication of cardinals is associative and commutative and we have the distributive law for multiplication over addition, and for all cardinals κ, λ, μ, we have*

$$\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu, \quad \kappa^{\mu\cdot\lambda} = \big(\kappa^\lambda\big)^\mu, \quad (\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu.$$

Proof. It is obvious that addition and multiplication is associative and commutative and that we have the distributive law for multiplication over addition. Now, let κ, λ, μ, be any cardinal numbers. Firstly, for every function $f : \big(\lambda \times \{0\}\big) \cup \big(\mu \times \{1\}\big) \to \kappa$ let the functions $f_\lambda : \big(\lambda \times \{0\}\big) \to \kappa$ and $f_\mu : \big(\mu \times \{1\}\big) \to \kappa$ be such that for each $x \in \big(\lambda \times \{0\}\big) \cup \big(\mu \times \{1\}\big)$,

$$f(x) = \begin{cases} f_\lambda(x) & \text{if } x \in \lambda \times \{0\}, \\ f_\mu(x) & \text{if } x \in \mu \times \{1\}. \end{cases}$$

It is easy to see that each function $f : \big(\lambda \times \{0\}\big) \cup \big(\mu \times \{1\}\big) \to \kappa$ corresponds to a unique pair $\langle f_\lambda, f_\mu\rangle$, and vice versa, each pair $\langle f_\lambda, f_\mu\rangle$ defines uniquely a function $f : \big(\lambda \times \{0\}\big) \cup \big(\mu \times \{1\}\big) \to \kappa$. Thus, we have a bijection between $\kappa^{\lambda+\mu}$ and $\kappa^\lambda \cdot \kappa^\mu$.

Secondly, for every function $f : \mu \to {}^\lambda\kappa$ let $\tilde{f} : \mu \times \lambda \to \kappa$ be such that for all $\alpha \in \mu$ and all $\beta \in \lambda$ we have

$$\tilde{f}\big(\langle\alpha, \beta\rangle\big) = f(\alpha)(\beta)\,.$$

We leave it as an exercise to the reader to verify that the mapping

$$\begin{aligned} {}^{\mu}\big({}^{\lambda}\kappa\big) &\longrightarrow {}^{\mu\times\lambda}\kappa \\ f &\longmapsto \tilde{f} \end{aligned}$$

is bijective, and therefore we have $\kappa^{\mu\cdot\lambda} = \big(\kappa^{\lambda}\big)^{\mu}$.

Thirdly, for every function $f : \mu \to \kappa \times \lambda$ let the functions $f_\kappa : \mu \to \kappa$ and $f_\lambda : \mu \to \lambda$ be such that for each $\alpha \in \mu$, $f(\alpha) = \big\langle f_\kappa(\alpha), f_\lambda(\alpha)\big\rangle$. We leave it again as an exercise to the reader to show that the mapping

$$\begin{aligned} {}^{\mu}(\kappa\times\lambda) &\longrightarrow {}^{\mu}\kappa \times {}^{\mu}\lambda \\ f &\longmapsto \langle f_\kappa, f_\lambda\rangle \end{aligned}$$

is a bijection. ⊣

The next result completes the proof of THEOREM 5.5.(d):

THEOREM 5.7. *For any ordinal numbers $\alpha, \beta \in \Omega$ we have:*

$$\omega_\alpha + \omega_\beta = \omega_\alpha \cdot \omega_\beta = \omega_{\alpha\cup\beta} = \max\{\omega_\alpha, \omega_\beta\}$$

In particular, for every infinite cardinal κ we have $\kappa^2 = \kappa$.

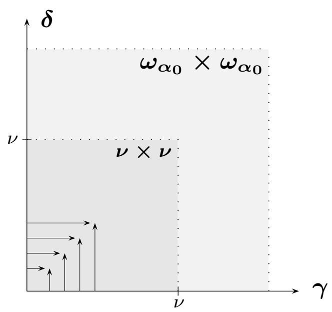
Proof. It is enough to show that for all $\alpha \in \Omega$ we have $\omega_\alpha \cdot \omega_\alpha = \omega_\alpha$. For $\alpha = 0$ we already know that $|\omega \times \omega| = \omega$, thus, $\omega_0 \cdot \omega_0 = \omega_0$. Assume towards a contradiction that there exists a $\beta_0 \in \Omega$ such that $\omega_{\beta_0} \cdot \omega_{\beta_0} > \omega_{\beta_0}$. Let

$$\alpha_0 = \bigcap \big\{\alpha \in \beta_0 + 1 : \omega_\alpha \cdot \omega_\alpha > \omega_\alpha\big\}\,.$$

On $\omega_{\alpha_0} \times \omega_{\alpha_0}$ we define an ordering "$<$" by stipulating

$$\langle\gamma_1,\delta_1\rangle < \langle\gamma_2,\delta_2\rangle \iff \begin{cases} \gamma_1\cup\delta_1 \in \gamma_2\cup\delta_2\,, \ \textit{or} \\ \gamma_1\cup\delta_1 = \gamma_2\cup\delta_2 \wedge \gamma_1 \in \gamma_2\,, \ \textit{or} \\ \gamma_1\cup\delta_1 = \gamma_2\cup\delta_2 \wedge \gamma_1 = \gamma_2 \wedge \delta_1 \in \delta_2\,. \end{cases}$$

This linear ordering can be visualised as follows:



It is easily verified that "<" is a well-ordering on $\omega_{\alpha_0} \times \omega_{\alpha_0}$. Now, let ρ be the order type of the well-ordering "<" and let $\Gamma : \omega_{\alpha_0} \times \omega_{\alpha_0} \to \rho$ be the unique order preserving bijection between $\omega_{\alpha_0} \times \omega_{\alpha_0}$ and ρ, *i.e.*, $\langle \gamma_1, \delta_1 \rangle < \langle \gamma_2, \delta_2 \rangle$ *iff* $\Gamma\big(\langle \gamma_1, \delta_1 \rangle\big) \in \Gamma\big(\langle \gamma_2, \delta_2 \rangle\big)$. Because $\omega_{\alpha_0} \cdot \omega_{\alpha_0} > \omega_{\alpha_0}$ we have $|\rho| > \omega_{\alpha_0}$. Now, by the definition of the well-ordering "<", there are $\gamma_0, \delta_0 \in \omega_{\alpha_0}$ such that $\Gamma\big(\langle \gamma_0, \delta_0 \rangle\big) = \omega_{\alpha_0}$ and for $\nu = \gamma_0 \cup \delta_0$ we have $|\nu \times \nu| \geq \omega_{\alpha_0}$. Thus, for $\omega_\beta = |\nu|$ we have $\omega_\beta < \omega_{\alpha_0}$ (since $\nu \in \omega_{\alpha_0}$) and $\omega_\beta \cdot \omega_\beta \geq \omega_{\alpha_0}$. In particular, $\omega_\beta \cdot \omega_\beta > \omega_\beta$, which is a contradiction to the choice of α_0. ⊣

As a consequence of THEOREM 5.7 we get the following

COROLLARY 5.8. *If κ is an infinite cardinal, then* $\operatorname{seq}(\kappa) = \kappa$ *and* $\kappa^\kappa = 2^\kappa$.

Proof. Firstly we have $\operatorname{seq}(\kappa) = \big|\bigcup_{n\in\omega} \kappa^n\big| = 1 + \kappa + \kappa^2 + \ldots = 1 + \kappa \cdot \omega = \kappa$. Secondly, by definition we have $\kappa^\kappa = |{}^\kappa\kappa|$. By identifying each function $f \in {}^\kappa\kappa$ by its graph, which is a subset of $\kappa \times \kappa$, we get $|{}^\kappa\kappa| \leq |\mathscr{P}(\kappa \times \kappa)|$, and since $|\kappa \times \kappa| = \kappa$ we finally have $\kappa^\kappa \leq |\mathscr{P}(\kappa)| = 2^\kappa$. ⊣

Let λ be an infinite limit ordinal. A subset $\mathcal{C}$ of λ is called **cofinal** in λ if $\bigcup \mathcal{C} = \lambda$. The **cofinality** of λ, denoted $\operatorname{cf}(\lambda)$, is the cardinality of a smallest cofinal set $\mathcal{C} \subseteq \lambda$. In other words,

$$\operatorname{cf}(\lambda) = \min\big\{|\mathcal{C}| : \mathcal{C} \textit{ is cofinal in } \lambda\big\}.$$

Notice that by definition, $\operatorname{cf}(\lambda)$ is always a cardinal number.

Let again λ be an infinite limit ordinal and let $\mathcal{C} = \big\{\beta_\xi : \xi \in \operatorname{cf}(\lambda)\big\} \subseteq \lambda$ be cofinal in λ. Now, for every $\nu \in \operatorname{cf}(\lambda)$ let $\alpha_\nu := \bigcup\{\beta_\xi : \xi \in \nu\}$ (notice that all the α_ν's belong to λ). Then $\big\langle \alpha_\nu : \nu \in \operatorname{cf}(\lambda)\big\rangle$ is an increasing sequence (not necessarily in the strict sense) of length $\operatorname{cf}(\lambda)$ with $\bigcup\big\{\alpha_\nu : \nu \in \operatorname{cf}(\lambda)\big\} = \lambda$. Thus, instead of cofinal *subsets* of λ we could equally well work with cofinal *sequences*.

Since every infinite cardinal is an infinite limit ordinal, $\operatorname{cf}(\kappa)$ is also defined for cardinals κ. An infinite *cardinal* κ is called **regular** if $\operatorname{cf}(\kappa) = \kappa$; otherwise, κ is called **singular**. For example ω is regular and ω_ω is singular (since $\{\omega_n : n \in \omega\}$ is cofinal in ω_ω). In general, for non-zero limit ordinals λ we have $\operatorname{cf}(\omega_\lambda) = \operatorname{cf}(\lambda)$. For example $\operatorname{cf}(\omega_\omega) = \operatorname{cf}(\omega_{\omega+\omega}) = \operatorname{cf}(\omega_{\omega_{\omega_\omega}}) = \omega$.

FACT 5.9. *For all infinite limit ordinals λ, the cardinal* $\operatorname{cf}(\lambda)$ *is regular.*

Proof. Let $\kappa = \operatorname{cf}(\lambda)$ and let $\big\langle \alpha_\xi : \xi \in \kappa\big\rangle$ be an increasing, cofinal sequence of λ. Further, let $\mathcal{C} \subseteq \kappa$ be cofinal in κ with $|\mathcal{C}| = \operatorname{cf}(\kappa)$. Now, $\langle \alpha_\nu : \nu \in \mathcal{C}\rangle$ is still a cofinal sequence of λ, which implies that $\operatorname{cf}(\lambda) \leq \operatorname{cf}(\kappa)$. On the other hand we have $\operatorname{cf}(\kappa) \leq \kappa = \operatorname{cf}(\lambda)$. Hence, $\operatorname{cf}(\kappa) = \kappa = \operatorname{cf}(\lambda)$, which shows that $\operatorname{cf}(\lambda)$ is regular. ⊣

The following result — which implicitly uses AC — shows that all infinite successor cardinals are regular.

PROPOSITION 5.10. *If κ is an infinite cardinal, then κ^+ is regular.*

Proof. Assume towards a contradiction that there exists a subset $\mathcal{C} \subseteq \kappa^+$ such that $\mathcal{C}$ is cofinal in κ^+ and $|\mathcal{C}| < \kappa^+$, i.e., $|\mathcal{C}| \leq \kappa$. Since $\mathcal{C} \subseteq \kappa^+$, for every $\alpha \in \mathcal{C}$ we have $|\alpha| \leq \kappa$. Now, by AC, for each $\alpha \in \mathcal{C}$ we can choose a one-to-one mapping $f_\alpha : \alpha \hookrightarrow \kappa$ and further let g be a one-to-one mapping from $\mathcal{C}$ into κ. Then,

$$\big\{\langle g(\alpha), f_\alpha(\nu)\rangle : \alpha \in \mathcal{C} \wedge \nu \in \alpha\big\}$$

is a subset of $\kappa \times \kappa$ and consequently $\big|\bigcup \mathcal{C}\big| \leq |\kappa \times \kappa| = \kappa$. Thus, $\bigcup \mathcal{C} \neq \kappa^+$ which implies that $\mathcal{C}$ is not cofinal in κ^+. ⊣

For example, ω_1, ω_{17}, and $\omega_{\omega+5}$ are regular, since $\omega_1 = \omega_0^+$, $\omega_{17} = \omega_{16}^+$, and $\omega_{\omega+5} = \omega_{\omega+4}^+$.

We now consider arbitrary sums and products of cardinal numbers. For this, let I be a non-empty set and let $\{\kappa_\iota : \iota \in I\}$ be a family of cardinals. We define

$$\sum_{\iota \in I} \kappa_\iota = \Big|\bigcup_{\iota \in I} A_\iota\Big|$$

where $\{A_\iota : \iota \in I\}$ is a family of pairwise disjoint sets such that $|A_\iota| = \kappa_\iota$ for each $\iota \in I$, e.g., $A_\iota = \kappa_\iota \times \{\iota\}$ will do.
Similarly we define

$$\prod_{\iota \in I} \kappa_\iota = \Big|\prod_{\iota \in I} A_\iota\Big|$$

where $\{A_\iota : \iota \in I\}$ is a family of sets such that $|A_\iota| = \kappa_\iota$ for each $\iota \in I$, e.g., $A_\iota = \kappa_\iota$ will do.

THEOREM 5.11 (INEQUALITY OF KÖNIG-JOURDAIN-ZERMELO). *Let I be a non-empty set and let $\{\kappa_\iota : \iota \in I\}$ and $\{\lambda_\iota : \iota \in I\}$ be families of cardinal numbers such that $\kappa_\iota < \lambda_\iota$ for every $\iota \in I$. Then*

$$\sum_{\iota \in I} \kappa_\iota < \prod_{\iota \in I} \lambda_\iota \,.$$

Proof. Let $\{A_\iota : \iota \in I\}$ be a family of pairwise disjoint sets such that $|A_\iota| = \kappa_\iota$ for each $\iota \in I$. Firstly, for each $\iota \in I$ choose a injection $f_\iota : A_\iota \hookrightarrow \lambda_\iota$ and an element $y_\iota \in \lambda_\iota \setminus f_\iota[A_\iota]$ (notice that since $|A_\iota| < \lambda_\iota$, the set $\lambda_\iota \setminus f_\iota[A_\iota]$ is non-empty).

As a first step we show that $\sum_{\iota \in I} \kappa_\iota \leq \prod_{\iota \in I} \lambda_\iota$: For this, define $\bar{f} : \bigcup_{\iota \in I} A_\iota \to \prod_{\iota \in I} \lambda_\iota$ by stipulating $\bar{f}(x) := \langle \bar{f}_\iota(x) : \iota \in I\rangle$ where

$$\bar{f}_\iota(x) = \begin{cases} f_\iota(x) & \text{if } x \in A_\iota, \\ y_\iota & \text{otherwise.} \end{cases}$$

Then $\bar{f}$ is obviously a one-to-one function from $\bigcup_{\iota \in I} A_\iota$ into $\prod_{\iota \in I} \lambda_\iota$, which shows that $\sum_{\iota \in I} \kappa_\iota \leq \prod_{\iota \in I} \lambda_\iota$.

To see that $\sum_{\iota\in I}\kappa_\iota < \prod_{\iota\in I}\lambda_\iota$, take any function $g:\bigcup_{\iota\in I}A_\iota \to \prod_{\iota\in I}\lambda_\iota$. For every $\iota\in I$, let $P_\iota\big(g[A_\iota]\big)$ be the projection of $g[A_\iota]$ on κ_ι. Then, for each $\iota\in I$ we can choose an element $z_\iota \in \lambda_\iota \setminus P_\iota\big(g[A_\iota]\big)$. Evidently, the sequence $\langle z_\iota : \iota\in I\rangle$ does not belong to $g\big[\bigcup_{\iota\in I}A_\iota\big]$ which shows that g is not surjective, and consequently, g is not bijective. ⊣

As an immediate consequence we get the following

COROLLARY 5.12. *For every infinite cardinal κ we have*

$$\kappa < \kappa^{\mathrm{cf}(\kappa)} \quad \textit{and} \quad \mathrm{cf}(2^\kappa) > \kappa\,.$$

In particular we get that $\mathrm{cf}(\mathfrak{c}) > \omega$.

Proof. Let $\big\langle \alpha_\nu : \nu\in\mathrm{cf}(\kappa)\big\rangle$ be a cofinal sequence of κ. On the one hand we have

$$\kappa = \Big|\bigcup_{\nu\in\mathrm{cf}(\kappa)}\alpha_\nu\Big| \;\le\; \sum_{\nu\in\mathrm{cf}(\kappa)}|\alpha_\nu| \;\le\; \mathrm{cf}(\kappa)\cdot\kappa \;=\; \kappa\,,$$

and hence, $\kappa = \sum_{\nu\in\mathrm{cf}(\kappa)}|\alpha_\nu|$. On the other hand, for each $\nu\in\mathrm{cf}(\kappa)$ we have $|\alpha_\nu|<\kappa$, and therefore, by THEOREM 5.11, we have

$$\sum_{\nu\in\mathrm{cf}(\kappa)}|\alpha_\nu| \;<\; \prod_{\nu\in\mathrm{cf}(\kappa)}\kappa \;=\; \kappa^{\mathrm{cf}(\kappa)}\,.$$

Thus, we have $\kappa<\kappa^{\mathrm{cf}(\kappa)}$.

In order to see that $\mathrm{cf}(2^\kappa)>\kappa$, notice that $\mathrm{cf}(2^\kappa)\le\kappa$ would imply that $(2^\kappa)^{\mathrm{cf}(2^\kappa)} \le (2^\kappa)^\kappa = 2^{\kappa\cdot\kappa} = 2^\kappa$, which contradicts the fact that $2^\kappa < (2^\kappa)^{\mathrm{cf}(2^\kappa)}$. ⊣

Some Weaker Forms of the Axiom of Choice

The Prime Ideal Theorem and Related Statements

The following maximality principle — which is frequently used in areas like Algebra and Topology — is just slightly weaker than the Axiom of Choice. However, in order to formulate this choice principle we have to introduce the notion of *Boolean algebra* and *ideal*:

A **Boolean algebra** is an algebraic structure, say

$$\big(B,+,\,\cdot\,,-,\mathbf{0},\mathbf{1}\big)$$

where B is a non-empty set, "$+$" and "$\cdot$" are two binary operations (called *Boolean sum* and *product*), "$-$" is an unary operation (called *complement*), and $\mathbf{0}, \mathbf{1}$ are two constants. For all $u, v, w \in B$, the Boolean operations satisfy the following axioms:

$u + v = v + u$	$u \cdot v = v \cdot u$	(commutativity)
$u + (v + w) = (u + v) + w$	$u \cdot (v \cdot w) = (u \cdot v) \cdot w$	(associativity)
$u \cdot (v + w) = (u \cdot v) + (u \cdot w)$	$u + (v \cdot w) = (u + v) \cdot (u + w)$	(distributivity)
$u \cdot (u + v) = u$	$u + (u \cdot v) = u$	(absorption)
$u + (-u) = \mathbf{1}$	$u \cdot (-u) = \mathbf{0}$	(complementation)

An **algebra of sets** is a collection $\mathscr{S}$ of subsets of a given set S such that $S \in \mathscr{S}$ and whenever $X, Y \in \mathscr{S}$, then $S \setminus (X \cap Y) \in \mathscr{S}$ (*i.e.*, $\mathscr{S}$ is closed under unions, intersections and complements). An algebra of sets $\mathscr{S} \subseteq \mathscr{P}(S)$ is a Boolean algebra, with Boolean sum and product being $\cup$ and $\cap$ respectively, the complement $-X$ of a set $X \in \mathscr{S}$ being $S \setminus X$, and with $\emptyset$ and S being the constants $\mathbf{0}$ and $\mathbf{1}$ respectively. In particular, for any set S, $\big(\mathscr{P}(S), \cup, \cap, -, \emptyset, S\big)$ is a Boolean algebra. The case when $S = \omega$ plays an important role throughout this book and some combinatorial properties of the Boolean algebra $\big(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega\big)$ will be investigated in Chapters 8–10.

From the axioms above one can derive additional Boolean algebraic rules that correspond to rules for the set operations $\cup$, $\cap$ and $-$. Among others we have

$$u+u = u \cdot u = -(-u) = u\,, \quad u+\mathbf{0} = u\,, \quad u \cdot \mathbf{0} = \mathbf{0}\,, \quad u+\mathbf{1} = \mathbf{1}\,, \quad u \cdot \mathbf{1} = u\,,$$

as well as the two **De Morgan laws**

$$-(u+v) = -u \cdot -v \quad \text{and} \quad -(u \cdot v) = -u + -v\,.$$

The De Morgan laws might be better recognised for example in set-theoretic notation as

$$S \setminus (X \cup Y) = (S \setminus X) \cap (S \setminus Y)$$

where $X, Y \in \mathscr{P}(S)$; or in Propositional Logic as

$$\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$$

where φ and ψ are any sentences formulated in a certain language.

This last formulation in the language of Propositional Logic shows the relation between Boolean algebra and Logic and provides other examples of Boolean algebras:

Let $\mathscr{L}$ be a first-order language and let S be the set of all $\mathscr{L}$-sentences. We define an equivalence relation "$\sim$" on S by stipulating

$$\varphi \sim \psi \iff \vdash \varphi \leftrightarrow \psi\,.$$

The set $B := S/\!\sim$ of all equivalence classes $[\varphi]$ is a Boolean algebra under the operations $[\varphi] + [\psi] := [\varphi \vee \psi]$, $[\varphi] \cdot [\psi] := [\varphi \wedge \psi]$, $-[\varphi] := [\neg\varphi]$, where

$\mathbf{0} := [\varphi \wedge \neg\varphi]$ and $\mathbf{1} := [\varphi \vee \neg\varphi]$. This algebra is called the **Lindenbaum algebra**.

Let us define
$$u - v = u \cdot (-v)$$
and
$$u \leq v \iff u - v = \mathbf{0}\,.$$
We leave it as an exercise to the reader to verify that "$\leq$" is a partial ordering on B and that
$$u \leq v \iff u + v = v \iff u \cdot v = u\,.$$
Notice also that $[\varphi] \leq [\psi]$ is equivalent to $\vdash \varphi \rightarrow \psi$.

With respect to that ordering, $\mathbf{1}$ is the greatest element of B and $\mathbf{0}$ is the least element. Also, for any $u, v \in B$, $u + v$ is the least upper bound of $\{u, v\}$, and $u \cdot v$ is the greatest lower bound of $\{u, v\}$. Moreover, since $-u$ is the unique element v of B such that $u + v = \mathbf{1}$ and $u \cdot v = \mathbf{0}$ we get that all Boolean-algebraic operations can be defined in terms of the partial ordering "$\leq$" (*e.g.*, $-u$ is the least element v of B with the property that $u + v = \mathbf{1}$).

Now, let us define an additional operation "$\oplus$" on B by stipulating
$$u \oplus v = (u - v) + (v - u)\,.$$
Notice that for every $u \in B$ we have $u \oplus u = \mathbf{0}$, thus, with respect to the operation "$\oplus$", every element of B is its own (and unique) inverse. We leave it as an exercise to the reader to show that B with the two binary operations $\oplus$ and $\cdot$ is a *ring* with zero $\mathbf{0}$ and unit $\mathbf{1}$.

Before we give the definition of ideals in Boolean algebras, let us briefly recall the *algebraic notion* of ideals in commutative rings: Let $\mathcal{R} = (R, +, \cdot, \mathbf{0})$ be an arbitrary commutative ring. An non-empty subset $\mathcal{I} \subseteq R$ is an *ideal* in R if and only if for all $x, y \in \mathcal{I}$ and all $r \in R$ we have $x - y \in \mathcal{I}$ and $r \cdot x \in \mathcal{I}$. The ideal $\{\mathbf{0}\}$ is called the *trivial ideal*. An ideal $I \subseteq R$ of a ring is called *maximal* if $I \neq R$ and the only ideals J in R for which $I \subseteq J$ are $J = I$ and $J = R$. If $\mathcal{R}$ is a commutative ring and $I \neq R$ is an ideal in R, then I is called a *prime ideal* if given any $r, s \in R$ with $r \cdot s \in I$ we always have $r \in I$ or $s \in I$. It is not hard to verify that in a commutative ring with $\mathbf{1}$, every maximal ideal is prime. Finally, if an ideal $J \subseteq R$ is generated by a single element of R, then J is so-called *principal ideal*.

With respect to the ring $(B, \oplus, \cdot, \mathbf{0}, \mathbf{1})$, this leads to the following definition of ideals in Boolean algebras.

Let $\big(B, +, \cdot, -, \mathbf{0}, \mathbf{1}\big)$ be a Boolean algebra. An **ideal** I in B is a non-empty proper subset of B with the following properties:

- $\mathbf{0} \in I$ but $\mathbf{1} \notin I$.
- If $u \in I$ and $v \in I$, then $u + v \in I$.
- For all $w \in B$ and all $u \in I$, $w \cdot u \in I$ (or equivalently, if $w \in B$, $u \in I$ and $w \leq u$, then $w \in I$).

Considering the Boolean algebra $\big(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega\big)$, one easily verifies that the set of all finite subsets of ω is an ideal *over* ω, *i.e.*, an ideal *on* $\mathscr{P}(\omega)$. This ideal is called the **Fréchet ideal**.

The dual notion of an ideal is a so-called filter. Thus, a **filter** F in B is a non-empty proper subset of B with the following properties:

- $\mathbf{0} \notin F$ but $\mathbf{1} \in F$.
- If $u \in F$ and $v \in F$, then $u \cdot v \in F$.
- For all $w \in B$ and all $u \in F$, $w + u \in I$ (or equivalently, if $w \in B$, $u \in F$ and $w \geq u$, then $w \in F$).

Moreover, if I is an ideal in B, then $I^* := \{-u : u \in I\}$ is a filter, called **dual filter**. Similarly, if F is a filter in B, then $F^* := \{-u : u \in F\}$ is an ideal, called **dual ideal**. The dual filter $I_0^* = \{x \subseteq \omega : \omega \setminus x \text{ is finite}\}$ of the Fréchet ideal I_0 on $\mathscr{P}(\omega)$ is called the **Fréchet filter**.

Let I be an ideal in B, and let F be a filter in B.

I is called

- **trivial** if $I = \{\mathbf{0}\}$;
- **principal** if there is an $u \in B$ such that $I = \{v : v \leq u\}$;
- **prime** if for all $u \in B$, *either* $u \in I$ *or* $-u \in I$;

F is called

- **trivial** if $F = \{\mathbf{1}\}$;
- **principal** if there is an $u \in B$ such that $F = \{v : v \geq u\}$;
- an **ultrafilter** if for all $u \in B$, *either* $u \in F$ *or* $-u \in F$.

Let us consider a few ideals and filters over ω, *i.e.*, ideals and filters in the Boolean algebra $\big(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega\big)$: The trivial ideal is $\{\emptyset\}$, and the trivial filter is $\{\omega\}$. For any non-empty subset $x \subseteq \omega$, $F_x := \big\{y \in \mathscr{P}(\omega) : y \supseteq x\big\}$ is a principal filter, and the dual ideal $I_{\omega\setminus x} := (F_x)^* = \{z \in \mathscr{P}(\omega) : \omega \setminus z \in F_x\} = \big\{z \in \mathscr{P}(\omega) : z \cap x = \emptyset\big\}$ is also principal. In particular, if $x = \{a\}$ for some $a \in \omega$, then F_x is a principal ultrafilter and $I_{\omega\setminus x}$ is a principal prime ideal. We leave it as an exercise to the reader to show that every principal ultrafilter over ω is of the form $F_{\{a\}}$ for some $a \in \omega$, and that every principal prime ideal is of the form $I_{\omega\setminus\{a\}}$. Considering the Fréchet filter F on $\mathscr{P}(\omega)$, one easily verifies that F is a non-principal filter, but not an ultrafilter (notice that neither $x = \{2n : n \in \omega\}$ nor $\omega \setminus x$ belongs to F). Similarly, the Fréchet ideal is not prime but non-principal.

Let us now summarise a few basic properties of ultrafilters over sets (the proofs are left to the reader):

FACT 5.13. *Let U be an ultrafilter over a set S.*

(a) If $\{x_0, \ldots, x_{n-1}\} \subseteq \mathscr{P}(S)$ (for some $n \in \omega$) such that $x_0 \cup \ldots \cup x_{n-1} \in U$ and for any distinct $i, j \in n$ we have $x_i \cap x_j \notin U$, then there is a unique $k \in n$ such that $x_k \in U$.

(b) If $x \in U$ and $|x| \geq 2$, then there is a proper subset $y \subsetneq x$ such that $y \in U$.

(c) If U contains a finite set, then U is principal.

On the one hand, prime ideals and ultrafilters in Boolean algebras are always maximal. On the other hand, one cannot prove in ZF that for example the Fréchet filter over ω can be extended to an ultrafilter. In particular, there are models of ZF in which every ultrafilter over ω is principal (*cf.* RELATED RESULT 38 and Chapter 17).

However, there is a choice principle which guarantees that every ideal in a Boolean algebra can be extended to a prime ideal, and consequently, that every filter can be extended to an ultrafilter.

> Prime Ideal Theorem: If I is an ideal in a Boolean algebra, then I can be extended to a prime ideal.

In fact, the Prime Ideal Theorem, denoted PIT, is a choice principle which is just slightly weaker than the full Axiom of Choice. Below we shall present some equivalent formulations of the Prime Ideal Theorem, but first let us show that the Prime Ideal Theorem follows from the Axiom of Choice (for the fact that the converse implication does not hold see THEOREM 7.16).

PROPOSITION 5.14. AC $\Rightarrow$ PIT.

Proof. By THEOREM 5.3 it is enough to show that the Prime Ideal Theorem follows from Teichmüller's Principle. Let $(B,+,\cdot,-,\mathbf{0},\mathbf{1})$ be a Boolean algebra and let $I_0 \subsetneq B$ be an ideal. Further, let $\mathscr{F}$ be the family of all sets $X \subseteq B \setminus I_0$ such that for every finite subset $\{u_0,\dots,u_n\} \subseteq X \cup I_0$ we have

$$u_0 + \ldots + u_n \neq \mathbf{1}\,.$$

Obviously, $\mathscr{F}$ has finite character, and therefore, by Teichmüller's Principle, $\mathscr{F}$ has a maximal element. In other words, there is a maximal subset I_1 of B which has the property that whenever we pick finitely many elements $\{u_0,\dots,u_n\}$ from $I := I_0 \cup I_1$ we have $u_0+\ldots+u_n \neq \mathbf{1}$. Since I_1 is maximal we get that I is an *ideal* in B which extends I_0. Moreover, the ideal I has the property that for any element $v \in B \setminus I$ there is a $u \in I$ such that $u + v = \mathbf{1}$, *i.e.*, for any $v \in B$, $v \notin I$ implies $-v \in I$. Thus, I is a prime ideal in B which extends I_0.

A seemingly weaker version of PIT is the following statement.

> Ultrafilter Theorem: If F is a filter over a set S, then F can be extended to an ultrafilter.

Notice that the Ultrafilter Theorem is the dual version of the Prime Ideal Theorem in the case when the Boolean algebra is an algebra of sets.

For the next version of the Prime Ideal Theorem we have to introduce first some terminology: Let S be a set and let $\mathcal{B}$ be a set of binary functions (*i.e.*, with values 0 or 1) defined on finite subsets of S. We say that $\mathcal{B}$ is a **binary mess** on S if $\mathcal{B}$ satisfies the following properties:

- For each finite set $P \subseteq S$, there is a function $g \in \mathcal{B}$ such that $\operatorname{dom}(g) = P$, i.e., g is defined on P.
- For each $g \in \mathcal{B}$ and each finite set $P \subseteq S$, the restriction $g|_P$ belongs to $\mathcal{B}$.

Let f be a binary function on S and let $\mathcal{B}$ be a binary mess on S. Then f is **consistent with** $\mathcal{B}$ if for every finite set $P \subseteq S$, $f|_P \in \mathcal{B}$.

> Consistency Principle: For every binary mess $\mathcal{B}$ on a set S, there exists a binary function f on S which is consistent with $\mathcal{B}$.

In order to state the last version of the Prime Ideal Theorem we have to introduce first some terminology from **Propositional Logic**: The alphabet of Propositional Logic consists of an arbitrarily large but fixed set $\mathcal{P} := \{p_\lambda : \lambda \in \Lambda\}$ of so-called **propositional variables**, as well as of the logical operators "$\neg$", "$\wedge$", and "$\vee$". The formulae of Propositional Logic are defined recursively as follows:

- A single propositional variable $p \in \mathcal{P}$ by itself is a formula.
- If φ and ψ are formulae, then so are $\neg(\varphi)$, $(\varphi \wedge \psi)$, and $(\varphi \vee \psi)$; in Polish notation, the three composite formulae are $\neg\varphi$, $\wedge\varphi\psi$, and $\vee\varphi\psi$, respectively.

A **realisation** of Propositional Logic is a map of $\mathcal{P}$, the set of propositional variables, to the two element Boolean algebra $\big(\{\mathbf{0},\mathbf{1}\}, +, \cdot, -, \mathbf{0}, \mathbf{1}\big)$. Given a realisation f of Propositional Logic. By induction on the complexity of formulae we extend f to all formulae of Propositional Logic (compare with the definition of Lindenbaum's algebra): For any formulae φ and ψ, if $f(\varphi)$ and $f(\psi)$ have already been defined, then

$$f(\wedge\varphi\psi) = f(\varphi) \cdot f(\psi)\,, \quad f(\vee\varphi\psi) = f(\varphi) + f(\psi)\,,$$

and

$$f(\neg\varphi) = -f(\varphi)\,.$$

Let φ be any formula of Propositional Logic. If the realisation f, extended in the way just described, maps the formula φ to $\mathbf{1}$, then we say that f **satisfies** φ. Finally, a set Σ of formulae of Propositional Logic is **satisfiable** if there is a realisation which simultaneously satisfies all the formulae in Σ.

> Compactness Theorem for Propositional Logic: Let Σ be a set of formulae of Propositional Logic. If every finite subset of Σ is satisfiable, then also Σ is satisfiable.

Notice that the reverse implication of the Compactness Theorem for Propositional Logic is trivially satisfied.

Now we show that the above principles are all equivalent to the Prime Ideal Theorem.

THEOREM 5.15. *The following statements are equivalent:*

(a) Prime Ideal Theorem.

(b) Ultrafilter Theorem.

(c) Consistency Principle.

(d) Compactness Theorem for Propositional Logic.

(e) Every Boolean algebra has a prime ideal.

Proof. (a)⇒(b) The Ultrafilter Theorem is an immediate consequence of the dual form of the Prime Ideal Theorem.

(b)⇒(c) Let $\mathcal{B}$ be a binary mess on a non-empty set S. Assuming the Ultrafilter Theorem we show that there is a binary function f on S which is consistent with $\mathcal{B}$. Let $\operatorname{fin}(S)$ be the set of all finite subsets of S. For each $P \in \operatorname{fin}(S)$, let

$$A_P = \left\{ g \in {}^S 2 : g|_P \in \mathcal{B} \right\}.$$

Since $\mathcal{B}$ is a binary mess, the intersection of finitely many sets A_P is non-empty. Thus, the family $\mathscr{F}$ consisting of all supersets of intersections of finitely many sets A_P is a filter over ${}^S 2$. By the Ultrafilter Theorem, $\mathscr{F}$ can be extended to an ultrafilter $\mathscr{U} \subseteq \mathscr{P}\left({}^S 2\right)$. Since $\mathscr{U}$ is an ultrafilter, for each $s \in S$, either $\left\{ g \in {}^S 2 : g(s) = 0 \right\}$ or $\left\{ g \in {}^S 2 : g(s) = 1 \right\}$ belongs to $\mathscr{U}$, and we define the function $f \in {}^S 2$ by stipulating that for each $s \in S$, the set $A_s = \left\{ g \in {}^S 2 : g(s) = f(s) \right\}$ belongs to $\mathscr{U}$. Now, for any finite set $P = \{s_0, \dots, s_n\} \subseteq S$, $\bigcap_{i \le n} A_{s_i} \in \mathscr{U}$, which shows that $f|_P \in \mathcal{B}$, *i.e.*, f is consistent with $\mathcal{B}$.

(c)⇒(d) Let Σ be a set of formulae of Propositional Logic and let $S \subseteq \mathcal{P}$ be the set of propositional variables which appear in formulae of Σ. Assume that every finite subset of Σ is satisfiable, *i.e.*, for every finite subset $\Sigma_0 \subseteq \Sigma$ there is a realisation $g_{\Sigma_0} : S_{\Sigma_0} \to \{\mathbf{0}, \mathbf{1}\}$ which satisfies Σ_0, where S_{Σ_0} denotes the set of propositional variables which appear in formulae of Σ_0. Let

$$\mathcal{B}_\Sigma := \left\{ g_{\Sigma_0}|_P : \Sigma_0 \in \operatorname{fin}(\Sigma) \wedge P \subseteq S_{\Sigma_0} \right\}.$$

Then $\mathcal{B}_\Sigma$ is obviously a binary mess and by Consistency Principle there exists a binary function f on S which is consistent with $\mathcal{B}_\Sigma$. Now, f is a realisation of Σ and therefore Σ is satisfiable.

(d)⇒(e) Let $\left(B, +, \cdot, -, \mathbf{0}, \mathbf{1}\right)$ be a Boolean algebra and let $\mathcal{P} := \{p_u : u \in B\}$ be a set of propositional variables. Further, let Σ_B be the following set of formulae of Propositional Logic:

- $p_{\mathbf{0}}$, $\neg p_{\mathbf{1}}$;
- $p_u \vee \neg p_{-u}$ (for each $u \in B$);
- $\neg(p_{u_1} \wedge \ldots \wedge p_{u_n}) \vee p_{u_1 + \ldots + u_n}$ (for each finite set $\{u_1, \dots, u_n\} \subseteq B$).
- $\neg(p_{u_1} \vee \ldots \vee p_{u_n}) \vee p_{u_1 \cdot \ldots \cdot u_n}$ (for each finite set $\{u_1, \dots, u_n\} \subseteq B$).

Notice that every finite subset of B generates a finite subalgebra of B and that every finite Boolean algebra has a prime ideal. Now, since every finite prime ideal in a finite subalgebra of B corresponds to a realisation of a finite subset of Σ_B, and vice versa, every finite subset of Σ_B is satisfiable. Thus, by the Compactness Theorem for Propositional Logic, Σ_B is satisfiable. Let f be a realisation of Σ_B and let $I = \{u \in B : f(p_u) = 1\}$. By definition of Σ_B and I respectively we get:

- $f(p_{\mathbf{0}}) = 1$ and $f(p_{\mathbf{1}}) = 0$; thus, $\mathbf{0} \in I$ but $\mathbf{1} \notin I$.
- $f(p_u) = 1 - f(\neg p_u)$; thus, for all $u \in B$, either $u \in I$ or $-u \in I$.
- If $f(p_{u_1}) = f(p_{u_2}) = 1$, then $f(p_{u_1} \wedge p_{u_2}) = 1$; thus, for all $u_1, u_2 \in I$ we have $u_1 + u_2 \in I$.
- if $f(p_{u_1}) = 1$, then $f(p_{u_1} \vee p_{u_2}) = 1$; thus, for all $u_1 \in I$ and all $u_2 \in B$ we have $u_1 \cdot u_2 \in I$.

Thus, the set $I = \{u \in B : f(p_u) = 1\}$ is a prime ideal in B.

(e)⇒(a) Let $(B, +, \cdot, -, \mathbf{0}, \mathbf{1})$ be a Boolean algebra and $I \subseteq B$ an ideal in B. Define the following equivalence relation on B:

$$u \sim v \iff (u - v) + (v - u) \in I$$

Let C be the set of all equivalence classes $[u]^{\tilde{}}$ and define the operations "+", "$\cdot$", and "$-$" on C as follows:

$$[u]^{\tilde{}} + [v]^{\tilde{}} = [u + v]^{\tilde{}}, \quad [u]^{\tilde{}} \cdot [v]^{\tilde{}} = [u \cdot v]^{\tilde{}}, \quad -[u]^{\tilde{}} = [-u]^{\tilde{}}.$$

Now,

$$\big(C, +, \cdot, -, [\mathbf{0}]^{\tilde{}}, [\mathbf{1}]^{\tilde{}}\big)$$

is a Boolean algebra, the so-called *quotient of B modulo I*. By the Prime Ideal Theorem, C has a prime ideal J. We leave it as an exercise to the reader to verify that the set

$$\{u \in B : [u]^{\tilde{}} \in J\}$$

is a prime ideal in B which extends I. ⊣

König's Lemma and other Choice Principles

Let us begin by defining some choice principles:

- $\mathsf{C}(\aleph_0, \infty)$: Every countable family of non-empty sets has a choice function (this choice principle is usually called Countable Axiom of Choice).
- $\mathsf{C}(\aleph_0, \aleph_0)$: Every countable family of non-empty countable sets has a choice function.
- $\mathsf{C}(\aleph_0, < \aleph_0)$: Every countable family of non-empty finite sets has a choice function.
- $\mathsf{C}(\aleph_0, n)$: Every countable family of n-element sets, where $n \in \omega$, has a choice function.
- $\mathsf{C}(\infty, < \aleph_0)$: Every family of non-empty finite sets has a choice function (this choice principle is usually called Axiom of Choice for Finite Sets).

- $\mathsf{C}(\infty, n)$: Every family of n-element sets, where $n \in \omega$, has a choice function. This choice principle is usually denoted C_n.

Another — seemingly unrelated — choice principle is the Ramseyan Partition Principle, denoted RPP.

- RPP: If X is an infinite set and $[X]^2$ is 2-coloured, then there is an infinite subset Y of X such that $[Y]^2$ is monochromatic.

Below we show how these choice principles are related to each other, but first let us show that $\mathsf{C}(\aleph_0, < \aleph_0)$ and König's Lemma, denoted by KL, are equivalent.

PROPOSITION 5.16. $\mathsf{C}(\aleph_0, < \aleph_0) \iff \mathsf{KL}$.

Proof. ($\Rightarrow$) Let $T = (V, E)$ be an infinite, finitely branching tree with vertex set V, edge set E, and root say v_0. The edge set E can be considered as a subset of $V \times V$, *i.e.*, as a set of ordered pairs of vertices indicating the direction from the root to the top of the tree. Let $S_0 := \{v_0\}$, and for $n \in \omega$ let

$$S_{n+1} := \big\{v \in V : \exists u \in S_n(\langle u, v\rangle \in E)\big\}$$

and let $S := \bigcup_{n\in\omega} S_n$. Since T is infinite and finitely branching, S is infinite and for every $n \in \omega$, S_n is a non-empty finite set. Further, for every $v \in S$ let $S(v)$ be the set of all vertices $u \in S$ such that there exists a non-empty finite sequence $s \in \operatorname{seq}(S)$ of length $k+1$ (for some $k \in \omega$) with $s(0) = v$ and $s(k) = u$, and for all $i \leq k$ we have $\big\langle s(i), s(i+1)\big\rangle \in E$. In other words, $S(v)$ is the set of all vertices which can be reached from v. Notice that $\big(S(v), E|_{S(v)}\big)$ is a subtree of T. Since S is infinite and for all $n \in \omega$, $\bigcup_{i\in n} S_i$ is finite, for each $n \in \omega$ there exists a vertex $v \in S_n$ such that $S(v)$ is infinite.

We now proceed as follows: By $\mathsf{C}(\aleph_0, < \aleph_0)$, for each $n \in \omega$ we can choose a well-ordering "$<_n$" on S_n and then construct a branch $v_0, v_1, \ldots, v_n, \ldots$ through T, where for all $n \in \omega$, v_{n+1} is the $<_{n+1}$-minimal element of the non-empty set $\big\{v \in S_{n+1} : \langle v_n, v\rangle \in E \wedge \text{“}S(v) \text{ is infinite”}\big\}$.

($\Leftarrow$) Let $\mathscr{F} = \{F_n : n \in \omega\}$ be a countable family of non-empty finite sets. Further, let $V = \bigcup_{k\in\omega} \big(\prod_{n\in k} F_n\big)$ and let $E \subseteq V \times V$ be the set of all ordered pairs $\langle s, t\rangle$ of the form $s = \langle x_0, \ldots, x_n\rangle$ and $t = \langle x_0, \ldots, x_n, x_{n+1}\rangle$ respectively, where for each $i \in n+2$, $x_i \in F_i$ (*i.e.*, the sequence t is obtained by adding an element of F_{n+1} to s). Obviously, $T = (V, E)$ is an infinite, finitely branching tree and therefore, by KL, has an infinite branch, say $\langle a_n : n \in \omega\rangle$. Since, for all $n \in \omega$, a_n belongs to F_n, the function

$$\begin{aligned} f : \mathscr{F} &\longrightarrow \bigcup \mathscr{F} \\ F_n &\longmapsto \ a_n \end{aligned}$$

is a choice function for $\mathscr{F}$, and since the countable family of finite sets $\mathscr{F}$ was arbitrary, we get $\mathsf{C}(\aleph_0, < \aleph_0)$. $\dashv$

Obviously, $\mathsf{C}(\aleph_0, < \aleph_0) \Rightarrow \mathsf{C}(\aleph_0, n)$ for all positive integers $n \in \omega$. However, as a matter of fact we would like to mention that for each $n \geq 2$, $\mathsf{C}(\aleph_0, n)$ is a proper axiom, *i.e.*, not provable within ZF (for $n = 2$ see for example PROPOSITION 7.7).

The following result shows the strength of the choice principles RPP and KL compared to $\mathsf{C}(\aleph_0, \infty)$ and $\mathsf{C}(\aleph_0, n)$ respectively:

THEOREM 5.17. $\mathsf{C}(\aleph_0, \infty) \Longrightarrow \mathsf{RPP} \Longrightarrow \mathsf{KL} \Longrightarrow \mathsf{C}(\aleph_0, n)$.

Proof. $\mathsf{C}(\aleph_0, \infty) \Rightarrow \mathsf{RPP}$: Firstly we show that $\mathsf{C}(\aleph_0, \infty)$ implies that every infinite set X is transfinite, *i.e.*, there is an infinite sequence of elements of X in which no element appears twice: Let X be an infinite set and for every $n \in \omega$ let F_{n+1} be the set of all injections from $n+1$ into X. Consider the family $\mathscr{F} = \{F_{n+1} : n \in \omega\}$. Since X is infinite, $\mathscr{F}$ is a countable family of non-empty sets. Thus, by $\mathsf{C}(\aleph_0, \infty)$, there is a choice function, say f, on $\mathscr{F}$. For every $n \in \omega$ let $g_n := f(F_{n+1})$. With the countably many injections g_n we can easily construct an injection from ω into X. In particular, we get an infinite sequence $\langle a_i : i \in \omega \rangle$ of elements of X in which no element appears twice. For $S := \{a_i : i \in \omega\} \subseteq X$, every 2-colouring of $[X]^2$ induces a 2-colouring of $[S]^2$. Now, by RAMSEY'S THEOREM 2.1, there exists an infinite subset Y of S such that $[Y]^2$ is monochromatic (notice that no choice is needed to establish RAMSEY'S THEOREM for countable sets).

$\mathsf{RPP} \Rightarrow \mathsf{KL}$: Let $T = (V, E)$ be an infinite, finitely branching tree and let the sets S_n (for $n \in \omega$) be as in the first part of the proof of PROPOSITION 5.16. Define the colouring $\pi : [V]^2 \to \{0, 1\}$ by stipulating $\pi(\{u, v\}) = 0 \iff \{u, v\} \subseteq S_n$ for some $n \in \omega$. By RPP there exists an infinite subset $X \subseteq V$ such that $[X]^2$ is monochromatic. Now, since T is finitely branching, we get that if $X \subseteq V$ is infinite and $[X]^2$ is monochromatic, then $[X]^2$ is of colour 1, *i.e.*, no two distinct elements of X are in the same set S_n. In order to construct an infinite branch through T, just proceed as in the first part of the proof of PROPOSITION 5.16.

$\mathsf{KL} \Rightarrow \mathsf{C}(\aleph_0, n)$: Because $\mathsf{C}(\aleph_0, < \aleph_0) \Rightarrow \mathsf{C}(\aleph_0, n)$, this is an immediate consequence of PROPOSITION 5.16. ⊣

The last result of this chapter deals with the relationship of the choice principles C_n (*i.e.*, $\mathsf{C}(\infty, n)$) for different natural numbers n. Before we can state the theorem we have to introduce the following number-theoretical condition: Let m, n be two positive integers. Then we say that m, n satisfy condition (S) if the following condition holds:

> *There is no decomposition of n into a sum of primes, $n = p_1 + \ldots + p_s$, such that $p_i > m$ for all $1 \leq i \leq s$.*

THEOREM 5.18. *If the positive integers m, n satisfy condition (S) and if C_k holds for every $k \leq m$, then also C_n holds.*

Proof. Firstly notice that C_1 is obviously true. Secondly notice that for $n \leq m$, the implication of the theorem is trivially true. So, without loss of generality we may assume that $n > m$.

The proof is now by induction on n: Let $m < n$ be a fixed positive integer such that m, n satisfy condition (S) and assume that the implication of the theorem is true for every $l < n$. Since n, m satisfy (S), n is not a prime and consequently n is divisible by some prime $p < n$. Necessarily, $p \leq m$, since otherwise we could write $n = p + \ldots + p$, contrary to (S). Let $\mathscr{F} = \{A_\lambda : \lambda \in \Lambda\}$ be a family of n-element sets. We have to describe a way to choose an element from each set A_λ ($\lambda \in \Lambda$). Take an arbitrary $A \in \mathscr{F}$ and consider $[A]^p$ (*i.e.*, the set of all p-element subsets of A). Since $p \leq m$, by the premise of the theorem there is a choice function g for $[A]^p$. In other words, for every $X \in [A]^p$, $g(X) \in X$, in particular, $g(X) \in A$. For every $a \in A$ let

$$q(a) = \left|\left\{X \in [A]^p : g(X) = a\right\}\right|$$

and let $q := \min\left\{q(a) : a \in A\right\}$. Further, let $B := \left\{a \in A : q(a) = q\right\}$. Obviously, the set B is non-empty and the set $[A]^p$ has $\binom{n}{p}$ elements. In order to prove that $A \setminus B$ is non-empty, we have to show that $\binom{n}{p}$ is not divisible by n. Indeed, because p divides n, there is a positive integer k which is not divisible by p such that $n = k \cdot p^{a+1}$ (for some $a \in \omega$). We have

$$\binom{n}{p} = \frac{k \cdot p^{a+1}}{p} \cdot \frac{(n-1) \cdot \;\cdots\; \cdot (n-p+1)}{(p-1) \cdot \;\cdots\; \cdot \qquad 1} = \frac{k \cdot p^{a+1}}{p} \cdot \binom{n-1}{p-1},$$

and since p does obviously not divide $\binom{n-1}{p-1}$, we get that $\binom{n}{p}$ is divisible by p^a, but not by p^{a+1}; in particular, $\binom{n}{p}$ is not divisible by $n = k \cdot p^{a+1}$. Thus, the sets B and $A \setminus B$ are both non-empty, and for $l_1 := |B|$ and $l_2 := |A \setminus B|$ we get that l_1 and l_2 are positive integers with $l_1 + l_2 = n$. Moreover, m, l_1 or m, l_2 satisfy condition (S), since otherwise we could write $l_1 = p_1 + \ldots + p_r$ and $l_2 = p_{r+1} + \ldots + p_s$, where $p_1, \ldots, p_s$ are primes bigger than m, which would imply that $n = p_1 + \ldots + p_s$, contrary to the assumption that m, n satisfy (S). Thus, by the induction hypothesis, either C_{l_1} holds and we choose an element in B, or, if C_{l_1} fails, C_{l_2} holds and we choose an element in $A \setminus B$. Finally, since $A \in \mathscr{F}$ was arbitrary, this completes the proof. $\dashv$

NOTES

The Axiom of Choice. Fraenkel writes in [26, p. 56 f.] that *the* Axiom of Choice *is probably the most interesting and, in spite of its late appearance, the most discussed axiom of Mathematics, second only to Euclid's axiom of parallels which was introduced more than two thousand years ago.* We would also like to mention a different view to choice functions, namely the view of Peano. In 1890, Peano published a proof in which he was constrained to choose a single element from each set in a certain infinite sequence $A_1, A_2, \ldots$ of infinite subsets of $\mathbb{R}$. In that proof, he remarked carefully (*cf.* [73, p. 210]): *But as one cannot apply infinitely many times an* arbitrary *rule by which one assigns to a class A an individual of this class, a* determinate *rule is stated here, by which, under suitable hypotheses, one assigns to each class A an individual of this class.* To obtain his rule, he employed least upper bounds. According to Moore [66, p 76], Peano was the first mathematician who — while accepting infinite collections — categorically rejected the use of infinitely many arbitrary choices.

The difficulty is well illustrated by a Russellian anecdote (*cf.* Sierpiński [82, p. 125]): *A millionaire possesses an infinite number of pairs of shoes, and an infinite number of pairs of socks. One day, in a fit of eccentricity, he summons his valet and asks him to select one shoe from each pair. When the valet, accustomed to receiving precise instructions, asks for details as to how to perform the selection, the millionaire suggests that the left shoe be chosen from each pair. Next day the millionaire proposes to the valet that he select one sock from each pair. When asked as to how this operation is to be carried out, the millionaire is at a loss for a reply, since, unlike shoes, there is no intrinsic way of distinguishing one sock of a pair from the other. In other words, the selection of the socks cannot be carried out without the aid of some choice function.*

As long as the implicit and unconscious use of the Axiom of Choice by Cantor and others involved only generalised arithmetical concepts and properties well-known from finite numbers, nobody took offence. However, the situation changed drastically after Zermelo [107] published his first proof that every set can be well-ordered — which was one of the earliest assertions of Cantor. It is worth mentioning that, according to Zermelo [107, p. 514] & [108, footnote p. 118], it was in fact the idea of Erhard Schmidt to use the Axiom of Choice in order to build the f-sets. Zermelo considered the Axiom of Choice as a *logical principle*, that *cannot be reduced to a still simpler one, but is used everywhere in mathematical deductions without hesitation* (see [107, p. 516]). Even though in Zermelo's view the Axiom of Choice was "self-evident", which is not the same as "obvious" (see Shapiro [81, §5] for a detailed discussion of the meaning of "self-evidence"), not all mathematicians at that time shared Zermelo's opinion. Moreover, after the first proof of the Well-Ordering Principle was published in 1904, the mathematical journals (especially volume 60 of *Mathematische Annalen*) were flooded with critical notes rejecting the proof (see for example Moore [66, Chapter 2]), mostly arguing that the Axiom of Choice was either illegitimate or meaningless (*cf.* Fraenkel, Bar-Hillel, and Lévy [26, p. 82]). The reason for this was not only due to the non-constructive character of the Axiom of Choice, but also because it was not yet clear what a "set" should be. So, Zermelo decided to publish a more detailed proof, and at the same time taking the opportunity to reply to his critics. This resulted in [108], his second proof of the Well-Ordering Principle which was published in 1908, the same year as he presented his first axiomatisation of Set Theory in [108]. It seems that this was not a coincidence. Moore [66, p. 159] writes that *Zermelo's axiomatisation was primarily motivated by a desire to secure his demonstration of the* Well-Ordering Principle *and, in particular, to save his* Axiom of Choice. Moreover, Hallett [32, p. xvi] goes even further by trying to show *that the selection of the axioms themselves was guided by the demands of Zermelo's reconstructed [second] proof.* Hallett's statement is motivated by a remark on page 124 in Zermelo [108], where he emphasises that the proof is just based on certain fixed principles to *build initial sets* and to *derive new sets from given ones* — exactly what we would require for principles to form an axiomatic system of Set Theory.

We would like to mention that because of its different character (*cf.* Bernays [3]) and since he considered the Axiom of Choice as a general logical principle, he did not include the Axiom of Choice to his second axiomatic system of Set Theory.

For a comprehensive survey of Zermelo's Axiom of Choice, its origins, development, and influence, we refer the reader to Moore [66] (see also Kanamori [46], Jech [41], and Fraenkel, Bar-Hillel, and Lévy [26, Chapter II, §4]); and for a biography of Zermelo (including the history of AC and axiomatic Set Theory) we refer the reader to Ebbinghaus [17].

Gödel's constructible universe. According to Kanamori [45, p. 28 ff.], in October of 1935 Gödel informed von Neumann at the Institute for Advanced Study in Princeton that he had established the relative consistency of the Axiom of Choice. This he did by devising his constructible (not *constructive*!) hierarchy **L** (for "law") and verifying the Axiom of Choice and the rest of the ZF axioms there. Gödel conjectured that the Continuum Hypothesis would also hold in **L**, but he soon fell ill and only gave a proof of this and the Generalised Continuum Hypothesis (*i.e.*, for all $\alpha \in \Omega$, $2^{\omega_\alpha} = \omega_{\alpha+1}$) two years later. The crucial idea apparently came to him during the night of June 14/15, 1937 (see also [31, pp. 1–8]).

Gödel's article [28] was the first announcement of these results, in which he describes the model **L** as the class *of all "mathematically constructible" sets, where the term "constructible" is to be understood in the semi-intuitionistic sense which excludes impredicative procedures. This means "constructible" sets are defined to be those sets which can be obtained by Russell's ramified hierarchy of types, if extended to include transfinite orders.* In the succeeding article [29], Gödel provided more details in the context of ZF, and in his monograph [30] — based on lectures given at the Institute for Advanced Study during the winter of 1938/39 — Gödel gave another presentation of **L**. This time he generated **L** set by set with a transfinite recursion in terms of eight elementary set generators, a sort of Gödel numbering into the transfinite (*cf.* Kanamori [45, p. 30], and for Gödel's work in Set Theory see Kanamori [47]).

Equivalent Forms of the Axiom of Choice. The literature gives numerous examples of theorems which are equivalent to the Axiom of Choice and a huge collection of such equivalent forms of the Axiom of Choice was accumulated by Rubin and Rubin [79, 80].

The most popular variants of the Axiom of Choice — and the most often used in mathematical proofs — are probably the Well-Ordering Principle (discussed above), the Kuratowski-Zorn Lemma, and Teichmüller's Principle.

The Kuratowski-Zorn Lemma was proved independently by Kuratowski [53] and more than a decade later by Zorn [106] (see Moore [66, p. 223] and also Campbell [13]). Usually, the Kuratowski-Zorn Lemma is deduced quite easily from the Well-Ordering Principle. The direct deduction from the Axiom of Choice presented above (THEOREM 5.3) is due to Kneser [51], who also proved LEMMA 5.2 which was stated without proof by Bourbaki [12, p. 37 (lemme fondamental)].

Teichmüller's Principle was formulated independently by Tukey [103] and slightly earlier by Teichmüller in [97], where he provides also some equivalent forms of this very useful principle. Teichmüller himself was a member of the Nazi party and joined the army in 1939. Fighting first in Norway and then at the Eastern Front, he eventually died in 1943.

Kurepa's Principle was introduced by Kurepa in [54], where he showed that Kurepa's Principle together with the Linear-Ordering Principle — which states that every set can be linearly ordered — implies the Axiom of Choice. The proof that — in the presence of the Axiom of Foundation — Kurepa's Principle implies the Axiom of Choice is due to Felgner [18] (see also Felgner and Jech [20] or Jech [40, Theorem 9.1.(a)]).

The proof that "every vector space has an algebraic basis" implies Multiple Choice is taken from Blass [9], and the proof that Multiple Choice implies Kurepa's Principle is taken from Jech [40, Theorem 9.1.(a)] (compare with Chapter 7 | RELATED RESULT 44).

Among the dozens of cardinal relations which are equivalent to the Axiom of Choice (see for example Lindenbaum and Tarski [60], Bachmann [1, §31], or Moore [66, p. 330 f.]), we just mentioned three.

In 1895, Cantor [14, §2] asserted the Trichotomy of Cardinals without proof, and in a letter of 28 July 1899 (*cf.* [16, pp. 443–447]) he wrote to Dedekind that the Trichotomy of Cardinals follows from the Well-Ordering Principle. However, their equivalence remained unproven until Hartogs [34] established it in 1915 (*cf.* also Moore [66, p. 10]). As a matter of fact we would like to mention that — according to Sierpiński [82, p. 99 f.] — Leśniewski showed that Trichotomy of Cardinals is equivalent to the statement that for any two cardinals $\mathfrak{n}$ and $\mathfrak{m}$, where at least one of these cardinals is infinite, we always have $\mathfrak{n}+\mathfrak{m}=\mathfrak{n}$ or $\mathfrak{n}+\mathfrak{m}=\mathfrak{m}$.

THEOREM 5.5.(c) — which is to some extent a dualisation of the Trichotomy of Cardinals — was stated without proof by Lindenbaum [60, p. 312 (A_6)] and the proof given above is taken from Sierpiński [83, p. 426].

The fact that the cardinal equation $\mathfrak{m}^2=\mathfrak{m}$ implies the Axiom of Choice is due to Tarski [87] (see also Bachmann [1, V, p. 140 ff.]).

***Cardinal arithmetic in the presence of* AC.** The definition of cardinals given above can also be found for example in von Neumann [72, VII.2. p.731].

The first proof of THEOREM 5.7 appeared in Hessenberg [38, p. 593] (see also Jourdain [44]).

Regularity of cardinals was investigated by Hausdorff, who also raised the question of existence of regular limit cardinals (*cf.* [35, p. 131]).

The INEQUALITY OF KÖNIG-JOURDAIN-ZERMELO 5.11 — also known as KÖNIG'S THEOREM — was proven by König [52] (but only for countable sums and products), and independently by Jourdain [43] and by Zermelo [110] (for historical facts see Moore [66, p. 154] and Fraenkel [25, p. 98]). Obviously, the INEQUALITY OF KÖNIG-JOURDAIN-ZERMELO implies the Axiom of Choice (since it guarantees that every Cartesian product of non-empty sets is non-empty), and consequently we get that the INEQUALITY OF KÖNIG-JOURDAIN-ZERMELO is *equivalent* to the Axiom of Choice.

Algebras. Boolean algebra is named after George Boole who — according to Russell — discovered Pure Mathematics. Even though this might be an exaggeration, it is true that Boole was one of the first to view Mathematics as the study of abstract structures rather than as the science of magnitude, and he was the first who applied successfully mathematical techniques to Logic (*cf.* Boole [11, 10]) and his work evolved into the modern theory of Boolean algebras and algebraic Logic. In 1849, Boole was appointed at the newly founded Queen's College in Cork, where he died in 1864 as a result of pneumonia caused by walking to a lecture in a December downpour and lecturing all day in wet clothes (see also MacHale [61]).

Lindenbaum's algebra is named in memory of the Polish mathematician Adolf Lindenbaum, who was killed by the Gestapo at Nowa Wilejka in the summer of 1941. Lindenbaum and Tarski (see for example Tarski [90, 89, 91]) developed the idea of viewing the set of formulae as an algebra (with operations induced by the logical connectives) independently around 1935; however, Lindenbaum's results were not published (see Rasiowa and Sikorski [78, footnote to page 245]).

For the history of abstract algebraic Logic and Boolean algebras we refer the reader to Font, Jansana, and Pigozzi [22].

Prime Ideals. Ideals and prime ideals on algebras of sets where investigated for example by Tarski in [93].

The notion of Lindenbaum's algebra and the Compactness Theorem for Propositional Logic is taken from Bell and Slomson [2, Chapter 2]. The equivalent forms of the Prime Ideal Theorem are taken from Jech [40, Chapter 2, §3], and the corresponding references can be found in [40, Chapter 2, §7]. We would like to mention that the Ultrafilter Theorem, which is just the dual form of the Prime Ideal Theorem, is due to Tarski [88].

Ramsey's Theorem as a choice principle. RAMSEY'S ORIGINAL THEOREM (*cf.* Chapter 2) implies that every infinite set X has the following property: For every 2-colouring of $[X]^2$ there is an infinite subset Y of X such that $[Y]^2$ is monochromatic. As mentioned in Chapter 2, Ramsey [76] explicitly indicated that his proof of this theorem used the Axiom of Choice. Later, Kleinberg [50] showed that every proof of RAMSEY'S ORIGINAL THEOREM must use the Axiom of Choice, although rather weak forms of the Axiom of Choice like $\mathsf{C}(\aleph_0, \infty)$ suffice (see THEOREM 5.17). For the position of RAMSEY'S ORIGINAL THEOREM in the hierarchy of choice principles we refer the reader to Blass [8] (see also RELATED RESULT 31).

For the fact that none of the implications in THEOREM 5.17 is reversible we refer the reader to Howard and Rubin [39].

From countable choice to choice for finite sets. The Countable Axiom of Choice asserts that every *countable* family of non-empty sets has a choice function, whereas the Axiom of Choice for Finite Sets asserts that every family of non-empty *finite* sets has a choice function. Replacing the finite sets in the latter choice principle by n-element sets (for natural numbers $n \geq 2$), we obtained the choice principles C_n which assert that every family of n-element sets has a choice function. Combining these two choice principles we get in fact versions of König's Lemma, namely choice principles like $\mathsf{C}(\aleph_0, < \aleph_0)$ and $\mathsf{C}(\aleph_0, n)$ (for positive integers $n \geq 2$).

The proof of THEOREM 5.18 is taken from Jech [40, p. 111] and is optimal in the following sense: If the positive integers m, n do not satisfy condition (S), then there is a model of Set Theory in which C_k holds for every $k \leq m$ but C_n fails (see the proof of Theorem 7.16 in Jech [40]).

Related Results

22. *Hausdorff's Principle.* Among the numerous maximality principles which are equivalent to the Axiom of Choice, we like to mention the one known as Hausdorff's Principle (*cf.* Hausdorff [35, VI, §1, p. 140]):

    Hausdorff's Principle: Every partially ordered set has a maximal chain (maximal with respect to inclusion "$\subseteq$").

    For the history of Hausdorff's Principle see Moore [66, Section 3.4, p. 167 ff.] and a proof of the equivalence with the Axiom of Choice can be found for example in Bernays [5, p. 142 ff.].

23. *Bases in vector spaces and the Axiom of Choice.* Relations between the existence or non-existence of bases in vector spaces and some weaker forms of the Axiom of Choice are investigated for example in Keremedis [48, 49], Läuchli [55], and Halpern [33].

24. *Cardinal relations which are equivalent to* AC. Below we list a few of the dozens of cardinal relations which are equivalent to the Axiom of Choice (mainly taken from Tarski [87]):
    (a) $\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{m} + \mathfrak{n}$ for all infinite cardinals $\mathfrak{m}$ and $\mathfrak{n}$.
    (b) If $\mathfrak{m}^2 = \mathfrak{n}^2$, then $\mathfrak{m} = \mathfrak{n}$.
    (c) If $\mathfrak{m} < \mathfrak{n}$ and $\mathfrak{p} < \mathfrak{q}$, then $\mathfrak{m} + \mathfrak{p} < \mathfrak{n} + \mathfrak{q}$.
    (d) If $\mathfrak{m} < \mathfrak{n}$ and $\mathfrak{p} < \mathfrak{q}$, then $\mathfrak{m} \cdot \mathfrak{p} < \mathfrak{n} \cdot \mathfrak{q}$.
    (e) If $\mathfrak{m} + \mathfrak{p} < \mathfrak{n} + \mathfrak{p}$, then $\mathfrak{m} < \mathfrak{n}$.
    (f) If $\mathfrak{m} \cdot \mathfrak{p} < \mathfrak{n} \cdot \mathfrak{p}$, then $\mathfrak{m} < \mathfrak{n}$.
    (g) If $2\mathfrak{m} < \mathfrak{m} + \mathfrak{n}$, then $\mathfrak{m} < \mathfrak{n}$.

    For the proofs we refer the reader to Tarski [87] and Sierpiński [83, p. 421] (compare (g) with Chapter 4 | Related Result 17). More such cardinal relations can be found for example in Howard and Rubin [39, p. 82 ff.], Rubin and Rubin [80, p. 137 ff.], Moore [66, p. 330 f.], and Bachmann [1, §31]).

25. *Successors of Cardinals.* In [96] Tarski investigated the following three types of successor of a cardinal number:

    S_1. For every cardinal $\mathfrak{m}$ there is a cardinal $\mathfrak{n}$ such that $\mathfrak{m} < \mathfrak{n}$ and the formula $\mathfrak{m} < \mathfrak{p} < \mathfrak{n}$ does not hold for any cardinal $\mathfrak{p}$.

    S_2. For every cardinal $\mathfrak{m}$ there is a cardinal $\mathfrak{n}$ such that $\mathfrak{m} < \mathfrak{n}$ and for every cardinal $\mathfrak{p}$ the formula $\mathfrak{m} < \mathfrak{p}$ implies $\mathfrak{n} \leq \mathfrak{p}$.

    S_3. For every cardinal $\mathfrak{m}$ there is a cardinal $\mathfrak{n}$ such that $\mathfrak{m} < \mathfrak{n}$ and for every cardinal $\mathfrak{p}$ the formula $\mathfrak{p} < \mathfrak{n}$ implies $\mathfrak{p} \leq \mathfrak{m}$.

    Tarski [96] showed that S_1 can be proved without the help of the Axiom of Choice, whereas S_2 is equivalent to this axiom. The relation of S_3 with the Axiom of Choice was further investigated by Sobociński [84] and Truss [100] (see also Bachmann [1, §31, p. 141]).

26. *A formulation by Sudan.* Sudan [85] showed that the following statement is equivalent to the Axiom of Choice: Let $\mathfrak{m}$, $\mathfrak{n}$, and $\mathfrak{p}$ be arbitrary infinite cardinals. If $\mathfrak{m}$ and $\mathfrak{n}$ are either equal or $\mathfrak{n}$ is a S_1-successor (*i.e.*, a successor in the in the sense of S_1) of $\mathfrak{m}$, then also $\mathfrak{p} \cdot \mathfrak{m}$ and $\mathfrak{p} \cdot \mathfrak{n}$ are either equal or $\mathfrak{p} \cdot \mathfrak{n}$ is an S_1-successor of $\mathfrak{p} \cdot \mathfrak{m}$. For the influence of Tarski [87] on Sudan see Moore [66, p. 218].

27. *A formulation by Tarski.* There are also some equivalents of the Axiom of Choice which seemingly are far away of being choice principles. The following formulation by Tarski [92] is surely of this type: For every set N there is a set M such that $X \in M$ if and only if $X \subseteq M$ and for all $Y \subseteq X$ we have $|Y| \neq |N|$. Similar statements can be found in Tarski [94, 95] (see also Bachmann [1, §31.3]).

28. *Singular Cardinal Hypothesis.* The SINGULAR CARDINAL HYPOTHESIS states that for every singular cardinal κ, $2^{\mathrm{cf}(\kappa)} < \kappa$ implies $\kappa^{\mathrm{cf}(\kappa)} = \kappa^+$. Obviously, the SINGULAR CARDINAL HYPOTHESIS follows from the Generalised Continuum Hypothesis. On the other hand, the SINGULAR CARDINAL HYPOTHESIS is not provable within ZFC and in fact, the failure of the SINGULAR CARDINAL HYPOTHESIS is equiconsistent with the existence of a certain large cardinal (*cf.* Jech [42, p. 58 f. & Chapter 24]).

29. *Model Theory and the Prime Ideal Theorem.* Using Lindenbaum's algebra, Rasiowa and Sikorski [77] gave an alternative proof of GÖDEL'S COMPLETENESS THEOREM 3.4, and Henkin [36] proved that the Prime Ideal Theorem is equivalent to the COMPACTNESS THEOREM 3.7. Notice that by THEOREM 5.15 we just get that the Prime Ideal Theorem is equivalent to the Compactness Theorem for Propositional Logic, which is a seemingly weaker statement than the COMPACTNESS THEOREM 3.7.

30. *Colouring infinite graphs and the Prime Ideal Theorem*.* For n a positive integer consider the following statement:

    P_n. If G is a graph such that every finite subgraph of G is n-colourable, then G itself is n-colourable.

    The following implications are provable in Set Theory without the Axiom of Choice (see Mycielski [69, 70]):

    $$\mathsf{PIT} \Rightarrow \mathsf{P}_{n+1} \Rightarrow \mathsf{P}_n \Rightarrow \mathsf{C}(\infty, n)\,, \quad \mathsf{C}(\infty, 2) \Rightarrow \mathsf{P}_2$$

    On the other hand, Lévy [59] showed that for any n, $\mathsf{ZF} \nvdash \mathsf{C}(\infty, n) \Rightarrow \mathsf{P}_3$. Surprisingly, Läuchli showed in [57] that P_3 implies PIT, and consequently, for all $n \geq 3$, the equivalence $\mathsf{P}_n \Rightarrow \mathsf{PIT}$ is provable in Set Theory without the Axiom of Choice. However, the question whether there is a "direct" proof of $\mathsf{P}_3 \Rightarrow \mathsf{P}_4$ without involving PIT is still open.

31. *Ramsey's Theorem, König's Lemma, and countable choice.* Truss investigated in [102] versions of König's Lemma, where restrictions are placed on the degree of branching of the finitely branching tree. In particular, he investigated $\mathsf{C}(\aleph_0, n)$ for different $n \in \omega$. Later in [24], Forster and Truss considered the relation between versions of RAMSEY'S ORIGINAL THEOREM and these versions of König's Lemma.
    The choice principle $\mathsf{C}(\aleph_0, n)$ was also investigated by Wiśniewski [105], where it is compared with $\mathsf{C}(\infty, n)$ and other weak forms of the Axiom of Choice.

32. *Ramsey Choice*.* Related to C_n are the following two choice principles: C_n^- states that every infinite family X of n-element sets has an infinite subfamily $Y \subseteq X$ with a choice function; and RC_n states that for every infinite set X there is an infinite subset $Y \subseteq X$ such that $[Y]^n$ has a choice function. These two choice principles are both strictly weaker than C_n (*cf.* Truss [99]). Montenegro

investigated in [65] the relation between RC_n and C_n^- for some small values of n: It is not hard to see that $\mathsf{RC}_2 \Rightarrow \mathsf{C}_2^-$ and $\mathsf{RC}_3 \Rightarrow \mathsf{C}_3^-$ (*cf.* [65, Lemma]). However it is quite tricky to prove that $\mathsf{RC}_4 \Rightarrow \mathsf{C}_4^-$ (*cf.* [65, Theorem]) and it is still open whether RC_5 implies C_5^-.

33. *Well-ordered and well-orderable subsets of a set.* For a set x, $s(x)$ is the set of all subsets of x which can be well-ordered, and $w(x)$ is the set of all well-orderings of subsets of x. Notice that $s(x) \subseteq \mathscr{P}(x)$, whereas $w(x) \subseteq \mathscr{P}(x \times x)$. Tarski [94] showed — without the help of the Axiom of Choice — that $|x| < |s(x)|$, for any set x, and his proof also yields $|x| < |w(x)|$. Later, Truss showed in [101] that for any infinite set x and for any $n \in \omega$ we have $|s(x)| \nleq |x^n|$ as well as $|x^n| < |w(x)|$. Furthermore, he showed that if there is a choice function for the set of finite subsets of x, then $|x^n| < |s(x)|$. According to Howard and Rubin [39, p. 371] it is not known whether $|x^n| < |s(x)|$ (Form 283 of [39]) is provable in ZF. The cardinality of the set $w(x)$ was further investigated by Forster and Truss in [23].

34. *Axiom of Choice for families of n-element sets.* For different $n \in \omega$, C_n has been extensively studied by Mostowski in [67], and most of the following results — which are all provable without the help of the Axiom of Choice — can be found in that paper (see also Truss [99], Gauntt [27], or Jech [40, Chapter 7, §4]):
    (a) If m, n satisfy condition (S), then $n < 8m^2$.
    (b) $\mathsf{C}_2 \Rightarrow \mathsf{C}_n$ is provable if and only if $n \in \{1, 2, 4\}$.
    (c) For a finite set $Z = \{m_1, \dots, m_k\}$ of positive integers let C_Z denote the statement $\mathsf{C}_{m_1} \wedge \dots \wedge \mathsf{C}_{m_k}$. We say that Z, n satisfy condition (S) if for every decomposition of n into a sum of primes, $n = p_1 + \ldots + p_s$, at least one prime p_i belongs to Z. Now, the following condition holds: *If Z, n satisfy condition (S), then C_Z implies C_n.*
    (d) Let S_n be the group of all permutation of $\{1, \dots, n\}$. A subgroup G of S_n is said to be *fixed point free* if for every $i \in \{1, \dots, n\}$ there is a $\pi \in S_n$ such that $\pi(i) \neq i$. Let Z be again a finite set of positive integers. We say that Z, n satisfy condition (T) if for every fixed point free subgroup G of S_n there is a subgroup H of G and a finite sequence $H_1, \dots, H_k$ of proper subgroups of H such that the sum of indices $[H : H_1] + \ldots + [H : H_k]$ is in Z. Now, the following condition holds: *If Z, n satisfy condition (T), then C_Z implies C_n.* Moreover we have: *If Z, n do not satisfy condition (T), then there is a model of* ZF *in which C_Z holds and C_n fails.*

    We would also like to mention that the Axiom of Choice for Finite Sets $\mathsf{C}(\infty, < \aleph_0)$ is unprovable in ZF, even if we assume that C_n is true for each $n \in \omega$ (*cf.* Jech [40, Chapter 7, §4], or Lévy [58] and Pincus [75]).

35. *Ordering principles.* Among the numerous choice principles which deal with ordering we mention just two:

    Ordering Principle: Every set can be linearly ordered.

    If "$<$" and "$\prec$" are partial orderings of a set P, then we say that "$\prec$" **extends** "$<$" if for any $p, q \in P$, $p < q$ implies $p \prec q$.

    Order-Extension Principle: Every partial ordering of a set P can be extended to a linear ordering of P.

Obviously, the Order-Extension Principle implies the Ordering Principle, but the other direction fails (see Mathias [62]). Thus, the Ordering Principle is slightly weaker than the Order-Extension Principle. Furthermore, Szpilrajn (who changed his name from Szpilrajn to Marczewski while hiding from the Nazi persecution) showed in [86] that the Order-Extension Principle follows from the Axiom of Choice, where one can even replace the Axiom of Choice by the Prime Ideal Theorem (see for example Jech [40, 2.3.2]). We leave it as an exercise to the reader to show that the Ordering Principle implies $\mathsf{C}(\infty, < \aleph_0)$. Thus, we get the following sequence of implications:

$$\mathsf{PIT} \Rightarrow \text{Order-Extension Principle} \Rightarrow \text{Ordering Principle} \Rightarrow \mathsf{C}(\infty, < \aleph_0)$$

On the other hand, none of these implications is reversible (see Läuchli [56] and Pincus [74, §4B], Felgner and Truss [21, Lemma 2.1], Mathias [62], or Jech [40, Chapter 7]; compare also with Chapter 7 | RELATED RESULT 48).

36. *More ordering principles.* Mathias showed in [62] that the following assertion does not imply the Order-Extension Principle:

    If X is a set of well-orderable sets, then there is a function f such that for each $x \in X$, $f(x)$ is a well-ordering of x.

    On the other hand, Truss [98] showed that following assertion, apparently only slightly stronger than the ordering principle above, implies the Axiom of Choice:

    If X is a set and f a function on X such that for each $x \in X$, $f(x)$ is a non-empty set of well-orderings of x, then $\{f(x) : x \in X\}$ has a choice function.

37. *Principle of Dependent Choices.* Finally, let us mention a choice principle which is closely related to the Countable Axiom of Choice. Its meaning is that one is allowed to make a countable number of consecutive choices.

    Principle of Dependent Choices: If R is a binary relation on a non-empty set S, and if for every $x \in S$ there exists $y \in S$ with xRy, then there is a sequence $\langle x_n : n \in \omega \rangle$ of elements of S such that for all $n \in \omega$ we have $x_n R x_{n+1}$.

    The Principle of Dependent Choices, usually denoted DC, was formulated by Bernays in [4] and for example investigated by Mostowski [68] (see also Jech [40, Chapter 8]). Even though DC is significantly weaker than AC, it is stronger than $\mathsf{C}(\aleph_0, \infty)$ and (thus) implies for example that every Dedekind-finite set is finite (*i.e.*, every infinity set is transfinite). Thus, in the presence of DC, many — kind of natural — propositions are still provable. On the other hand, having just DC instead of full AC, most of the somewhat paradoxical constructions (*e.g.*, making two balls from one) cannot be carried out anymore (see Herrlich [37] for some 'disasters' that happen with and without AC). In my opinion, DC reflects best our intuition, and consequently, ZF+DC would be a quite reasonable and smooth axiomatic system for Set Theory; however, it is not suitable for really exciting results.

38. *An alternative to the Axiom of Choice.* Let $\omega \to (\omega)^\omega$ be the statement that whenever the set $[\omega]^\omega$ is coloured with 2 colours, there exists an infinite subset

of ω, all whose infinite subsets have the same colour (compare with the *Ramsey property* defined in Chapter 9). In Chapter 2 we have seen that $\omega \to (\omega)^\omega$ fails in the presence of the Axiom of Choice. On the other hand, Mathias proved that under the assumption of the existence of an *inaccessible cardinal* (defined on page 315), $\omega \to (\omega)^\omega$ is consistent with ZF+DC (see Mathias [64, Theorem 5.1]). The combinatorial statement $\omega \to (\omega)^\omega$ has many interesting consequences: For example Mathias [63] gave an elementary proof of the fact that if $\omega \to (\omega)^\omega$ holds, then there are no so-called *rare filters* and every ultrafilter over ω is principal (see Mathias [64, p. 91 ff.] for similar results).

39. *The Axiom of Determinacy.* Another alternative to the Axiom of Choice is the Axiom of Determinacy, which asserts that all games of a certain type are determined. In order to be more precise we have to introduce first some terminology: With each subset A of ${}^\omega\omega$ we associate the following game $\mathcal{G}_A$, played by two players I and II. First I chooses a natural number a_0, then II chooses a natural number b_0, then I chooses a_1, then II chooses b_1, and so on. The game ends after ω steps: if the resulting sequence $\langle a_0, b_0, a_1, b_1, \ldots \rangle$ is in A, then I wins, otherwise II wins. A *strategy* (for I or II) is a rule that tells the player what move to make depending on the previous moves of both players; and a strategy is a *winning strategy* if the player who follows it always wins (for a more formal definition see Chapter 10). The game $\mathcal{G}_A$ is *determined* if one of the players has a winning strategy.

Axiom of Determinacy (AD): For every set $A \subseteq {}^\omega\omega$ the game $\mathcal{G}_A$ is determined, *i.e.*, either player I or player II has winning strategy.

An easy diagonal argument shows that AC is incompatible with AD, *i.e.*, assuming the Axiom of Choice there exists a set $A \subseteq {}^\omega\omega$ such that the game $\mathcal{G}_A$ is not determined (*cf.* Jech [42, Lemma 33.1]). In contrast we have that AD implies that every countable family of non-empty sets of reals has a choice function (*cf.* Jech [42, Lemma 33.2]). Moreover, one can show that Con(ZF+AD) implies Con(ZF + AD + DC), thus, even in the presence of AD we still can have DC. Furthermore, AD implies that sets of reals are well behaved, *e.g.*, every set of reals is *Lebesgue measurable*, has the *property of Baire*, and every uncountable set of reals contains a *perfect subset*, *i.e.*, a closed set without isolated points (*cf.* Jech [42, Theorem 33.3]); however, it also implies that every ultrafilter over ω is principal (*cf.* Kanamori [45, Proposition 28.1]) and that $\aleph_1$ and $\aleph_2$ are both measurable cardinals (*cf.* Jech [42, Theorem 33.12]). Because of its nice consequences for sets of reals, AD is a reasonable alternative to AC, especially for the investigation of the real line (for the beauty of ZF + AD see for example Herrlich [37, Section 7.2]). In 1962, when Mycielskiand Steinhaus [71] introduced the Axiom of Determinacy, they did not claim this new axiom to be intuitively true, but stated that the purpose of their paper is *only to propose another theory which seems very interesting although its consistency is problematic.* Since AD implies the existence of large cardinals, the consistency of ZF + AD cannot be derived from that of ZF. Moreover, using very sophisticated techniques — far beyond the scope of this book — Woodin proved that ZF + AD is equiconsistent with ZFC + "There are infinitely many Woodin cardinals" (*cf.* Kanamori [45, Theorem 32.16] or Jech [42, Theorem 33.27]). Further results and the corresponding references can be found for example in Kanamori [45, Chapter 6] and Jech [42, Chapter 33].

References

1. Heinz Bachmann, ***Transfinite Zahlen***, Springer-Verlag, Berlin · Heidelberg, 1967.
2. John L. Bell and Alan B. Slomson, ***Models and Ultraproducts: An Introduction***, North-Holland, Amsterdam, 1969.
3. Paul Bernays, *Sur le platonisme dans les mathématiques*, ***L'Enseignement Mathématique***, vol. 34 (1935), 52–69 (see [7]/[6] for a translation into English/German).
4. ———, *A system of axiomatic set theory. III: Infinity and enumerability. Analysis.*, ***The Journal of Symbolic Logic***, vol. 7 (1942), 65–89.
5. ———, ***Axiomatic Set Theory.*** *With a historical introduction by Abraham A. Fraenkel*, 2nd ed., [Studies in Logic and the Foundations of Mathematics], North-Holland, Amsterdam, 1968 [reprint: Dover Publications, New York, 1991].
6. ———, ***Abhandlungen zur Philosophie der Mathematik***, Wissenschaftliche Buchgesellschaft, Darmstadt, 1976.
7. ———, *On platonism in mathematics*, in ***Philosophy of Mathematics. Selected Readings*** (Paul Benacerraf and Hilary Putnam, eds.), Cambridge University Press, Cambridge, 2nd ed., 1983, pp. 258–271.
8. Andreas Blass, *Ramsey's theorem in the hierarchy of choice principles*, ***The Journal of Symbolic Logic***, vol. 42 (1977), 387–390.
9. ———, *Existence of bases implies the axiom of choice*, in ***Axiomatic Set Theory*** (James E. Baumgartner, Donald A. Martin, and Saharon Shelah, eds.), Contemporary Mathematics, vol. 31, American Mathematical Society, Providence, RI, 1984, pp. 31–33.
10. George Boole, *The calculus of logic*, ***The Cambridge and Dublin Mathematical Journal***, vol. 3 (1848), 183–198.
11. ———, ***An Investigation of the Laws of Thought, on Which are Founded the Mathematical Theories of Logic and Probabilities***, Walton and Maberley, London, 1854 [reprint: Prometheus Books, New York, 2003].
12. Nicolas Bourbaki, ***Éléments de mathématique. Première partie: Les structures fondamentales de l'analyse. Livre I. Théorie des ensembles (Fascicule de résultats)***, Hermann & Cie., Paris, 1939.
13. Paul J. Campbell, *The origin of "Zorn's lemma"*, ***Historia Mathematica***, vol. 5 (1978), 77–89.
14. Georg Cantor, *Beiträge zur Begründung der transfiniten Mengenlehre. I./ II.*, ***Mathematische Annalen***, vol. 46/49 (1895/1897), 481–512/207–246 (see [15] for a translation into English).
15. ———, ***Contributions to the Founding of the Theory of Transfinite Numbers,*** (translation into English of [14]), [translated, and provided with an introduction and notes, by Philip E. B. Jourdain], Open Court Publishing Company, Chicago and London, 1915 [reprint: Dover Publications, New York, 1952].
16. ———, ***Gesammelte Abhandlungen mathematischen und philosophischen Inhalts***, *Mit Erläuternden Anmerkungen sowie mit Ergänzungen aus dem Briefwechsel Cantor-Dedekind*, edited by E. Zermelo, Julius Springer, Berlin, 1932.
17. Heinz-Dieter Ebbinghaus (in cooperation with Volker Peckhaus), ***Ernst Zermelo, An Approach to His Life and Work***, Springer-Verlag, Berlin · Heidelberg, 2007.

18. Ulrich Felgner, *Die Existenz wohlgeordneter, konfinaler Teilmengen in Ketten und das Auswahlaxiom*, ***Mathematische Zeitschrift***, vol. 111 (1969), 221–232 (*cf.* also [19]).
19. ———, *Berichtigung zu "Die Existenz wohlgeordneter, konfinaler Teilmengen in Ketten und das Auswahlaxiom"*, ***Mathematische Zeitschrift***, vol. 115 (1970), 392.
20. Ulrich Felgner and Thomas Jech, *Variants of the axiom of choice in set theory with atoms*, ***Fundamenta Mathematicae***, vol. 79 (1973), 79–85.
21. Ulrich Felgner and John K. Truss, *The independence of the prime ideal theorem from the order-extension principle*, ***The Journal of Symbolic Logic***, vol. 64 (1999), 199–215.
22. Josep Maria Font, Ramon Jansana, and Don Pigozzi, *A survey of abstract algebraic logic*, ***Studia Logica***, vol. 74 (2003), 13–97.
23. Thomas E. Forster and John K. Truss, *Non-well-foundedness of well-orderable power sets*, ***The Journal of Symbolic Logic***, vol. 68 (2003), 879–884.
24. ———, *Ramsey's Theorem and König's Lemma*, ***Archive for Mathematical Logic***, vol. 46 (2007), 37–42.
25. Abraham A. Fraenkel, ***Abstract Set Theory***, [Studies in Logic and the Foundations of Mathematics], North-Holland, Amsterdam, 1961.
26. Abraham A. Fraenkel, Yehoshua Bar-Hillel, and Azriel Levy, ***Foundations of Set Theory***, [Studies in Logic and the Foundations of Mathematics 67], North-Holland, Amsterdam, 1973.
27. Robert. J. Gauntt, *Axiom of choice for finite sets – A solution to a problem of Mostowski*, ***Notices of the American Mathematical Society***, vol. 17 (1970), 454.
28. Kurt Gödel, *The consistency of the axiom of choice and of the generalized continuum-hypothesis*, ***Proceedings of the National Academy of Sciences (U.S.A.)***, vol. 24 (1938), 556–557 (reprinted in [31]).
29. ———, *Consistency-proof for the generalized continuum-hypothesis*, ***Proceedings of the National Academy of Sciences (U.S.A.)***, vol. 25 (1939), 220–224 (reprinted in [31]).
30. ———, ***The Consistency of the Axiom of Choice and of the Generalized Continuum-Hypothesis with the Axioms of Set Theory***, [Annals of Mathematics Studies 3], Princeton University Press, Princeton (New Jersey), 1940 (reprinted in [31]).
31. ———, ***Collected Works, Volume II: Publications 1938–1974***, edited by S. Feferman (Editor-in-chief), J. W. Dawson, Jr., S. C. Kleene, G. H. Moore, R. M. Solovay, J. van Heijenoort, Oxford University Press, New York, 1990.
32. Michael Hallett, ***Cantorian Set Theory and Limitation of Size***, Oxford Logic Guides 10, The Clarendon Press Oxford University Press, New York, 1984.
33. James D. Halpern, *Bases in vector spaces and the axiom of choice*, ***Proceedings of the American Mathematical Society***, vol. 17 (1966), 670–673.
34. Friedrich Hartogs, *Über das Problem der Wohlordnung*, ***Mathematische Annalen***, vol. 76 (1915), 438–443.
35. Felix Hausdorff, ***Grundzüge der Mengenlehre***, de Gruyter, Leipzig, 1914 [reprint: Chelsea, New York, 1965].

36. Leon Henkin, *Metamathematical theorems equivalent to the prime ideal theorems for Boolean algebras*, ***Bulletin of the American Mathematical Society***, vol. 60 (1954), 388.
37. Horst Herrlich, ***Axiom of Choice***, [Lecture Notes in Mathematics 1876], Springer-Verlag, Berlin · Heidelberg, 2006.
38. Gerhard Hessenberg, ***Grundbegriffe der Mengenlehre***, Vandenhoeck & Ruprecht, Göttingen, 1906.
39. Paul Howard and Jean E. Rubin, ***Consequences of the Axiom of Choice***, [Mathematical Surveys and Monographs], vol. 59, American Mathematical Society, 1998.
40. Thomas Jech, ***The Axiom of Choice***, Studies in Logic and the Foundations of Mathematics 75, North-Holland, Amsterdam, 1973.
41. ———, *About the axiom of choice*, in ***Handbook of Mathematical Logic*** (J. Barwise, ed.), North-Holland, Amsterdam, 1977, pp. 345–370.
42. ———, ***Set Theory***, *The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
43. Philip E. B. Jourdain, *On infinite sums and products of cardinal numbers*, ***The Quarterly Journal of Pure and Applied Mathematics***, vol. 39 (1907), 375–384.
44. ———, *The multiplication of Alephs*, ***Mathematische Annalen***, vol. 65 (1908), 506–512.
45. Akihiro Kanamori, ***The Higher Infinite, Large Cardinals in Set Theory from Their Beginnings***, [Perspectives in Mathematical Logic], Springer-Verlag, Heidelberg, 1994.
46. ———, *The mathematical import of Zermelo's well-ordering theorem*, ***The Bulletin of Symbolic Logic***, vol. 3 (1997), 281–311.
47. ———, *Gödel and set theory*, ***The Bulletin of Symbolic Logic***, vol. 13 (2007), 153–188.
48. Kyriakos Keremedis, *Bases for vector spaces over the two-element field and the axiom of choice*, ***Proceedings of the American Mathematical Society***, vol. 124 (1996), 2527–2531.
49. ———, *Extending independent sets to bases and the axiom of choice*, ***Mathematical Logic Quarterly***, vol. 44 (1998), 92–98.
50. Eugene M. Kleinberg, *The independence of Ramsey's theorem*, ***The Journal of Symbolic Logic***, vol. 34 (1969), 205–206.
51. Hellmuth Kneser, *Eine direkte Ableitung des Zornschen Lemmas aus dem Auswahlaxiom*, ***Mathematische Zeitschrift***, vol. 53 (1950), 110–113.
52. Julius König, *Zum Kontinuum-Problem*, ***Mathematische Annalen***, vol. 60 (1905), 177–180.
53. Casimir Kuratowski, *Une méthode d'élimination des nombres transfinis des raisonnements mathématiques*, ***Fundamenta Mathematicae***, vol. 3 (1922), 76–108.
54. Djuro (George) Kurepa, *Über das Auswahlaxiom*, ***Mathematische Annalen***, vol. 126 (1953), 381–384.
55. Hans Läuchli, *Auswahlaxiom in der Algebra*, ***Commentarii Mathematici Helvetici***, vol. 37 (1962), 1–18.
56. ———, *The independence of the ordering principle from a restricted axiom of choice*, ***Fundamenta Mathematicae***, vol. 54 (1964), 31–43.
57. ———, *Coloring infinite graphs and the Boolean prime ideal theorem*, ***Israel Journal of Mathematics***, vol. 9 (1971), 422–429.

58. Azriel Lévy, *Axioms of multiple choice*, ***Fundamenta Mathematicae***, vol. 50 (1961), 475–483.
59. ———, *Remarks on a paper by J. Mycielski*, ***Acta Mathematica Academiae Scientiarum Hungaricae***, vol. 14 (1963), 125–130.
60. Adolf Lindenbaum and Alfred Tarski, *Communication sur les recherches de la théorie des ensembles*, ***Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III***, vol. 19 (1926), 299–330.
61. Desmond MacHale, *George Boole 1815–64*, in ***Creators of Mathematics: The Irish Connection*** (Ken Houston, ed.), University College Dublin Press, Dublin, 2000, pp. 27–32.
62. Adrian Richard David Mathias, *The order extension principle*, in ***Axiomatic set theory*** (Thomas J. Jech, ed.), [Proceedings of Symposia in Pure Mathematics, Vol. XIII, Part II], American Mathematical Society, Providence, Rhode Island, 1974, pp. 179–183.
63. ———, *A remark on rare filters*, in ***Infinite and Finite Sets*** (A. Hajnal, R. Rado, and V. Sós, eds.), [Colloquium Keszthely, Hungary, 1973; dedicated to P. Erdős on his 60th birthday], Colloquia Mathematica Societatis János Bolyai, vol. 10, North-Holland, Amsterdam, 1975, pp. 1095–1097.
64. ———, *Happy families*, ***Annals of Mathematical Logic***, vol. 12 (1977), 59–111.
65. Carlos H. Montenegro, *Weak versions of the axiom of choice for families of finite sets*, in ***Models, algebras, and proofs,*** *Selected papers of the X Latin American symposium on mathematical logic held in Bogotá, Colombia, June 24–29, 1995* (X. Caicedo and C. Montenegro, eds.), [Lecture Notes in Pure and Applied Mathematics 203], Marcel Dekker, New York · Basel, 1999, pp. 57–60.
66. Gregory H. Moore, ***Zermelo's Axiom of Choice. Its origins, development, and influence***, [Studies in the History of Mathematics and Physical Sciences 8], Springer-Verlag, New York, 1982.
67. Andrzej Mostowski, *Axiom of choice for finite sets*, ***Fundamenta Mathematicae***, vol. 33 (1945), 137–168.
68. ———, *On the principle of dependent choices*, ***Fundamenta Mathematicae***, vol. 35 (1948), 127–130.
69. Jan Mycielski, *Some remarks and problems on the colouring of infinite graphs and the theorem of Kuratowski*, ***Acta Mathematica Academiae Scientiarum Hungaricae***, vol. 12 (1961), 125–129.
70. ———, *Correction to: "On the colouring of infinite graphs and the theorem of Kuratowski"*, ***Acta Mathematica Academiae Scientiarum Hungaricae***, vol. 18 (1967), 339–340.
71. Jan Mycielski and Hugo Steinhaus, *A mathematical axiom contradicting the axiom of choice*, ***Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques***, vol. 10 (1962), 1–3.
72. John von Neumann, *Die Axiomatisierung der Mengenlehre*, ***Mathematische Zeitschrift***, vol. 27 (1928), 669–752.
73. Giuseppe Peano, *Démonstration de l'intégrabilité des équations différentielles ordinaires*, ***Mathematische Annalen***, vol. 37 (1890), 182–228.
74. David Pincus, *Zermelo-Fraenkel consistency results by Fraenkel-Mostowski methods*, ***The Journal of Symbolic Logic***, vol. 37 (1972), 721–743.

75. ______, *The strength of the Hahn-Banach theorem*, in ***Victoria Symposium on Nonstandard Analysis** (Univ. Victoria, Victoria, B.C., 1972)*, [Lecture Notes in Mathematics 369], Springer-Verlag, Berlin, 1974, pp. 203–248.
76. Frank P. Ramsey, *On a problem of formal logic*, ***Proceedings of the London Mathematical Society, Ser. II***, vol. 30 (1930), 264–286.
77. Helena Rasiowa and Roman Sikorski, *A proof of the completeness theorem of Gödel*, ***Fundamenta Mathematicae***, vol. 37 (1950), 193–200.
78. ______, ***The Mathematics of Metamathematics***, [Monografie Matematyczne, Tom 41], Państwowe Wydawnictwo Naukowe, Warsaw, 1963.
79. Herman Rubin and Jean E. Rubin, ***Equivalents of the Axiom of Choice***, [Studies in Logic and the Foundations of Mathematics], North-Holland, Amsterdam, 1963.
80. ______, ***Equivalents of the Axiom of Choice, II***, [Studies in Logic and the Foundations of Mathematics 116], North-Holland, Amsterdam, 1985.
81. Stewart Shapiro, *We hold these truths to be self-evident: but what do we mean by that?*, ***The Review of Symbolic Logic***, vol. 2 (2009), 175–207.
82. Wacław Sierpiński, ***Leçons sur les nombres transfinis***, Gauthier-Villars et Fils, Paris, 1928.
83. ______, ***Cardinal and Ordinal Numbers***, Państwowe Wydawnictwo Naukowe, Warszawa, 1958.
84. Bolesław Sobociński, *A remark concerning the third theorem about the existence of successors of cardinals*, ***Notre Dame Journal of Formal Logic***, vol. 3 (1962), 279–283.
85. Gabriel Sudan, *Sur une note de A. Tarski*, ***Comptes Rendus des Séances de l'Institut des Sciences de Roumanie***, vol. 3 (1939), 7–8.
86. Edward Szpilrajn, *Sur l'extension de l'ordre partiel*, ***Fundamenta Mathematicae***, vol. 16 (1930), 386–389.
87. Alfred Tajtelbaum-Tarski, *Sur quelques théorèmes qui équivalent à l'axiome du choix*, ***Fundamenta Mathematicae***, vol. 5 (1924), 147–154.
88. Alfred Tarski, *Une contribution à la théorie de la mesure*, ***Fundamenta Mathematicae***, vol. 15 (1930), 42–50.
89. ______, *Grundzüge des Systemenkalküls. I.*, ***Fundamenta Mathematicae***, vol. 25 (1935), 503–526.
90. ______, *Zur Grundlegung der Boole'schen Algebra I.*, ***Fundamenta Mathematicae***, vol. 24 (1935), 177–198.
91. ______, *Grundzüge des Systemenkalküls. II.*, ***Fundamenta Mathematicae***, vol. 26 (1936), 283–301.
92. ______, *Eine äquivalente Formulierung des Auswahlaxioms*, ***Fundamenta Mathematicae***, vol. 30 (1938), 197–201.
93. ______, *Ideale in vollstï£¡digen Mengenkï£¡pern. I.*, ***Fundamenta Mathematicae***, vol. 32 (1939), 45–63.
94. ______, *On well-ordered subsets of any set*, ***Fundamenta Mathematicae***, vol. 32 (1939), 176–183.
95. ______, *Axiomatic and algebraic aspects of two theorems on sums of cardinals*, ***Fundamenta Mathematicae***, vol. 35 (1948), 79–104.
96. ______, *Theorems on the existence of successors of cardinals and the axiom of choice*, ***Koninklijke Nederlandse Akademie van Wetenschappen. Proceedings of the Section of Sciences, Ser. A***, vol. 57 (1954), 26–32.
97. Oswald Teichmüller, *Braucht der Algebraiker das Auswahlaxiom?*, ***Deutsche Mathematik***, vol. 4 (1939), 567–577.

98. John K. Truss, *Two equivalents of the axiom of choice*, ***Journal of the London Mathematical Society (2)***, vol. 6 (1972), 175–176.
99. ______, *Finite axioms of choice*, ***Annals of Mathematicsl Logic***, vol. 6 (1973), 147–176.
100. ______, *On successors in cardinal arithmetic*, ***Fundamenta Mathematicae***, vol. 78 (1973), 7–21.
101. ______, *The well-ordered and well-orderable subsets of a set*, ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik***, vol. 19 (1973), 211–214.
102. ______, *Some cases of König's lemma*, in ***Set Theory and Hierarchy Theory*** (W. Marek, M. Srebrny, and A. Zarach, eds.), [Lecture Notes in Mathematics 537], Springer-Verlag, Berlin, 1976, pp. 273–284.
103. John W. Tukey, ***Convergence and Uniformity in Topology***, [Annals of Mathematics Studies 2], Princeton University Press, Princeton (New Jersey), 1940.
104. Jean van Heijenoort, ***From Frege to Gödel. A Source Book in Mathematical Logic, 1879–1931***, [Source Books in the History of Science], Harvard University Press, Cambridge, Massachusetts, 1967.
105. Kazimierz Wiśniewski, *On the axiom of choice for families of finite sets*, ***Fundamenta Mathematicae***, vol. 73 (1972), 187–192.
106. Max Zorn, *A remark on method in transfinite algebra*, ***Bulletin of the American Mathematical Society***, vol. 41 (1935), 667–670.
107. Ernst Zermelo, *Beweis, dass jede Menge wohlgeordnet werden kann*, ***Mathematische Annalen***, vol. 59 (1904), 514–516 (see [104, 109] for a translation into English).
108. ______, *Neuer Beweis für die Möglichkeit einer Wohlordnung*, ***Mathematische Annalen***, vol. 65 (1908), 107–128 (see [104, 109] for a translation into English).
109. ______, ***Collected Works / Gesammelte Werke***, *Volume I: Set Theory, Miscellanea / Band I: Mengenlehre, Varia*, [Schriften der Mathematisch-naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften, Nr. 21 (2010)], edited by Heinz-Dieter Ebbinghaus, Craig G. Fraser, and Akihiro Kanamori, Springer-Verlag, Berlin · Heidelberg, 2010.
110. ______, *Untersuchungen über die Grundlagen der Mengenlehre. I.*, ***Mathematische Annalen***, vol. 65 (1908), 261–281 (see [104, 109] for a translation into English).

6

How to Make Two Balls from One

Rests, which are so convenient to the composer and singer, arose for two reasons: necessity and the desire for ornamentation. As for necessity, it would be impossible to sing an entire composition without pausing, for it would cause fatigue that might well prevent a singer from finishing.
Rest were adopted also for the sake of ornament. With them parts could enter one after another in fugue or consequence, procedures that give a composition an artful and pleasing effect.

Gioseffo Zarlino
Le Istitutioni Harmoniche, 1558

For two reasons we shall give the reader a rest: one reason is that the reader deserves a pause to reflect on the axioms of ZFC; the other reason is that we would like to show Robinson's beautiful construction — relying on AC — of how to make two balls from one by dividing the ball into only five parts.

Equidecomposability

Two geometrical figures A and A' (*i.e.*, two sets of points lying on the straight line $\mathbb{R}$, on the plane $\mathbb{R}^2$, or in the three-dimensional space $\mathbb{R}^3$) are said to be **congruent**, denoted $A \cong A'$, if A can be obtained from A' by translation and/or rotation, but we shall exclude reflections. Two geometrical figures A and A' are said to be **equidecomposable**, denoted $A \simeq A'$, if there is a positive integer n and partitions $A = A_1 \dot\cup \ldots \dot\cup A_n$ and $A' = A'_1 \dot\cup \ldots \dot\cup A'_n$

such that for all $1 \leq i \leq n$: $A_i \cong A'_i$. To indicate that A and A' are equidecomposable using at most n pieces we shall write $A \simeq_n A'$.

Below we shall present two somewhat paradoxical decompositions of the 2-*dimensional unit sphere* S_2 as well as of the 3-*dimensional solid unit ball* B_1:

Firstly we show that the unit sphere S_2 can be partitioned into four parts, say $S_2 = A \dot{\cup} B \dot{\cup} C \dot{\cup} F$, such that F is countable, $A \cong B \cong C$, and $A \cong B \dot{\cup} C$. This result is known as Hausdorff's Paradox, even though it is just a paradoxical partition of the sphere S_2 rather than a paradox.

Secondly we show how to make two balls from one, in fact we show that $B_1 \simeq_5 B_1 \dot{\cup} B_1$. This result is due to Robinson and is optimal with respect to the number of pieces needed, *i.e.*, $B_1 \not\simeq_4 B_1 \dot{\cup} B_1$. We would like to mention that about two decades earlier, Banach and Tarski already showed that a unit ball and two unit balls are equidecomposable; however, their construction requires many more than five pieces.

Both decompositions, Hausdorff's partition of the sphere as well as Robinson's decomposition of the ball, rely on the Axiom of Choice. Moreover, it can be shown that in the absence of the Axiom of Choice neither decomposition is provable — but this is beyond the scope of this book (see RELATED RESULT 41). However, before we start the constructions, let us briefly discuss the measure-theoretical background of these somewhat paradoxical partitions, in particular of the decomposition of the ball: Firstly, why does Robinson's decomposition of the ball seem paradoxical? Of course, it is because the volume is not preserved; but what are volumes? One could consider the notion of volume as a function μ which assigns to each set $X \subseteq \mathbb{R}^3$ a non-negative real number, called the *volume of* A. We require that the function μ has the following basic properties:

- $\mu(\emptyset) = 0$ and $\mu(B_1) > 0$ (*e.g.*, $\mu(B_1) = 1$),
- $\mu(X \cup Y) = \mu(X) + \mu(Y)$ whenever X and Y are disjoint, and
- $\mu(X) = \mu(Y)$ whenever X and Y are congruent.

Now, by the fact that a unit ball and two unit balls are equidecomposable, and implicitly by Hausdorff's result (see below), we see that there is no such measure on $\mathbb{R}^3$, *i.e.*, μ is not defined for all subsets of $\mathbb{R}^3$. Roughly speaking, there are some dust-like subsets of $\mathbb{R}^3$ (like the sets we shall construct) to which we cannot assign a volume. Having this in mind, Robinson's decomposition loses its paradoxical character — but certainly not its beauty.

Hausdorff's Paradox

Before we show how to make two balls from one, we will present Hausdorff's partition of the sphere. The itinerary is as follows: Firstly we define an infinite subgroup H of SO(3), where SO(3) is the so-called *special orthogonal group* consisting of all rotations in $\mathbb{R}^3$ leaving fixed the origin. Even though the group H is infinite, it is generated by just two elements. Since H is a subgroup of SO(3), there is a natural action of H on the unit sphere S_2 which induces an equivalence relation on S_2 by $x \sim y \iff \exists g \in H\big(g(x) = y\big)$ (*i.e.*, $x \sim y$ *iff* y belongs to the *orbit* of x). Then we choose from each equivalence class a representative — this is where the Axiom of Choice comes in — and use the set of representatives to define Hausdorff's partition of the sphere.

We begin the construction by defining the group H. For this, consider the following two elements of SO(3), which will be the generators of H:

$$\varphi = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad\qquad \psi = \frac{1}{4}\begin{pmatrix} -2 & -\sqrt{6} & \sqrt{6} \\ \sqrt{6} & 1 & 3 \\ -\sqrt{6} & 3 & 1 \end{pmatrix}$$

The linear mapping φ is the rotation through π about the axis $(0,0,1)$, and ψ is the rotation through $2\pi/3$ about the axis $(0,1,1)$. Thus, $\varphi^2 = \psi^3 = \iota$ where ι denotes the identity. We leave it as an exercise to the reader to show by induction on n that for all integers $n \geq 1$ and for all $\varepsilon_k = \pm 1$ (where $1 \leq k \leq n$) we have:

$$\big(\varphi\,\psi^{\varepsilon_n}\cdots\varphi\,\psi^{\varepsilon_1}\big) \;=\; \frac{1}{2^{n+1}}\begin{pmatrix} a_1 & a_2\sqrt{6} & a_3\sqrt{6} \\ b_1\sqrt{6} & b_2 & b_3 \\ b_1'\sqrt{6} & b_2' & b_3' \end{pmatrix}$$

where all numbers $a_1, a_2, \ldots, b_3'$ are integers with

- $a_1 \equiv 2 \mod 4$,
- $a_2, a_3, b_1, \ldots, b_3'$ are odd, and
- $b_1 \equiv b_1'$, $b_2 \equiv b_2'$, $b_3 \equiv b_3' \mod 4$.

Hence, we conclude that for all $n \geq 1$: $\big(\varphi\,\psi^{\varepsilon_n}\cdots\varphi\,\psi^{\varepsilon_1}\big) \notin \{\iota, \varphi\}$. Consequently, for all $n \geq 1$, for all $\varepsilon_k = \pm 1$ (where $1 \leq k \leq n$), and for $\varepsilon_0 \in \{0,1\}$ and $\varepsilon_{n+1} \in \{0, \pm 1\}$, we get:

$$\psi^{\varepsilon_{n+1}} \cdot \big(\varphi\,\psi^{\varepsilon_n}\cdots\varphi\,\psi^{\varepsilon_1}\big) \cdot \varphi^{\varepsilon_0} \;\neq\; \iota \qquad (*)$$

In other words, the only relations between φ and ψ are $\varphi^2 = \psi^3 = \iota$. Let H be the group of linear transformations — in fact rotations — of $\mathbb{R}^3$ generated by the two rotations φ and ψ. Then H is a subgroup of SO(3) and every element of H is a rotation which corresponds, by $(*)$, to a unique reduced "word" of the form

$$\psi^{\varepsilon_{n+1}}\varphi\,\psi^{\varepsilon_n}\cdots\varphi\,\psi^{\varepsilon_1}\varphi^{\varepsilon_0}$$

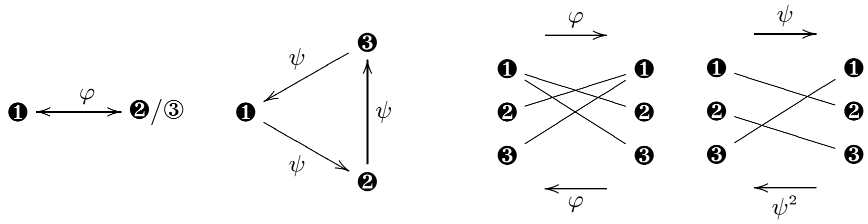
where $n \geq 0$, $\varepsilon_k = \pm 1$ (for all $1 \leq k \leq n$), $\varepsilon_0 \in \{0,1\}$, and $\varepsilon_{n+1} \in \{0, \pm 1\}$.

We now consider the so-called Cayley graph of H: The **Cayley graph** of H is a graph with vertex set H, where for $\rho_1, \rho_2 \in H$ there is a directed edge from ρ_1 to ρ_2 if either $\rho_2 = \varphi\rho_1$ or $\rho_2 = \psi\rho_1$. In the former case, the edge is labelled φ, in the latter case it is labelled ψ, *e.g.*, $\psi\varphi \xrightarrow{\varphi} \varphi\psi\varphi$ or $\psi^2\varphi \xrightarrow{\psi} \varphi$.

To each vertex of the Cayley graph of H (*i.e.*, to each element of H) we assign a label, which is either ❶, ❷, or ❸. The labelling is done according to the following rules:

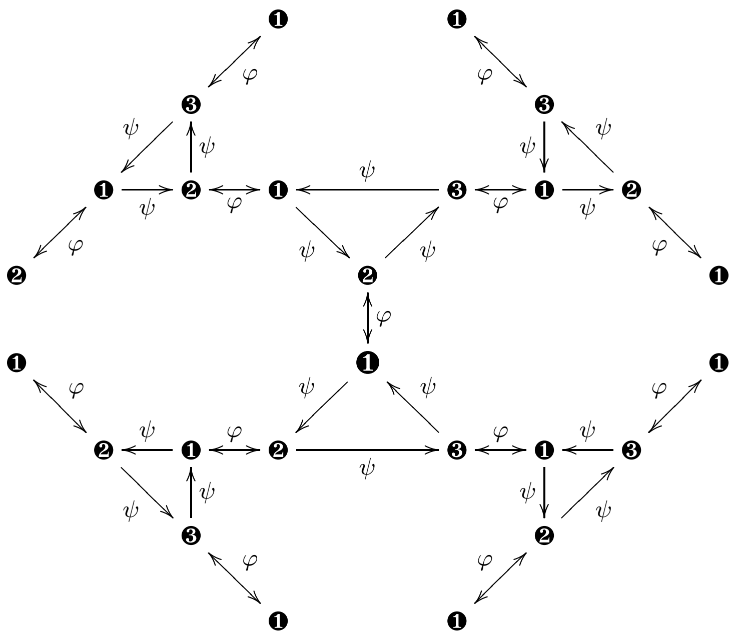
- The identity ι gets the label ❶.
- If $\rho \in H$ is labelled ❷ or ❸ and $\sigma = \varphi\rho$, then σ is labelled ❶.
- If $\rho \in H$ is labelled ❶ and $\sigma = \varphi\rho$, then σ is labelled *either* ❷ *or* ❸.
- If $\rho \in H$ is labelled ❶ (or ❷, or ❸) and $\sigma = \psi\rho$, then σ is labelled ❷ (or ❸, or ❶, respectively).

These rules are illustrated by the following figures and diagrams:



The lightface label ③ indicates that if ρ is a reduced word in H, labelled ❶, of the form $\psi^{\varepsilon}\rho'$ for $\varepsilon = \pm 1$, then $\varphi\rho$ is always labelled ❷ (not ③).

The following figure shows part of the labelled Cayley graph of H:



The group H acts on the 2-dimensional unit sphere S_2 and we define the equivalence relation "$\sim$" on S_2 via $x \sim y$ *iff* there is a $\rho \in H$ such that

$\rho(x) = y$. The equivalence classes of "$\sim$" are usually called H-orbits, and the H-orbit containing $x \in S_2$ is written $[x]\tilde{}$. Let $F \subseteq S_2$ be the set of all fixed points (*i.e.*, the set of all $y \in S_2$ such that there is a $\rho \in H \setminus \{\iota\}$ with $\rho(y) = y$). Since H is countable and every rotation $\rho \in H$ has two fixed points, F is countable. We notice first that any point equivalent to a fixed point is a fixed point (*i.e.*, for every $x \in S_2 \setminus F$ we have $[x]\tilde{} \subseteq S_2 \setminus F$). Indeed, if $\rho(y) = y$ for some $\rho \in H$ and $y \in S_2$, then $\sigma\rho\sigma^{-1}\big(\sigma(y)\big) = \sigma(y)$; that is, if y is fixed for ρ, then $\sigma(y)$ is fixed for $\sigma\rho\sigma^{-1}$. Thus, a class of equivalent points consists *either* entirely of fixed points, *or* entirely of non-fixed points.

By the Axiom of Choice there is a choice function f for $\mathscr{F} = \big\{[x]\tilde{} : x \in S_2 \setminus F\big\}$ and let $M = \big\{f\big([x]\tilde{}\big) : x \in S_2 \setminus F\big\}$.

Now we define labels for all non-fixed points (*i.e.*, points in $S_2 \setminus F$) as follows: Firstly, every element in M is labelled ➊. Secondly, if $x \in S_2 \setminus F$, then there is a unique rotation $\rho \in H$ such that $\rho(y) = x$, where $\{y\} = M \cap [x]\tilde{}$. We define the label of the point x by the label of ρ in the labelled Cayley graph of H. This induces a partition of $S_2 \setminus F$ into the following three parts:

$$A = \big\{x \in S_2 \setminus F : x \text{ is labelled } ➊\big\}$$
$$B = \big\{x \in S_2 \setminus F : x \text{ is labelled } ➋\big\}$$
$$C = \big\{x \in S_2 \setminus F : x \text{ is labelled } ➌\big\}$$

Thus, $S_2 = A \,\dot\cup\, B \,\dot\cup\, C \,\dot\cup\, F$ and by the labelling of the vertices of the Cayley graph of H we get:

$$B = \psi[A]\,, \quad C = \psi^{-1}[A]\,, \quad B \,\dot\cup\, C = \varphi[A]\,.$$

Hence, we get that $A \cong B$, $A \cong C$, and that $A \cong B \,\dot\cup\, C$. We leave it as an exercise to the reader to show that this implies $(S_2 \setminus F) \simeq_4 (S_2 \setminus F) \,\dot\cup\, (S_2 \setminus F)$.

For each point $x \in S_2$ let l_x be the line joining the origin (*i.e.*, the centre of the sphere) with x, and for $S \subseteq S_2$ define $\bar{S} := \bigcup\{l_x : x \in S\}$. Then the sets $\bar{A}$, $\bar{B}$, and $\bar{C}$, cannot be Lebesgue measurable (otherwise we would have $0 < \mu(\bar{B}) = \mu(\bar{C}) = \mu(\bar{B} \cup \bar{C})$, a contradiction). In fact, Hausdorff's decomposition shows that there is no non-vanishing measure on S_2 which is defined for all subsets of S_2 such that congruent sets have the same measure.

Robinson's Decomposition

Robinson's decomposition of the ball is similar to Hausdorff's partition of the sphere: Firstly we define an infinite subgroup G of SO(3), where G is generated by four generators. The action of G on the unit ball B_1 (with centre the origin) induces an equivalence relation on B_1, and we choose from each equivalence class a representative. With the set of representatives and a sophisticated labelling we finally define a partition of B_1 into five parts $A_1, \dots, A_5$, such that we can make a solid unit ball with either the two sets A_1 and A_3, or with the three sets A_2, A_4 and A_5.

Let the rotations φ and ψ be as above. Let $\chi := \psi\varphi\psi$. Then, one easily verifies by induction on m that for all positive $m \in \omega$ we have $\chi^m = \psi(\varphi\psi^2)^{m-1}\varphi\psi$ and $\chi^{-m} = \psi^2\varphi(\psi\varphi)^{m-1}\psi^2$. Now, by $(*)$, we get that for every $k \geq 1$ and any non-zero integers $p_1, p_2, \dots, p_k$:

$$\chi^{p_1}\varphi\chi^{p_2}\varphi\dots\varphi\chi^{p_k} \neq \iota$$

For $1 \leq m \leq 4$ define

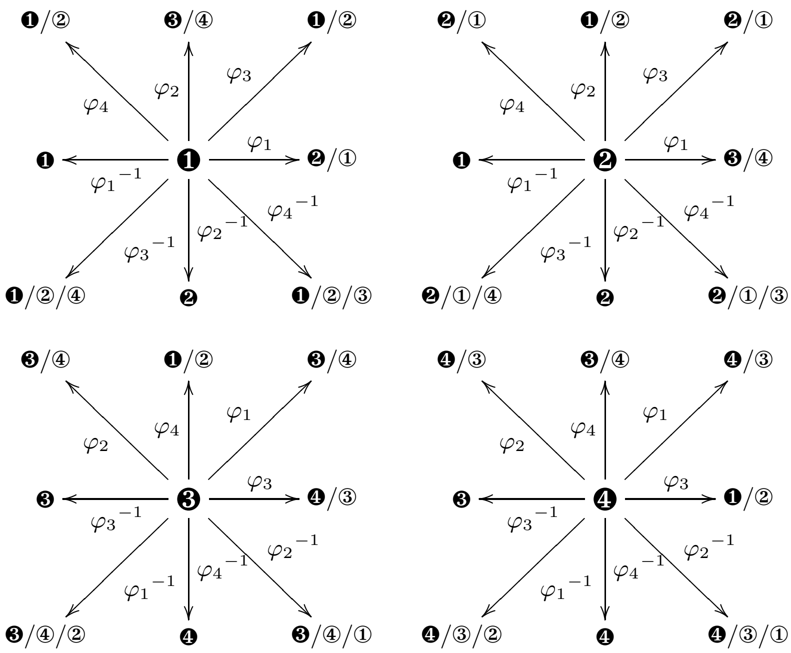
$$\varphi_m = \chi^m\varphi\chi^m .$$

We leave it again as an exercise to the reader to verify that for every $k \geq 1$, any non-zero integers $p_1, p_2, \dots, p_k$, and any $i_1, \dots, i_k \in \{1, 2, 3, 4\}$ where $i_l \neq i_{l+1}$ for all $1 \leq l < k$:

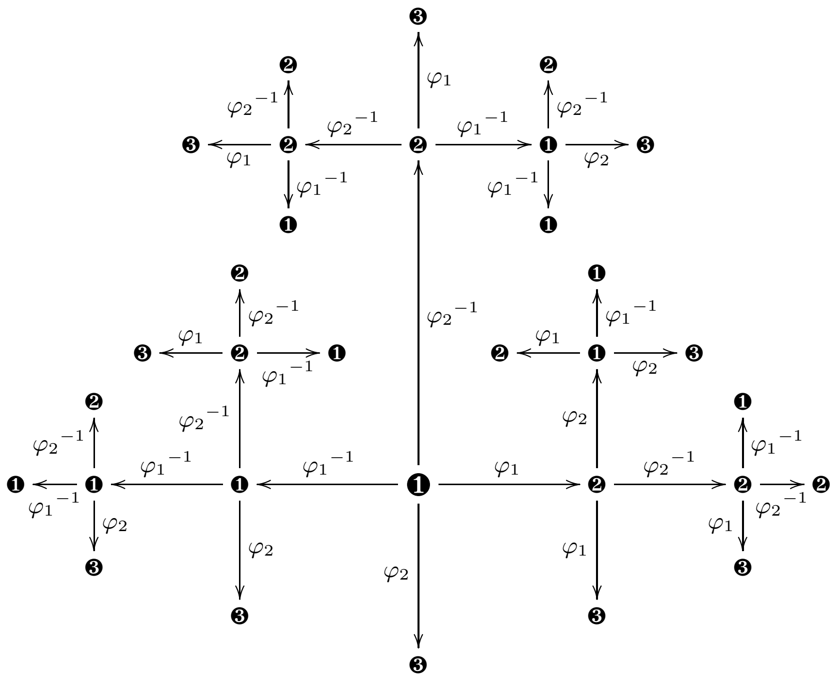
$$\varphi_{i_1}^{p_1}\varphi_{i_2}^{p_2}\dots\varphi_{i_k}^{p_k} \neq \iota \tag{$\binom{*}{*}$}$$

Let G be the subgroup of SO(3) generated by the four rotations $\varphi_1, \dots, \varphi_4$.

We consider now the labelled Cayley graph of G, where we allow again some freedom in the labelling process (indicated by lightface labels). The *rules* for labelling the vertices of the Cayley graph of G are illustrated by the following figure:



The following figure shows part of the labelled Cayley graph of G in which just φ_1 and φ_2 are involved:



The group G acts on the solid unit ball B_1 and we define the equivalence relation "$\sim$" on B_1 like above via $x \sim y$ *iff* there is a $\rho \in G$ such that $\rho(x) = y$. The G-orbit containing $x \in B_1$ is again written $[x]^{\tilde{}}$. Let P be an arbitrary point on the unit sphere (*i.e.*, on the surface of B_1), which does not belong to any rotation axis, and finally let $E \subseteq B_1$ be the set of all points which belong to a rotation axis and which are distinct from the origin. It is easy to see that for every $x \in B_1 \setminus E$ we have $[x]^{\tilde{}} \subseteq B_1 \setminus E$. By the Axiom of Choice there is a choice function f for $\mathscr{F} = \{[x]^{\tilde{}} : x \in B_1 \setminus E\}$ and let $M = \{f([x]^{\tilde{}}) : x \in B_1 \setminus E\} \setminus \{0\}$, where 0 denotes the origin.

We first define labels for all points in $B_1 \setminus (E \cup [P]^{\tilde{}})$ as follows:

- Every element in M is labelled ❶.
- The origin is labelled ③.
- If $x \in B_1 \setminus E$ and $\rho(y) = x$, where $\{y\} = M \cap [x]^{\tilde{}}$, then the label of the point x is defined as the label of ρ in the labelled Cayley graph of G.

Consider now the set E and fix any class $[z]^{\tilde{}} \subseteq E$. Choose a rotation $\theta \neq \iota$ having a fixed point in $[z]^{\tilde{}}$ and which is as short as possible, or more precisely, which is expressible as a product of the smallest possible number of factors of the form $\varphi_m^{\pm 1}$ with $m \in \{1,2,3,4\}$. Fix an arbitrary point $x_0 \in [z]^{\tilde{}}$ such that $\theta(x_0) = x_0$.

Firstly we show that if $\rho(x_0) = x_0$, then $\rho = \theta^n$ for some integer n. If $\rho = \iota$, then $\rho = \theta^0$ and we are done. Thus, we may assume that $\rho \neq \iota$. Notice first that the initial and final factors of θ — where θ and all other products of rotations are read from the right to the left — cannot be inverse, since otherwise, for some $\sigma = \varphi_m^\varepsilon$ where $m \in \{1,2,3,4\}$ and $\varepsilon \in \{-1,1\}$, the rotation $\sigma\theta\sigma^{-1}$ would be shorter than θ and would have a fixed point in the same equivalence class $[z]^{\tilde{}}$. Thus, the rotations θ and θ^{-1} neither begin nor end with the same factor. Now, if ρ has the same fixed point x_0 as θ, then $\rho\theta = \theta\rho$. If $\rho\theta$ does not simplify when ρ and θ are written in terms of the $\varphi_m^{\pm 1}$ where $m \in \{1,2,3,4\}$, then, by $\binom{*}{*}$, $\theta\rho$ must also not simplify. Hence, ρ must begin with the block θ. Inductively one finds that ρ is obtained by writing the block θ n-times, that is, $\rho = \theta^n$, where n is a positive integer. In case $\rho\theta$ does simplify, then $\rho\theta^{-1}$ does not (since θ and θ^{-1} end with different factors). Thus, we may apply the same argument as before to the equation $\rho\theta^{-1} = \theta^{-1}\rho$, and find that $\rho = \theta^{-n}$, where n is again a positive integer.

Secondly, notice that each point $y \in [z]^{\tilde{}}$ may be written in the form $\sigma_y(x_0)$, where $\sigma_y \in G$ is a rotation which starts neither with the block θ (when written in terms of the $\varphi_k^{\pm 1}$), nor with the inverse of the last factor of θ — where θ is still read from the right to the left. The former property is obvious; and to achieve the latter property consider $\sigma_y\theta^n$, where n is sufficiently large, and then simplify and remove any remaining blocks θ. Notice that this representation is unique: For suppose that $\sigma(x_0) = \rho(x_0)$, where σ and ρ are again written in terms of the $\varphi_m^{\pm 1}$. Then $\rho^{-1}\sigma(x_0) = x_0$, hence, $\rho^{-1}\sigma = \theta^n$. If $n > 0$, this yields $\sigma = \rho\theta^n$, which is impossible since $\rho\theta^n$ does not simplify and σ does not begin with the block θ. If $n < 0$, we may interchange the roles of σ andρ and again reach a contradiction. Hence we have $n = 0$, which is $\sigma = \rho$.

Thirdly, assume that θ is of the form

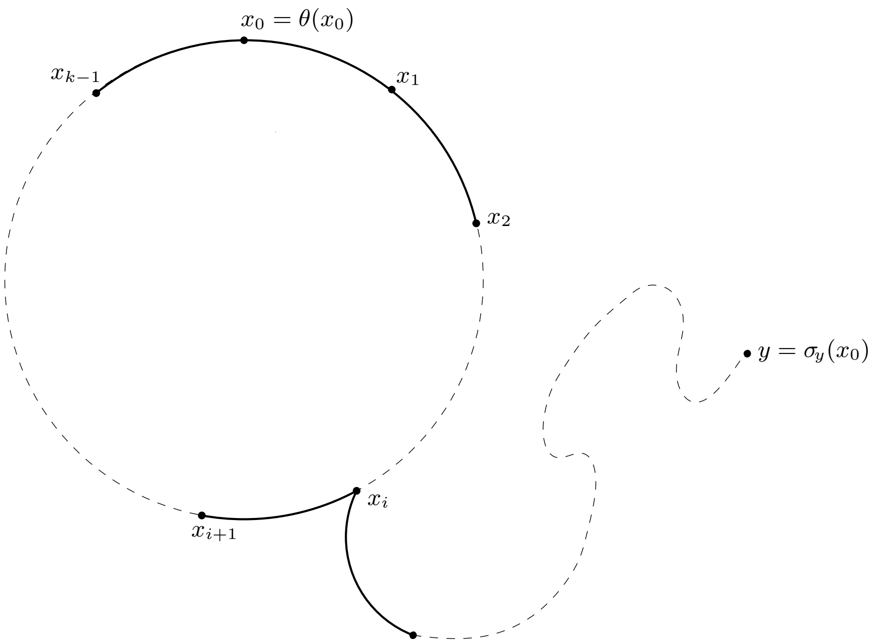
$$\theta = \varphi_{i_k}^{j_k} \varphi_{i_{k-1}}^{j_{k-1}} \cdots \varphi_{i_1}^{j_1}$$

where the i_l's $(1 \leq l \leq k)$ belong to $\{1,2,3,4\}$ and each exponent j_l is ± 1. So, starting with the point x_0, we obtain successively the k distinct points

$$x_0\,,\ x_1 = \varphi_{i_1}^{j_1}(x_0)\,,\ x_2 = \varphi_{i_2}^{j_2}\varphi_{i_1}^{j_1}(x_0)\,,\ \ldots, x_k = \varphi_{i_k}^{j_k}\varphi_{i_{k-1}}^{j_{k-1}} \cdots \varphi_{i_1}^{j_1}(x_0) = x_0$$

which form a closed cycle. As shown above, each point $y \in [z]^{\tilde{}}$ can be written uniquely in the form $\sigma_y(x_0)$, where σ_y starts neither with the block θ nor with the rotation $\varphi_{i_k}^{-j_k}$.

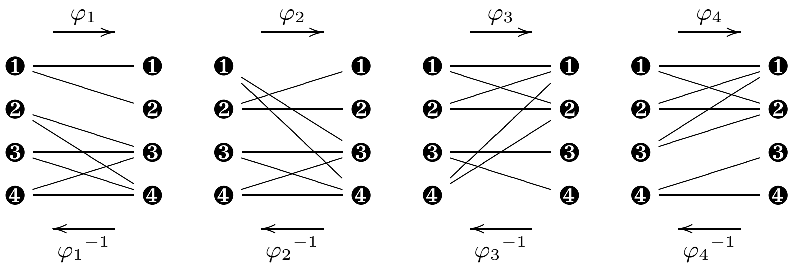
Consider the following figure:



As a consequence of the preceding arguments we get that, starting with x_0, there are no other closed cycles in $[z]^{\tilde{}}$: Indeed, let $y \in [z]^{\tilde{}}$ and $\rho \neq \iota$ be such that $\rho(y) = y$. Now, $y = \sigma_y(x_0)$ where σ_y is as above. Now, $\rho\sigma_y(x_0) = \sigma_y(x_0)$ and therefore $\sigma_y^{-1}\rho\sigma_y(x_0) = x_0$. Consequently we have $\sigma_y^{-1}\rho\sigma_y = \theta^n$ which implies $y \in \{x_0, \ldots, x_k\}$.

Now we are ready to assign a label to each point in E: Firstly, for every $[z]^{\tilde{}}$, where $z \in E$, we choose a rotation $\theta_z \neq \iota$ having a fixed point in $[z]^{\tilde{}}$ and which is as short as possible, and then choose a point $x_0^z \in [z]^{\tilde{}}$ such that $\theta(x_0^z) = x_0^z$. Assume that θ_z is of the form $\theta_z = \varphi_{i_k}^{j_k}\,\varphi_{i_{k-1}}^{j_{k-1}} \cdots \varphi_{i_1}^{j_1}$ where the i_l's (for $1 \leq l \leq k$) belong to $\{1, 2, 3, 4\}$ and each exponent j_l is ± 1. Then from the point x_0^z we obtain successively the points $x_1^z, \ldots, x_{k-1}^z, x_k^z = x_0^z$. We know that every point $y \in [z]^{\tilde{}}$ can be written uniquely in the form $\sigma_y(x_0^z)$, where σ_y starts neither with the block θ_z nor with the rotation $\varphi_{i_k}^{-j_k}$, and that, starting with x_0^z, there are no other closed cycles in $[z]^{\tilde{}}$. Thus, in order to label the points in $[z]^{\tilde{}}$ it is enough to assign a label to the k points of the cycle in a way which respects the labelling rules given above; the remaining points may be labelled like the non-fixed points, *i.e.*, like the points in $B_1 \setminus \big(E \cup [P]^{\tilde{}}\big)$.

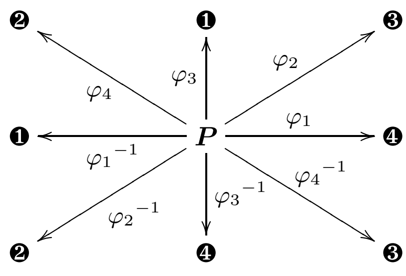
For this, consider the following schemata which illustrate the labelling rules:



$$\underbrace{\begin{pmatrix} 1&0&0&0\\ 1&0&0&0\\ 0&1&1&1\\ 0&1&1&1 \end{pmatrix}}_{=R_1} \qquad \underbrace{\begin{pmatrix} 0&1&0&0\\ 0&1&0&0\\ 1&0&1&1\\ 1&0&1&1 \end{pmatrix}}_{=R_2} \qquad \underbrace{\begin{pmatrix} 1&1&0&1\\ 1&1&0&1\\ 0&0&1&0\\ 0&0&1&0 \end{pmatrix}}_{=R_3} \qquad \underbrace{\begin{pmatrix} 1&1&1&0\\ 1&1&1&0\\ 0&0&0&1\\ 0&0&0&1 \end{pmatrix}}_{=R_4}$$

For $1 \le m \le 4$, the matrix R_m, which corresponds to φ_m, is such that $a_{ij} = 0$ *iff* whenever σ has label ⓘ, $\varphi_m\sigma$ cannot get label ⓙ. It is easy to see that for $1 \le m \le 4$, the matrix R_m^T corresponds to ${\varphi_m}^{-1}$. Consequently, the rotation θ_z corresponds to a certain product of the matrices $R_1, \dots, R_4$ and their transposes. In particular, θ_z corresponds to a 4×4 matrix Q. By considering the trace of Q, $\mathrm{tr}(Q)$, and by applying the fact that for any matrices A and B we have $\mathrm{tr}(A^T) = \mathrm{tr}(A)$ and $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, one can easily verify that $\mathrm{tr}(Q) \neq 0$. This implies that there exists a sequence of labels say l_0, $l_1, \dots, l_k$ with $l_0 = l_k$ (here we use that $\mathrm{tr}(Q) \neq 0$) such that labelling x_i^z with l_i (for $0 \le i \le k$) respects the labelling rules.

So, we can assign a label to each of the k points $x_0^z, \dots, x_{k-1}^z$ of the cycle in a way which respects the labelling rules, and consequently, we can assign a label to every point in E. Thus, the only points which are not labelled yet are the points in $[P]^{\sim}$: For the point P, and only for this single point, we modify the labelling as illustrated by the following figure (the further labelling of the points in $[P]^{\sim}$ is done according to the labelling rules):



Finally, we have labelled all points of $B_1 \setminus \{P\}$ with four labels, which induces a partition of B_1 into the following five parts:

$$
\begin{aligned}
A_1 &= \big\{x \in B_1 : x \text{ is labelled } ❶\big\} \\
A_2 &= \big\{x \in B_1 : x \text{ is labelled } ❷\big\} \\
A_3 &= \big\{x \in B_1 : x \text{ is labelled } ❸\big\} \\
A_4 &= \big\{x \in B_1 : x \text{ is labelled } ❹\big\} \\
A_5 &= \{P\}
\end{aligned}
$$

Obviously, $B_1 = A_1 \dot\cup A_2 \dot\cup A_3 \dot\cup A_4 \dot\cup A_5$. We leave it as an exercise to the reader to check that by the labelling rules (and the labelling of P) we have:

- $\varphi_1[A_1] = A_1 \dot\cup A_2 \dot\cup A_5$.
- $\varphi_2[A_2] = A_1 \dot\cup A_2 \dot\cup A_5$.
- $\varphi_3[A_3] = A_3 \dot\cup A_4$.
- $\varphi_4[A_4] = (A_3 \dot\cup A_4) \setminus \{0\}$, where 0 denotes the origin.

Hence, we get that $A_1 \cong A_1 \dot\cup A_2 \dot\cup A_5 \cong A_2$, $A_3 \cong A_3 \dot\cup A_4$, and $A_4 \cong (A_3 \dot\cup A_4) \setminus \{0\}$, and obviously we have $\{P\} \cong \{0\}$.

Now, with the two sets A_1 and A_3, as well as with the three sets A_2, A_4 and A_5, we can make a solid unit ball: Firstly, notice that $B_1 = \varphi_1[A_1] \dot\cup \varphi_3[A_3]$. Secondly, let o be a translation which moves P to the origin 0. Then $B_1 = \varphi_2[A_2] \dot\cup \varphi_4[A_4] \dot\cup o[A_5]$. Hence, we finally get

$$B_1 \simeq_5 B_1 \dot\cup B_1 \,.$$

This result is optimal with respect to the number of pieces needed, in other words we have

$$B_1 \not\simeq_4 B_1 \dot\cup B_1 \,.$$

To see this, assume towards a contradiction that there are distance-preserving (not necessarily orientation-preserving) transformations $\psi_1, \psi_2, \psi_3, \psi_4$ and a partition $B_1 = P_1 \dot\cup P_2 \dot\cup P_3 \dot\cup P_4$ such that $B_1 = \psi_1[P_1] \cup \psi_2[P_2]$ and $B_1 = \psi_3[P_3] \cup \psi_4[P_4]$. Firstly notice that not all transformations $\psi_1, \psi_2, \psi_3, \psi_4$ could leave the origin fixed, for then one copy of B_1 would be without a centre. Now suppose for example that $\psi_4(0) \neq 0$. Then $S_2 \setminus \psi_4[B_1]$ (where S_2 denotes the surface of B_1) contains more than a hemisphere (*i.e.*, more than half of S_2). In other words, $\psi_4[B_1] \cap S_2$, and in particular $\psi_4[P_4] \cap S_2$, is contained in *less* than a hemisphere. Since $\psi_3[P_3]$ must cover $S_2 \setminus \psi_4[P_4]$, it must cover more than a hemisphere, which is only possible if $\psi_3(0) = 0$ (otherwise, $\psi_3[P_3] \cup \psi_4[P_4]$ would not cover S_2). Thus, P_3 itself must cover *more* than a hemisphere, and consequently, $(P_1 \cup P_2) \cap S_2$ is contained in *less* than a hemisphere. Hence, $\big(\psi_1[P_1] \cup \psi_2[P_2]\big) \cap S_2$ is properly contained in S_2, and therefore $\psi_1[P_1] \cup \psi_2[P_2]$ cannot cover S_2.

Notes

In 1924, Banach and Tarski proved in [2] that if A and A' are bounded subsets of Euclidean space of three or more dimensions and both sets have interior points, then A and A' are equidecomposable. In particular, for $A = B_1$ and $A' = B_1 \dot\cup B_1$, $B_1 \simeq B_1 \dot\cup B_1$ (*cf.* [2, p. 262 (Lemme 22)]). However, no estimate was given for the number of pieces required to make two balls from one. Some years later, von Neumann [8, p. 77] stated without proof that nine pieces are sufficient, and about two decades later, Sierpiński improved von Neumann's result by showing that eight pieces are sufficient (*cf.* [13]). Finally, Robinson was able to show that in fact just five pieces are sufficient and that 5 is the smallest possible number of pieces, *i.e.*, $B_1 \not\simeq_4 B_1 \dot\cup B_1$.

The proof of $B_1 \simeq_5 B_1 \dot\cup B_1$ given above is taken essentially from [10]. However, we have made a few modifications: For example we have taken Sierpiński's construction given in [12] to obtain the four independent rotations $\varphi_1, \varphi_2, \varphi_3, \varphi_4$. Furthermore we have replaced the parts in Robinson's proof which deal with products of relations with products of matrices, and introduced the trick with the trace in order to find fixed points in products of relations. Finally, we tried to visualise a few key steps in the proof by some figures.

The results of Banach and Tarski [2] — and indirectly also the other paradoxical decompositions of geometrical figures — were motivated by Hausdorff's decomposition of the sphere, given in [3] (see also [5, pp. 5–10] or [4, p. 469 ff.]). The aim of Hausdorff's decomposition was to show that it is impossible to define a non-vanishing measure μ on S_2 which is defined for all subsets of S_2, is finitely additive (*i.e.*, $\mu(A \cup B) = \mu(A) + \mu(B)$ whenever A and B are disjoint), and has the property that congruent sets have the same measure.

Like Hartogs, also Hausdorff had to retire 1935 from his chair in Bonn and by October 1941 he was forced to wear the "yellow star". Around the end of the year he was informed that he would be sent to Cologne — which he knew was just a preliminary to deportation to Poland — but managed to avoid being sent. Shortly later, in January 1942, he was informed again that he was to be interned now in Endenich, and together with his wife and his wife's sister, he committed suicide on 26 January.

Related Results

40. *Further paradoxical decompositions.* In [8, p. 85 f.] von Neumann introduced the following notion of decomposability: Let A and B be two subsets of a metric space (X, d). A is said to be *metrically smaller* than B if there is a bijection $f : A \to B$ such that for any distinct points $x, y \in A$ we have $d(x, y) < d\big(f(x), f(y)\big)$. Furthermore, A is *smaller by finite decomposition* than B if there is a positive integer n and partitions $A = A_1 \dot\cup \ldots \dot\cup A_n$ and $B = B_1 \dot\cup \ldots \dot\cup B_n$ such that for all $1 \leq i \leq n$ we have that A_i is metrically smaller than B_i. Now, von Neumann [8, p. 115 f.] showed that every interval of the real line is smaller by finite decomposition than every other interval of the real line. About two decades later, Sierpiński [14] proved a 2-dimensional analogue by showing that every disc is smaller by finite decomposition than every other disc.

    For the consequences of the paradoxical decompositions for Measure Theory and its connections with Group Theory, Geometry, and Logic, we refer the reader to Wagon [18], and for some historical background see Wapner [19]. For other paradoxical decompositions see Laczkovich [7] or Sierpiński [15], and for a seemingly stronger notion of equidecomposability we refer the reader to Wilson [20].

41. *Limits of decomposability.* In 1923, Banach showed that there exists a finitely additive measure m on $\mathbb{R}^2$, extending the Lebesgue measure μ, such that m is defined for *all* subsets of $\mathbb{R}^2$ and has the property that $m(A) = m(A')$ whenever $A \cong A'$ (see Banach [1, Théorème I]). This implies that whenever A and A' are Lebesgue measurable subsets of $\mathbb{R}^2$ and $A \simeq A'$, then $\mu(A) = \mu(A')$ (see Banach and Tarski [2, Théorème 16]). In particular, the unit disc and two unit discs are not equidecomposable.
Neither Hausdorff's partition of the sphere nor Robinson's decomposition of the ball can be carried out without the aid of some form of the Axiom of Choice. The reason for this is that in the presence of inaccessible cardinals (*cf.* Chapter 15 | Related Result 85), there exists a model of ZF in which every set of reals is Lebesgue measurable (see Solovay [17], and Shelah [11] or Raisonnier [9]).

42. *Squaring the circle.* As mentioned above, there is no 2-dimensional analogue of Robinson's decomposition of the ball, *i.e.*, there is no way of making two unit discs from one unit disc. However, Laczkovich [6] showed that a disc is equidecomposable — by translations only — with a square of the same area. The construction makes use of the Axiom of Choice and the figures are partitioned into about 10^{50} pieces.

References

1. Stefan Banach, *Sur le problème de la mesure*, ***Fundamenta Mathematicae***, vol. 4 (1923), 7–33.
2. Stefan Banach and Alfred Tarski, *Sur la décomposition des ensembles de points en parties respectivement congruentes*, ***Fundamenta Mathematicae***, vol. 6 (1924), 244–277.
3. Felix Hausdorff, *Bemerkungen über den Inhalt von Punktmengen*, ***Mathematische Annalen***, vol. 75 (1914), 428–433.
4. ———, ***Grundzüge der Mengenlehre***, de Gruyter, Leipzig, 1914 [reprint: Chelsea, New York, 1965].
5. ———, ***Gesammelte Werke, Band IV: Analysis, Algebra und Zahlentheorie***, Springer-Verlag, Berlin, 2001.
6. Miklós Laczkovich, *Equidecomposability and discrepancy; a solution of Tarski's circle-squaring problem*, ***Journal für die Reine und Angewandte Mathematik***, vol. 404 (1990), 77–117.
7. ———, *Paradoxical decompositions: A survey of recent results*, First European Congress of Mathematics Paris, July 6–10, 1992, Vol. II (A. Joseph, F. Mignot, F. Murat, B. Prum, and R. Rentschler, eds.), [Progress in Mathematics 120], Birkhäuser, Basel, 1994, pp. 159–184.
8. John von Neumann, *Zur allgemeinen Theorie des Masses*, ***Fundamenta Mathematicae***, vol. 13 (1929), 73–116.

9. Jean Raisonnier, *A mathematical proof of S. Shelah's theorem on the measure problem and related results*, ***Israel Journal of Mathematics***, vol. 48 (1984), 48–56.
10. Raphael M. Robinson, *On the decomposition of spheres*, ***Fundamenta Mathematicae***, vol. 34 (1947), 246–260.
11. Saharon Shelah, *Can you take Solovay's inaccessible away?*, ***Israel Journal of Mathematics***, vol. 48 (1984), 1–47.
12. Wacław Sierpiński, *Sur le paradoxe de la sphère*, ***Fundamenta Mathematicae***, vol. 33 (1945), 235–244.
13. ———, *Sur le paradoxe de MM. Banach et Tarski*, ***Fundamenta Mathematicae***, vol. 33 (1945), 228–234.
14. ———, *Sur un paradoxe de M. J. von Neumann*, ***Fundamenta Mathematicae***, vol. 35 (1948), 203–207.
15. ———, ***On the congruence of sets and their equivalence by finite decomposition***, [Lucknow University Studies, no. xx], The Lucknow University, Lucknow, 1954 (reprinted in [16]).
16. Wacław Sierpiński *et al.*, ***On the Congruence of Sets and Other Monographs***, Chelsea Publishing Company, Bronx, New York, 1960.
17. Robert M. Solovay, *A model of set theory in which every set of reals is Lebesgue measurable*, ***Annals of Mathematics (2)***, vol. 92 (1970), 1–56.
18. Stan Wagon, ***The Banach-Tarski Paradox***, [Encyclopedia of Mathematics and its Applications 24], Cambridge University Press, Cambridge, 1985, With a foreword by Jan Mycielski.
19. Leonard M. Wapner, ***The Pea and the Sun: a mathematical paradox***, A.K. Peters, Wellesley, 2007.
20. Trevor M. Wilson, *A continuous movement version of the Banach-Tarski Paradox: A solution to de Groot's problem*, ***The Journal of Symbolic Logic***, vol. 70 (2005), 946–952.

7

Models of Set Theory with Atoms

A musician regards consonances more highly than dissonances, so he composes principally with them. Nevertheless, it seems that he also values those sounds which are dissonant.
Now intervals that are dissonant produce a sound that is disagreeable to the ear and render a composition harsh and without any sweetness. Therefore a musician must know them not only to avoid them where consonances are required, but to use them within the parts of a composition.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

In this chapter, we shall construct various models of Set Theory in which the Axiom of Choice fails. In particular, we shall construct a model in which $\mathsf{C}(\aleph_0, 2)$ fails, and another one in which a cardinal $\mathfrak{m}$ exists such that $\mathfrak{m}^2 < [\mathfrak{m}]^2$. These somewhat strange models are constructed in a similar way to models of ZF (see the cumulative hierarchy introduced in Chapter 3). However, instead of starting with the empty set (in order to build the cumulative hierarchy) we start with a set of *atoms* and define a certain group $\mathscr{G}$ of permutations of these atoms. Roughly speaking, a set x is in the model if x is "stable" under certain subgroups $\mathscr{H} \subseteq \mathscr{G}$ (*i.e.*, for all permutations $\pi \in \mathscr{H}$, $\pi x = x$). In this way we can make sure that some particular sets (*e.g.*, choice functions for a given family in the model) do not belong to the model. Unfortunately, since we have to introduce atoms to construct these models, we do not get models of ZF; however, using the JECH-SOCHOR EMBEDDING THEOREM 17.2, we can embed arbitrarily large fragments of these models into models of ZF, which is sufficient for our purposes.

Permutation Models

In this section we shall give the definition of so-called *permutation models*, but first have to say a few words about Set Theory with atoms, denoted ZFA: Set theory with atoms is characterised by the fact that it admits so-called **atoms** or **urelements**.

Atoms are objects which do not have any elements but are distinct from the empty set. The collection of atoms — assumed to be a set — is usually denoted by A, and we add the constant symbol $\mathtt{A}$ to the language of Set Theory. Thus, the language of Set Theory with atoms consists of the relation symbol "$\in$" and the constant symbol "$\mathtt{A}$", *i.e.*, $\mathscr{L}_{\mathsf{ZFA}} = \{\in, \mathtt{A}\}$.

In ZFA we have two types of objects, namely sets and atoms, and since atoms behave slightly different than sets (*e.g.*, they do not contain elements but are different from $\emptyset$), we have to add a new axiom for atoms (*i.e.*, an axiom for the symbol $\mathtt{A}$) and have to modify the Axiom of Empty Set as well as the Axiom of Extensionality.

Axiom of Empty Set (for ZFA):

$$\exists x\big(x \notin \mathtt{A} \wedge \forall z(z \notin x)\big)$$

Axiom of Extensionality (for ZFA):

$$\forall x \forall y\big((x \notin \mathtt{A} \wedge y \notin \mathtt{A}) \rightarrow \forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y\big)$$

Roughly speaking, any two objects, which are not atoms but have the same elements, are equal. Notice that the Axiom of Extensionality implies that the empty set is unique, *i.e.*, $\emptyset$ is the only object that has no elements but does not belong to A.

Axiom of Atoms:

$$\forall x\big(x \in \mathtt{A} \leftrightarrow (x \neq \emptyset \wedge \neg\exists z(z \in x))\big)$$

In other words, an object is an atom if and only if it contains no elements but is different from the set $\emptyset$. For an alternative definition of atoms see RELATED RESULT 43.

It is time to mention that if $\forall z \neg\varphi(z)$, then we stipulate $\big\{z : \varphi(z)\big\} := \emptyset$ (not some atom, which would also be possible). For example, if x and y do not have any elements in common, *i.e.*, $\forall z \neg(z \in x \wedge z \in y)$, then $x \cap y = \emptyset$. Notice that with this convention we do not have to modify the Axiom of Extensionality for ZFA.

The development of the theory ZFA is very much the same as that of ZF (except for the definition of ordinals, where we have to require that an ordinal does not have atoms among its elements). Let S be a set. Then by transfinite recursion on $\alpha \in \Omega$ we can define $\mathscr{P}^\alpha(S)$ as follows: $\mathscr{P}^\emptyset(S) := S$, $\mathscr{P}^{\alpha+1}(S) := \mathscr{P}^\alpha(S) \cup \mathscr{P}(\mathscr{P}^\alpha(S))$ and $\mathscr{P}^\alpha(S) := \bigcup_{\beta\in\alpha} \mathscr{P}^\alpha(S)$ when α is a limit ordinal. Furthermore, let $\mathscr{P}^{\infty}(S) := \bigcup_{\alpha\in\Omega}\mathscr{P}^{\alpha}(S)$. If $\boldsymbol{\mathcal{M}}$ is a model of ZFA and A is the set of atoms of $\boldsymbol{\mathcal{M}}$, then $\boldsymbol{\mathcal{M}} = \mathscr{P}^{\infty}(A)$. The class $\hat{\mathbf{V}} := \mathscr{P}^{\infty}(\emptyset)$, which is a subclass of $\boldsymbol{\mathcal{M}}$, is a model of ZF and is called the **kernel**. Notice that all ordinals belong to the kernel.

Now, the underlying idea of permutation models, which are models of ZFA, is the fact that the axioms of ZFA do not distinguish between the atoms, and so a permutation of the set of atoms induces an automorphism of the universe.

Let A be a set of atoms and let $\boldsymbol{\mathcal{M}} = \mathscr{P}^{\infty}(A)$ be a model of ZFA. Furthermore, in $\boldsymbol{\mathcal{M}}$, let $\mathscr{G}$ be a group of permutations (or automorphisms) of A, where a permutation of A is a one-to-one mapping from A onto A. We say that a set $\mathscr{F}$ of subgroups of $\mathscr{G}$ is a **normal filter** on $\mathscr{G}$ if for all subgroups H, K of $\mathscr{G}$ we have:

(A) $\mathscr{G} \in \mathscr{F}$
(B) if $H \in \mathscr{F}$ and $H \subseteq K$, then $K \in \mathscr{F}$
(C) if $H \in \mathscr{F}$ and $K \in \mathscr{F}$, then $H \cap K \in \mathscr{F}$
(D) if $\pi \in \mathscr{G}$ and $H \in \mathscr{F}$, then $\pi H \pi^{-1} \in \mathscr{F}$
(E) for each $a \in A$, $\{\pi \in \mathscr{G} : \pi a = a\} \in \mathscr{F}$

For every set $x \in \boldsymbol{\mathcal{M}}$ there is a least ordinal α such that $x \in \mathscr{P}^{\alpha}(A)$. So, by induction on the ordinals, for every $\pi \in \mathscr{G}$ and for every set $x \in \boldsymbol{\mathcal{M}}$ we can define πx by stipulating

$$\pi x = \begin{cases} \emptyset & \text{if } x = \emptyset, \\ \pi x & \text{if } x \in A, \\ \{\pi y : y \in x\} & \text{otherwise.} \end{cases}$$

Notice that for all $x, y \in \boldsymbol{\mathcal{M}}$ and every $\pi \in \mathscr{G}$ we have $\pi x = y \iff x = \pi^{-1} y$ and $x \in y \iff \pi x \in \pi y$, which leads to the following definition: A bijective class function $F : \boldsymbol{\mathcal{M}} \to \boldsymbol{\mathcal{M}}$ is called an **$\in$-automorphism** of $\boldsymbol{\mathcal{M}}$ if for all $x, y \in \boldsymbol{\mathcal{M}}$ we have $x \in y \iff F(x) \in F(y)$. In particular, $\pi : \boldsymbol{\mathcal{M}} \to \boldsymbol{\mathcal{M}}$ is an $\in$-automorphism of $\boldsymbol{\mathcal{M}}$.

For $x \in \boldsymbol{\mathcal{M}}$, the **symmetry group** of x, denoted $\mathrm{sym}_{\mathscr{G}}(x)$, is the group of all permutations in $\mathscr{G}$ which map x to x, in other words

$$\mathrm{sym}_{\mathscr{G}}(x) = \{\pi \in \mathscr{G} : \pi x = x\}.$$

A set x is said to be **symmetric** (with respect to a normal filter $\mathscr{F}$) if the symmetry group of x belongs to $\mathscr{F}$, *i.e.*, $\mathrm{sym}_{\mathscr{G}}(x) \in \mathscr{F}$. By (E) we have that every atom $a \in A$ is symmetric. A set x is called **hereditarily symmetric** if x as well as each element of its transitive closure is symmetric. Notice that for all $x \in \boldsymbol{\mathcal{M}}$ and every $\pi \in \mathscr{G}$, x is hereditarily symmetric *iff* πx is hereditarily symmetric.

Let $\boldsymbol{\mathcal{V}} \subseteq \boldsymbol{\mathcal{M}}$ be the class of all hereditarily symmetric sets. Then $\boldsymbol{\mathcal{V}}$ is a transitive model of ZFA and we call $\boldsymbol{\mathcal{V}}$ a **permutation model**. Because A, as well as every $a \in A$, is symmetric, we get that the set of atoms A belongs to $\boldsymbol{\mathcal{V}}$.

Because $\emptyset$ is hereditarily symmetric and for all ordinals α the set $\mathscr{P}^{\alpha}(\emptyset)$ is hereditarily symmetric too, the kernel $\hat{\mathbf{V}} = \mathscr{P}^{\infty}(\emptyset)$ is a subclass of $\boldsymbol{\mathcal{V}}$. Notice that every $\pi \in \mathscr{G}$ which is not the identity mapping is a non-trivial $\in$-automorphism of $\boldsymbol{\mathcal{V}}$. On the other hand, all $\in$-automorphisms of models of ZF are trivial. In particular, by induction on α one easily verifies the following

FACT 7.1. *For any set $x \in \hat{\mathbf{V}}$ and any $\pi \in \mathscr{G}$ we have $\pi x = x$.*

Since the atoms $a \in A$ do not contain any elements, but are distinct from the empty set, the permutation models are not models of ZF. However, by the JECH-SOCHOR EMBEDDING THEOREM 17.2 one can embed arbitrarily large fragments of a permutation model into a well-founded model of ZF.

Most of the well-known permutation models are of the following simple type: Let $\mathscr{G}$ be a group of permutations of A. A family I of subsets of A, for example $I = \operatorname{fin}(A)$, is a **normal ideal** if for all subsets E, F of A we have:

(a) $\emptyset \in I$
(b) if $E \in I$ and $F \subseteq E$, then $F \in I$
(c) if $E \in I$ and $F \in I$, then $E \cup F \in I$
(d) if $\pi \in \mathscr{G}$ and $E \in I$, then $\pi E \in I$
(e) for each $a \in A$, $\{a\} \in I$

For each set $S \subseteq A$, let

$$\operatorname{fix}_{\mathscr{G}}(S) = \big\{\pi \in \mathscr{G} : \pi a = a \text{ for all } a \in S\big\}$$

and let $\mathscr{F}$ be the filter on $\mathscr{G}$ generated by the subgroups $\{\operatorname{fix}_{\mathscr{G}}(E) : E \in I\}$. Then $\mathscr{F}$ is a normal filter. Furthermore, x is symmetric if and only if there exists a set of atoms $E_x \in I$ such that

$$\operatorname{fix}_{\mathscr{G}}(E_x) \subseteq \operatorname{sym}_{\mathscr{G}}(x)$$

where E_x is called a **support** of x. Notice that if E_x is a support of x and $E_x \subseteq F_x \in I$, then F_x is a support of x as well.

Below, we give some relationships which are consistent with ZF between the cardinals defined in Chapter 4. We will do this by investigating the relations between certain sets in some permutation models. The general construction will be as follows: Let $\boldsymbol{\mathcal{V}}$ be a permutation model with a set of atoms A and let m be a set in $\boldsymbol{\mathcal{V}}$. Let $\mathfrak{C}(m) := \big\{x \in \boldsymbol{\mathcal{V}} : \boldsymbol{\mathcal{V}} \vDash |x| = |m|\big\}$. Then $\mathfrak{C}(m)$ is in general a class in $\boldsymbol{\mathcal{V}}$. The cardinality of m in the model $\boldsymbol{\mathcal{V}}$ (denoted by $\mathfrak{m}$) is defined by $\mathfrak{m} := \mathfrak{C}(m) \cap \mathscr{P}^{\alpha}(A) \cap \boldsymbol{\mathcal{V}}$, where α is the smallest ordinal such that $\mathfrak{C}(m) \cap \mathscr{P}^{\alpha}(A) \cap \boldsymbol{\mathcal{V}} \neq \emptyset$.

If m is a set in a permutation model $\boldsymbol{\mathcal{V}}$ and we have for example $\boldsymbol{\mathcal{V}} \vDash |\operatorname{seq}(m)| < |\operatorname{fin}(m)|$, and therefore $\boldsymbol{\mathcal{V}} \vDash \operatorname{seq}(\mathfrak{m}) < \operatorname{fin}(\mathfrak{m})$, then, by the JECH-SOCHOR EMBEDDING THEOREM 17.2, there exist a well-founded model $\hat{\mathbf{V}}$

of ZF and a set $\hat{m}$ such that $\hat{\mathbf{V}} \models |\mathrm{seq}(\hat{m})| < |\mathrm{fin}(\hat{m})|$ and consequently $\hat{\mathbf{V}} \models \mathrm{seq}(\hat{\mathfrak{m}}) < \mathrm{fin}(\hat{\mathfrak{m}})$, where $\hat{\mathfrak{m}}$ and $\hat{\mathfrak{n}}$ are the cardinalities of the sets $\hat{m}$ and $\hat{n}$ respectively. In fact, the JECH-SOCHOR EMBEDDING THEOREM 17.2 enables us to translate every relation between sets in a permutation model to a well-founded model. Hence, in order to prove that a relation between some cardinals is consistent with ZF, it is enough to find a permutation model in which the desired relation holds between the corresponding sets. Below we shall make use of this method without explicitly mentioning it.

The Basic Fraenkel Model

In this section we shall present a simple example of a permutation model in which the Axiom of Choice fails.

Let A be a countable infinite set (the atoms), let $\mathscr{G}$ be the group of *all* permutations of A, and let I_{fin} be the set of all finite subsets of A. Obviously, I_{fin} is a normal ideal and the filter derived from I_{fin} as described above is a normal filter.

Let $\mathcal{V}_{F_0}$ (F for Fraenkel) be the corresponding permutation model, the so-called **basic Fraenkel model**. Note that a set x belongs to $\mathcal{V}_{F_0}$ if and only if x is symmetric and each $y \in x$ belongs to $\mathcal{V}_{F_0}$, too.

Before we start with some results involving subsets of A, let us recall that a set S is *transfinite* if $\aleph_0 \leq |S|$; otherwise S is called *D-finite*.

LEMMA 7.2. *Let $E \in I_{\mathrm{fin}}$; then each $S \subseteq A$ with support E is either finite or co-finite, i.e., $A \setminus S$ is finite. Furthermore, if S is finite, then $S \subseteq E$, and if S is co-finite, then $(A \setminus S) \subseteq E$.*

Proof. Let $S \subseteq A$ with support E. Because E is a support of S, for all $\pi \in \mathrm{fix}(E)$ and every $a \in A$ we have $\pi a \in S$ *iff* $a \in S$. If S contains an element a_0 of $A \setminus E$, then it contains them all, since permutations in $\mathrm{fix}(E)$ can send a_0 to any other element of $A \setminus E$. Thus, either $S \subseteq E$ or $(A \setminus S) \subseteq E$.

As a consequence we get the following result (*cf.* Chapter 4 | RELATED RESULT 18): Let $\mathfrak{m}$ denote the cardinality of the set of atoms of the basic Fraenkel model. Then

$$\mathcal{V}_{F_0} \models \left(2^{2^{\mathfrak{m}}}\right)^{\aleph_0} = 2^{\mathrm{fin}(\mathfrak{m})}.$$

Indeed, every subset of A in $\mathcal{V}_{F_0}$ is either finite or co-finite, and therefore, $2^{\mathfrak{m}} = 2 \cdot \mathrm{fin}(\mathfrak{m})$. Hence, $\left(2^{2^{\mathfrak{m}}}\right)^{\aleph_0} = \left(2^{\mathrm{fin}(\mathfrak{m})}\right)^{2\cdot\aleph_0}$ and by LÄUCHLI'S LEMMA 4.27 this is equal to $2^{\mathrm{fin}(\mathfrak{m})}$.

PROPOSITION 7.3. *Let A be the set of atoms of the basic Fraenkel model and let $\mathfrak{m}$ denote its cardinality. Then $\mathcal{V}_{F_0} \models \aleph_0 \not\leq \mathfrak{m}$; in particular, in $\mathcal{V}_{F_0}$ there are infinite D-finite sets. In particular, it is not provable in ZF that every D-finite set is finite.*

Proof. If there is a one-to-one mapping $f : \omega \to A$, then the set $S = \{f(2n) : n \in \omega\}$ would be an infinite, co-infinite set of atoms, which is a contradiction to LEMMA 7.2. $\dashv$

We have seen in Chapter 4 that for every infinite cardinal $\mathfrak{m}$, $2^{\aleph_0} \leq 2^{\operatorname{fin}(\mathfrak{m})}$. In contrast to this fact, the following result shows that in the model $\mathcal{V}_{F_0}$, the power set of an infinite set can be D-finite, which shows that even for infinite cardinals $\mathfrak{m}$, the statement $\aleph_0 \leq 2^{\mathfrak{m}}$ is in general not provable in ZF.

PROPOSITION 7.4. *Let A be the set of atoms of the basic Fraenkel model and let $\mathfrak{m}$ denote its cardinality. Then $\mathcal{V}_{F_0} \vDash \aleph_0 \not\leq 2^{\mathfrak{m}}$. In particular, it is not provable in* ZF *that the power set of an infinite set is transfinite.*

Proof. Assume towards a contradiction that there exists a one-to-one function $f : \omega \to \mathscr{P}(A)$ which belongs to $\mathcal{V}_{F_0}$. Then, because f is symmetric, there is a finite set $E_f \subseteq A$ (a support of f) such that $\operatorname{fix}_{\mathscr{G}}(E_f) \subseteq \operatorname{sym}_{\mathscr{G}}(f)$. Now, let $n \in \omega$ be such that $\operatorname{fix}_{\mathscr{G}}(E_f) \nsubseteq \operatorname{sym}_{\mathscr{G}}\big(f(n)\big)$ (such an n exists because, by LEMMA 7.2, E_f supports only finitely many subsets of A). Further, let $\pi \in \operatorname{fix}_{\mathscr{G}}(E_f)$ be such that $\pi f(n) \neq f(n)$. By FACT 7.1 we get that $\pi n = n$, and therefore, $f(\pi n) = f(n)$. So, E_f cannot be a support of f which contradicts the choice of E_f and shows that a one-to-one function from ω into $\mathscr{P}(A)$ cannot belong to the model $\mathcal{V}_{F_0}$. $\dashv$

By PROPOSITION 4.22 we know that if $2^{\mathfrak{m}} = n \cdot \operatorname{fin}(\mathfrak{m})$ for some $n \in \omega$, then $n = 2^k$ for some $k \in \omega$. The next result shows that also a kind of converse is true:

PROPOSITION 7.5. *For every number n of the form $n = 2^k$, where $k \in \omega$, there is a set A_k in $\mathcal{V}_{F_0}$ such that $\mathcal{V}_{F_0} \vDash \big|\mathscr{P}(A_k)\big| = \big|n \times \operatorname{fin}(A_k)\big|$.*

Proof. If $n = 2^0$, then the statement is true for every finite set A_0 (in every model of Set Theory).

Let $k \in \omega \setminus \{0\}$ and let $n = 2^k$. Further, let A be the set of atoms of $\mathcal{V}_{F_0}$ and let $A_k = k \times A$. By LEMMA 7.2 we know that every subset of A (in $\mathcal{V}_{F_0}$) is either finite or co-finite and therefore $|\mathscr{P}(A)| = 2 \cdot |\operatorname{fin}(A)|$. Thus, in $\mathcal{V}_{F_0}$ we have $|\mathscr{P}(A_k)| = |\mathscr{P}(k \times A)| = |\mathscr{P}(A)^k| = \big|\big(2 \times \operatorname{fin}(A)\big)^k\big| = \big|2^k \times \operatorname{fin}(A)^k\big| = \big|2^k \times \operatorname{fin}(A_k)\big|$, and therefore $\mathcal{V}_{F_0} \vDash \big|\mathscr{P}(A_k)\big| = \big|n \times \operatorname{fin}(A_k)\big|$. $\dashv$

The Second Fraenkel Model

The set of atoms of the second Fraenkel model consists of countably many mutually disjoint 2-element sets:

$$A = \bigcup_{n \in \omega} P_n\,, \text{ where } P_n = \{a_n, b_n\} \text{ (for } n \in \omega)$$

Let $\mathscr{G}$ be the group of those permutations of A which preserve the pairs P_n, *i.e.*, $\pi\big(\{a_n, b_n\}\big) = \{a_n, b_n\}$ (for each $\pi \in \mathscr{G}$ and every $n \in \omega$). Further, let I_{fin} be the set of all finite subsets of A. Then I_{fin} is a normal ideal and the filter generated by I_{fin} is a normal filter.

Let $\mathcal{V}_{F_2}$ be the corresponding permutation model, called the **second Fraenkel model**. The following theorem summarises the main features of this model.

THEOREM 7.6. *(a) For each $n \in \omega$ the set P_n belongs to $\mathcal{V}_{F_2}$.*

(b) The sequence $\langle P_n : n \in \omega\rangle$ belongs to $\mathcal{V}_{F_2}$. In particular, the set of pairs $\{P_n : n \in \omega\}$ is countable in $\mathcal{V}_{F_2}$.

(c) There is no choice function on $\{P_n : n \in \omega\}$. In particular, $\mathsf{C}(\aleph_0, 2)$ fails in $\mathcal{V}_{F_2}$ which shows that $\mathsf{ZF} \nvdash \mathsf{C}(\aleph_0, 2)$.

Proof. (a) For each $\pi \in \mathscr{G}$ and for every $n \in \omega$ we have $\pi P_n = P_n$, which implies that every P_n is symmetric.

(b) For each $\pi \in \mathscr{G}$ we have $\pi\big(\langle P_n : n \in \omega\rangle\big) = \langle \pi P_n : n \in \omega\rangle = \langle P_n : n \in \omega\rangle$, and therefore by (a), $\langle P_n : n \in \omega\rangle$ is hereditarily symmetric.

(c) Assume that there is a choice function f on $\{P_n : n \in \omega\}$ which belongs to $\mathcal{V}_{F_2}$. The choice function f would be a function from ω into $\bigcup\{P_n : n \in \omega\}$ such that $f(n) \in P_n$ (for every $n \in \omega$). Let $\{a_0, b_0, \ldots, a_k, b_k\}$ be a support of f and let $\pi \in \text{fix}_{\mathscr{G}}\big(\{a_0, b_0, \ldots, a_k, b_k\}\big)$ be such that $\pi a_{k+1} = b_{k+1}$. Then $\pi(k+1) = k+1$, but $\pi\big(f(k+1)\big) \neq f(k+1)$, which implies that $\pi f \neq f$ and contradicts the fact that $\{a_0, b_0, \ldots, a_k, b_k\}$ is a support of f. $\dashv$

We leave it as an exercise to the reader to show that C_2, which is a more general choice principle than $\mathsf{C}(\aleph_0, 2)$, already fails in $\mathcal{V}_{F_0}$.

The following result shows that in $\mathcal{V}_{F_2}$, König's Lemma fails even for binary trees.

PROPOSITION 7.7. *In $\mathcal{V}_{F_2}$ there exists an infinite binary tree which does not have an infinite branch.*

Proof. We construct the binary tree $T = (V, E)$ with vertex set V and edge set E as follows: For $n \in \omega$ let $V_n = \big\{s \in {}^nA : \forall i \in n\,(s(i) \in P_i)\big\}$ and let $V = \bigcup_{n\in\omega} V_n$. Further, let $\langle s, t\rangle \in E$ *iff* for some $n \in \omega$, $s \in V_n$, $t \in V_{n+1}$, and $t|_n = s$. It is easily verified that T is an infinite tree and since every vertex $s \in V$ has exactly two successors, namely $s^\frown a_n$ and $s^\frown b_n$, where $s \in V_n$ and $s^\frown x$ denotes the concatenation of the sequence s and the element x, T is even a binary tree. On the other hand, an infinite branch through T would yield a choice function on $\{P_n : n \in \omega\}$, a contradiction to THEOREM 7.6.(c). $\dashv$

In a similar way one can show that Ramsey's original theorem fails in $\mathcal{V}_{F_2}$:

PROPOSITION 7.8. *In $\mathcal{V}_{F_2}$ there exist an infinite set S and a 2-colouring of $[S]^2$ such that no infinite subset of S is homogeneous.*

Proof. Let S be the set of atoms of $\mathcal{V}_{F_2}$ and colour a 2-element set of atoms $\{a,b\}$ red, if $\{a,b\} = P_n$ for some $n \in \omega$; otherwise, colour it blue. We leave it as an exercise to the reader to show that no infinite homogeneous set belongs to $\mathcal{V}_{F_2}$. ⊣

The last result of this section is a kind of infinite version of PROPOSITION 7.5.

PROPOSITION 7.9. *In $\mathcal{V}_{F_2}$, let $\mathfrak{m}$ denote the cardinality of the set of atoms. Then $\mathcal{V}_{F_2} \vDash 2^{\mathfrak{m}} = 2^{\aleph_0} \cdot \operatorname{fin}(\mathfrak{m})$.*

Proof. By the CANTOR-BERNSTEIN THEOREM 3.17 it is enough to find two one-to-one mappings $f : \mathscr{P}(A) \to {}^{\omega}2 \times \operatorname{fin}(A)$ and $g : {}^{\omega}2 \times \operatorname{fin}(A) \to \mathscr{P}(A)$. For every $n \in \omega$ let $U_n = \bigcup_{i \in n} P_i$.

For $S \subseteq A$ let $m = \bigcup\{n+1 : |P_n \cap S| = 1\}$. Then $F_S = S \cap U_m$ is finite and for every $n > m$ we have *either* $P_n \subseteq S$ *or* $P_n \cap S = \emptyset$. Now define $\chi_S : \omega \to 2$ by stipulating $\chi_S(n) = 0$ *iff* $P_{n+m+1} \cap S = \emptyset$, and define $f(S) := \langle \chi_S, F_S \rangle$. It is easily verified that the function f is one-to-one.

Let $\langle \chi, F \rangle \in {}^{\omega}2 \times \operatorname{fin}(A)$ and define again $m = \bigcup\{n+1 : |P_n \cap F| = 1\}$. Then $F_0 = F \cap U_m$ and $F_1 = F \setminus F_0$ are finite. Further, let

$$S_{\chi,F} = F_0 \cup \bigcup \bigl\{P_{2n} : P_n \subseteq F_1\bigr\} \cup \bigcup \bigl\{P_{2n+m+1} : \chi(n) = 1\bigr\} \subseteq A$$

and define $g\bigl(\langle \chi, F \rangle\bigr) := S_{\chi,F}$. It is again easy to check that the function g is one-to-one. ⊣

The Ordered Mostowski Model

The set of atoms A of the ordered Mostowski model consists of an infinite countable set together with an ordering "$<^M$" such that A is densely ordered and does not have a smallest or greatest element, *i.e.*, A is order-isomorphic to the rational numbers. Let $\mathscr{G}$ be the group of all order-preserving permutations of A and let I_{fin} be the ideal of the finite subsets of A. Then again, I_{fin} is a normal ideal and the filter generated by I_{fin} is a normal filter.

Let $\mathcal{V}_M$ (M for Mostowski) be the corresponding permutation model, called the **ordered Mostowski model**.

First let us show that the binary relation "$<^M$" belongs to the model $\mathcal{V}_M$. In other words, for any two distinct atoms a_1 and a_2 we can decide in $\mathcal{V}_M$ whether we have $a_1 <^M a_2$ or $a_2 <^M a_1$.

LEMMA 7.10. *The set $R_< = \bigl\{\langle a_1, a_2 \rangle : a_1 <^M a_2\bigr\} \subseteq A \times A$ belongs to $\mathcal{V}_M$.*

Proof. If $a_1 <^M a_2$, then $\pi a_1 <^M \pi a_2$ (for any $\pi \in \mathscr{G}$), and therefore, $\langle a_1, a_2 \rangle \in R_<$ *iff* $\langle \pi a_1, \pi a_2 \rangle \in R_<$, which implies that $\operatorname{sym}_{\mathscr{G}}(R_<) = \mathscr{G}$. ⊣

Because by definition all sets in the ordered Mostowski model must be symmetric, each set in $\mathcal{V}_M$ has a finite support. Moreover, each set in $\mathcal{V}_M$ has a unique least support:

LEMMA 7.11. *(a) If E_1 and E_2 are supports of x, then also $E = E_1 \cap E_2$ is a support of x.*

(b) Every set $x \in \boldsymbol{\mathcal{V}}_M$ has a least support.

(c) The class of all pairs (x, E), where $x \in \boldsymbol{\mathcal{V}}_M$ and E is the least support of x, is symmetric.

Proof. (a) Let E_1 and E_2 be two finite supports of the set $x \in \boldsymbol{\mathcal{V}}_M$ and let $E = E_1 \cap E_2$. Notice that for every $\pi \in \text{fix}_{\mathscr{G}}(E)$ there are finitely many $\rho_1, \dots, \rho_n \in \text{fix}_{\mathscr{G}}(E_1)$ and $\sigma_1, \dots, \sigma_n \in \text{fix}_{\mathscr{G}}(E_2)$ such that $\pi = \rho_1\sigma_1 \cdots \rho_n\sigma_n$. To see this, it might be better to draw a picture than to prove it formally (e.g., let $E_1 = \{a_0, a_1, a_2\}$ and $E_2 = \{b_0, b_1, b_2\}$ be such that $a_0 = b_0 <^{M} a_1 <^{M} b_1 <^{M} a_2 <^{M} b_2$, and let $\pi \in \text{fix}_{\mathscr{G}}\big(\{a_0\}\big)$ be such that $b_2 <^{M} \pi c$ for some $a_0 <^{M} c <^{M} b_1$). Since $\rho_i x = x = \sigma_i x$ (for all $1 \le i \le n$) we have

$$\pi x = \rho_1\sigma_1 \cdots \rho_n\sigma_n x = \rho_1\sigma_1 \cdots \sigma_{n-1}\rho_n x = \ldots = \rho_1 x = x$$

for all $\pi \in \text{fix}_{\mathscr{G}}(E)$, which shows that $\pi \in \text{sym}_{\mathscr{G}}(x)$. Hence, $\text{fix}_{\mathscr{G}}(E) \subseteq \text{sym}_{\mathscr{G}}(x)$ which implies that E is a support of x.

(b) Let E_0 be a support of x. The least support of x is the intersection of all supports of x which are subsets of E_0. Since there are only finitely many of such supports, by (a), the intersection is a support of x.

(c) Let $x \in \boldsymbol{\mathcal{V}}_M$ and let E be the least support of x. If $\pi \in \mathscr{G}$, then $\text{fix}_{\mathscr{G}}(\pi E) = \pi \cdot \text{fix}_{\mathscr{G}}(E) \cdot \pi^{-1}$ and $\text{sym}_{\mathscr{G}}(\pi x) = \pi \cdot \text{sym}_{\mathscr{G}}(x) \cdot \pi^{-1}$, and thus, if E is a support of x, then πE is a support of πx. ⊣

For every finite set $E \subseteq A$, one can give a complete description of the subsets of A with support E, which leads to the following

LEMMA 7.12. *If $E \subseteq A$ is a finite set of cardinality n, then there are 2^{2n+1} sets $S \subseteq A$ in $\boldsymbol{\mathcal{V}}_M$ such that E is a support of S.*

Proof. Let $E = \{a_1, \dots, a_n\}$ be such that $a_1 <^{M} \ldots <^{M} a_n$. Assume that E is a support of the set $S \subseteq A$. If there is an $s_0 \in S$ such that $a_i <^{M} s_0 <^{M} a_{i+1}$ (for some $1 \le i < n$), then $\{s \in A : a_i <^{M} s <^{M} a_{i+1}\} \subseteq S$. To see this, notice that for every s with $a_i <^{M} s <^{M} a_{i+1}$ there is a $\pi \in \text{fix}_{\mathscr{G}}(E)$ such that $\pi s_0 = s$. Similarly, if there is an $s \in S$ such that $s <^{M} a_1$ (or $a_n <^{M} s$), then $\{s \in A : s <^{M} a_1\} \subseteq S$ (or $\{s \in A : a_n <^{M} s\} \subseteq S$). Now, there are $n+1$ such intervals and every interval is entirely contained in S or disjoint from S. Further, for each $1 \le i \le n$, either $a_i \in S$ or $a_i \notin S$. Hence, there are 2^{2n+1} different subsets of A which have E as a support. ⊣

Since the set of atoms in the ordered Mostowski model is infinite, the following result implies that the Axiom of Choice fails in $\boldsymbol{\mathcal{V}}_M$ (compare this result with PROPOSITION 7.4).

LEMMA 7.13. *Let A be the set of atoms of the ordered Mostowski model and let $\mathfrak{m}$ denote its cardinality. Then $\boldsymbol{\mathcal{V}}_M \vDash \aleph_0 \not\le 2^{\mathfrak{m}}$.*

Proof. We have to show that there is no one-to-one mapping $f : \omega \to \mathscr{P}(A)$. Now, if a finite set $E \subseteq A$ is a support of f, then E supports each of the infinitely many distinct sets $f(n)$ $(n \in \omega)$, because all permutations fix each $n \in \omega$. On the other hand, by LEMMA 7.12, a finite set $E \subseteq A$ can support just finitely many sets. ⊣

By THEOREM 4.21, for every infinite cardinal $\mathfrak{m}$ we have $\text{fin}(\mathfrak{m}) < 2^{\mathfrak{m}}$. In contrast to this result we show now that $\mathcal{V}_M \vDash 2^{\mathfrak{m}} \leq^* \text{fin}(\mathfrak{m})$, where $\mathfrak{m}$ denotes the cardinality of the set of atoms of $\mathcal{V}_M$. As a consequence we get by FACT 4.8 that $2^{2^{\mathfrak{m}}} \leq 2^{\text{fin}(\mathfrak{m})}$, which implies by the CANTOR-BERNSTEIN THEOREM 3.17 that $\mathcal{V}_M \vDash 2^{2^{\mathfrak{m}}} = 2^{\text{fin}(\mathfrak{m})}$.

PROPOSITION 7.14. *Let A be the set of atoms of the ordered Mostowski model. Then in $\mathcal{V}_M$ there is a surjection from $\text{fin}(A)$ onto $\mathscr{P}(A)$. Thus, it is consistent with* ZF *that there are infinite cardinals $\mathfrak{m}$ such that $2^{\mathfrak{m}} \leq^* \text{fin}(\mathfrak{m})$, even though $\text{fin}(\mathfrak{m}) < 2^{\mathfrak{m}}$ is provable in* ZF *for every infinite cardinal $\mathfrak{m}$.*

Proof. The key idea in order to construct a surjective function $g : \text{fin}(A) \twoheadrightarrow \mathscr{P}(A)$ is to define an ordering of the subsets of A sharing a given finite support. For $E = \{a_1 <^M \ldots <^M a_n\} \in \text{fin}(A)$ let $I_0 = \{a \in A : a <^M a_1\}$, $I_n = \{a \in A : a_n <^M a\}$, and $I_i = \{a \in A : a_i <^M a <^M a_{i+1}\}$ for $1 \leq i \leq n-1$. For every function $\chi \in {}^{2n+1}2$ we assign a set $S_\chi \in \mathscr{P}(A)$ by

$$S_\chi = \bigcup_{\chi(2i)=1} I_i \,\cup\, \bigl\{a_i : \chi(2i-1) = 1\bigr\}.$$

Then for every $\chi \in {}^{2n+1}2$, E is a support of S_χ and for every $S_0 \subseteq A$ such that E is a support of S_0 there is a $\chi_0 \in {}^{2n+1}2$ such that $S_0 = S_{\chi_0}$ (this follows from LEMMA 7.12).

We now consider for a moment the set ${}^{2n+2}2$: Let "$<_l$" be the lexicographic ordering on ${}^{2n+2}2$, *i.e.*, $\xi <_l \xi'$ if there is a $j \in 2n+2$ such that $\xi(j) < \xi'(j)$, but for all $i < j$ we have $\xi(i) = \xi'(i)$. For $\xi \in {}^{2n+2}2$ let $\bar{\xi} \in {}^{2n+2}2$ be such that for all $i \in 2n+2$, $\bar{\xi}(i) := 1 - \xi(i)$. We define the function $\mu : {}^{2n+2}2 \to {}^{2n+2}2$ by stipulating

$$\mu(\xi) = \begin{cases} \xi & \text{if } \xi <_l \bar{\xi}, \\ \bar{\xi} & \text{otherwise,} \end{cases}$$

in other words, $\mu(\xi)$ is ξ or $\bar{\xi}$, whichever begins with 0.

Let us turn back to the set ${}^{2n+1}2$. For $\chi \in {}^{2n+1}2$ let $\chi^+ := \chi \cup \bigl\{\langle 2n+1, 0\rangle\bigr\}$. Notice that $\chi^+ \in {}^{2n+2}2$. We define the ordering "$\prec_n$" on ${}^{2n+1}2$ by stipulating

$$\chi_0 \prec_n \chi_1 \iff \mu(\chi_0^+) <_l \mu(\chi_1^+).$$

Now, we are ready to define a surjection from $\text{fin}(A)$ onto $\mathscr{P}(A)$. For this, consider the following function:

$$\begin{aligned} g : \text{fin}(A) &\longrightarrow \mathscr{P}(A) \\ E \quad &\longmapsto S_{\chi^*_{|E|}} \end{aligned}$$

where for $|E| = n$, χ_n^* denotes the n^{th} function of ${}^{2n+1}2$ with respect to the ordering "$\prec_n$".

By construction, for every set $S_0 \in \mathscr{P}(A)$ there is a finite set E such that E is a support of S_0 and $S_0 = S_{\chi^*_{|E|}}$. Indeed, let E_0 be the least support of S_0. Then there is an $n \in \omega$ such that $S_0 = S_{\chi^*_n}$. By the properties of the ordering "$\prec_{|E_0|}$", $n \geq |E_0|$ and we leave it as an exercise to show that E_0 can be extended to a finite set E such that $|E| = n$ and $S_{\chi^*_{|E|}} = S_0$. Hence, the mapping g is surjective as required. $\dashv$

PROPOSITION 7.15. *Let $\mathfrak{m}$ denote the cardinality of the set of atoms of the ordered Mostowski model. Then*

$$\mathcal{V}_M \vDash n \cdot \operatorname{fin}(\mathfrak{m}) < 2^{\mathfrak{m}} < \aleph_0 \cdot \operatorname{fin}(\mathfrak{m})$$

for every $n \in \omega$.

Proof (Sketch). $2^{\mathfrak{m}} \leq \aleph_0 \cdot \operatorname{fin}(\mathfrak{m})$: For $S \subseteq A$ let E be the least support of S, let $n = |E|$, and let $k \in \omega$ be such that $S = S_{\chi_k}$, where χ_k denotes the k^{th} function of ${}^{2n+1}2$ with respect to the ordering "$\prec_n$" defined above. Then the mapping $S \mapsto (k, S_{\chi_k})$ is an injective function from $\mathscr{P}(A)$ into $\omega \times \operatorname{fin}(A)$.

$2^{\mathfrak{m}} \neq \aleph_0 \cdot \operatorname{fin}(\mathfrak{m})$: This is an immediate consequence of LEMMA 7.13.

$n \cdot \operatorname{fin}(\mathfrak{m}) \leq 2^{\mathfrak{m}}$: For $j \in n$ and $E \in \operatorname{fin}(A)$ large enough we can define $S_{j,E}$ as the j^{th} set which has E as its least support. For $E \in \operatorname{fin}(A)$ which are not large enough to allow such an encoding, we have to work with a large enough auxiliary set E_0 and then do some encoding for example on $E \cup E_0$.

$n \cdot \operatorname{fin}(\mathfrak{m}) \neq 2^{\mathfrak{m}}$: Assume towards a contradiction that there is an injective function $f : \mathscr{P}(A) \hookrightarrow n \times \operatorname{fin}(A)$. Let $k \in \omega$ be such that $2^{2k+1} > n \cdot 2^k$ and let $E_0 \subseteq A$ be a finite set of size k. By LEMMA 7.12 there are 2^{2k+1} subsets of A, say $S_1, S_2, \ldots$, which have E_0 as their support. Since there are only 2^k subsets of E_0, by the choice of k there is a first S_i ($1 \leq i \leq 2^{2k+1}$) such that $f(S_i) \notin n \times \operatorname{fin}(E_0)$. Now, $f(S_i) = \langle m, F_0 \rangle$ for some $m \in k$ and $F_0 \in \operatorname{fin}(A)$. Since $F_0 \nsubseteq E_0$ we have $|E_0 \cup F_0| > |E_0|$ and can proceed with $E_1 = E_0 \cup F_0$. Finally, with the sets $E_0, E_1, \ldots$ we get $\aleph_0 \leq 2^{\mathfrak{m}}$, which contradicts LEMMA 7.13. $\dashv$

The Prime Ideal Theorem Revisited

In this section we show that the Prime Ideal Theorem holds in the ordered Mostowski model. In other words, the Axiom of Choice is not provable in ZFA from the Prime Ideal Theorem.

THEOREM 7.16. *The* Prime Ideal Theorem *holds in the ordered Mostowski model.*

Proof. By THEOREM 5.15 it is enough to show that in $\boldsymbol{\mathcal{V}}_M$, for every binary mess $\mathcal{B}$ there is a function f which is consistent with $\mathcal{B}$.

Let $\mathcal{B} \in \boldsymbol{\mathcal{V}}_M$ be a binary mess on a set S, and let $E_{\mathcal{B}}$ be the least support of $\mathcal{B}$. On S define an equivalence relation by stipulating $x \sim y$ *iff* there is a $\pi \in \mathrm{fix}_{\mathscr{G}}(E_{\mathcal{B}})$ such that $y = \pi x$. For every $x \in S$ let

$$[x]^{\sim} = \{\pi x : \pi \in \mathrm{fix}_{\mathscr{G}}(E_{\mathcal{B}})\} \qquad \text{(the orbit of } x\text{)}$$

and let $\tilde{S} = \{[x]^{\sim} : x \in S\}$. Notice that $x \sim y$ *iff* $[x]^{\sim} = [y]^{\sim}$.

The goal — which will become clear later — is to lift some functions t of the binary mess on S to functions h defined on finite subsets of $\tilde{S}$ in order to get a binary mess $\tilde{\mathcal{B}}$ on $\tilde{S}$ so that every function g on $\tilde{S}$ which is consistent with $\tilde{\mathcal{B}}$ induces a function $f \in \boldsymbol{\mathcal{V}}_M$ which is consistent with $\mathcal{B}$. Let $\tilde{\mathcal{B}}$ consist of all binary functions h defined on finite subsets $\tilde{Q}$ of $\tilde{S}$ that satisfy the following condition: For every finite set $P \subseteq \bigcup\{[x]^{\sim} : [x]^{\sim} \in \tilde{Q}\}$ there is a $t \in \mathcal{B}$ such that t is defined on P and

$$t(x) = h([x]^{\sim}) \ \textit{ for every } x \in P.$$

If this is the case, we say that the set P *admits* the function h. In other words, P admits h if and only if there is a binary function $t \in \mathcal{B}$ which is defined on P such that whenever $x, y \in P$ and $x \sim y$, then $t(x) = t(y) = h([x]^{\sim})$. In order to show that $\tilde{\mathcal{B}}$ is a binary mess, we have to verify that for every finite set $\tilde{Q} \subseteq \tilde{S}$ there is a binary function $h \in \tilde{\mathcal{B}}$ which is defined on $\tilde{Q}$.

Once we know that $\tilde{\mathcal{B}}$ is a binary mess, we can take any g on $\tilde{S}$ consistent with $\tilde{\mathcal{B}}$ and define

$$f(x) = g([x]^{\sim})$$

for every $x \in S$. The function f is obviously symmetric, hence $f \in \boldsymbol{\mathcal{V}}_M$, and we are done. So, all that we have to do is to prove the following claim:

> For every finite set $\tilde{Q} \subseteq \tilde{S}$ there is a binary function $h \in \tilde{\mathcal{B}}$ defined on $\tilde{Q}$, such that for every finite set $P \subseteq \bigcup\{[x]^{\sim} : [x]^{\sim} \in \tilde{Q}\}$, P admits h.

For simplicity we distinguish two cases:

$E_{\mathcal{B}}$ is empty: Let $\tilde{Q}$ be a finite subset of $\tilde{S} = \{[x]^{\sim} : x \in S\}$ and let $Q = \{x \in S : [x]^{\sim} \in \tilde{Q}\}$. We are looking for a binary function h on $\tilde{Q}$ such that every finite subset of Q admits h. Notice that we have $r = 2^q$ binary functions h on $\tilde{Q}$ to choose from, where $q = |\tilde{Q}|$. In $\boldsymbol{\mathcal{M}}$, fix some $P_0 \subseteq Q$ which has exactly one element in each equivalence class $[x]^{\sim} \in \tilde{Q}$ and notice that by definition of $\tilde{S}$, $Q = \bigcup\{\pi P_0 : \pi \in \mathscr{G}\}$. Let us say that $P \subseteq Q$ is a *k-set* if there are k permutations $\pi_1, \ldots, \pi_k \in \mathscr{G}$ such that $P = \pi_1 P_0 \cup \ldots \cup \pi_k P_0$. Since every finite subset of Q is included in a k-set for some k, it is sufficient to show that for every k and for every k-set P there is a binary function h on $\tilde{Q}$ such that P admits h.

Let k be arbitrary but fixed. We say that two k-sets P_1 and P_2 are *isomorphic* if $P_2 = \pi(P_1)$ for some $\pi \in \mathscr{G}$. Notice that being isomorphic is an equivalence relation. If P_1 and P_2 are isomorphic and P_1 admits h (where h is some binary function on $\tilde{Q}$), then also P_2 admits h. To see this, first notice that since $E_{\mathcal{B}} = \emptyset$, a binary function t belongs to $\mathcal{B}$ *iff* πt belongs to $\mathcal{B}$ (for any $\pi \in \mathscr{G}$). If P_1 admits h, then there is a $t \in \mathcal{B}$ such that t is defined on P_1 and for all $x \in P_1$ we have $t(x) = h([x]\tilde{})$. Let $P_2 = \pi(P_1)$ and consider the binary function $\pi t \in \mathcal{B}$: Since $t(x) \in \{0,1\}$, $\pi\big(t(x)\big) = h([x]\tilde{})$. Further, for each $y \in P_2$ there is an $x \in P_1$ such that $y = \pi x$, which implies that the binary function πt is defined on P_2. Hence, for any $y \in P_2$ and $x = \pi^{-1} y \in P_1$ we have $(\pi t)(y) = (\pi t)(\pi x) = t(x) = h([x]\tilde{}) = h([y]\tilde{})$, which shows that P_2 admits h. Thus, if a k-set P admits the binary function h, then all k-sets belonging to the same isomorphism class as P also admit h.

Now we show that there are only finitely many isomorphism classes of k-sets: Let E_0 be the least support of P_0 and let $n = |E_0|$. Let $\{E_1, \dots, E_k\}$ and $\{E'_1, \dots, E'_k\}$ be two sets of n-element subsets of A (where A is the set of atoms of $\boldsymbol{\mathcal{V}}_M$). We say that these two so-called (k,n)-sets are *isomorphic* if there is a $\pi \in \mathscr{G}$ which transforms the set $\{E_1, \dots, E_k\}$ into the set $\{E'_1, \dots, E'_k\}$. Notice that there are only finitely many isomorphism classes of (k,n)-sets. To see this, let us just consider the case when $n = k = 2$: Let $E_1 = \{a, b\}$ and $E_2 = \{c, d\}$, and without loss of generality let us assume that $a < b$, $c < d$, and that $a = \min\{a, b, c, d\}$. Then the seven different types we can have are represented by $a < b < c < d$, $a < b = c < d$, $a < c < b < d$, $a < c < b = d$, $a = c < b < d$, $a = c < b = d$, and $a < c < d < b$.

For each $E = \pi E_0$ let $P_E := \pi P_0$. Notice that for every $E = \pi E_0$ there is a function h defined on $\tilde{Q}$ such that P_E admits h. (Let $t \in \mathcal{B}$ be any function defined on P_E.) Further, for each (k,n)-set $\bar{E} = \{E_1, \dots, E_k\} = \{\pi_1 E_0, \dots, \pi_k E_0\}$ let $P_{\bar{E}} := \pi_1 P_0 \cup \ldots \cup \pi_k P_0$. If $\bar{E}$ and $\bar{E}'$ are isomorphic, then so are the two k-sets $P_{\bar{E}}$ and $P_{\bar{E}'}$. On the other hand, for every k-set P there are k permutations $\pi_1, \dots, \pi_k \in \mathscr{G}$ such that $P = \pi_1 P_0 \cup \ldots \cup \pi_k P_0$, which implies that $P = P_{\bar{E}}$ where $\bar{E} = \{\pi_1 E_0, \dots, \pi_k E_0\}$, and consequently we get that $P_{\bar{E}}$ and $P_{\bar{E}'}$ are isomorphic *iff* $\bar{E}$ and $\bar{E}'$ are isomorphic. Hence, since there are only finitely many isomorphism classes of (k,n)-sets, there are only finitely many isomorphism classes of k-sets.

Thus it suffices to find a binary function h such that for any set of representatives $\{\bar{E}_1, \dots, \bar{E}_p\}$, where p is the number of isomorphism classes of (k,n)-sets, we have that each k-set $P_{\bar{E}_i}$ $(1 \le i \le p)$ admits h.

Now we apply the FINITE RAMSEY THEOREM 2.3 which tells us that for all $m, n, r \in \omega$ there exists an $N \in \omega$ such that for every colouring of $[N]^n$ with r colours, there exists a set $H \in [N]^m$, all whose n-element subsets have the same colour: Let $m = k \cdot n$ and $r = 2^q$, and let $F \in [A]^N$ be a set of N atoms. Further, let $P = \bigcup \big\{ P_E : E \in [F]^n \big\}$ and take any $t \in \mathcal{B}$ which is defined on P. Then each $t|_{P_E}$ corresponds to one of the r possible binary functions $h_1, \dots, h_r$ defined on $\tilde{Q}$, which induces a colouring on $[F]^n$ with r colours. By the FINITE RAMSEY THEOREM 2.3 we find a set $H \in [F]^m$ such that for every $E \in [H]^n$, $t|_{P_E}$ is the same function and therefore induces a unique function on Q, say h. Finally, by the choice of m, the set H contains members from each isomorphism class, which implies that each k-set $P \subseteq Q$ admits h.

$E_{\mathcal{B}}$ is non-empty: Assume $E_{\mathcal{B}} = \{a_1, \ldots, a_l\}$ where $a_1 < \ldots < a_l$. Instead of $\mathscr{G}$ we have to work with $\text{fix}_{\mathscr{G}}(E_{\mathcal{B}})$. Let $I_1 = |\{a \in A : a < a_1\}|$, $I_j = |\{a \in A : a_{j-1} < a < a_j\}|$ (for $1 < j < l$), and $I_l = |\{a \in A : a_l < a\}|$. Let P_0 and E_0 be as above and for $1 \leq j \leq l$ let $n_j := |E_0 \cap I_j|$. Instead of (k,n)-sets consider sets of the form $\{\mathcal{E}_1, \ldots, \mathcal{E}_n\}$, where for $1 \leq i \leq n$, $\mathcal{E}_i = \langle E_{i,1}, \ldots, E_{i,l}\rangle$ and for each $1 \leq j \leq l$, $E_{i,j} \subseteq I_j$ and $|E_{i,j}| = n_j$. Now we can proceed as above until we reach the point where the FINITE RAMSEY THEOREM comes in. Here, the combinatorics gets slightly more involved and instead of the FINITE RAMSEY THEOREM we need Rado's generalisation, which is THEOREM 2.7 given in Chapter 2: It says that for all $r, l, m, n_1, \ldots, n_l \in \omega$ there is some $N \in \omega$ such that whenever $[N]^{n_1} \times \ldots \times [N]^{n_l}$ is coloured with r colours, then there are $M_1, \ldots, M_l \in [N]^m$ such that $[M_1]^{n_1} \times \ldots \times [M_l]^{n_l}$ is monochromatic. Let $m = \max\{k \cdot n_i : 1 \leq i \leq l\}$ and $r = 2^q$, and let $F_1, \ldots, F_l \in [A]^N$ be N-element sets of atoms such that for every $1 \leq j \leq l$, $F_j \subseteq I_j$. Then we find l sets $M_j \in [F_j]^m$ such that $[M_1]^{n_1} \times \ldots \times [M_l]^{n_l}$ is monochromatic, which implies again that each k-set $P \subseteq Q$ admits the same function h. $\dashv$

Custom-Built Permutation Models

Below we shall construct two permutation models. The first one is designed in order to show that the existence of infinite cardinals $\mathfrak{m}$ for which $\text{seq}(\mathfrak{m}) < \text{fin}(\mathfrak{m})$ is consistent with ZF. By modifying the first custom-built permutation model, this somewhat counter intuitive result can even be pushed a little bit further by showing that also the existence of infinite cardinals $\mathfrak{m}$ for which $\mathfrak{m}^2 < [\mathfrak{m}]^2$ is consistent with ZF.

The first custom-built permutation model

The set of atoms of the first custom-built permutation model is built by induction, where every atom encodes a finite sequence of atoms on a lower level and every finite sequence of atoms appears in finitely many atoms.

By induction on $n \in \omega$ we construct sets A_n, functions Seq_n from A_n to $\text{seq}(A_{n-1})$, and groups G_n which are subgroups of the group of permutations of A_n as follows:

(α) $A_0 := \{a_0\}$, where a_0 is an atom, $Seq_0(a_0) = \langle\ \rangle$, and $G_0 = \{\iota\}$ is the group of all permutations of A_0.

For $n \in \omega$ let $k_n = |G_n|$, and let $\mathscr{S}_n$ be the set of sequences of A_n of length less than or equal to $n+1$ which do not belong to the range of Seq_n. Then

(β) $A_{n+1} := A_n \dot\cup \big\{(n+1,\zeta,i) : \zeta \in \mathscr{S}_n \wedge i < k_n + k_n\big\}$.

(γ) Seq_{n+1} is a function from A_{n+1} to $\operatorname{seq}(A_n)$ defined as follows:

$$Seq_{n+1}(x) = \begin{cases} Seq_n(x) & \text{if } x \in A_n, \\ \zeta & \text{if } x = (n+1,\zeta,i) \in A_{n+1} \setminus A_n. \end{cases}$$

(δ) G_{n+1} is the subgroup of the group of permutations of A_{n+1} containing all permutations h such that for some $g_h \in G_n$ and $j_h < k_n + k_n$ we have

$$h(x) = \begin{cases} g_h(x) & \text{if } x \in A_n, \\ \big(n+1, g_h(\zeta), i +_n j_h\big) & \text{if } x = (n+1,\zeta,i) \in A_{n+1} \setminus A_n, \end{cases}$$

where $g_h(\zeta)(m) := g_h\big(\zeta(m)\big)$ and $+_n$ is addition modulo $(k_n + k_n)$.

Let $A := \bigcup\{A_n : n \in \omega\}$. For each triple $(n,\zeta,i) \in \tilde{A}$ we assign an atom $\alpha_{(n,\zeta,i)}$ and define the set of atoms by stipulating $\tilde{A} := A_0 \cup \big\{\alpha_{(n,\zeta,i)} : (n,\zeta,i) \in A\big\}$. However, for the sake of simplicity we shall work with A as the set of atoms rather than with $\tilde{A}$. Let $Seq := \bigcup\{Seq_n : n \in \omega\}$; then Seq is a function from A onto $\operatorname{seq}(A)$. Furthermore, let $\operatorname{Aut}(A)$ be the group of all permutations of A. Then $\mathscr{G} := \big\{H \in \operatorname{Aut}(A) : \forall n \in \omega(H|_{A_n} \in G_n)\big\}$ is a group of permutations of A. Finally, let $\mathscr{F}$ be the filter on $\mathscr{G}$ generated by $\big\{\operatorname{fix}_{\mathscr{G}}(E) : E \in \operatorname{fin}(A)\big\}$ (which happens to be normal) and let $\boldsymbol{\mathcal{V}}_s$ (s for sequences) be the class of all hereditarily symmetric objects. Now we are ready to prove the following result.

Proposition 7.17. *Let $\mathfrak{m}$ denote the cardinality of the set of atoms A of $\boldsymbol{\mathcal{V}}_s$. Then $\boldsymbol{\mathcal{V}}_s \vDash \operatorname{seq}(\mathfrak{m}) < \operatorname{fin}(\mathfrak{m})$.*

Proof. Firstly we prove that $\boldsymbol{\mathcal{V}}_s \vDash \operatorname{seq}(\mathfrak{m}) \leq \operatorname{fin}(\mathfrak{m})$ by constructing a one-to-one function f in $\boldsymbol{\mathcal{V}}_s$ which maps $\operatorname{seq}(A)$ into $\operatorname{fin}(A)$. For any sequence $\zeta \in \operatorname{seq}(A)$ there is a least $n_\zeta \in \omega$ such that $\zeta \in \mathscr{S}_{n_\zeta}$. Define $f : \operatorname{seq}(A) \to \operatorname{fin}(A)$ by stipulating

$$f(\zeta) = \big\{a \in A : \exists i(a = \alpha_{(n_\zeta+1,\zeta,i)})\big\}.$$

Obviously, f is injective and it remains to show that f belongs to $\boldsymbol{\mathcal{V}}_s$. Take an arbitrary permutation $\pi \in \mathscr{G}$ and let $\zeta \in \operatorname{seq}(A)$ be an arbitrary sequence. Notice first that by the definition of $\mathscr{G}$, $n_\zeta = n_{\pi\zeta}$. Thus, for each $i < k_{n_\zeta} + k_{n_\zeta}$ there is a $j < k_{n_\zeta} + k_{n_\zeta}$ such that $\pi(n_\zeta+1,\zeta,i) = (n_{\pi\zeta}+1,\pi\zeta,j)$, which shows that $\pi\big\langle\zeta, f(\zeta)\big\rangle = \big\langle\pi\zeta, f(\pi\zeta)\big\rangle$, and since ζ was arbitrary we get $\pi f = f$.

In order to prove that $\boldsymbol{\mathcal{V}}_s \vDash \operatorname{seq}(\mathfrak{m}) \neq \operatorname{fin}(\mathfrak{m})$ assume towards a contradiction that there is a one-to-one function $g \in \boldsymbol{\mathcal{V}}_s$ from $\operatorname{fin}(A)$ into $\operatorname{seq}(A)$.

Notice first that for every $E \in \operatorname{fin}(A)$ there are $C, F \in \operatorname{fin}(A)$ such that $E \subseteq C$, and for all $x \in A \setminus C$ we have $\big|\{\pi x : \pi \in \operatorname{fix}_{\mathscr{G}}(C)\}\big| > 2$, and $\big|\big\{\pi F : \pi \in \operatorname{fix}_{\mathscr{G}}(C)\big\}\big| = 2$. Indeed, choose $n \geq 1$ such that $E \subseteq A_n$, and let

$C := A_n$ and $F := \{(n+1,\zeta,i) \in A_{n+1} : i \textit{ is even}\}$. Then F has exactly two images under the permutations of $\text{fix}_{\mathscr{G}}(C)$, and for all $x \in A \setminus C$ we have $\left|\{\pi x : \pi \in \text{fix}_{\mathscr{G}}(C)\}\right| \geq (k_n + k_n) > 2$.

Let E be a support of g and let C and F be as above. If the sequence $g(F)$ belongs to $\text{seq}(C)$, then for some $\pi \in \text{fix}_{\mathscr{G}}(C)$, $\pi F \neq F$, hence, $g(\pi F) \neq g(F)$. But this contradicts that C is a support of g and that $\pi \in \text{fix}_{\mathscr{G}}(C)$. Otherwise, if the sequence $g(F)$ does not belong to $\text{seq}(C)$, there is an $m \in \omega$ such that $x_0 := g(F)(m) \notin C$. Hence, by the choice of C and F we have $\left|\{\pi x_0 : \pi \in \text{fix}_{\mathscr{G}}(C)\}\right| > 2$, and $\left|\{\pi F : \pi \in \text{fix}_{\mathscr{G}}(C)\}\right| = 2$. Since every $\pi \in \text{fix}_{\mathscr{G}}(C)$ maps g to itself, in particular $\langle F, g(F)\rangle$ to $\langle \pi F, \pi g(F)\rangle$, and since

$$\left|\{\pi F : \pi \in \text{fix}_{\mathscr{G}}(C)\}\right| < \left|\{\pi x_0 : \pi \in \text{fix}_{\mathscr{G}}(C)\}\right|,$$

the image under g of a 2-element set has strictly more than two elements, which is obviously a contradiction. ⊣

The second custom-built permutation model

The set of atoms of the second custom-built permutation model is also built by induction, and every atom encodes an ordered pair of atoms on a lower level. The model we finally get will be a model in which there exists a cardinal $\mathfrak{m}$ such that $\mathfrak{m}^2 < [\mathfrak{m}]^2$, which is to some extent just a finite version of PROPOSITION 7.17. The atoms are constructed as follows:

(α) A_0 is an arbitrary countable infinite set of atoms.

(β) $\mathscr{G}_0$ is the group of all permutations of A_0.

(γ) $A_{n+1} := A_n \dot\cup \{(n+1,p,\varepsilon) : p \in A_n \times A_n \wedge \varepsilon \in \{0,1\}\}$.

(δ) $\mathscr{G}_{n+1}$ is the subgroup of the permutation group of A_{n+1} containing all permutations h for which there are $g_h \in \mathscr{G}_n$ and $\varepsilon_h \in \{0,1\}$ such that

$$h(x) = \begin{cases} g_h(x) & \text{if } x \in A_n, \\ (n+1, g_h(p), \varepsilon_h +_2 \varepsilon) & \text{if } x = (n+1,p,\varepsilon), \end{cases}$$

where for $p = \langle p_1, p_2\rangle \in A_n$, $g_h(p) := \langle g_h(p_1), g_h(p_2)\rangle$ and $+_2$ denotes addition modulo 2.

Let $A := \bigcup\{A_n : n \in \omega\}$ and let $\text{Aut}(A)$ be the group of all permutations of A. Then

$$\mathscr{G} := \{H \in \text{Aut}(A) : \forall n \in \omega\, (H|_{A_n} \in \mathscr{G}_n)\}$$

is a group of permutations of A. Let $\mathscr{F}$ be the filter on $\mathscr{G}$ generated by $\{\text{fix}_{\mathscr{G}}(E) : E \in \text{fin}(A)\}$ (which happens to be normal) and let $\boldsymbol{\mathcal{V}}_p$ (p for pairs) be the class of all hereditarily symmetric objects. Now we are ready to prove the following

PROPOSITION 7.18. *Let $\mathfrak{m}$ denote the cardinality of the set of atoms A of $\boldsymbol{\mathcal{V}}_p$. Then $\boldsymbol{\mathcal{V}}_p \vDash \mathfrak{m}^2 < [\mathfrak{m}]^2$.*

Proof. First we show that $\boldsymbol{\mathcal{V}}_p \vDash \mathfrak{m}^2 \leq [\mathfrak{m}]^2$. For this it is sufficient to find a one-to-one function $f \in \boldsymbol{\mathcal{V}}_p$ from A^2 into $[A]^2$. We define such a function as follows. For $x, y \in A$ let

$$f\big(\langle x, y\rangle\big) := \big\{(n+m+1, \langle x, y\rangle, 0), (n+m+1, \langle x, y\rangle, 1)\big\}\,,$$

where n and m are the smallest numbers such that $x \in A_n$ and $y \in A_m$, respectively. For any $\pi \in \mathscr{G}$ and $x, y \in A$ we have $\pi f(\langle x, y\rangle) = f(\langle \pi x, \pi y\rangle)$ and therefore, the function f is as desired and belongs to $\boldsymbol{\mathcal{V}}_p$.

Now assume towards a contradiction that there exists a one-to-one function $g \in \boldsymbol{\mathcal{V}}_p$ from $[A]^2$ into A^2 and let E_g be a finite support of g. Without loss of generality we may assume that if $\big(n+1, \langle x, y\rangle, \varepsilon\big) \in E_g$, then also $x, y \in E_g$ (this will be needed later). Let $k := |E_g|$ and for $x, y \in A$ let $g(\{x, y\}) = \langle t^0_{\{x,y\}}, t^1_{\{x,y\}}\rangle$. Let $r := k+4$ and let $N \in \omega$ be such that for every colouring $\tau : [N]^2 \to r^2$ we find a 3-element set $H \in [N]^3$ such that $\tau|_{[H]^2}$ is constant. Such a number N exists by the FINITE RAMSEY THEOREM 2.3. Choose N distinct elements $x_0, \ldots, x_{N-1} \in A_0 \setminus E_g$, let $X = \{x_0, \ldots, x_{N-1}\}$ and let $\{c_h : h < k\}$ be an enumeration of E_g (recall that $k = |E_g|$). We define a colouring $\tau : [X]^2 \to r \times r$ as follows. For $\{x_i, x_j\} \in [X]^2$, where $i < j$, let $\tau(\{x_i, x_j\}) = \langle \tau_0(\{x_i, x_j\}), \tau_1(\{x_i, x_j\})\rangle$ where for $l \in \{0, 1\}$ we define

$$\tau_l(\{x_i, x_j\}) := \begin{cases} h & \text{if } t^l_{\{x_i,x_j\}} = c_h, \\ k & \text{if } t^l_{\{x_i,x_j\}} = x_i, \\ k+1 & \text{if } t^l_{\{x_i,x_j\}} = x_j, \\ k+2 & \text{if } t^l_{\{x_i,x_j\}} \in A_0 \setminus \big(\{x_i, x_j\} \cup E_g\big), \\ k+3 & \text{if } t^l_{\{x_i,x_j\}} \in A \setminus (A_0 \cup E_g). \end{cases}$$

By the definition of N we find 3 elements $x_{\iota_0}, x_{\iota_1}, x_{\iota_2} \in X$ with $\iota_0 < \iota_1 < \iota_2$ such that for both $l \in \{0, 1\}$, τ_l is constant on $[\{x_{\iota_0}, x_{\iota_1}, x_{\iota_2}\}]^2$. So, for $\{x_{\iota_i}, x_{\iota_j}\} \in [\{x_{\iota_0}, x_{\iota_1}, x_{\iota_2}\}]^2$ with $i < j$ and for some $l \in \{0, 1\}$, we are in at least one of the following cases:

(1) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} = c_{h_0}$ and $t^{1-l}_{\{x_{\iota_i},x_{\iota_j}\}} = c_{h_1}$

(2) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} = c_h$ and $t^{1-l}_{\{x_{\iota_i},x_{\iota_j}\}} = x_{\iota_i}$

(3) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} = c_h$ and $t^{1-l}_{\{x_{\iota_i},x_{\iota_j}\}} = x_{\iota_j}$

(4) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} = t^{1-l}_{\{x_{\iota_i},x_{\iota_j}\}}$ and $t^l_{\{x_{\iota_i},x_{\iota_j}\}} \in \{x_{\iota_i}, x_{\iota_j}\}$

(5) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} = x_{\iota_i}$ and $t^{1-l}_{\{x_{\iota_i},x_{\iota_j}\}} = x_{\iota_j}$

(6) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} \in A_0 \setminus (E_g \cup \{x_{\iota_i}, x_{\iota_j}\})$

(7) $t^l_{\{x_{\iota_i},x_{\iota_j}\}} \in A \setminus (E_g \cup A_0)$

If we are in case (1) or (2), then $g(\{x_{\iota_0}, x_{\iota_1}\}) = g(\{x_{\iota_0}, x_{\iota_2}\})$, and therefore g is not a one-to-one function. If we are in case (3), then g is also not a one-to-one function because $g(\{x_{\iota_0}, x_{\iota_2}\}) = g(\{x_{\iota_1}, x_{\iota_2}\})$, and the same is true for g if we are in case (4), *e.g.*, $g(\{x_{\iota_0}, x_{\iota_1}\}) = \langle x_{\iota_0}, x_{\iota_0}\rangle = g(\{x_{\iota_0}, x_{\iota_2}\})$.

If we are in case (5), then let $\pi \in \operatorname{fix}(E_g)$ be such that $\pi x_{\iota_0} = x_{\iota_1}$ and $\pi x_{\iota_1} = x_{\iota_0}$. Assume that $g(\{x_{\iota_0}, x_{\iota_1}\}) = \langle x_{\iota_0}, x_{\iota_1}\rangle$ (the case when $g(\{x_{\iota_0}, x_{\iota_1}\}) = \langle x_{\iota_1}, x_{\iota_0}\rangle$ is similar). Then we have $\pi\{x_{\iota_0}, x_{\iota_1}\} = \{x_{\iota_0}, x_{\iota_1}\}$, but $\pi g(\{x_{\iota_0}, x_{\iota_1}\}) = \langle x_{\iota_1}, x_{\iota_0}\rangle \neq \langle x_{\iota_0}, x_{\iota_1}\rangle$, and therefore E_g is not a support of g which contradicts the choice of E_g — which, by our assumption, has the property that whenever $\big(n+1, \langle x, y\rangle, \varepsilon\big) \in E_g$ also $x, y \in E_g$.

If we are in case (6), then let $l \in \{0,1\}$ be such that $t^l_{\{x_{\iota_0}, x_{\iota_1}\}} \in A_0 \setminus (E_g \cup \{x_{\iota_0}, x_{\iota_1}\})$ and let $a := t^l_{\{x_{\iota_0}, x_{\iota_1}\}}$. Without loss of generality we may assume $l = 0$, thus, $a = t^0_{\{x_{\iota_0}, x_{\iota_1}\}}$. Take an arbitrary $a' \in A_0 \setminus (E_g \cup \{a, x_{\iota_0}, x_{\iota_1}\})$ and let $\pi \in \operatorname{fix}(E_g \cup \{x_{\iota_0}, x_{\iota_1}\})$ be such that $\pi a = a'$ and $\pi a' = a$. Then we get $\pi\{x_{\iota_0}, x_{\iota_1}\} = \{x_{\iota_0}, x_{\iota_1}\}$ but

$$g\big(\pi\{x_{\iota_0}, x_{\iota_1}\}\big) = g\big(\{x_{\iota_0}, x_{\iota_1}\}\big) = \langle a, x\rangle \neq \langle a', x'\rangle = \pi\langle a, x\rangle = \pi g\big(\{x_{\iota_0}, x_{\iota_1}\}\big)\,.$$

Hence, E_g is not a support of g which contradicts the choice of E_g.

If we are in case (7), then let $l \in \{0,1\}$ be such that $t^l_{\{x_{\iota_0}, x_{\iota_1}\}} \in A \setminus (E_g \cup A_0)$, thus $t^l_{\{x_{\iota_0}, x_{\iota_1}\}} = (n+1, p, \varepsilon)$ for some $(n+1, p, \varepsilon) \in A$. Further, let $\pi \in \operatorname{fix}(E_g \cup \{x_{\iota_0}, x_{\iota_1}\})$ be such that $\pi(n+1, p, \varepsilon) = (n+1, p, 1-\varepsilon)$. Then we have $\pi\{x_{\iota_0}, x_{\iota_1}\} = \{x_{\iota_0}, x_{\iota_1}\}$ but $\pi g(\{x_{\iota_0}, x_{\iota_1}\}) \neq g(\{x_{\iota_0}, x_{\iota_1}\})$, and therefore E_g is not a support of g which contradicts the choice of E_g.

So, in all the cases, either g is not one-to-one or E_g is not a support of g, which contradicts our assumption and completes the proof. ⊣

Notes

Permutation models. The method of permutation models was introduced by Fraenkel [2, 4, 3, 5, 6], and, in a precise version with supports, by Lindenbaum and Mostowski [18] and by Mostowski [20, 21, 22]. The present version with filters is due to Specker [23]. In particular, the second Fraenkel model can be found for example in Fraenkel [2], where he proved that the Axiom of Choice for countable families of pairs is unprovable in ZFA (for a proof in a more general setting see Mendelson [19]), and the ordered Mostowski model is introduced in [21, § 4, p. 236] in order to show that the Axiom of Choice is independent from the Ordering Principle. (Some more background can be found for example in Lévy [17].)

The Prime Ideal Theorem. The independence of the Axiom of Choice from the Prime Ideal Theorem in ZFA was proved first by Halpern [10] (but the proof presented above is taken from Jech [13, Chapter 7, §1]). A few years later, the same result in ZF was proved by Halpern and Lévy [12], using the Halpern-Läuchli Theorem.

The custom-built models. The first custom-built permutation model as well as Proposition 7.17 is due to Shelah and can be found in [8, Theorem 2]. The second custom-built permutation model, which is just a modification of the first one, is due to Halbeisen, but the crucial part of PROPOSITION 7.18 is again due to Shelah (*cf.* Halbeisen and Shelah [9, Propostition 7.3.1]).

RELATED RESULTS

43. *Alternative definition of atoms.* Atoms could also be defined by stipulating $a \in A \iff a = \{a\}$. This approach has the advantage that we do not need to modify the AXIOM OF EXTENSIONALITY; however, it has the disadvantage that models of ZFA would not be well-founded — except in the case when $A = \emptyset$.

44. *The Axiom of Choice in Algebra.* Läuchli shows in [14] that many classical results in Algebra cannot be proved without the aid of the Axiom of Choice. For example he shows that it is consistent with ZFA that there exists vector spaces without algebraic bases, or in which there exist two algebraic bases with different cardinalities.

45. *More cardinal relations.* Let $\mathfrak{m}$ denote the cardinality of the set of atoms of the *basic Fraenkel model* $\mathcal{V}_{F_0}$. Then the following statements hold in $\mathcal{V}_{F_0}$ (*cf.* Halbeisen and Shelah [9, Proposition 7.1.3]):
   (a) $\text{fin}(\mathfrak{m}) \perp \text{seq}^{1\text{-}1}(\mathfrak{m})$ and $\text{fin}(\mathfrak{m}) \perp \text{seq}(\mathfrak{m})$.
   (b) $\text{seq}^{1\text{-}1}(\mathfrak{m}) \perp 2^{\mathfrak{m}}$ and $\text{seq}(\mathfrak{m}) \perp 2^{\mathfrak{m}}$.
   (c) $\text{seq}^{1\text{-}1}(\mathfrak{m}) < \text{seq}(\mathfrak{m})$.

   Unlike in the basic Fraenkel model, the cardinalities $\text{fin}(\mathfrak{m})$, $2^{\mathfrak{m}}$, $\text{seq}^{1\text{-}1}(\mathfrak{m})$, and $\text{seq}(\mathfrak{m})$ are all comparable in the *ordered Mostowski model*. Let $\mathfrak{m}$ denote the cardinality of the set of atoms of $\mathcal{V}_M$. Then the following sequence of inequalities holds in $\mathcal{V}_M$:

   $$\mathfrak{m} < [\mathfrak{m}]^2 < \mathfrak{m}^2 < \text{fin}(\mathfrak{m}) < 2^{\mathfrak{m}} < \text{seq}^{1\text{-}1}(\mathfrak{m}) < \text{fin}^2(\mathfrak{m}) < \text{seq}^{1\text{-}1}(\text{fin}(\mathfrak{m})) < \\ < \text{fin}(2^{\mathfrak{m}}) < \text{fin}^3(\mathfrak{m}) < \text{fin}^4(\mathfrak{m}) < \ldots < \text{fin}^n(\mathfrak{m}) < \text{seq}(\mathfrak{m}) < 2^{\text{fin}(\mathfrak{m})} = 2^{2^{\mathfrak{m}}}$$

   (See for example Halbeisen and Shelah [9, p. 249] or Halbeisen [7], or just use the ideas of the proof of PROPOSITION 7.15.) Furthermore we have that

   $$\mathcal{V}_M \vDash \left(2^{2^{\mathfrak{m}}}\right)^{\aleph_0} = 2^{2^{\mathfrak{m}}}$$

   which follows for example from the fact that $\mathcal{V}_M \vDash 2^{2^{\mathfrak{m}}} = 2^{\text{fin}(\mathfrak{m})}$ and LÄUCHLI'S LEMMA 4.27.
   Finally, let $\mathfrak{m}$ denote the cardinality of the set of atoms of the *second Fraenkel model*. Then, by PROPOSITION 7.9 and LÄUCHLI'S LEMMA 4.27 we have

   $$\mathcal{V}_{F_2} \vDash \left(2^{2^{\mathfrak{m}}}\right)^{\aleph_0} = 2^{2^{\mathfrak{m}}}.$$

46. *Multiple Choice and Kurepa's Principle in Fraenkel's models.* In Chapter 5 we have seen that Multiple Choice and Kurepa's Principle are both equivalent in ZF to the Axiom of Choice. On the other hand, one can show that Multiple Choice holds in the model $\mathcal{V}_{F_0}$ and that Kurepa's Principle holds in the model $\mathcal{V}_{F_2}$ (see Lévy [16] and Halpern [11] respectively, or Jech [13, Theorem 9.2]). This shows that these two choice principles — which imply AC in ZF — are weaker than AC in ZFA.

47. *Countable unions of countable sets.* In order to show that a union of countably many countable sets is not necessarily countable, one can work for example in the permutation model given by Fraenkel [6]: The set of atoms consists of countably many mutually disjoint countable sets. So, $A = \bigcup_{n\in\omega} C_n$ where each C_n is countable. For each $n \in \omega$, the group G_n consists of all permutations of C_n and $\mathscr{G} = \prod_{n\in\omega} G_n$. The normal filter $\mathscr{F}$ on $\mathscr{G}$ is generated by products of the form $\prod_{n\in\omega} H_n$, where H_n is either equal to G_n or the trivial group, and the former is the case for all but finitely many n's.

48. *Ordering principles in Mostowski's model.* Mostowski showed in [21] that in ZFA, the Axiom of Choice is not provable from the Ordering Principle (see also Jech [13, Theorem 4.7]). In fact he showed that the Ordering Principle holds in the ordered Mostowski model $\mathcal{V}_M$, whereas the Axiom of Choice obviously fails in that model. Notice also that even the Prime Ideal Theorem, which implies the Ordering Principle, holds in $\mathcal{V}_M$.
In [1], Felgner and Truss gave a direct proof — not referring to the Prime Ideal Theorem — of the fact that the Order-Extension Principle holds in $\mathcal{V}_M$, and then, by modifying $\mathcal{V}_M$, they were able to show that in ZFA, the Prime Ideal Theorem is not provable from the Order-Extension Principle.
Läuchli showed in [15] (see also Jech [13, p. 53]) that the following form of the Axiom of Choice holds in $\mathcal{V}_M$: *For every family of non-empty well-orderable sets there is a choice function.* Notice that this implies that in $\mathcal{V}_M$, the union of a countable set of countable sets is always countable.

49. *Another custom-built permutation model.* Let $\mathfrak{m}$ denote the cardinality of the set of atoms of the first custom-built permutation model $\mathcal{V}_s$. Then one can show that $\mathcal{V}_s \vDash \operatorname{seq}^{1\text{-}1}(\mathfrak{m}) < \operatorname{seq}(\mathfrak{m}) < 2^{\mathfrak{m}}$ (see Halbeisen and Shelah [9, Proposition 7.4.1], or use PROPOSITION 7.17 and show that $\mathfrak{m}$ is D-finite.)
So, for an infinite cardinals $\mathfrak{m}$ we can have $\operatorname{seq}^{1\text{-}1}(\mathfrak{m}) < \operatorname{seq}(\mathfrak{m}) < 2^{\mathfrak{m}}$ (which holds in $\mathcal{V}_s$) as well as $2^{\mathfrak{m}} < \operatorname{seq}^{1\text{-}1}(\mathfrak{m}) < \operatorname{seq}(\mathfrak{m})$ (which holds in $\mathcal{V}_M$), and therefore both statements are consistent with ZF. It is now natural to ask whether it is also possible to put $2^{\mathfrak{m}}$ between the cardinals $\operatorname{seq}^{1\text{-}1}(\mathfrak{m})$ and $\operatorname{seq}(\mathfrak{m})$ (recall that by THEOREM 4.24, for all infinite cardinals $\mathfrak{m}$ we have $\operatorname{seq}^{1\text{-}1}(\mathfrak{m}) \neq 2^{\mathfrak{m}} \neq \operatorname{seq}(\mathfrak{m})$). Indeed, the existence of an infinite cardinal $\mathfrak{m}$ for which

$$\operatorname{seq}^{1\text{-}1}(\mathfrak{m}) < 2^{\mathfrak{m}} < \operatorname{seq}(\mathfrak{m})$$

is also consistent with ZF and the permutation model in which this holds — given in Halbeisen and Shelah [9, Section 7.4] — is due to Shelah.

References

1. ULRICH FELGNER AND JOHN K. TRUSS, *The independence of the prime ideal theorem from the order-extension principle*, ***The Journal of Symbolic Logic***, vol. 64 (1999), 199–215.
2. ADOLF FRAENKEL, *Der Begriff "definit" und die Unabhängigkeit des Auswahlaxioms*, ***Sitzungsberichte der Preussischen Akademie der Wissenschaften zu Berlin. Physicalisch-Mathematische Klasse***, vol. 21 (1922), 253–257 (see [24] for a translation into English).

3. ———, *Über die Ordnungsfähigkeit beliebiger Mengen*, ***Sitzungsberichte der Preussischen Akademie der Wissenschaften zu Berlin. Physicalisch-Mathematische Klasse***, vol. 29 (1928), 90–91.
4. ———, *Gelöste und ungelöste Probleme im Umkreis des Auswahlprinzips*, Atti del congresso internationale dei matematici, Bologna 3–10 Settembre 1928, Vol. II, Bologna, 1930, pp. 255–259.
5. ———, *Sur l'axiome du choix*, ***L'Enseignement Mathématique***, vol. 34 (1935), 32–51.
6. ———, *Über eine abgeschwächte Fassung des Auswahlaxioms*, ***The Journal of Symbolic Logic***, vol. 2 (1937), 1–25.
7. Lorenz Halbeisen, *Vergleiche zwischen unendlichen Kardinalzahlen in einer Mengenlehre ohne Auswahlaxiom*, Diplomarbeit (1990), University of Zürich (Switzerland).
8. Lorenz Halbeisen and Saharon Shelah, *Consequences of arithmetic for set theory*, ***The Journal of Symbolic Logic***, vol. 59 (1994), 30–40.
9. ———, *Relations between some cardinals in the absence of the axiom of choice*, ***The Bulletin of Symbolic Logic***, vol. 7 (2001), 237–261.
10. James D. Halpern, *The independence of the axiom of choice from the Boolean prime ideal theorem*, ***Fundamenta Mathematicae***, vol. 55 (1964), 57–66.
11. ———, *On a question of Tarski and a maximal theorem of Kurepa*, ***Pacific Journal of Mathematics***, vol. 41 (1972), 111–121.
12. James D. Halpern and Azriel Lévy, *The Boolean prime ideal theorem does not imply the axiom of choice*, *in* ***Axiomatic Set Theory*** (Dana S. Scott, ed.), [Proceedings of Symposia in Pure Mathematics, Vol. XIII, Part I], American Mathematical Society, Providence, Rhode Island, 1971, pp. 83–134.
13. Thomas Jech, ***The Axiom of Choice***, Studies in Logic and the Foundations of Mathematics 75, North-Holland, Amsterdam, 1973.
14. Hans Läuchli, *Auswahlaxiom in der Algebra*, ***Commentarii Mathematici Helvetici***, vol. 37 (1962), 1–18.
15. ———, *The independence of the ordering principle from a restricted axiom of choice*, ***Fundamenta Mathematicae***, vol. 54 (1964), 31–43.
16. Azriel Lévy, *Axioms of multiple choice*, ***Fundamenta Mathematicae***, vol. 50 (1961), 475–483.
17. ———, *The Fraenkel-Mostowski method for independence proofs in set theory*, *in* ***The Theory of Models,*** *Proceedings of the 1963 International Symposium at Berkeley* (J.W. Addison, L. Henkin, and A. Tarski, eds.), [Studies in Logic and the Foundation of Mathematics], North-Holland, Amsterdam, 1965, pp. 221–228.
18. Adolf Lindenbaum and Andrzej Mostowski, *Über die Unabhängigkeit des Auswahlaxioms und einiger seiner Folgerungen*, ***Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III***, vol. 31 (1938), 27–32.
19. Elliott Mendelson, *The independence of a weak axiom of choice*, ***The Journal of Symbolic Logic***, vol. 21 (1956), 350–366.
20. Andrzej Mostowski, *Über den Begriff einer endlichen Menge*, ***Comptes rendus des séances de la Société des Sciences et des Lettres de Varsovie, Cl. III***, vol. 31 (1938), 13–20.
21. ———, *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip*, ***Fundamenta Mathematicae***, vol. 32 (1939), 201–252.

22. ———, *Axiom of choice for finite sets*, ***Fundamenta Mathematicae***, vol. 33 (1945), 137–168.
23. Ernst Specker, *Zur Axiomatik der Mengenlehre (Fundierungs- und Auswahlaxiom)*, ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik***, vol. 3 (1957), 173–210.
24. Jean van Heijenoort, ***From Frege to Gödel. A Source Book in Mathematical Logic, 1879–1931***, [Source Books in the History of Science], Harvard University Press, Cambridge, Massachusetts, 1967.

8

Twelve Cardinals and their Relations

The consonances are those intervals which are formed from the natural steps.
An interval may be diminished when one of its steps is replaced by a smaller one.
Or it may be augmented when one of its steps is replaced by a larger one.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

In this chapter we investigate twelve cardinal characteristics and their relations to one another. A cardinal characteristic of the continuum is an uncountable cardinal number which is less than or equal to $\mathfrak{c}$ that describes a combinatorial or analytical property of the continuum. Like the power of the continuum itself, the size of a cardinal characteristic is often independent from ZFC. However, some restrictions on possible sizes follow from ZFC, and we shall give a complete list of what is known to be provable in ZFC about their relation. Later in Part II, but mainly in Part III, we shall see how one can diminish or augment some of these twelve cardinals without changing certain other cardinals. In fact, these cardinal characteristics are also used to investigate combinatorial properties of the various forcing notions introduced in Part III.

We shall encounter some of these cardinal characteristics (*e.g.*, $\mathfrak{p}$) more often than others (*e.g.*, $\mathfrak{i}$). However, we shall encounter each of these twelve cardinals again, and like the twelve notes of the chromatic scale, these twelve cardinals will build the framework of our investigation of the combinatorial properties of forcing notions that is carried out in Part III.

On the one hand, it would be good to have the definition of a cardinal characteristic at hand when it is needed; but on the other hand, it is also convenient to have all the definitions together (especially when a cardinal characteristic is used several times), rather than scattered over the entire book. Defining all twelve cardinals at once also gives us the opportunity to show what is known to be provable in ZFC about the relationship between these twelve cardinals. Thus, one might first skip this chapter and go back to it later and take bits and pieces when necessary.

The Cardinals ω_1 and $\mathfrak{c}$

We have already met both cardinals, $\mathfrak{c}$ and ω_1: $\mathfrak{c}$ is the cardinality of the continuum $\mathbb{R}$, and ω_1 is the smallest uncountable cardinal. According to FACT 4.3, $\mathfrak{c} = 2^\omega$ is also the cardinality of the sets $[0,1]$, ${}^\omega 2$, ${}^\omega\omega$, and $[0,1] \setminus \mathbb{Q}$; and by LEMMA 4.10, ω_1 can also be considered as the set of order types of well-orderings of $\mathbb{Q}$.

The Continuum Hypothesis, denoted CH, states that $\mathfrak{c}$ is the least uncountable cardinal, *i.e.*, $\mathfrak{c} = \omega_1$ (*cf.* Chapter 4), which is equivalent to saying that every subset of $\mathbb{R}$ is either countable or of the same cardinality as $\mathbb{R}$. Furthermore, the Generalised Continuum Hypothesis, denoted GCH, states that for every ordinal $\alpha \in \Omega$, $2^{\omega_\alpha} = \omega_{\alpha+1}$. Gödel showed that $\mathbf{L} \vDash \mathsf{GCH}$, where $\mathbf{L}$ is the constructible universe (see the corresponding note in Chapter 5), thus, GCH is consistent with ZFC.

Each of the following ten combinatorial cardinal characteristics of the continuum is uncountable and less than or equal to $\mathfrak{c}$. Thus, if we assume CH, then these cardinals are all equal to $\mathfrak{c}$. However, as we shall see in Part II, CH is not provable in ZFC. In other words, if ZFC is consistent then there are models of ZFC in which CH fails, *i.e.*, models in which $\omega_1 < \mathfrak{c}$. In those models, possible (*i.e.*, consistent) relations between the following cardinal characteristics will be provided in Part II and Part III.

The Cardinal $\mathfrak{p}$

For two sets $x, y \subseteq \omega$ we say that x is **almost contained** in y, denoted $x \subseteq^* y$, if $x \setminus y$ is finite, *i.e.*, all but finitely many elements of x belong to y. For example a finite subset of ω is almost contained in $\emptyset$, and ω is almost contained in every co-finite subset of ω (*i.e.*, in every $y \subseteq \omega$ such that $\omega \setminus y$ is finite). A **pseudo-intersection** of a family $\mathscr{F} \subseteq [\omega]^\omega$ of infinite subsets of ω is an infinite subset of ω that is almost contained in every member of $\mathscr{F}$. For example ω is a pseudo-intersection of the family of co-finite sets. Furthermore, a family $\mathscr{F} \subseteq [\omega]^\omega$ has the **strong finite intersection property** (*sfip*) if every finite subfamily has infinite intersection. Notice that every family with a pseudo-intersection necessarily has the *sfip*, but not vice versa. For example any filter $\mathscr{F} \subseteq [\omega]^\omega$ has the *sfip*, but no ultrafilter on $[\omega]^\omega$ has a pseudo-intersection.

DEFINITION OF $\mathfrak{p}$. The **pseudo-intersection number $\mathfrak{p}$** is the smallest cardinality of any family $\mathscr{F} \subseteq [\omega]^\omega$ which has the *sfip* but which does not have a pseudo-intersection; more formally

$$\mathfrak{p} = \min\big\{|\mathscr{F}| : \mathscr{F} \subseteq [\omega]^\omega \text{ has the } \textit{sfip} \text{ but no pseudo-intersection}\big\}.$$

Since ultrafilters on $[\omega]^\omega$ are families which have the *sfip* but do not have a pseudo-intersection, and since every ultrafilter on $[\omega]^\omega$ is of cardinality $\mathfrak{c}$, the cardinal $\mathfrak{p}$ is well-defined and $\mathfrak{p} \leq \mathfrak{c}$. It is natural to ask whether $\mathfrak{p}$ can be smaller than $\mathfrak{c}$; however, the following result shows that $\mathfrak{p}$ cannot be too small.

THEOREM 8.1. $\omega_1 \leq \mathfrak{p}$.

Proof. Let $\mathscr{E} = \{X_n \in [\omega]^\omega : n \in \omega\}$ be a countable family which has the *sfip*. We construct a pseudo-intersection of $\mathscr{E}$ as follows: Let $a_0 := \bigcap X_0$ and for positive integers n let

$$a_n = \bigcap\Big(\bigcap\{X_i : i \in n\} \setminus \{a_i : i \in n\}\Big).$$

Further, let $Y = \{a_n : n \in \omega\}$; then for every $n \in \omega$, $Y \setminus \{a_i : i \in n\} \subseteq X_n$ which shows that $Y \subseteq^* X_n$, hence, Y is a pseudo-intersection of $\mathscr{E}$. $\dashv$

The Cardinals $\mathfrak{b}$ and $\mathfrak{d}$

For two functions $f, g \in {}^\omega\omega$ we say that g **dominates** f, denoted $f <^* g$, if for all but finitely many integers $k \in \omega$, $f(k) < g(k)$, *i.e.*, if there is an $n_0 \in \omega$ such that for all $k \geq n_0$, $f(k) < g(k)$. Notice that ordering "$<^*$" is transitive, however, "$<^*$" it is not a linear ordering (we leave it as an exercise to the reader to find functions $f, g \in {}^\omega\omega$ such that neither $f <^* g$ nor $g <^* f$).

A family $\mathscr{D} \subseteq {}^\omega\omega$ is **dominating** if for each $f \in {}^\omega\omega$ there is a function $g \in \mathscr{D}$ such that $f <^* g$.

DEFINITION OF $\mathfrak{d}$. The **dominating number $\mathfrak{d}$** is the smallest cardinality of any dominating family; more formally

$$\mathfrak{d} = \min\big\{|\mathscr{D}| : \mathscr{D} \subseteq {}^\omega\omega \text{ is dominating}\big\}.$$

A family $\mathscr{B} \subseteq {}^\omega\omega$ is **unbounded** if there is no single function $f \in {}^\omega\omega$ which dominates all functions of $\mathscr{B}$, *i.e.*, for every $f \in {}^\omega\omega$ there is a $g \in \mathscr{B}$ such that $g \not<^* f$. Since "$<^*$" is not a linear ordering, an unbounded family is not necessarily dominating — but vice versa (see FACT 8.2).

DEFINITION OF $\mathfrak{b}$. The **bounding number $\mathfrak{b}$** is the smallest cardinality of any unbounded family; more formally

$$\mathfrak{b} = \min\big\{|\mathscr{B}| : \mathscr{B} \subseteq {}^\omega\omega \text{ is unbounded}\big\}.$$

Obviously, the family ${}^{\omega}\omega$ itself is dominating and therefore unbounded, which shows that $\mathfrak{d}$ and $\mathfrak{b}$ are well-defined and $\mathfrak{b}, \mathfrak{d} \leq \mathfrak{c}$. Moreover, we have the following

FACT 8.2. $\mathfrak{b} \leq \mathfrak{d}$.

Proof. It is enough to show that every dominating family is unbounded. So, let $\mathscr{D} \subseteq {}^{\omega}\omega$ be a dominating family and let $f \in {}^{\omega}\omega$ be an arbitrary function. Since $\mathscr{D}$ is dominating, there is a $g \in \mathscr{D}$ such that $f <^* g$, *i.e.*, there is an $n_0 \in \omega$ such that for all $k \geq n_0$, $f(k) < g(k)$. Hence we get $g \not<^* f$, and since f was arbitrary this implies that $\mathscr{D}$ is unbounded. ⊣

It is natural to ask whether $\mathfrak{b}$ can be smaller than $\mathfrak{d}$, or at least smaller than $\mathfrak{c}$; however, the following result shows that $\mathfrak{b}$ cannot be too small.

THEOREM 8.3. $\omega_1 \leq \mathfrak{b}$.

Proof. Let $\mathscr{E} = \{g_n \in {}^{\omega}\omega : n \in \omega\}$ be a countable family. We construct a function $f \in {}^{\omega}\omega$ which dominates all functions of $\mathscr{E}$: For each $k \in \omega$ let

$$f(k) = \bigcup \{g_i(k) : i \in k\}.$$

Then for every $k \in \omega$ and each $i \in k$ we have $f(k) \geq g_i(k)$ which shows that for all $n \in \omega$, $g_n <^* f$, hence, f dominates all functions of $\mathscr{E}$. ⊣

One could also define dominating and unbounded families with respect to the ordering "$<$" defined by stipulating $f < g \iff \forall k \in \omega\big(f(k) < g(k)\big)$. Then the corresponding dominating number would be the same as $\mathfrak{d}$, as any dominating family can be made dominating in the new sense by adding all finite modifications of its members; but the corresponding bounding number would drop to ω, as the family of all constant functions is unbounded (we leave the details to the reader).

The Cardinals $\mathfrak{s}$ and $\mathfrak{r}$

A set $x \subseteq \omega$ **splits** an infinite set $y \in [\omega]^\omega$ if both $y \cap x$ and $y \setminus x$ are infinite (*i.e.*, $|y \cap x| = |y \setminus x| = \omega$). Notice that any $x \subseteq \omega$ which splits a set $y \in [\omega]^\omega$ must be infinite. A **splitting family** is a family $\mathscr{S} \subseteq [\omega]^\omega$ such that each $y \in [\omega]^\omega$ is split by at least one $x \in \mathscr{S}$.

DEFINITION OF $\mathfrak{s}$. The **splitting number** $\mathfrak{s}$ is the smallest cardinality of any splitting family; more formally

$$\mathfrak{s} = \min\big\{|\mathscr{S}| : \mathscr{S} \subseteq [\omega]^\omega \text{ is splitting}\big\}.$$

By THEOREM 8.1 and later results we get $\omega_1 \leq \mathfrak{s}$ — we leave it as an exercise to the reader to find a direct proof of the uncountability of $\mathfrak{s}$.

In the proof of the following result we will see how to construct a splitting family from a dominating family.

THEOREM 8.4. $\mathfrak{s} \leq \mathfrak{d}$.

Proof. For each strictly increasing function $f \in {}^\omega\omega$ with $f(0) > 0$ let

$$\sigma_f = \bigcup \Big\{ \big[f^{2n}(0), f^{2n+1}(0)\big) : n \in \omega \Big\} ,$$

where for $a, b \in \omega$, $[a, b) := \{k \in \omega : a \leq k < b\}$ and $f^{n+1}(0) = f\big(f^n(0)\big)$ with $f^0(0) := 0$. Let $\mathscr{D} \subseteq {}^\omega\omega$ be a dominating family. Without loss of generality we may assume that every $f \in \mathscr{D}$ is strictly increasing and $f(0) > 0$, and let

$$\mathscr{S}_{\mathscr{D}} = \big\{\sigma_f : f \in \mathscr{D}\big\} .$$

We show that $\mathscr{S}_{\mathscr{D}}$ is a splitting family. So, fix an arbitrary $x \in [\omega]^\omega$ and let $f_x \in {}^\omega\omega$ be the (unique) strictly increasing bijection between ω and x. More formally, define $f_x : \omega \twoheadrightarrow x$ by stipulating

$$f_x(k) = \bigcap \Big(x \setminus \big\{f_x(i) : i \in k\big\} \Big) .$$

Notice that for all $k \in \omega$, $f_x(k) \geq k$. Since $\mathscr{D}$ is dominating there is an $f \in \mathscr{D}$ such that $f_x <^* f$, which implies that there is an $n_0 \in \omega$ such that for all $k \geq n_0$ we have $f_x(k) < f(k)$. For each $k \in \omega$ we have $k \leq f^k(0)$ as well as $k \leq f_x(k)$. Moreover, for $k \geq n_0$ we have

$$f^k(0) \leq f_x\big(f^k(0)\big) < f\big(f^k(0)\big) = f^{k+1}(0)$$

and therefore $f_x\big(f^k(0)\big) \in \big[f^k(0), f^{k+1}(0)\big)$. Thus, for all $k \geq n_0$ we have $f_x\big(f^k(0)\big) \in \sigma_f$ *iff* k is even, which shows that both $x \cap \sigma_f \cap x$ and $x \setminus \sigma_f$ are infinite. Hence, σ_f splits x, and since x was arbitrary, $\mathscr{S}_{\mathscr{D}}$ is a splitting family. ⊣

A **reaping family** — also known as *refining* or *unsplittable* family — is a family $\mathscr{R} \subseteq [\omega]^\omega$ such that there is no single set $x \in [\omega]^\omega$ which splits all elements of $\mathscr{R}$, *i.e.*, for every $x \in [\omega]^\omega$ there is a $y \in \mathscr{R}$ such that $y \cap x$ or $y \setminus x$ is finite. In other words, a family $\mathscr{R}$ is reaping if for every $x \in [\omega]^\omega$ there is a $y \in \mathscr{R}$ such that $y \subseteq^* (\omega \setminus x)$ or $y \subseteq^* x$. The origin of "reaping" in this context is that A *reaps* B *iff* A *splits* B, by analogy with a scythe cutting the stalks of grain when one reaps the grain. So, a *reaping family* would be a *splitting family*. However, the more logical approach, where "reaps" means "is unsplit by", seems to have no connection with the everyday meaning of the word "reap".

Definition of $\mathfrak{r}$. The **reaping number** $\mathfrak{r}$ is the smallest cardinality of any reaping family; more formally

$$\mathfrak{r} = \min\left\{|\mathscr{R}| : \mathscr{R} \subseteq [\omega]^\omega \text{ is reaping}\right\}.$$

Since the family $[\omega]^\omega$ is obviously reaping, $\mathfrak{r}$ is well-defined and $\mathfrak{r} \leq \mathfrak{c}$. Furthermore, by Theorem 8.3, the following result implies that every reaping family is uncountable:

Theorem 8.5. $\mathfrak{b} \leq \mathfrak{r}$.

Proof. Let $\mathscr{E} = \{x_\xi \in [\omega]^\omega : \xi \in \kappa < \mathfrak{b}\}$ be an arbitrary family of infinite subsets of ω of cardinality strictly less than $\mathfrak{b}$. We show that $\mathscr{E}$ is not a reaping family. For each $x_\xi \in \mathscr{E}$ let $g_\xi \in {}^\omega\omega$ be the unique strictly increasing bijection between ω and $x_\xi \setminus \{0\}$. Further, let $\tilde{g}_\xi(k) := g_\xi^k(0)$, where $g_\xi^{k+1}(0) = g_\xi\big(g_\xi^k(0)\big)$ and $g_\xi^0(0) := 0$. Consider $\tilde{\mathscr{E}} = \{\tilde{g}_\xi : \xi \in \kappa\}$. Since $\kappa < \mathfrak{b}$, the family $\tilde{\mathscr{E}}$ is bounded, *i.e.*, there exists an $f \in {}^\omega\omega$ such that for all $\xi \in \kappa$, $\tilde{g}_\xi <^* f$. Let $x = \bigcup_{k\in\omega}\big[f^{2k}(0), f^{2k+1}(0)\big)$. Then for each $\xi \in \kappa$ there is an $n_\xi \in \omega$ such that for all $k \geq n_\xi$, $f^k(0) \leq \tilde{g}_\xi\big(f^k(0)\big) < f\big(f^k(0)\big)$. This implies that neither $x_\xi \subseteq^* x$ nor $x_\xi \subseteq^* (\omega \setminus x)$, and hence, $\mathscr{E}$ is not a reaping family. ⊣

The Cardinals $\mathfrak{a}$ and $\mathfrak{i}$

Two sets $x, y \in [\omega]^\omega$ are **almost disjoint** if $x \cap y$ is finite. A family $\mathscr{A} \subseteq [\omega]^\omega$ of pairwise almost disjoint sets is called an **almost disjoint** family; and a **maximal almost disjoint** (*mad*) family is an infinite almost disjoint family $\mathscr{A} \subseteq [\omega]^\omega$ which is maximal with respect to inclusion, *i.e.*, $\mathscr{A}$ is not properly contained in any almost disjoint family $\mathscr{A}' \subseteq [\omega]^\omega$.

Definition of $\mathfrak{a}$. The **almost disjoint number** $\mathfrak{a}$ is the smallest cardinality of any maximal almost disjoint family; more formally

$$\mathfrak{a} = \min\left\{|\mathscr{A}| : \mathscr{A} \subseteq [\omega]^\omega \text{ is } mad\right\}.$$

Before we show that $\mathfrak{b} \leq \mathfrak{a}$ (which implies that $\mathfrak{a}$ is uncountable), let us show first that there is a *mad* family of cardinality $\mathfrak{c}$.

Proposition 8.6. *There exists a maximal almost disjoint family of cardinality* $\mathfrak{c}$.

Proof. Notice that by Teichmüller's Principle, every almost disjoint family can be extended to a *mad* family. So, it is enough to construct an almost disjoint family $\mathscr{A}_0$ of cardinality $\mathfrak{c}$. Let $\{s_i : i \in \omega\}$ be an enumeration of $\bigcup_{n\in\omega} {}^n\omega$, *i.e.*, for each $t : n \to \omega$ there is a unique $i \in \omega$ such that $t = s_i$. For $f \in {}^\omega\omega$ let

$$x_f = \left\{i \in \omega : \exists n \in \omega\,(f|_n = s_i)\right\}.$$

Then, for any distinct functions $f, g \in {}^{\omega}\omega$, $x_f \cap x_g$ is finite. Indeed, if $f \neq g$, then there is an $n_0 \in \omega$ such that $f(n_0) \neq g(n_0)$ which implies that for all $k > n_0$, $f|_k \neq g|_k$, and hence, $|x_f \cap x_g| \leq n_0 + 1$. Now, let $\mathscr{A}_0 := \{x_f : f \in {}^{\omega}\omega\}$. Then $\mathscr{A}_0 \subseteq [\omega]^{\omega}$ is a set of pairwise almost disjoint infinite subsets of ω, therefore, $\mathscr{A}_0$ is an almost disjoint family of cardinality $|{}^{\omega}\omega| = \mathfrak{c}$. ⊣

The following result implies that $\mathfrak{a}$ is uncountable and in the proof we will show how one can construct an unbounded family from a *mad* family.

THEOREM 8.7. $\mathfrak{b} \leq \mathfrak{a}$.

Proof. Let $\mathscr{A} = \{x_\xi : \xi \in \kappa\}$ be a *mad* family. It is enough to construct an unbounded family of cardinality $|\mathscr{A}|$. Let $z = \omega \setminus \bigcup_{\xi\in\kappa} x_\xi$; then z is finite (otherwise, $\mathscr{A} \cup \{z\}$ would be an almost disjoint family which properly contains $\mathscr{A}$). Let $x'_0 := x_0 \cup z \cup \{0\}$ and for positive integers $n \in \omega$ let $x'_n := \big(x_n \cup \{n\}\big) \setminus \bigcup_{k\in n} x'_k$. Then, since $\mathscr{A}$ is an almost disjoint family, $\{x'_n : n \in \omega\}$ is a family of pairwise disjoint infinite subsets of ω and by construction, $\bigcup_{n\in\omega} x'_n = \omega$. Moreover, $\big(\mathscr{A} \setminus \{x_\xi : \xi \in \omega\}\big) \cup \{x'_n : n \in \omega\}$ is still *mad*. For $n \in \omega$ let $g_n \in {}^{\omega}\omega$ be the unique strictly increasing bijection from x'_n to ω, and let $h : \omega \to \omega \times \omega$ defined by stipulating

$$h(m) = \langle n, k\rangle \quad \text{where } m \in x'_n \text{ and } k = g_n(m)\,.$$

By definition, for each $n \in \omega$, $h[x'_n] = \big\{\langle n, k\rangle : k \in \omega\big\}$, and for all $\xi \in \kappa$, $h[x_{\omega+\xi}] \cap x'_n$ is finite. Further, for each $\xi \in \kappa$ define $f_\xi \in {}^{\omega}\omega$ by stipulating

$$f_\xi(k) = \bigcup \big(h[x_{\omega+\xi}] \cap x'_k\big)$$

and let $\mathscr{B} = \{f_\xi \in {}^{\omega}\omega : \xi \in \kappa\}$. Then by definition $|\mathscr{B}| = |\mathscr{A}|$; moreover, $\mathscr{B}$ is unbounded. Indeed, if there would be a function $f \in {}^{\omega}\omega$ which dominates all functions of $\mathscr{B}$, then the infinite set $\big\{h^{-1}\big(\langle n, f(n)\rangle\big) : n \in \omega\big\}$ would have finite intersection which each element of $\mathscr{A}$ contrary to maximality of $\mathscr{A}$. ⊣

A family $\mathscr{I} \subseteq [\omega]^{\omega}$ is called **independent** if the intersection of any finitely many members of $\mathscr{I}$ and the complements of any finitely many other members of $\mathscr{I}$ is infinite. More formally, $\mathscr{I} \subseteq [\omega]^{\omega}$ is independent if for any $n, m \in \omega$ and disjoint sets $\{x_i : i \in n\}, \{y_j : j \in m\} \subseteq \mathscr{I}$,

$$\bigcap_{i\in n} x_i \cap \bigcap_{j\in m} (\omega \setminus y_j) \quad \text{is infinite}\,,$$

where we stipulate $\bigcap \emptyset := \omega$. Equivalently, $\mathscr{I} \subseteq [\omega]^{\omega}$ is independent if for any $I, J \in \operatorname{fin}(\mathscr{I})$ with $I \cap J = \emptyset$ we have

$$\bigcap I \setminus \bigcup J \quad \text{is infinite}\,.$$

We leave it as an exercise to the reader to show that if $\mathscr{I}$ is infinite, then $\mathscr{I}$ is independent *iff* for any disjoint sets $I, J \in \operatorname{fin}(\mathscr{I})$, $\bigcap I \setminus \bigcup J \neq \emptyset$.

A **maximal independent** family is an independent family $\mathscr{I} \subseteq [\omega]^\omega$ which is maximal with respect to inclusion, *i.e.*, $\mathscr{I}$ is not properly contained in any independent family $\mathscr{I}' \subseteq [\omega]^\omega$.

DEFINITION OF $\mathfrak{i}$. The **independence number $\mathfrak{i}$** is the smallest cardinality of any maximal independent family; more formally

$$\mathfrak{i} = \min\big\{|\mathscr{I}| : \mathscr{I} \subseteq [\omega]^\omega \text{ is independent}\big\}.$$

We shall see that $\max\{\mathfrak{r}, \mathfrak{d}\} \leq \mathfrak{i}$ (which implies that $\mathfrak{i}$ is uncountable), but first let us show that there is a maximal independent family of cardinality $\mathfrak{c}$.

PROPOSITION 8.8. *There is a maximal independent family of cardinality* $\mathfrak{c}$.

Proof. It is enough to construct an independent family of cardinality $\mathfrak{c}$ on some countably infinite set. So, let us construct an independent family of cardinality $\mathfrak{c}$ on the countably infinite set

$$C = \big\{\langle s, A\rangle : s \in \operatorname{fin}(\omega) \wedge A \subseteq \mathscr{P}(s)\big\}.$$

Further, for each $x \subseteq [\omega]^\omega$ define

$$P_x := \big\{\langle s, A\rangle \in C : x \cap s \in A\big\}.$$

Notice that for any distinct $x, y \in [\omega]^\omega$ there is a finite set $s \in \operatorname{fin}(\omega)$ such that $x \cap s \neq y \cap s$, and consequently we get $P_x \neq P_y$ which implies that the set $\mathscr{I}_0 = \big\{P_x : x \in [\omega]^\omega\big\} \subseteq [C]^\omega$ is of cardinality $\mathfrak{c}$. Moreover, $\mathscr{I}_0$ is an independent family on C. Indeed, for any finitely many distinct infinite subsets of ω, say $x_0, \ldots, x_m, \ldots, x_{m+n}$ where $m, n \in \omega$, there is a finite set $s \subseteq \omega$ such that for all i, j with $0 \leq i < j \leq m+n$ we have $x_i \cap s \neq x_j \cap s$. Let $A = \{s \cap x_i : 0 \leq i \leq m\} \subseteq \mathscr{P}(s)$, and for every $k \in \omega \setminus s$ let $s_k := s \cup \{k\}$ and $A_k := A \cup \big\{t \cup \{k\} : t \in A\big\}$. Then

$$\big\{\langle s_k, A_k\rangle : k \in \omega \setminus s\big\} \subseteq \bigcap_{0 \leq i \leq m} P_{x_i} \setminus \bigcup_{1 \leq j \leq n} P_{x_{m+j}},$$

which shows that $\bigcap\{P_{x_i} : 0 \leq i \leq m\} \setminus \bigcup\{P_{x_{m+j}} : 1 \leq j \leq n\}$ is infinite, and therefore, $\mathscr{I}_0$ is an independent family on C of cardinality $\mathfrak{c}$. ⊣

The following result implies that $\mathfrak{i}$ is uncountable.

THEOREM 8.9. $\max\{\mathfrak{r}, \mathfrak{d}\} \leq \mathfrak{i}$.

Proof. $\mathfrak{r} \leq \mathfrak{i}$: The idea is to show that every maximal independent family yields a reaping family of the same cardinality. For this, let $\mathscr{I} \subseteq [\omega]^\omega$ be a maximal independent family of cardinality $\mathfrak{i}$ and let

$$\mathscr{R} = \Big\{\bigcap I \setminus \bigcup J : I, J \in \operatorname{fin}(\mathscr{I}) \wedge I \cap J = \emptyset\Big\}.$$

Then $\mathscr{R}$ is a family of cardinality $\mathfrak{i}$. Furthermore, since $\mathscr{I}$ is a maximal independent family, for every $x \in [\omega]^\omega$ we find a $y \in \mathscr{R}$ (*i.e.*, $y = \bigcap I \setminus \bigcup J$) such that either $x \cap y$ or $(\omega \setminus x) \cap y$ is finite, and because $(\omega \setminus x) \cap y = y \setminus x$, this shows that x does not split all elements of $\mathscr{R}$. Thus, $\mathscr{R}$ is a reaping family of cardinality $\mathfrak{i}$, and therefore $\mathfrak{r} \leq \mathfrak{i}$.

$\mathfrak{d} \leq \mathfrak{i}$: The idea is to show that an independent family of cardinality strictly less than $\mathfrak{d}$ cannot be maximal. For this, suppose $\mathscr{I} = \{X_\xi : \xi \in \kappa < \mathfrak{d}\} \subseteq [\omega]^\omega$ is an infinite independent family of cardinality $\kappa < \mathfrak{d}$. We shall construct a set $Z \in [\omega]^\omega$ such that $\mathscr{I} \cup \{Z\}$ is still independent, which implies that the independent family $\mathscr{I}$ is not maximal. For this it is enough to show that for any finite, disjoint subfamilies of $\mathscr{I}$, say I and J, the infinite set $\bigcap I \setminus \bigcup J$ meets both Z and $\omega \setminus Z$ in an infinite set.

Let $\mathscr{I}_\omega := \{X_n : n \in \omega\} \subseteq \mathscr{I}$ be a countably infinite subfamily of $\mathscr{I}$ and for each $n \in \omega$ let $X_n^0 := X_n$ and $X_n^1 := \omega \setminus X_n$. Further, for each $g \in {}^\omega 2$ let

$$C_{n,g} = \bigcap_{k \in n} X_k^{g(k)}$$

and for $\mathscr{I}' := \mathscr{I} \setminus \mathscr{I}_\omega$ define

$$\mathscr{F} = \Big\{ \bigcap I' \setminus \bigcup J' : I' \text{ and } J' \text{ are finite, disjoint subfamilies of } \mathscr{I}' \Big\}.$$

Claim. *The family $\mathscr{C} = \{C_{n,g} : n \in \omega\}$ has a pseudo-intersection that has infinite intersection with every set in $\mathscr{F}$.*

Proof of Claim. Since $\mathscr{I}$ is an infinite independent family of cardinality $\kappa < \mathfrak{d}$, $\mathscr{F} \subseteq [\omega]^\omega$ is a family of cardinality κ such that each set in $\mathscr{F}$ has infinite intersection with every member of $\mathscr{C}$. For any $h \in {}^\omega\omega$ define

$$Y_g^h = \bigcup_{n \in \omega} \big(C_{n,g} \cap h(n) \big).$$

Since $\langle C_{n,g} : n \in \omega \rangle$ is decreasing (*i.e.*, $C_{n,g} \supseteq C_{m,g}$ whenever $n \leq m$), Y_g^h is almost contained in each member of $\mathscr{C}$ — however, Y_g^h is not necessarily infinite. It remains to choose the function $h \in {}^\omega\omega$ so that Y_g^h is infinite (*i.e.*, Y_g^h is a pseudo-intersection of $\mathscr{C}$) and has infinite intersection with every set in $\mathscr{F}$. Notice first that for every $A \in \mathscr{F}$ and for every $n \in \omega$, $A \cap C_{n,g}$ is infinite; thus, for every $A \in \mathscr{F}$ we can define a function $f_A(n) \in {}^\omega\omega$ by stipulating

$$f_A(n) = \text{the } n^{th} \text{ element (in increasing order) of } A \cap C_{n,g}.$$

Since $|\mathscr{F}| < \mathfrak{d}$, the family $\{f_A : A \in \mathscr{F}\}$ is not dominating. In particular, there is a function $h_0 \in {}^\omega\omega$ with the property that for each $A \in \mathscr{F}$ the set

$$D_A = \big\{ n \in \omega : h_0(n) > f_A(n) \big\}$$

is infinite. Now, for each $A \in \mathscr{F}$ and every $n \in D_A$ we have $h_0(n) \geq f_A(n) + 1$ which implies that $|A \cap h_0(n)| \geq |A \cap f_A(n) + 1| = n$, and since D_A is infinite, also $A \cap Y_g^{h_0}$ is infinite. Finally, by construction $Y_g^{h_0}$ is a pseudo-intersection of $\mathscr{C}$ that has infinite intersection with every set in $\mathscr{F}$. $\dashv_{\text{Claim}}$

By the CLAIM, for every $g \in {}^{\omega}2$ there is a set, say $Y_g \in [\omega]^{\omega}$, which has the following two properties:

(1) For all $n \in \omega$, $Y_g \subseteq^* \bigcap_{k\in n} X_k^{g(k)}$.

(2) $Y_g \cap \big(\bigcap I' \setminus \bigcup J'\big)$ is infinite whenever I' and J' are finite, disjoint subfamilies of $\mathscr{I}'$.

It follows from (1) that for any distinct $g, g' \in {}^{\omega}\omega$, Y_g and $Y_{g'}$ are almost disjoint. Let now

$$Q_0 = \big\{g \in {}^{\omega}\omega : \exists n_0 \in \omega\, \forall k \geq n_0 \,\big(g(k) = 0\big)\big\}$$

and

$$Q_1 = \big\{g \in {}^{\omega}\omega : \exists n_1 \in \omega\, \forall k \geq n_1 \,\big(g(k) = 1\big)\big\}\,.$$

Then $Q_0 \cup Q_1$ is a countably infinite subset of ${}^{\omega}\omega$. Let $\{g_n : n \in \omega\}$ be an enumeration of $Q_0 \cup Q_1$ and for each $n \in \omega$ let $Y'_{g_n} := Y_{g_n} \setminus \bigcup\{Y_{g_k} : k \in n\}$. Then $\{Y'_{g_n} : n \in \omega\}$ is a countable family of pairwise disjoint infinite subsets of ω. Finally let

$$Z = \bigcup_{g\in Q_0} Y'_g \quad \text{and} \quad Z' = \bigcup_{g\in Q_1} Y'_g\,.$$

Then Z and Z' are disjoint. Now we show that Z has infinite intersection with every $\bigcap I \setminus \bigcup J$, where I and J are arbitrary finite subfamilies of $\mathscr{I}$; and since the same also holds for $Z' \subseteq \omega \setminus Z$, $\mathscr{I} \cup \{Z\}$ is an independent family, *i.e.*, the independent family $\mathscr{I}$ of cardinality $< \mathfrak{i}$ is not maximal.

Given any finite, disjoint subfamilies $I, J \subseteq \mathscr{I}$, and let $I_0 = I \cap \mathscr{I}_\omega$, $J_0 = J \cap \mathscr{I}_\omega$, $I' = I \setminus I_0$, $J' = J \setminus J_0$, where $\mathscr{I}_\omega = \{X_n : n \in \omega\}$. Further, let $m \in \omega$ be such that $I_0 \cup J_0 \subseteq \{X_n : n \in m\} \subseteq \mathscr{I}_\omega$ and fix $g \in Q_0$ such that for all $n \in m$,

$$\big(X_n \in (I_0 \cup J_0) \wedge g(n) = 0\big) \leftrightarrow X_n \in I_0\,.$$

We get the following inclusions:

$$\bigcap I \setminus \bigcup J \;\supseteq\; \Big(\bigcap I' \setminus \bigcap J'\Big) \cap \bigcap_{n\in m} X_n^{g(n)} \;{}^*\!\supseteq\; \Big(\bigcap I' \setminus \bigcap J'\Big) \cap Y_g$$

The intersection on the very right is infinite (by property (2) of Y_g) and is contained in Z (because $g \in Q_0$). Hence, we have found an infinite set which is almost contained in $Z \cap \big(\bigcap I \setminus \bigcup J\big)$, and therefore Z is infinite. $\dashv$

The Cardinals $\mathfrak{par}$ and $\mathfrak{hom}$

By RAMSEY'S THEOREM 2.1, for every colouring $\pi : [\omega]^2 \to 2$ there is an $x \in [\omega]^{\omega}$ which is homogeneous for π, *i.e.*, $\pi|_{[x]^2}$ is constant. This leads to the following cardinal characteristic:

DEFINITION OF $\mathfrak{hom}$. The **homogeneity number $\mathfrak{hom}$** is the smallest cardinality of any family $\mathscr{F} \subseteq [\omega]^\omega$ with the property that for every colouring $\pi : [\omega]^2 \to 2$ there is an $x \in \mathscr{F}$ which is homogeneous for π.

The following result implies that $\mathfrak{hom}$ is uncountable. In fact we will show that each family which contains a homogeneous set for every 2-colouring of $[\omega]^2$ is reaping and that each such family yields a dominating family of the same cardinality.

THEOREM 8.10. $\max\{\mathfrak{r}, \mathfrak{d}\} \leq \mathfrak{hom}$.

Proof. Let $\mathscr{F} \subseteq [\omega]^\omega$ be a family such that for every colouring $\pi : [\omega]^2 \to 2$ there is an $x \in \mathscr{F}$ which is homogeneous for π. We shall show that $\mathscr{F}$ is reaping and that $\mathscr{F}' = \{f_x \in {}^\omega\omega : x \in \mathscr{F}\}$ is dominating, where f_x is the strictly increasing bijection between ω and x.

$\mathfrak{d} \leq \mathfrak{hom}$: Firstly we show that $\mathscr{F}$ is a dominating family. For any strictly increasing function $f \in {}^\omega\omega$ with $f(0) = 0$ define $\pi_f : [\omega]^2 \to 2$ by stipulating

$$\pi_f\big(\{n, m\}\big) = 0 \iff \exists k \in \omega\big(f(2k) \leq n, m < f(2k+2)\big)\,.$$

Then, for every $x \in \mathscr{F}$ which is homogeneous for π_f we have $f <^* f_x$ which implies that $\mathscr{F}'$ is dominating.

$\mathfrak{r} \leq \mathfrak{hom}$: Now we show that $\mathscr{F}$ is a reaping family. Take any $y \in [\omega]^\omega$ and define $\pi_y : [\omega]^2 \to 2$ by stipulating

$$\pi_y\big(\{n, m\}\big) = 0 \iff \{n, m\} \subseteq y \vee \{n, m\} \cap y = \emptyset\,.$$

Now, for every $x \in \mathscr{F}$ which is homogeneous for π_y we have either $x \subseteq y$ or $x \cap y = \emptyset$, and since y was arbitrary, $\mathscr{F}$ is reaping. $\dashv$

Recall that a set $H \in [\omega]^\omega$ is called **almost homogeneous** for a colouring $\pi : [\omega]^2 \to 2$ if there is a finite set $K \subseteq H$ such that $H \setminus K$ is homogeneous for π. This leads to the following cardinal characteristic:

DEFINITION OF $\mathfrak{par}$. The **partition number $\mathfrak{par}$** is the smallest cardinality of any family $\mathscr{P}$ of 2-colourings of $[\omega]^2$ such that no single $H \in [\omega]^\omega$ is almost homogeneous for all $\pi \in \mathscr{P}$.

By PROPOSITION 2.8 we get that $\mathfrak{par}$ is uncountable, and the following result gives an upper bound for $\mathfrak{par}$.

THEOREM 8.11. $\mathfrak{par} = \min\{\mathfrak{s}, \mathfrak{b}\}$.

Proof. First we show that $\mathfrak{par} \leq \min\{\mathfrak{s}, \mathfrak{b}\}$ and then we show that $\mathfrak{par} \geq \min\{\mathfrak{s}, \mathfrak{b}\}$. $\mathfrak{par} \leq \mathfrak{s}$: Let $\mathscr{S} \subseteq [\omega]^\omega$ be a splitting family and for each $x \in \mathscr{S}$ define the colouring $\pi_x : [\omega]^2 \to 2$ by stipulating

$$\pi_x\big(\{n, m\}\big) = 0 \iff \{n, m\} \subseteq x \vee \{n, m\} \cap x = \emptyset$$

and let $\mathscr{P} = \{\pi_x : x \in \mathscr{S}\}$. Then, since $\mathscr{S}$ is splitting, no infinite set is almost homogeneous for all $\pi \in \mathscr{P}$.

$\mathfrak{par} \leq \mathfrak{b}$: Let $\mathscr{B} \subseteq {}^\omega\omega$ be an unbounded family. Without loss of generality we may assume that each $g \in \mathscr{B}$ is strictly increasing. For each $g \in \mathscr{B}$ define the colouring $\pi_g : [\omega]^2 \to 2$ by stipulating

$$\pi_g\bigl(\{n,m\}\bigr) = 0 \iff g(n) < m \quad \text{where } n < m\,.$$

Assume towards a contradiction that some infinite set $H \in [\omega]^\omega$ is almost homogeneous for all colourings in $\mathscr{P} = \{\pi_g : g \in \mathscr{B}\}$. We shall show that H yields a function which dominates the unbounded family $\mathscr{B}$, which is obviously a contradiction. Consider the function $h \in {}^\omega\omega$ which maps each natural number n to the second member of H above n; more formally, $h(n) := \min\bigl\{m \in H : \exists k \in H(n < k < m)\bigr\}$. For each $n \in \omega$ we have $n < k < h(n)$ with both k and $h(n)$ in H. By almost homogeneity of H, for each $g \in \mathscr{B}$ there is a finite set $K \subseteq \omega$ such that $H \setminus K$ is homogeneous for π_g, *i.e.*, for all $\{n,m\} \in [H \setminus K]^2$ with $n < m$ we have either $g(n) < m$ or $g(n) \geq m$. Since H is infinite, the latter case is impossible. On the other hand, the former case implies that for all $n \in H \setminus K$, $g(n) < h(n)$, hence, h dominates g and consequently h dominates each function of $\mathscr{B}$.

$\mathfrak{par} \geq \min\{\mathfrak{s},\mathfrak{b}\}$: Suppose $\mathscr{P} = \bigl\{\pi_\xi : \xi \in \kappa < \min\{\mathfrak{s},\mathfrak{b}\}\bigr\}$ is a family of 2-colouring of $[\omega]^2$. We shall construct a set $H \in [\omega]^\omega$ which is almost homogeneous for all colourings $\pi \in \mathscr{P}$. For each $\xi \in \kappa$ and all $n \in \omega$ define the function $f_{\xi,n} \in {}^\omega 2$ by stipulating

$$f_{\xi,n}(m) = \begin{cases} \pi_\xi\bigl(\{n,m\}\bigr) & \text{for } m \neq n, \\ 0 & \text{otherwise.} \end{cases}$$

Since $|\{f_{\xi,n} : \xi \in \kappa \wedge n \in \omega\}| = \kappa \cdot \omega = \kappa < \mathfrak{s}$, there is an infinite set $A \subseteq \omega$ on which all functions $f_{\xi,n}$ are almost constant; more formally, for each $\xi \in \kappa$ and each $n \in \omega$ there are $g_\xi(n) \in \omega$ and $j_\xi(n) \in \{0,1\}$ such that for all $m \geq g_\xi(n)$, $f_{\xi,n}(m) = j_\xi(n)$. Moreover, since $\kappa < \mathfrak{s}$ there is an infinite set $B \subseteq A$ on which each function $j_\xi \in {}^\omega 2$ is almost constant, say $j_\xi(n) = i_\xi$ for all $n \in B$ with $n \geq b_\xi$. Further, since $\kappa < \mathfrak{b}$ there is a strictly increasing function $h \in {}^\omega\omega$ which dominates each g_ξ, *i.e.*, for each $\xi \in \kappa$ there is an integer c_ξ such that for all $n \geq c_\xi$, $g_\xi(n) < h(n)$. Let $H = \{x_k : k \in \omega\} \subseteq B$ be such that for all $k \in \omega$, $h(x_k) < x_{k+1}$. Then H is almost homogeneous for each $\pi_\xi \in \mathscr{P}$. Indeed, if $n,m \in H$ are such that $\max\{b_\xi, c_\xi\} \leq n < m$, then $g_\xi(n) < h(n) < m$ and therefore $\pi_\xi\bigl(\{n,m\}\bigr) = f_{\xi,n}(m) = j_\xi(n) = i_\xi$, *i.e.*, $H \setminus \max\{b_\xi, c_\xi\}$ is homogeneous for π_ξ. $\dashv$

The Cardinal $\mathfrak{h}$

A family $\mathscr{H} = \{\mathscr{A}_\xi : \xi \in \kappa\} \subseteq \mathscr{P}\bigl([\omega]^\omega\bigr)$ of *mad* families of cardinality $\mathfrak{c}$ is called **shattering** if for each $x \in [\omega]^\omega$ there is a $\xi \in \kappa$ such that x has infinite intersection with at least two distinct members of $\mathscr{A}_\xi$, *i.e.*, at lest two sets of $\mathscr{A}_\xi$ split x. We leave it as an exercise to the reader to show that there are shattering families of cardinality $\mathfrak{c}$ (for each $x \in [\omega]^\omega$ take two disjoint sets $y, y' \subseteq x$ such that $\omega \setminus (y \cup y')$ is infinite and extend $\{y, y'\}$ to a *mad* family of cardinality $\mathfrak{c}$).

Definition of $\mathfrak{h}$. The **shattering number $\mathfrak{h}$** is the smallest cardinality of a shattering family; more formally

$$\mathfrak{h} = \min\left\{|\mathscr{H}| : \mathscr{H} \text{ is shattering}\right\}.$$

If one tries to visualise a shattering family, one would probably draw a kind of matrix with $\mathfrak{c}$ columns, where the rows correspond to the elements of the family (*i.e.*, to the *mad* families). Having this picture in mind, the size of the shattering family would then be the *height* of the matrix, and this where the letter "h" comes from.

In order to prove that $\mathfrak{h} \leq \mathfrak{par}$ we shall show how to construct a shattering family from any family $\mathscr{P}$ of 2-colourings of $[\omega]^2$ such that no single set is almost homogeneous for all $\pi \in \mathscr{P}$; the following lemma is the key idea in that construction:

Lemma 8.12. *For every colouring $\pi : [\omega]^2 \to 2$ there is a mad family $\mathscr{A}_\pi$ of cardinality $\mathfrak{c}$ such that each $A \in \mathscr{A}_\pi$ is homogeneous for π.*

Proof. Let $\mathscr{A} \subseteq [\omega]^\omega$ be an arbitrary almost disjoint family of cardinality $\mathfrak{c}$ and let π be a 2-colouring of $[\omega]^2$. By Ramsey's Theorem 2.1, for each $A \in \mathscr{A}$ we find an infinite set $A' \subseteq A$ such that A' is homogeneous for π. Let $\mathscr{A}' = \{A' : A \in \mathscr{A}\}$; then $\mathscr{A}'$ is an almost disjoint family of cardinality $\mathfrak{c}$ where each member of $\mathscr{A}'$ is homogeneous for π. Let $\{x_\xi : \xi \in \kappa \leq \mathfrak{c}\}$ be an enumeration of $[\omega]^\omega \setminus \mathscr{A}'$. By transfinite induction define $\mathscr{A}_0 = \mathscr{A}'$ and for each $\xi \in \kappa$ let

$$\mathscr{A}_{\xi+1} = \begin{cases} \mathscr{A}_\xi \cup \{x_\xi\} & \text{if } x_\xi \text{ is homogeneous for } \pi \text{ and} \\ & \quad \text{for each } A \in \mathscr{A}_\xi,\ x_\xi \cap A \text{ is finite,} \\ \mathscr{A}_\xi & \text{otherwise.} \end{cases}$$

By construction, $\mathscr{A}_\pi = \bigcup_{\xi\in\kappa} \mathscr{A}_\xi$ is an almost disjoint family of cardinality $\mathfrak{c}$, all whose members are homogeneous for π. Moreover, $\mathscr{A}_\pi$ is a *mad* family. Indeed, if there would be an $x \in [\omega]^\omega$ such that for all $A \in \mathscr{A}_\pi$, $x \cap A$ is finite, then, by Ramsey's Theorem 2.1, there would be an $x_{\xi_0} \in [x]^\omega$ (for some $\xi_0 \in \kappa$) which is homogeneous for π. In particular, x_{ξ_0} would belong to $\mathscr{A}_{\xi_0+1}$. Hence, $x \cap x_{\xi_0}$ is infinite, where $x_{\xi_0} \in \mathscr{A}$, which is a contradiction to the choice of x. $\dashv$

Theorem 8.13. $\mathfrak{h} \leq \mathfrak{par}$.

Proof. Let $\mathscr{P}$ be a family of 2-colourings of $[\omega]^2$ such that no single set is almost homogeneous for all $\pi \in \mathscr{P}$ and let $\mathscr{H}_{\mathscr{P}} = \{\mathscr{A}_\pi : \pi \in \mathscr{P}\}$, where $\mathscr{A}_\pi$ is like in LEMMA 8.12. We claim that $\mathscr{H}_{\mathscr{P}}$ is shattering. Indeed, let $H \subseteq \omega$ be an arbitrary infinite subset of ω. By the property of $\mathscr{P}$, there is a $\pi \in \mathscr{P}$ such that H is not almost homogeneous for π. Consider $\mathscr{A}_\pi \in \mathscr{H}_{\mathscr{P}}$: Since $\mathscr{A}_\pi$ is *mad*, there is an $A \in \mathscr{A}_\pi$ such that $H \cap A$ is infinite, and since A is homogeneous for π, $H \setminus A$ is infinite too; and again, since $\mathscr{A}_\pi$ is *mad*, there is an $A' \in \mathscr{A}_\pi$ (distinct from A) such that $(H \setminus A) \cap A'$ is infinite. This shows that H has infinite intersection with two distinct members of $\mathscr{A}_\pi$. Hence, $\mathscr{H}_{\mathscr{P}}$ is shattering. $\dashv$

In order to prove that $\mathfrak{p} \leq \mathfrak{h}$ we have to introduce some notions: If $\mathscr{A}$ and $\mathscr{A}'$ are *mad* families (of cardinality $\mathfrak{c}$), then $\mathscr{A}'$ **refines** $\mathscr{A}$, denoted $\mathscr{A}' \succ\!\!\succ \mathscr{A}$, if for each $A' \in \mathscr{A}'$ there is an $A \in \mathscr{A}$ such that $A' \subseteq^* A$ A shattering family $\{\mathscr{A}_\xi : \xi \in \kappa\}$ is called **refining** if $\mathscr{A}_{\xi'} \succ\!\!\succ \mathscr{A}_\xi$ whenever $\xi' > \xi$.

The next result is the key lemma in the proof that every shattering family of size $\mathfrak{h}$ induces a refining shattering family of the same cardinality.

LEMMA 8.14. *For every family $\mathscr{E} = \{\mathscr{A}_\xi : \xi \in \kappa < \mathfrak{h}\}$ of cardinality $\kappa < \mathfrak{h}$ of mad families of cardinality $\mathfrak{c}$ there exists a mad family $\mathscr{A}'$ which refines each $\mathscr{A}_\xi \in \mathscr{E}$. Furthermore, $\mathscr{A}'$ is of cardinality $\mathfrak{c}$.*

Proof. Let $\mathscr{E} = \{\mathscr{A}_\xi : \xi \in \kappa < \mathfrak{h}\}$ be a family of less than $\mathfrak{h}$ *mad* families of cardinality $\mathfrak{c}$. For every $x \in [\omega]^\omega$ we find an $x' \in [x]^\omega$ with the property that for each $\mathscr{A}_\xi \in \mathscr{H}$ there is an $A \in A_\xi$ such that $x' \subseteq^* A$. Indeed, if there is no such x' (for some given $x \in [\omega]^\omega$), then a bijection between x and ω would yield a shattering family of cardinality $\kappa < \mathfrak{h}$, contrary to the definition of $\mathfrak{h}$. Now, if $\mathscr{A}' \subseteq \{x' : x \in [\omega]^\omega\}$ is a *mad* family, then $\mathscr{A}'$ is of cardinality $\mathfrak{c}$ (since $\mathscr{A}_0$ is of cardinality $\mathfrak{c}$) and refines each $\mathscr{A}_\xi \in \mathscr{E}$ (since $\mathscr{A}' \subseteq \{x' : x \in [\omega]^\omega\}$). It remains to show that *mad* families $\mathscr{A}' \subseteq \{x' : x \in [\omega]^\omega\}$ exist. Indeed, if $\mathscr{A} \subseteq \{x' : x \in [\omega]^\omega\}$ is an almost disjoint family which is not maximal, then there exists an $x \in [\omega]^\omega$ such that for all $A \in \mathscr{A}$, $x \cap A$ is finite. Notice that $\mathscr{A} \cup \{x'\}$ is still an almost disjoint family, hence, by Teichmüller's Principle, every almost disjoint family $\mathscr{A} \subseteq \{x' : x \in [\omega]^\omega\}$ can be extended to a *mad* family $\mathscr{A}' \subseteq \{x' : x \in [\omega]^\omega\}$. $\dashv$

PROPOSITION 8.15. *If $\mathscr{H} = \{\mathscr{A}_\xi : \xi \in \mathfrak{h}\}$ is a shattering family of cardinality $\mathfrak{h}$, then there exists a refining shattering family $\mathscr{H}' = \{\mathscr{A}'_\xi : \xi \in \mathfrak{h}\}$ such that for each $\xi \in \mathfrak{h}$ we have $\mathscr{A}'_\xi \succ\!\!\succ \mathscr{A}_\xi$.*

Proof. The proof is by transfinite induction: Let $\mathscr{A}'_0 := \mathscr{A}_0$ and assume we have already defined $\mathscr{A}'_\xi$ for all $\xi \in \eta$ where $\eta \in \mathfrak{h}$. Apply LEMMA 8.14 to the family $\{\mathscr{A}'_\xi : \xi \in \eta\} \cup \{\mathscr{A}_\eta\}$ to obtain $\mathscr{A}'_\eta$ and let $\mathscr{H}' = \{\mathscr{A}'_\xi : \xi \in \mathfrak{h}\}$. $\dashv$

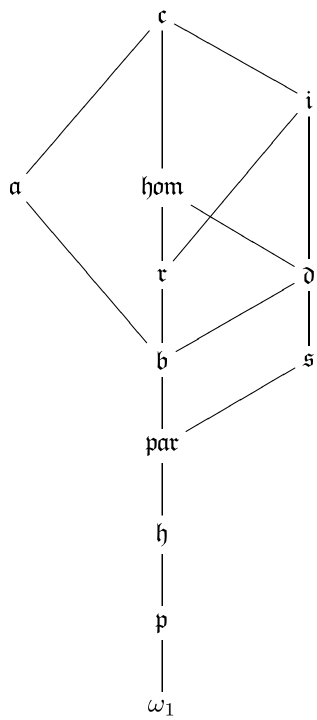
Now, the proof of $\mathfrak{p} \leq \mathfrak{h}$ is straightforward.

THEOREM 8.16. $\mathfrak{p} \leq \mathfrak{h}$.

Proof. By PROPOSITION 8.15 there exists a refining shattering family $\mathscr{H} = \{\mathscr{A}_\xi : \xi \in \mathfrak{h}\}$ of cardinality $\mathfrak{h}$. With $\mathscr{H}$ we shall build a family $\mathscr{F} \subseteq [\omega]^\omega$ of cardinality $\mathfrak{h}$ which has the *sfip* but which does not have a pseudo-intersection: Chose any $x_0 \in \mathscr{A}_0$ and assume we have already chosen $x_\xi \in \mathscr{A}_\xi$ for all $\xi \in \eta$ where $\eta \in \mathfrak{h}$. Since $\mathscr{H}$ is refining we can chose a $x_\eta \in \mathscr{A}_\eta$ such that x_η is a pseudo-intersection of $\{x_\xi : \xi \in \eta\}$. Finally let $\mathscr{F} = \{x_\xi : \xi \in \mathfrak{h}\}$. Then $\mathscr{F}$ is a family of cardinality $\leq \mathfrak{h}$ which has the *sfip*, but since $\mathscr{H}$ is shattering, no infinite set is almost contained in every member of $\mathscr{F}$, *i.e.*, $\mathscr{F}$ does not have a pseudo-intersection. ⊣

Summary

The diagram below shows the relations between the twelve cardinals. A line connecting two cardinals indicates that the cardinal lower on the diagram is less than or equal to the cardinal higher on the diagram (provably in ZFC).



Later we shall see that each of following relations is consistent with ZFC:

- $\mathfrak{a} < \mathfrak{c}$ (PROPOSITION 18.5)
- $\mathfrak{i} < \mathfrak{c}$ (PROPOSITION 18.11)
- $\omega_1 < \mathfrak{p} = \mathfrak{c}$ (PROPOSITION 19.1)

- $\mathfrak{a} < \mathfrak{d} = \mathfrak{r}$ (COROLLARY 21.11)
- $\mathfrak{s} = \mathfrak{b} < \mathfrak{d}$ (PROPOSITION 21.13)
- $\mathfrak{d} < \mathfrak{r}$ (PROPOSITION 22.4)
- $\mathfrak{d} > \mathfrak{r}$ (PROPOSITION 23.7)
- $\mathfrak{p} < \mathfrak{h}$ (PROPOSITION 24.12)

NOTES

Most of the classical cardinal characteristics and their relations presented here can be found for example in van Douwen [42] and Vaughan [43], where one finds also a few historical notes (for $\mathfrak{d}$ see also Kanamori [27, p. 179 f.]). PROPOSITION 8.8 is due to Fichtenholz and Kantorovitch [22], but the proof we gave is Hausdorff's, who generalised in [26] the result to arbitrary infinite cardinals (see also Exercise (A6) on p. 288 of Kunen [29]). THEOREM 8.9 is due to Shelah [33], however, the proof is taken from Blass [5] (see also [4, Theorem 21]), where the claim in the proof is due to Ketonen [28, Proposition 1.3]. THEOREM 8.10 and THEOREM 8.11 are due to Blass and the proofs are taken from Blass [5] (see also [4, Section 6]). The shattering cardinal $\mathfrak{h}$ was introduced and investigated by Balcar, Pelant, and Simon in [2] (*cf.* RELATED RESULT 51).

RELATED RESULTS

50. *The Continuum Hypothesis.* There are numerous statements from areas like Algebra, Combinatorics, or Topology, which are equivalent to CH. For example Erdős and Kakutani showed that CH is equivalent to the statement that $\mathbb{R}$ is the union of countably many sets of rationally independent numbers (*cf.* [20, Theorem 2]). Many more equivalents to CH can be found in Sierpiński [39]. For the historical background of CH we refer the reader to Felgner [21].

51. *On the shattering number* $\mathfrak{h}$. Balcar, Pelant, and Simon showed that $\mathfrak{h} \leq \mathrm{cf}(\mathfrak{c})$ (see [2, Theorem 4.2]), gave a direct prove for $\mathfrak{h} \leq \mathfrak{b}$ (see [2, Theorem 4.5]) and for $\mathfrak{h} \leq \mathfrak{s}$ (follows from [2, Lemma 2.11.(c)]), and showed that $\mathfrak{h}$ is regular (see [2, Lemma 2.11.(b)]. Furthermore, Lemma 2.11.(c) of Balcar, Pelant, and Simon [2] states that there are shattering families of size $\mathfrak{h}$ which have a very strong combinatorial property:

    BASE MATRIX LEMMA. *There exists a shattering family* $\mathscr{H} = \{\mathscr{A}_\xi \subseteq [\omega]^\omega : \xi \in \mathfrak{h}\}$ *which has the property that for each* $X \in [\omega]^\omega$ *there is a* $\xi \in \mathfrak{h}$ *and an* $A \in \mathscr{A}_\xi$ *such that* $A \subseteq^* X$.

    Proof. Let $\mathscr{F} = \{\mathscr{A}_\xi \subseteq [\omega]^\omega : \xi \in \mathfrak{h}\}$ be an arbitrary but fixed refining shattering family of cardinality $\mathfrak{h}$. We first prove the following

    CLAIM. *For every infinite set* $X \in [\omega]^\omega$ *there exists an ordinal* $\bar{\xi} \in \mathfrak{h}$ *such that* $\big|\{C \in \mathscr{A}_{\bar{\xi}} : |C \cap X| = \omega\}\big| = \mathfrak{c}$.

    Proof of Claim. Let $X \in [\omega]^\omega$ be an arbitrary infinite subset of ω. Firstly we show that there exists a strictly increasing sequence $\langle \xi_n : n \in \omega\rangle$ in $\mathfrak{h}$, such that for each $n \in \omega$ and $f \in {}^n 2$ we find a set $C_f \in \mathscr{A}_{\xi_n}$ with the following properties:

- $|C_f \cap X| = \omega$,
- if $f, f' \in {}^n2$ are distinct, then $C_f \neq C_{f'}$, and
- for all $f \in {}^n2$ and $m \in n$, $C_f \subseteq^* C_{f|m}$.

The sequence $\langle \xi_n : n \in \omega \rangle$ is constructed by induction on n: First we choose an arbitrary $\xi_0 \in \mathfrak{h}$. Now, suppose we have already found $\xi_n \in \mathfrak{h}$ for some $n \in \omega$. Since $\mathscr{F}$ is a shattering family, for every $h \in {}^n2$ there exists a $\zeta_h > \xi_n$ such that the infinite set $C_h \cap X$ has infinite intersection with at least two members of $\mathscr{A}_{\zeta_h}$. Let $\xi_{n+1} = \bigcup \{\zeta_h : h \in {}^n2\}$. Then, since $\mathscr{F}$ is refining, we find a family $\{C_f : f \in {}^{n+1}2\} \subseteq \mathscr{A}_{\xi_{n+1}}$ with the desired properties.

Let $\bar{\xi} := \bigcup_{n \in \omega} \xi_n$; then the ordinal $\bar{\xi}$ is smaller than $\mathfrak{h}$: Otherwise, since $\mathscr{F}$ is refining, the family $\{\mathscr{A}_{\xi_n} : n \in \omega\}$ would be a shattering family of cardinality ω, contradicting the fact that $\mathfrak{h} \geq \omega_1$.

By construction, for each $f \in {}^\omega 2$ we find a $C_f \in \mathscr{A}_{\bar{\xi}}$ such that $C_f \cap X$ is infinite (notice that for each $n \in \omega$, $|C_{f|n} \cap X| = \omega$), and since $\mathscr{F}$ is refining we have $C_f \neq C_{f'}$ whenever $f, f' \in {}^\omega 2$ are distinct. Thus, $\left|\{C_f \in \mathscr{A}_{\bar{\xi}} : f \in {}^\omega 2\}\right| = \mathfrak{c}$ and for each $f \in {}^\omega 2$ we have $|C_f \cap X| = \omega$. $\dashv_{\text{Claim}}$

Now we construct the shattering family $\mathscr{H} = \{\mathscr{A}_\xi \subseteq [\omega]^\omega : \xi \in \mathfrak{h}\}$ as follows: For each $\xi \in \mathfrak{h}$, let $\mathscr{X}_\xi$ be the family of all $X \in [\omega]^\omega$ such that

$$\left|\{C \in \mathscr{A}_\xi : |C \cap X| = \omega\}\right| = \mathfrak{c}.$$

If $\mathscr{X}_\xi = \emptyset$, then let $\mathscr{A}_\xi = \mathscr{A}_\xi$. Otherwise, define (*e.g.*, by transfinite induction) an injection $g_\xi : \mathscr{X}_\xi \hookrightarrow \mathscr{A}_\xi$ such that for each $X \in \mathscr{X}_\xi$, $\left|X \cap g_\xi(X)\right| = \omega$. Now, for each $C \in \mathscr{A}_\xi$, let $\mathscr{C}_C \subseteq [C]^\omega$ be an almost disjoint family such that $\bigcup \mathscr{C}_C = C$, and whenever $C = g_\xi(X)$ for some $X \in \mathscr{X}_\xi$ (*i.e.*, $|X \cap C| = \omega$), then there exists an $A \in \mathscr{C}_C$ with $A \subseteq^* X$. Let $\mathscr{A}_\xi := \{A \in \mathscr{C}_C : C \in \mathscr{A}_\xi\}$ and let $\mathscr{H} := \{\mathscr{A}_\xi : \xi \in \mathfrak{h}\}$. Then, by construction, for every $X \in [\omega]^\omega$ we find an ordinal $\xi \in \mathfrak{h}$ and an infinite set $A \in \mathscr{A}_\xi$ such that $A \subseteq^* X$. $\dashv$

52. *The tower number* $\mathfrak{t}$.* A family $\mathscr{T} = \{T_\alpha : \alpha \in \kappa\} \subseteq [\omega]^\omega$ is called a **tower** if $\mathscr{T}$ is well-ordered by ${}^*\supseteq$ (*i.e.*, $T_\beta \subseteq^* T_\alpha \leftrightarrow \alpha < \beta$) and does not have a pseudo-intersection. The **tower number** $\mathfrak{t}$ is the smallest cardinality (or height) of a tower. Obviously we have $\mathfrak{p} \leq \mathfrak{t}$ and the proof of THEOREM 8.16 shows that $\mathfrak{t} \leq \mathfrak{h}$. However, it is open whether $\mathfrak{p} < \mathfrak{t}$ is consistent with ZFC (for partial results see for example van Douwen [42], Blass [5], or Shelah [35]).

53. *A linearly ordered subset of* $[\omega]^\omega$ *of size* $\mathfrak{c}$. Let $\{q_n \in \mathbb{Q} : n \in \omega\}$ be an enumeration of the rational numbers $\mathbb{Q}$ and for every real number $r \in \mathbb{R}$ let $C_r := \{n \in \omega : q_n \leq r\}$. Then, for any real numbers $r_0 < r_1$ we have $C_{r_0} \subsetneq C_{r_1}$ and $|C_{r_1} \setminus C_{r_0}| = \omega$. Thus, with respect to the ordering "$\subsetneq$", $\{C_r : r \in \mathbb{R}\} \subseteq [\omega]^\omega$ is a linearly ordered set of size $\mathfrak{c}$. In general one can show that whenever M is infinite, the partially ordered set $(\mathscr{P}(M), \subsetneq)$ contains a linearly ordered subset of size strictly greater than $|M|$.

54. *The σ-reaping number* $\mathfrak{r}_\sigma$.* A family $\mathscr{R} \subseteq [\omega]^\omega$ is called **σ-reaping** if no countably many sets suffice to split all members of $\mathscr{R}$. The **σ-reaping number** $\mathfrak{r}_\sigma$ is the smallest cardinality of any σ-reaping family (for a definition of $\mathfrak{r}_\sigma$ in terms of bounded sequences see Vojtáš [44]). Obviously we have $\mathfrak{r} \leq \mathfrak{r}_\sigma$, but it is not known whether $\mathfrak{r} = \mathfrak{r}_\sigma$ is provable in ZFC, *i.e.*, it is not known whether $\mathfrak{r} < \mathfrak{r}_\sigma$ is consistent with ZFC (see also Vojtáš [44] and Brendle [8]).

55. *On* $\mathfrak{i}$ *and* $\mathfrak{hom}$*. We have seen that $\max\{\mathfrak{r}, \mathfrak{d}\} \leq \mathfrak{hom}$ (see THEOREM 8.10) and that $\max\{\mathfrak{r}, \mathfrak{d}\} \leq \mathfrak{i}$ (see THEOREM 8.9). Moreover, Blass [4, Section 6] showed that $\mathfrak{hom} = \max\{\mathfrak{r}_\sigma, \mathfrak{d}\}$ (see also Blass [5]). Thus, in every model in which $\mathfrak{r} = \mathfrak{r}_\sigma$ we have $\mathfrak{hom} \leq \mathfrak{i}$. Furthermore, one can show that $\mathfrak{hom} < \mathfrak{i}$ is consistent with ZFC: In Balcar, Hernández-Hernández, and Hrušák [1] it is shown that $\max\{\mathfrak{r}, cof(\mathscr{M})\} \leq \mathfrak{i}$, where $cof(\mathscr{M})$ is the *cofinality* of the ideal of meagre sets. On the other hand, it is possible to construct models in which $\mathfrak{d} = \mathfrak{r}_\sigma = \omega_1$ and $cof(\mathscr{M}) = \omega_2 = \mathfrak{c}$ (see for example Shelah and Zapletal [36] or Brendle and Khomskii [15]). Thus, in such models we have $\omega_1 = \mathfrak{hom} < \mathfrak{i} = \omega_2$. However, it is open whether $\mathfrak{i} < \mathfrak{hom}$ (which would imply $\mathfrak{r} < \mathfrak{r}_\sigma$) is consistent with ZFC.

56. *The ultrafilter number* $\mathfrak{u}$. A family $\mathscr{F} \subseteq [\omega]^\omega$ is a **base for an ultrafilter** $\mathscr{U} \subseteq [\omega]^\omega$ if $\mathscr{U} = \{y \in [\omega]^\omega : \exists x \in \mathscr{F}(x \subseteq y)\}$. The **ultrafilter number** $\mathfrak{u}$ is the smallest cardinality of any ultrafilter base. We leave it as an exercise to the reader to show that $\mathfrak{r} \leq \mathfrak{u}$.

57. *Consistency results.* The following statements are consistent with ZFC:
- $\mathfrak{r} < \mathfrak{u}$ (*cf.* Goldstern and Shelah [23])
- $\mathfrak{u} < \mathfrak{d}$ (*cf.* Blass and Shelah [6] or see Chapter 23 | RELATED RESULT 130)
- $\mathfrak{u} < \mathfrak{a}$ (*cf.* Shelah [34], see also Brendle [13])
- $\mathfrak{h} < \mathfrak{par}$ (*cf.* Shelah [32, Theorem 5.2] or Dow [19, Proposition 2.7])
- $\mathfrak{hom} < \mathfrak{c}$ (see Chapter 23 | RELATED RESULT 138)
- $\mathfrak{d} < \mathfrak{a}$ (*cf.* Shelah [34], see also Brendle [10])
- $\omega_1 = \mathfrak{b} < \mathfrak{a} = \mathfrak{s} = \mathfrak{d} = \omega_2$ (*cf.* Shelah [32, Sections 1 & 2])
- $\kappa = \mathfrak{b} = \mathfrak{a} < \mathfrak{s} = \lambda$ for any regular uncountable cardinals $\kappa < \lambda$ (*cf.* Brendle and Fischer [14])
- $\mathfrak{b} = \kappa < \kappa^+ = \mathfrak{a} = \mathfrak{c}$ for $\kappa > \omega_1$ (*cf.* Brendle [7])
- $\omega_1 = \mathfrak{s} < \mathfrak{b} = \mathfrak{d} = \mathfrak{r} = \mathfrak{a} = \omega_2$ (*cf.* Shelah [32, Section 4])
- $\mathrm{cf}(\mathfrak{a}) = \omega$ (*cf.* Brendle [11])
- $\mathfrak{h} = \omega_2 +$ *there are no towers of height* ω_2 (*cf.* Dordal [17]).

Some more results can be found for example in Blass [5], Brendle [9, 12], van Douwen [42], Dow [19], and Dordal [18].

58. *Combinatorial properties of maximal almost disjoint families.* An uncountable set of reals is a σ-set if every relative Borel subset is a relative G_δ set. Brendle and Piper showed in [16] that CH implies the existence of a *mad* family which is also a σ-set (in that paper, they also discuss related results assuming Martin's Axiom).

59. *Applications to Banach space theory.* Let $\ell_p(\kappa)$ denote the Banach space of bounded functions $f : \kappa \to \mathbb{R}$ with finite ℓ_p-norm, where for $1 \leq p < \infty$,

$$\|f\| = \sqrt[p]{\sum_{\alpha\in\kappa} |f(\alpha)|^p}\,,$$

and for $p = \infty$,

$$\|f\| = \sup\{|f(\alpha)| : \alpha \in \kappa\}\,.$$

As mentioned above, Hausdorff generalised PROPOSITION 8.8 to arbitrary infinite cardinals κ, *i.e.*, if κ is an infinite cardinal then there are independent families on κ of cardinality 2^κ. Now, using independent families on κ of cardinality 2^κ it is quite straightforward to show that $\ell_\infty(\kappa)$ contains an isomorphic

copy of $\ell_1(2^\kappa)$ (the details are left to the reader), and Halbeisen [24] showed that the dual of $\ell_\infty(\kappa)$ contains an isomorphic copy of $\ell_2(2^\kappa)$ (for an analytic proof in the case $\kappa = \omega$ see Rosenthal [31, Proposition 3.4]).
We have seen that there are almost disjoint families on ω of cardinality $\mathfrak{c} = 2^{\aleph_0}$. Unlike for independent families, this result cannot be generalised to arbitrary cardinals κ, *i.e.*, it is consistent with ZFC that for some infinite κ, there no almost disjoint family on κ of cardinality 2^κ (*see* Baumgartner[3, Theorem 5.6 (b)]). However, one can prove that for all infinite cardinals κ there is an almost disjoint family on κ of cardinality $> \kappa$ (*cf.* Tarski [41], Sierpiński [37, 38] or [40, p. 448 f.], or Baumgartner [3, Theorem 2.8]). Using an almost disjoint family of cardinality $> \kappa$ it is not hard to show that every infinite dimensional Banach space of cardinality κ has more than κ pairwise almost disjoint normalised Hamel bases (*cf.* Halbeisen [25]), and Pełczyński and Sudakov [30] showed that $c_0(\kappa)$, which is a subspace of $\ell_\infty(\kappa)$, is not complemented in $\ell_\infty(\kappa)$.

References

1. Bohuslav Balcar, Fernando Hernández-Hernández, and Michael Hrušák, *Combinatorics of dense subsets of the rationals*, ***Fundamenta Mathematicae***, vol. 183 (2004), 59–80.
2. Bohuslav Balcar, Jan Pelant, and Petr Simon, *The space of ultrafilters on N covered by nowhere dense sets*, ***Fundamenta Mathematicae***, vol. 110 (1980), 11–24.
3. James E. Baumgartner, *Almost-disjoint sets, the dense set problem and the partition calculus*, ***Annals of Mathematical Logic***, vol. 10 (1976), 401–439.
4. Andreas Blass, *Simple cardinal characteristics of the continuum*, *in* ***Set Theory of the Reals*** (H. Judah, ed.), [Israel Mathematical Conference Proceedings], Bar-Ilan University, Israel, 1993, pp. 63–90.
5. ______, *Combinatorial Cardinal Characteristics of the Continuum*, *in* ***Handbook of Set Theory,*** *Volume 1* (Matthew Foreman and Akihiro Kanamori, eds.), Springer-Verlag, Berlin, 2010, pp. 395–490.
6. Andreas Blass and Saharon Shelah, *Ultrafilters with small generating sets*, ***Israel Journal of Mathematics***, vol. 65 (1989), 259–271.
7. Jörg Brendle, *Mob families and mad families*, ***Archive for Mathematical Logic***, vol. 37 (1997), 183–197.
8. ______, *Around splitting and reaping*, ***Commentationes Mathematicae Universitatis Carolinae*** (1998), no. 39, 269–279.
9. ______, *Cardinal invariants of the continuum—a survey*, ***Sūrikaisekikenkyūsho Kōkyūroku*** (2001), no. 1202, 7–32.
10. ______, *Mad families and iteration theory*, *in* ***Logic and Algebra*** (Yi Zhang, ed.), Contemporary Mathematics, no. 302, American Mathematical Society, Providence, RI, 2002, pp. 1–31.
11. ______, *The almost-disjointness number may have countable cofinality*, ***Transactions of the American Mathematical Society***, vol. 355 (2003), 2633–2649.
12. ______, *Independence for distributivity numbers*, *in* ***Algebra, Logic, Set Theory: Festschrift für Ulrich Felgner zum 65. Geburtstag*** (B. Löwe, ed.), [Studies in Logic, 4], College Publications, London, 2007, pp. 63–84.

13. ———, *Mad families and ultrafilters*, ***Acta Universitatis Carolinae. Mathematica et Physica***, vol. 48 (2007), 19–35.
14. Jörg Brendle and Vera Fischer, *Mad families, splitting families and large continuum*, ***The Journal of Symbolic Logic***, vol. 76 (2011), 198–208.
15. Jörg Brendle and Yurii Khomskii, *Polarized partitions on the second level of the projective hierarchy*, ***Annals of Pure and Applied Logic*** (to appear).
16. Jörg Brendle and Greg Piper, *MAD families with strong combinatorial properties*, ***Fundamenta Mathematicae***, vol. 193 (2007), 7–21.
17. Peter Lars Dordal, *A model in which the base-matrix tree cannot have cofinal branches*, ***The Journal of Symbolic Logic***, vol. 52 (1987), 651–664.
18. ———, *Towers in $[\omega]^\omega$ and ${}^\omega\omega$*, ***Annals of Pure and Applied Logic***, vol. 45 (1989), 247–276.
19. Alan Dow, *Tree π-bases for $\beta N - N$ in various models*, ***Topology and its Applications***, vol. 33 (1989), 3–19.
20. Paul Erdős and Shizuo Kakutani, *On non-denumerable graphs*, ***Bulletin of the American Mathematical Society***, vol. 49 (1943), 457–461.
21. Ulrich Felgner, *Bericht über die Cantorsche Kontinuums-Hypothese*, in ***Mengenlehre, Wege mathematischer Grundlagenforschung*** (U. Felgner, ed.), Wissenschaftliche Buchgesellschaft, Darmstadt, 1985, pp. 166–205.
22. Grigorii Fichtenholz and Leonid V. Kantorovitch, *Sur les opérations linéaires dans l'espace des fonctions bornees*, ***Studia Mathematica***, vol. 5 (1935), 69–98.
23. Martin Goldstern and Saharon Shelah, *Ramsey ultrafilters and the reaping number*—Con($\mathfrak{r} < \mathfrak{u}$), ***Annals of Pure and Applied Logic***, vol. 49 (1990), 121–142.
24. Lorenz Halbeisen, *A set-theoretic approach to complete minimal systems in Banach spaces of bounded functions*, ***Matematychni Studii***, vol. 20 (2003), 162–166.
25. ———, *Families of almost disjoint Hamel bases*, ***Extracta Mathematicae***, vol. 20 (2005), 199–202.
26. Felix Hausdorff, *Über zwei Sätze von G. Fichtenholz und L. Kantorovitch*, ***Studia Mathematica***, vol. 6 (1936), 18–19.
27. Akihiro Kanamori, *Gödel and set theory*, ***The Bulletin of Symbolic Logic***, vol. 13 (2007), 153–188.
28. Jussi A. Ketonen, *On the existence of P-points in the Stone-Čech compactification of the integers*, ***Fundamenta Mathematicae***, vol. 92 (1976), 91–94.
29. Kenneth Kunen, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.
30. Aleksander Pełczyński and Vladimir N. Sudakov, *Remark on noncomplemented subspaces of the space $m(S)$*, ***Colloquium Mathematicum***, vol. 9 (1962), 85–88.
31. Haskell P. Rosenthal, *On quasi-complemented subspaces of Banach spaces, with an appendix on compactness of operators from $L^p(\mu)$ to $L^r(\mu)$*, ***Journal of Functional Analysis***, vol. 4 (1969), 176–214.
32. Saharon Shelah, *On cardinal invariants of the continuum*, in ***Axiomatic Set Theory*** (James E. Baumgartner, Donald A. Martin, and Saharon Shelah, eds.), Contemporary Mathematics, vol. 31, American Mathematical Society, Providence, RI, 1984, pp. 183–207.

33. ———, *Remarks on some cardinal invariants of the continuum* (Appendix of [43]), *in* ***Open Problems in Topology*** (J. van Mill and G. Reed, eds.), North-Holland, Amsterdam, 1990, pp. 217–218.
34. ———, *Two cardinal invariants of the continuum* ($\mathfrak{d} < \mathfrak{a}$) *and FS linearly ordered iterated forcing*, ***Acta Mathematica***, vol. 192 (2004), 187–223.
35. ———, *A comment on "$\mathfrak{p} < \mathfrak{t}$"*, ***Canadian Mathematical Bulletin. Bulletin Canadien de Mathématiques***, vol. 52 (2009), 303–314.
36. Saharon Shelah and Jindřich Zapletal, *Ramsey theorems for product of finite sets with submeasures*, ***Combinatorica***, vol. 31 (2011), 225–244.
37. Wacław Sierpiński, *Sur une décomposition effective d'ensembles*, ***Fundamenta Mathematicae***, vol. 29 (1937), 1–4.
38. ———, *Sur la décomposition des ensembles en sous-ensembles presque disjoints*, ***Fundamenta Mathematicae***, vol. 14 (1938), 15–17.
39. ———, ***Hypothèse du continu***, 2nd ed., Chelsea Publishing Company, New York, 1956.
40. ———, ***Cardinal and Ordinal Numbers***, Państwowe Wydawnictwo Naukowe, Warszawa, 1958.
41. Alfred Tarski, *Sur la décomposition des ensembles en sous-ensembles presque disjoints*, ***Fundamenta Mathematicae***, vol. 12 (1928), 188–205.
42. Eric K. van Douwen, *The integers and topology*, *in* ***Handbook of Set-Theoretic Topology*** (K. Kunen and J.E. Vaughan, eds.), North-Holland, Amsterdam, 1990, pp. 111–167.
43. Jerry E. Vaughan, *Small uncountable cardinals and topology*, *in* ***Open Problems in Topology*** (J. van Mill and G. Reed, eds.), North-Holland, Amsterdam, 1990, pp. 195–218.
44. Peter Vojtáš, *Cardinalities of noncentered systems of subsets of* ω, ***Discrete Mathematics***, vol. 108 (1992), 125–129.

9

The Shattering Number revisited

As variety brings pleasure and delight, so excessive repetition generates boredom and annoyance. Besides, the composer would be thought by connoisseurs of the art to have a meagre store of ideas. But it is not only permitted but admirable to duplicate a passage or melody as many times as one wishes if the counterpoint is always different and varied. For such repetitions strike us as being somehow ingenious, and we should try to write them wherever they seem suitable.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

In this chapter we shall have a closer look at the shattering number $\mathfrak{h}$. In the preceding chapter, $\mathfrak{h}$ was introduced as the minimum height of a shattering matrix. However, like other cardinal characteristics, $\mathfrak{h}$ has different facets. In this chapter we shall see that $\mathfrak{h}$ is closely related to the *Ramsey property*, a combinatorial property of subsets of ω (discussed at the end of Chapter 2) which can be regarded as a generalisation of RAMSEY'S THEOREM.

The Ramsey Property

By RAMSEY'S THEOREM 2.1, for every 2-colouring of $[\omega]^2$ there is a homogeneous set; on the other hand we have seen that there are 2-colourings of $[\omega]^\omega$ without a homogeneous set (see the example given in Chapter 2). Obviously, every colouring $\pi : [\omega]^\omega \to \{0,1\}$ induces a set $C_\pi \subseteq [\omega]^\omega$ by stipulating $C_\pi = \big\{x \in [\omega]^\omega : \pi(x) = 1\big\}$.

By identifying 2-colourings of $[\omega]^\omega$ with subsets of $[\omega]^\omega$, the existence of a 2-colouring of $[\omega]^\omega$ without a homogeneous set is equivalent to the existence of a set $C \subseteq [\omega]^\omega$ such that for all $x \in [\omega]^\omega$ there are $y_0, y_1 \in [x]^\omega$ such that $y_0 \notin A$ and $y_1 \in A$.

Now, a set $C \subseteq [\omega]^\omega$ has the **Ramsey property**, if there exists a set $x \in [\omega]^\omega$ such that either $[x]^\omega \subseteq C$ or $[x]^\omega \cap C = \emptyset$. Notice that the finite as well as the co-finite subsets of $[\omega]^\omega$ have the Ramsey property, but notice also that not all subsets of $[\omega]^\omega$ have the Ramsey property (*cf.* Chapter 5 | RELATED RESULT 38).

Below, we investigate a property of subsets of $[\omega]^\omega$ which is slightly stronger than the Ramsey property, but first we have to introduce the following notation.

For a finite set $s \in \text{fin}(\omega)$ and an infinite set $x \in [\omega]^\omega$ such that $\max(s) < \min(x)$ (*i.e.*, $\bigcup s < \bigcap x$), let

$$[s, x]^\omega = \left\{ z \in [\omega]^\omega : s \subseteq z \subseteq s \cup x \right\}.$$

Now, a set $C \subseteq [\omega]^\omega$ is called **completely Ramsey** if for every set $[s, x]^\omega$ there is a $y \in [x]^\omega$ such that either $[s, y]^\omega \subseteq C$ or $[s, y]^\omega \cap C = \emptyset$. If we are always in the latter case (*i.e.*, for each $[s, x]^\omega$ there is a $y \in [x]^\omega$ such that $[s, y]^\omega \cap C = \emptyset$), then C is called **completely Ramsey-null**. In particular, for $s = \emptyset$ and $x = \omega$ we conclude that any completely Ramsey set has the Ramsey property. On the other hand, not every set which has the Ramsey property is completely Ramsey (we leave it as an exercise to the reader to find a counterexample).

The proof of the following result uses a so-called *fusion argument*, a technique which we will meet again in Part III (LEMMA 9.1 itself is used in the proof of THEOREM 9.2).

LEMMA 9.1. *If $C \subseteq [\omega]^\omega$ is completely Ramsey-null, then for each $x \in [\omega]^\omega$ there is a $y \in [x]^\omega$ such that C contains no infinite set $z \subseteq^* y$.*

Proof. Let C be completely Ramsey-null and $x \in [\omega]^\omega$ be arbitrary. By definition of completely Ramsey-null there is a $y_0 \in [x]^\omega$ such that $[\emptyset, y_0]^\omega \cap C = \emptyset$ and let $a_0 = \min(y_0)$. Assume we have already constructed a sequence $x \supseteq y_0 \supseteq \ldots \supseteq y_n$ of infinite subsets of ω as well as a sequence $a_0 < \ldots < a_n$ of natural numbers such that for all $s \in \mathscr{P}(a_{n-1} + 1)$,

$$[s, y_k]^\omega \cap C = \emptyset.$$

For $h = 2^{a_n+1}$ let $\{s_i : i \in h\}$ be an enumeration of $\mathscr{P}(a_n + 1)$ where $s_0 = \emptyset$. Further let $z_0 = y_n \setminus (a_n + 1)$ and for each $i \in h$ choose an infinite set $z_{i+1} \subseteq z_i$ such that $[s_{i+1}, z_{i+1}]^\omega \cap C = \emptyset$ (notice that we can do this because C is completely Ramsey-null). Finally let $y_{n+1} = z_{h-1}$; then for all $s \in \mathscr{P}(a_n + 1)$ we have

$$[s, y_{n+1}]^\omega \cap C = \emptyset.$$

Let now $a_{n+1} = \min(y_{n+1})$ and start the process again with the sequences $x \supseteq y_0 \supseteq \ldots \supseteq y_{n+1}$ and $a_0 < \ldots < a_{n+1}$. At the end we get an infinite sequence $a_0 < a_1 < \ldots < a_n < \ldots$ and by construction the set $y = \{a_i : i \in \omega\}$ has the property that for each $s \in \text{fin}(\omega)$ with $\max(s) \in y$,

$$\big[s, y \setminus \big(\max(s)+1\big)\big]^\omega \cap C = \emptyset\,,$$

which implies that for each infinite set $z \subseteq^* y$ we have $[\emptyset, z]^\omega \cap C = \emptyset$, *i.e.*, C contains no infinite set $z \subseteq^* y$. ⊣

The Ideal of Ramsey-Null Sets

Below, we consider the set of completely Ramsey-null sets. So, let

$$\mathcal{R}_0 = \big\{C \subseteq [\omega]^\omega : C \text{ is completely Ramsey-null}\big\}$$

be the collection of all subsets of $[\omega]^\omega$ which are completely Ramsey-null. Since $\mathcal{R}_0$ is closed under subsets (*i.e.*, $C \in \mathcal{R}_0$ and $C' \subseteq C$ implies $C' \in \mathcal{R}_0$) and finite unions (*i.e.*, $C_0, \ldots, C_n \in \mathcal{R}_0$ implies $C_0 \cup \ldots \cup C_n \in \mathcal{R}_0$), $\mathcal{R}_0$ is an ideal on $\mathscr{P}\big([\omega]^\omega\big)$.

Obviously, $[\omega]^\omega \notin \mathcal{R}_0$ but for every $x \in [\omega]^\omega$ we have $\{x\} \in \mathcal{R}_0$. Thus, the set $[\omega]^\omega$ can be covered by $\mathfrak{c}$ completely Ramsey-null sets which implies that the union of $\mathfrak{c}$ sets from $\mathcal{R}_0$ can be a set which does not belong to $\mathcal{R}_0$. These observations lead to the following two cardinal numbers.

Definition. The **additivity** of $\mathcal{R}_0$, denoted $\boldsymbol{add(\mathcal{R}_0)}$, is the smallest number of sets in $\mathcal{R}_0$ with union not in $\mathcal{R}_0$; more formally

$$add(\mathcal{R}_0) = \min\big\{|\mathscr{C}| : \mathscr{C} \subseteq \mathcal{R}_0 \wedge \textstyle\bigcup\mathscr{C} \notin \mathcal{R}_0\big\}\,.$$

Definition. The **covering number** of $\mathcal{R}_0$, denoted $\boldsymbol{cov(\mathcal{R}_0)}$, is the smallest number of sets in $\mathcal{R}_0$ with union $[\omega]^\omega$; more formally

$$cov(\mathcal{R}_0) = \min\big\{|\mathscr{C}| : \mathscr{C} \subseteq \mathcal{R}_0 \wedge \textstyle\bigcup\mathscr{C} = [\omega]^\omega\big\}\,.$$

We leave it as an exercise to the reader to show (using a fusion argument) that any countable union of completely Ramsey-null sets is completely Ramsey-null. Hence, $\omega_1 \leq add(\mathcal{R}_0)$, and consequently we get $\omega_1 \leq add(\mathcal{R}_0) \leq cov(\mathcal{R}_0) \leq \mathfrak{c}$. Moreover, we even have the following result.

Theorem 9.2. $add(\mathcal{R}_0) = cov(\mathcal{R}_0) = \mathfrak{h}$.

Proof. Because $add(\mathcal{R}_0) \leq cov(\mathcal{R}_0)$ it is enough to show that $cov(\mathcal{R}_0) \leq \mathfrak{h}$ and that $\mathfrak{h} \leq add(\mathcal{R}_0)$.

$cov(\mathcal{R}_0) \leq \mathfrak{h}$: Let $\{\mathscr{A}_\xi : \xi \in \mathfrak{h}\}$ be a shattering family of cardinality $\mathfrak{h}$. For each $\xi \in \mathfrak{h}$ let $D_\xi = \big\{y \in [\omega]^\omega : \exists x \in \mathscr{A}_\xi (y \subseteq^* x)\big\}$ and let $C_\xi = [\omega]^\omega \setminus D_\xi$. Firstly notice that for each $\xi \in \mathfrak{h}$, $C_\xi \in \mathcal{R}_0$. Indeed, take any $[s, y]^\omega$, then, since $\mathscr{A}_\xi$ is *mad*, there is an $x \in \mathscr{A}_\xi$ such that $y \cap x$ is infinite; thus, $[s, y \cap x]^\omega \subseteq D_\xi$, or equivalently $[s, y \cap x]^\omega \cap C_\xi = \emptyset$. Secondly notice that $\bigcup_{\xi \in \mathfrak{h}} C_\xi = [\omega]^\omega$. Indeed, take any $y \in [\omega]^\omega$, then, since $\{\mathscr{A}_\xi : \xi \in \mathfrak{h}\}$ is shattering, there is a $\xi \in \mathfrak{h}$ and two distinct elements $x, x' \in \mathscr{A}_\xi$ such that $y \cap x$ as well as $y \cap x'$ is infinite; hence, $y \notin D_\xi$, or equivalently $y \in C_\xi$.

$\mathfrak{h} \leq add(\mathcal{R}_0)$: Let $\{C_\xi \subseteq [\omega]^\omega : \xi \in \kappa < \mathfrak{h}\} \subseteq \mathcal{R}_0$ be a family of completely Ramsey-null sets of cardinality $\kappa < \mathfrak{h}$. We will show that $\bigcup_{\xi \in \kappa} C_\xi \in \mathcal{R}_0$. For each $\xi \in \kappa$ let

$$D_\xi = \left\{ y \in [\omega]^\omega : \forall z \in [\omega]^\omega (z \subseteq^* y \to [\emptyset, z]^\omega \cap C = \emptyset) \right\}.$$

Now we choose for each $\xi \in \kappa$ an almost disjoint family $\mathscr{A}_\xi \subseteq D_\xi$ of cardinality $\mathfrak{c}$ which is maximal with respect to inclusion. Notice that by LEMMA 9.1, for each $x \in [\omega]^\omega$ there is a $y \in \mathscr{A}_\xi$ such that $x \cap y$ is infinite, *i.e.*, $\mathscr{A}_\xi \subseteq D_\xi$ is a *mad* family (on $[\omega]^\omega$) of cardinality $\mathfrak{c}$. Indeed, if there would be an $x \in [\omega]^\omega \mathscr{A}_\xi$ which has finite intersection with each member of $\mathscr{A}_\xi$, then, by LEMMA 9.1, there is a $y \in [x]^\omega$ such that $y \in D_\xi \setminus \mathscr{A}_\xi$ which would imply that $\mathscr{A}_\xi$ is not maximal. Because $\kappa < \mathfrak{h}$ we can apply LEMMA 8.14 and get a *mad* family $\mathscr{A}'$ which refines each $\mathscr{A}_\xi$. Take any set $[s, x]^\omega$. Since $\mathscr{A}'$ is *mad*, there is a $y' \in \mathscr{A}'$ such that $x \cap y'$ is infinite; let $z = x \cap y'$. Because $\mathscr{A}'$ refines all $\mathscr{A}_\xi$'s, for each $\xi \in \kappa$ there is a $y \in \mathscr{A}_\xi$ such that $z \subseteq^* y$, and since $\mathscr{A}_\xi \subseteq D_\xi$, by definition of D_ξ we get $[\emptyset, s \cup z]^\omega \cap C_\xi = \emptyset$, in particular, $[s, z]^\omega \cap C_\xi = \emptyset$. Thus, for every set $[s, x]^\omega$ there exists a $z \in [x]^\omega$ such that for all $\xi \in \kappa$, $[s, z]^\omega \cap C_\xi = \emptyset$, *i.e.*, $[s, z]^\omega \cap \bigcup_{\xi \in \kappa} C_\xi = \emptyset$, hence $\bigcup_{\xi \in \kappa} C_\xi \in \mathcal{R}_0$. ⊣

The Ellentuck Topology

Below, we give a topological characterisation of completely Ramsey sets, but before we have to introduce the basic notions of *General Topology*:

A **topological space** is a pair $(X, \mathscr{O})$ consisting of a set X and a family $\mathscr{O}$ of subsets of X satisfying the following conditions.

(O1) $\emptyset \in \mathscr{O}$ and $X \in \mathscr{O}$.

(O2) If $O_1 \in \mathscr{O}$ and $O_2 \in \mathscr{O}$, then $O_1 \cap O_2 \in \mathscr{O}$.

(O3) If $\mathscr{F} \subseteq \mathscr{O}$, then $\bigcup \mathscr{F} \in \mathscr{O}$.

The set X is called a **space**, the elements of X are called **points** of the space, and the subsets of X belonging to $\mathscr{O}$ are called **open** and the complements of open sets are called **closed**. The family $\mathscr{O}$ of open subsets of X is also called a **topology** on X.

Let us consider for example the real line $\mathbb{R}$. For $r_1, r_2 \in \mathbb{R}$ define $(r_1, r_2) := \{r \in \mathbb{R} : r_1 < r < r_2\}$. Now, a set $O \subseteq \mathbb{R}$ is called open if for every $r \in O$ there exists a real $\varepsilon > 0$ such that $(r - \varepsilon, r + \varepsilon) \subseteq O$ (*i.e.*, every $r \in O$ is contained in an open interval contained in O). We leave it as an exercise to the reader to show that the family of open sets satisfies conditions (O1)–(O3).

From (O2) is follows that the intersection of any *finite* family of open sets is an open set, and from (O3) it follows that the union of *any* family of open sets is open. Notice that arbitrary intersections of closed sets as well as finite unions of closed sets are closed sets. For an arbitrary set $A \subseteq X$ let

$$A^\circ = \bigcup \{O \in \mathscr{O} : O \subseteq A\}$$

be the **interior** of A; and let

$$\bar{A} = \bigcap \{C : C \text{ is closed and } A \subseteq C\}$$

be the **closure** of A. Notice that A° is the largest open set contained in A and that $\bar{A}$ is the smallest closed set containing A.

A family $\mathscr{B} \subseteq \mathscr{O}$ is called a **base** for a topological space $(X, \mathscr{O})$ if every non-empty open subset of X can be represented as the union of a subfamily of $\mathscr{B}$. The sets in a basis $\mathscr{B}$ are also called **basic open** sets. If a family $\mathscr{B}$ of subsets of X is such that $X \in \mathscr{B}$ and every non-empty finite intersection of sets in $\mathscr{B}$ belongs to $\mathscr{B}$, then $(X, \mathscr{O})$, where

$$\mathscr{O} = \left\{ \bigcup \mathscr{F} : \mathscr{F} \subseteq \mathscr{B} \right\},$$

is a topological space with base $\mathscr{B}$ (notice that $\bigcup \emptyset = \emptyset$). In this case we say that the topology on X is generated by the basic open sets $O \in \mathscr{B}$.

For example the topology on $\mathbb{R}$ introduced above is generated by the countably many basic open intervals (q_1, q_2), where $q_1, q_2 \in \mathbb{Q}$.

Let $(X, \mathscr{O})$ be a topological space and let $A \subseteq X$ be a subset of X.

- A is called **dense** if for every open set $O \in \mathscr{O}$, $A \cap O \neq \emptyset$.
- A is called **nowhere dense** if $X \setminus A$ contains an open dense set.
- A is called **meagre** if A is the union of countably many nowhere dense sets.
- A has the **Baire property** if there is an open set $O \in \mathscr{O}$ such that $O \triangle A$ is meagre, where $O \triangle A = (O \setminus A) \cup (A \setminus O)$ (*i.e.*, $x \notin O \triangle A$ *iff* either $x \in A \cap O$ or $x \notin A \cup O$).

Obviously, meagre sets and open sets have the Baire property and countable unions of meagre sets are meagre. Moreover, the following result shows that the Baire property is closed under complementation and countable unions and intersections.

FACT 9.3. *(a) Every closed set has the Baire property.*

(b) The complement of a set with the Baire property has the Baire property.

(c) Unions and intersections of countably many sets with the Baire property have the Baire property.

Proof. (a) Let $A \subseteq X$ be a closed subset of X. We shall show that $A \setminus A^\circ$ is nowhere dense. Firstly, $A \setminus A^\circ = A \cap (X \setminus A^\circ)$, thus, $A \setminus A^\circ$ is closed and $X \setminus (A \setminus A^\circ)$ is open. Secondly, no open set $O \in \mathscr{O}$ is contained in $A \setminus A^\circ$, and therefore $O \cap \big(X \setminus (A \setminus A^\circ)\big)$ is a non-empty open set. Thus, $X \setminus (A \setminus A^\circ)$ is open dense, or equivalently, $A \setminus A^\circ$ is nowhere dense. In particular, $A^\circ \triangle A$ is meagre which shows that A has the Baire property.

(b) Assume that $A \subseteq X$ has the Baire property and let $O \in \mathscr{O}$ be such that $O \triangle A$ is meagre. Let $\bar{O} := X \setminus (X \setminus O)^\circ$ be the closure of O. By (a), $\bar{O} \setminus O$ is nowhere dense. Thus, $A \triangle \bar{O}$ is meagre and therefore $(X \setminus A) \triangle (X \setminus \bar{O})$ is also meagre, which shows that $X \setminus A$ has the Baire property.

(c) By (b) it is enough to prove (c) for unions. So, let $\big\{A_n \subseteq X : n \in \omega\big\}$ be a family of sets which have the Baire property. For each $n \in \omega$ let $O_n \in \mathscr{O}$ be an open set such that $O_n \triangle A_n$ is meagre. Then

$$M = \bigcup_{n\in\omega} O_n \triangle \bigcup_{n\in\omega} A_n \subseteq \bigcup_{n\in\omega} (O_n \triangle A_n)$$

is a subset of a countable union of meagre sets. Hence, M is meagre which shows that $\bigcup_{n\in\omega} A_n$ has the Baire property. $\dashv$

Consider now the set $[\omega]^\omega$. The aim is to define a topology on $[\omega]^\omega$ such that a set $A \subseteq [\omega]^\omega$ has the Baire property (with respect to that topology) if and only if A is completely Ramsey. For this let

$$\mathscr{B} = \big\{[s,x]^\omega \subseteq [\omega]^\omega : s \in \operatorname{fin}(\omega) \wedge x \in [\omega]^\omega \wedge \max(s) < \min(x)\big\}\,,$$

where we defined $[s,x]^\omega := \big\{z \in [\omega]^\omega : s \subseteq z \subseteq s \cup x\big\}$. Obviously, $[\omega]^\omega = [\emptyset,\omega]^\omega \in \mathscr{B}$ and we leave it as an exercise to the reader to show that every non-empty finite intersection of sets in $\mathscr{B}$ belongs to $\mathscr{B}$ — notice that $[s,x]^\omega \cap [t,y]^\omega$ is either empty or it is $[s \cup t, x \cap y]^\omega$. Thus, $\mathscr{O} = \big\{\bigcup \mathscr{F} : \mathscr{F} \subseteq \mathscr{B}\big\}$ is a topology on $[\omega]^\omega$, called the **Ellentuck topology**.

In Chapter 21 we shall introduce a topology on ${}^\omega\omega$ which corresponds to the topology on $[\omega]^\omega$ generated by the basic open sets $[s, \omega \setminus \max(s)+1]^\omega$.

Notice that with respect to the Ellentuck topology, each singleton set $\{x\} \subseteq [\omega]^\omega$ is nowhere dense and all countable sets are meagre. Furthermore, by definition, subsets of meagre sets as well as countable unions of meagre sets are meagre. Thus, the collection of all meagre subsets of $[\omega]^\omega$ is an ideal on $\mathscr{P}\big([\omega]^\omega\big)$. The following theorem shows that the ideal of meagre sets coincide with the ideal of completely Ramsey-null sets, and that a set is completely Ramsey *iff* it has the Baire property; for the latter result we have to prove first the following lemma, whose proof uses twice a fusion argument.

LEMMA 9.4. *Every open set is completely Ramsey.*

Proof. Firstly we introduce some terminology: Let $\mathcal{O} \subseteq [\omega]^\omega$ be an arbitrary but fixed open set. A basic open set $[s,x]^\omega$ is called **good** (with respect to $\mathcal{O}$), if there is a set $y \in [x]^\omega$ such that $[s,y]^\omega \subseteq \mathcal{O}$; otherwise it is called **bad**. Further, $[s,x]^\omega$ is called **ugly** if $[s \cup \{a\}, x \setminus a^+]^\omega$ is bad for all $a \in x$, where $a^+ := a+1$. Notice that if $[s,x]^\omega$ is ugly, then $[s,x]^\omega$ is bad, too.

Finally, $[s,x]^\omega$ is called **completely ugly** if $[s\cup\{a_0,\dots,a_n\}, x\setminus a_n^+]^\omega$ is bad for all $\{a_0,\dots,a_n\}\subseteq x$ with $a_0<\ldots<a_n$. If $[s,x]^\omega$ is completely ugly, then $[s,x]^\omega\cap\mathcal{O}=\emptyset$ (notice that $[s,x]^\omega\cap\mathcal{O}$ is open, and therefore is either empty or contains a basic open set $[t,y]^\omega\subseteq[s,x]^\omega$).

Now, in order to show that the open set $\mathcal{O}$ is completely Ramsey it is enough to prove that every basic open set $[s,x]^\omega$ is either good or there exists a $z\in[x]^\omega$ such that $[s,z]^\omega$ is completely ugly. This is done in two steps: Firstly we show that if $[s,x]^\omega$ is bad, then there exists a $y\in[x]^\omega$ such that $[s,y]^\omega$ is ugly, and secondly we show that if $[s,y]^\omega$ is ugly, then there exists a $z\in[y]^\omega$ such that $[s,z]^\omega$ is completely ugly.

CLAIM 1. *If the basic open set $[s,x]^\omega$ is bad, then there exists a set $y\in[x]^\omega$ such that $[s,y]^\omega$ is ugly.*

Proof of Claim 1. Let $x_0:=x$ and $a_0:=\min(x_0)$, and for $i\in\omega$ let $x_{i+1}\subseteq(x_i\setminus a_i^+)$ such that $[s\cup\{a_i\},x_{i+1}]^\omega\subseteq\mathcal{O}$ if possible, and $x_{i+1}=x_i\setminus a_i^+$ otherwise. Further, let $a_{i+1}:=\min(x_{i+1})$. Strictly speaking we assume that $[\omega]^\omega$ is well-ordered and that x_{i+1} is the first element of $[\omega]^\omega$ with the required properties. Now, let $y=\big\{a_i : [s\cup\{a_i\},x_{i+1}]^\omega\nsubseteq\mathcal{O}\big\}$. Because $[s,x]^\omega$ is bad, $y\in[\omega]^\omega$, which implies that $[s,y]^\omega$ is ugly. $\dashv_{\text{Claim 1}}$

CLAIM 2. *If the basic open set $[s,y]^\omega$ is ugly, then there exists a set $z\in[y]^\omega$ such that $[s,z]^\omega$ is completely ugly.*

Proof of Claim 2. This follows by an iterative application of CLAIM 1. Let $y_0:=y$ and let $a_0:=\min(y_0)$. For every $i\in\omega$ we can choose a set $y_{i+1}\subseteq(y_i\setminus a_i^+)$, where $a_i:=\min(y_i)$, such that for each $t\subseteq\{a_0,\dots,a_i\}$ we have either $[s\cup t,y_{i+1}]^\omega$ is ugly or $[s\cup t,y_{i+1}]^\omega\subseteq\mathcal{O}$. Let $z:=\{a_i:i\in\omega\}$ and assume towards a contradiction that there exists a finite set $t\subseteq z$ such that $[s\cup t,z\setminus\max(t)^+]^\omega$ is good. Notice that since $[s,y]^\omega$ was assumed to be ugly, $t\neq\emptyset$. Now, let t_0 be a smallest finite subset of z such that $[s\cup t_0,z\setminus\max(t_0)^+]^\omega$ is good and let $t_0^-=t_0\setminus\{\max(t_0)\}$. By definition of t_0, $[s\cup t_0^-,z\setminus\max(t_0)]^\omega$ cannot be good (*i.e.*, it is bad), and therefore, by construction of z, it must be ugly. On the other hand, if $[s\cup t_0^-,z\setminus\max(t_0)]^\omega$ is ugly, then $[s\cup t_0,z\setminus\max(t_0)^+]^\omega$ is bad, which is a contradiction to our assumption that $[s\cup t_0,z\setminus\max(t_0)^+]^\omega$ is good. Thus, for all finite subsets $t\subseteq z$, $[s\cup t,z\setminus\max(t)^+]^\omega$ is ugly, and therefore $[s,z]^\omega$ is completely ugly. $\dashv_{\text{Claim 2}}$

Let $[s,x]^\omega$ be an arbitrary basic open set. If $[s,x]^\omega$ is good, then there exists a $y\in[x]^\omega$ such that $[s,y]^\omega\subseteq\mathcal{O}$. Otherwise, $[s,x]^\omega$ is bad and we find a $z\in[x]^\omega$ such that $[s,z]^\omega$ is completely ugly, *i.e.*, $[s,z]^\omega\cap\mathcal{O}=\emptyset$. Hence, the arbitrary open set $\mathcal{O}$ is completely Ramsey. $\dashv$

We shall use the very same fusion arguments again in Chapter 24 in order to prove that Mathias forcing has pure decision (see proof of THEOREM 24.3).

THEOREM 9.5 (ELLENTUCK). *For every $A\subseteq[\omega]^\omega$ we have:*

(a) A is nowhere dense if and only if A is completely Ramsey-null.

(b) A is meagre if and only if A is nowhere dense.

(c) A has the Baire property if and only if A is completely Ramsey.

Proof. (a) A set $A \subseteq [\omega]^\omega$ is nowhere dense *iff* for each basic open set $[s,x]^\omega$ there exists a basic open set $[t,y]^\omega \subseteq [s,x]^\omega$ such that $[t,y]^\omega \cap A = \emptyset$. Hence, we obviously have that every completely Ramsey-null set is nowhere dense. For the other direction assume that $A \subseteq [\omega]^\omega$ is not completely Ramsey-null, *i.e.*, there is a basic open set $[s,x]^\omega$ such that for all basic open sets $[s,y]^\omega \subseteq [s,x]^\omega$ we have $[s,y]^\omega \cap A \neq \emptyset$. By a fusion argument we can construct a set $z_0 \in [x]^\omega$ such that for all $[t,y]^\omega \subseteq [s,z_0]^\omega$ we have $[t,y]^\omega \cap A \neq \emptyset$, *i.e.*, A is not nowhere dense.

(b) On the one hand, nowhere dense sets are meagre. On the other hand, by THEOREM 9.2 we have $add(\mathcal{R}_0) = \mathfrak{h}$ and since $\mathfrak{h}$ is uncountable we get that countable unions of completely Ramsey-null sets (*i.e.*, of nowhere dense sets) are completely Ramsey-null. Thus, meagre sets are completely Ramsey-null and therefore nowhere dense.

(c) On the one hand, if $A \subseteq [\omega]^\omega$ is completely Ramsey, then $\mathcal{O} = \bigcup \big\{[s,y]^\omega : [s,y]^\omega \subseteq A\big\}$ is an open subset of A and for each basic open set $[s,x]^\omega$ there is a $y \in [x]^\omega$ such that either $[s,y]^\omega \subseteq A$ (*i.e.*, $[s,y]^\omega \subseteq (A \cap \mathcal{O})$ and in particular $[s,y]^\omega \cap (\mathcal{O} \triangle A) = \emptyset$), or $[s,y]^\omega \cap A = \emptyset$ (*i.e.*, $[s,y]^\omega \cap (A \cup \mathcal{O}) = \emptyset$ and in particular $[s,y]^\omega \cap (\mathcal{O} \triangle A) = \emptyset$). In both cases we have $[s,y]^\omega \cap (\mathcal{O} \triangle A) = \emptyset$ which implies that $\mathcal{O} \triangle A$ is meagre and shows that A has the Baire property.

On the other hand, if $A \subseteq [\omega]^\omega$ has the Baire property then there is an open set $\mathcal{O} \subseteq [\omega]^\omega$ such that $\mathcal{O} \triangle A$ is meagre, thus by (b), $\mathcal{O} \triangle A$ is completely Ramsey-null. Now, $\mathcal{O} \triangle A \in \mathcal{R}_0$ *iff* for each basic open set $[s,y]^\omega$ there is a $z \in [y]^\omega$ such that $[s,z]^\omega \cap (\mathcal{O} \triangle A) = \emptyset$. Because $\mathcal{O}$ is completely Ramsey (by LEMMA 9.4), for every basic open set $[s,x]^\omega$ there is a set $y \in [x]^\omega$ such that either $[s,y]^\omega \subseteq \mathcal{O}$ or $[s,y]^\omega \cap \mathcal{O} = \emptyset$, and in both cases there is a $z \in [y]^\omega$ such that $[s,z]^\omega \cap (\mathcal{O} \triangle A) = \emptyset$. Thus, we have either $[s,z]^\omega \subseteq A$ or $[s,z]^\omega \cap A = \emptyset$, which shows that A is completely Ramsey. ⊣

As a consequence we get the following

COROLLARY 9.6. *The union of less than* $\mathfrak{h}$ *completely Ramsey sets is completely Ramsey.*

Proof. Let $\kappa < \mathfrak{h}$ and let $\big\{C_\xi \subseteq [\omega]^\omega : \xi \in \kappa\big\}$ be a family of completely Ramsey sets. For each $\xi \in \kappa$ let $O_\xi \subseteq [\omega]^\omega$ be an open set such that $O_\xi \triangle C_\xi$ is meagre. Then

$$D = \bigcup_{\xi\in\kappa} O_\xi \triangle \bigcup_{\xi\in\kappa} C_\xi \subseteq \bigcup_{\xi\in\kappa} (O_\xi \triangle C_\xi)$$

is a subset of a union of κ meagre sets, and since $\kappa < \mathfrak{h}$, D is meagre and therefore $\bigcup_{\xi\in\kappa} C_\xi$ is completely Ramsey. ⊣

A generalised Suslin Operation

First we introduce an operation on certain families of sets and then we show that the collection of completely Ramsey sets is closed under that operation.

Recall that for arbitrary cardinals κ, $\mathrm{seq}(\kappa)$ denotes the set of all finite sequences which can be formed with elements of κ. As usual we identify the set $\mathrm{seq}(\kappa)$ with the set $\bigcup_{n\in\omega} {}^n\kappa$. Let $\{Q_s : s \in \mathrm{seq}(\kappa)\}$ be a family of sets indexed by elements of $\mathrm{seq}(\kappa)$ and define

$$\mathcal{A}_\kappa\{Q_s : s \in \mathrm{seq}(\kappa)\} = \bigcup_{f\in{}^\omega\kappa} \bigcap_{n\in\omega} Q_{f|_n} .$$

The operation $\mathcal{A}_\omega$ is called the **Suslin operation**.

Now we will show that the collection of completely Ramsey sets (*i.e.*, the collection of sets having the Baire property) is closed under the generalised Suslin operation $\mathcal{A}_\kappa$ whenever $\omega \leq \kappa < \mathfrak{h}$, *i.e.*, for every family $\{Q_s : s \in \mathrm{seq}(\kappa)\}$ of completely Ramsey sets, $\mathcal{A}_\kappa\{Q_s : s \in \mathrm{seq}(\kappa)\}$ is completely Ramsey.

A set $A \subseteq [\omega]^\omega$ is meagre *in* the basic open set $[s,x]^\omega$ if the intersection $A \cap [s,x]^\omega$ is meagre. Thus, by (a) & (b) of THEOREM 9.5, A is meagre in $[s,x]^\omega$ if for every $[t,y]^\omega \subseteq [s,x]^\omega$ there is a $y' \in [y]^\omega$ such that $A \cap [t,y']^\omega = \emptyset$. Now, for an arbitrary but fixed set $A \subseteq [\omega]^\omega$ let

$$M = \bigcup \{[s,x]^\omega : A \text{ is meagre in } [s,x]^\omega\} .$$

The main part of the following lemma is that $A \cup ([\omega]^\omega \setminus M)$ has the Baire property.

LEMMA 9.7. *For A and M as above we have:*

(a) A is meagre in each basic open set $[s,x]^\omega \subseteq M$.

(b) $M \cap A$ is meagre.

(c) $A \cup ([\omega]^\omega \setminus M)$ has the Baire property.

Proof. (a) Let $[s,x]^\omega \subseteq M$ be an arbitrary basic open subset of M and let

$$N = \{[t,y]^\omega \subseteq [s,x]^\omega : A \text{ is meagre in } [t,y]^\omega\} .$$

Then, by definition of M and since the basic open sets of the Ellentuck topology are closed under finite intersections, $\bigcup N = [s,x]^\omega$. So, for each basic open set $[u,z]^\omega \subseteq [s,x]^\omega$ there is a $[t,y]^\omega \subseteq [u,z]^\omega$ which belongs to N and we find a $y' \in [y]^\omega$ such that $[t,y']^\omega \cap A = \emptyset$. Since $[u,z]^\omega \subseteq [s,x]^\omega$ was arbitrary and $[t,y']^\omega \subseteq [u,z]^\omega$, this shows that A is meagre in $[s,x]^\omega$.

(b) We have to show that $[\omega]^\omega \setminus (M \cap A)$ contains an open dense set, *i.e.*, for every basic open set $[s,x]^\omega$ there is a $[t,y]^\omega \subseteq [s,x]^\omega$ such that $[t,y]^\omega \cap M \cap A = \emptyset$. Let $[s,x]^\omega$ be an arbitrary basic open set. If $[s,x]^\omega \cap M = \emptyset$, then we are done.

Otherwise, since M is open, $[s,x]^\omega \cap M \supseteq [t,y]^\omega$ for some basic open set $[t,y]^\omega$; and since $[t,y]^\omega \subseteq M$, by (a), A is meagre in $[t,y]^\omega$. Hence, there is a $[t,y']^\omega \subseteq [t,y]^\omega$ such that $[t,y']^\omega \cap A = \emptyset$ which shows that $[t,y']^\omega \cap (M \cap A) = \emptyset$.
(c) Notice that $A \cup \big([\omega]^\omega \setminus M\big) = \big([\omega]^\omega \setminus M\big) \cup (M \cap A)$. Now, by (b), $M \cap A$ is meagre, and because M is open, $[\omega]^\omega \setminus M$ is closed. Thus, $A \cup \big([\omega]^\omega \setminus M\big)$ is the union of a meagre set and a closed set and therefore has the Baire property. $\dashv$

The following result is used in the proof of THEOREM 9.9.

PROPOSITION 9.8. *For every $A \subseteq [\omega]^\omega$ there is a set $C \supseteq A$ which has the Baire property and whenever $Z \subseteq C \setminus A$ has Baire property, then Z is meagre.*

Proof. Let $C = A \cup \big([\omega]^\omega \setminus M\big)$ where $M = \bigcup \big\{[s,x]^\omega : A \text{ is meagre in } [s,x]^\omega\big\}$. By LEMMA 9.7.(c) we know that C has the Baire property. Now let $Z \subseteq C \setminus A$ be such that Z has the Baire property. If Z is not meagre, then there exists a basic open set $[t,y]^\omega$ such that $[t,y]^\omega \setminus Z$ is meagre. In particular, A is meagre in $[t,y]^\omega$ and therefore $[t,y]^\omega \subseteq M$. On the other hand, since $[t,y]^\omega \cap Z \neq \emptyset$ and $Z \cap M = \emptyset$ we get that $[t,y]^\omega \nsubseteq M$, a contradiction. $\dashv$

Now we are ready to prove that the collection of completely Ramsey sets (*i.e.*, the Baire property) is closed under the generalised Suslin operation $\mathcal{A}_\kappa$ whenever $\kappa < \mathfrak{h}$.

THEOREM 9.9. *Let $\kappa < \mathfrak{h}$ be an infinite cardinal and for each $s \in \operatorname{seq}(\kappa)$ let $Q_s \subseteq [\omega]^\omega$. If all sets Q_s are completely Ramsey, then*

$$\mathcal{A}_\kappa\big\{Q_s : s \in \operatorname{seq}(\kappa)\big\}$$

is completely Ramsey too.

Proof. Let $\big\{Q_s : s \in \operatorname{seq}(\kappa)\big\}$ be a family of completely Ramsey sets. We have to show that the set $A = \mathcal{A}_\kappa\big\{Q_s : s \in \operatorname{seq}(\kappa)\big\}$ is completely Ramsey. Without loss of generality we may assume that $Q_s \supseteq Q_t$ whenever $s \subseteq t$. For every $s \in \operatorname{seq}(\kappa)$ let

$$A_s := \bigcup_{\substack{f \in {}^\omega\kappa \\ s = f|_{|s|}}} \bigcap_{\substack{n \in \omega \\ n \geq |s|}} Q_{f|_n}.$$

We leave it as an exercise to the reader to verify that $A = A_\emptyset$ and that for every $s \in \operatorname{seq}(\kappa)$ we have $A_s \subseteq Q_s$ and $A_s = \bigcup_{\alpha \in \kappa} A_{s^\frown\langle\alpha\rangle}$. Further, notice that

$$A = \mathcal{A}_\kappa\big\{A_s : s \in \operatorname{seq}(\kappa)\big\}.$$

By PROPOSITION 9.8, for each $s \in \operatorname{seq}(\kappa)$ we find a set $C_s \supseteq A_s$ which is completely Ramsey and whenever $Z \subseteq C_s \setminus A_s$ is completely Ramsey, then Z is completely Ramsey-null. Because $Q_s \supseteq A_s$ and Q_s is completely Ramsey, we may assume that $C_s \subseteq Q_s$, and thus,

$$A = \mathcal{A}_\kappa\big\{C_s : s \in \operatorname{seq}(\kappa)\big\}\,.$$

Let $C := C_\emptyset$ and notice that $A = \bigcup_{\alpha\in\kappa} A_{\langle\alpha\rangle} \subseteq \bigcup_{\alpha\in\kappa} C_{\langle\alpha\rangle}$, in particular, $C \subseteq \bigcup_{\alpha\in\kappa} C_{\langle\alpha\rangle}$. Now we show that

$$C \setminus A \subseteq \bigcup_{\alpha\in\kappa} C_{\langle\alpha\rangle} \subseteq \bigcup_{f\in{}^\omega\kappa}\ \bigcap_{n\in\omega} C_{f|_n} \subseteq \bigcup_{s\in\operatorname{seq}(\kappa)} \Big(C_s \setminus \bigcup_{\alpha\in\kappa} C_{s^\frown\langle\alpha\rangle}\Big)\,.$$

Let $x \in [\omega]^\omega$ be such that

$$x \notin \bigcup_{s\in\operatorname{seq}(\kappa)} \Big(C_s \setminus \bigcup_{\alpha\in\kappa} C_{s^\frown\langle\alpha\rangle}\Big)\,. \tag{$\notin$}$$

If for all $\alpha \in \kappa$, $x \notin C_{\langle\alpha\rangle}$, then $x \notin C$. On the other hand, if there exists an $\alpha_0 \in \kappa$ such that $x \in C_{\langle\alpha_0\rangle}$, then by ($\notin$) we find an α_1 such that $x \in C_{\langle\alpha_0,\alpha_1\rangle}$, and again by ($\notin$) we find an α_2 such that $x \in C_{\langle\alpha_0,\alpha_1,\alpha_2\rangle}$, *et cetera*, and finally we find an $f \in {}^\omega\kappa$ such that for all $n \in \omega$, $x \in C_{f|_n}$, which implies that $x \in A$. Further, $C_s \setminus \bigcup_{\alpha\in\kappa} C_{s^\frown\langle\alpha\rangle} \subseteq C_s \setminus \bigcup_{\alpha\in\kappa} A_{s^\frown\langle\alpha\rangle} = C_s \setminus A_s$, and since $\bigcup_{\alpha\in\kappa} C_{s^\frown\langle\alpha\rangle}$ is the union of less than $\mathfrak{h}$ completely Ramsey sets, $C_s \setminus \bigcup_{\alpha\in\kappa} C_{s^\frown\langle\alpha\rangle}$ is completely Ramsey, and as a subset of $C_s \setminus A_s$ it is completely Ramsey-null. Thus, $C \setminus A$, as a subset of a union of less than $\mathfrak{h}$ completely Ramsey-null sets, is completely Ramsey-null, and because C is completely Ramsey, A is completely Ramsey too. ⊣

Notes

Lemma 9.1 and Theorem 9.2 are due to Plewik [18]. The Ellentuck topology on $[\omega]^\omega$ was introduced by Ellentuck in [6] (for a comprehensive exposition of General Topology we refer the reader to Engelking [7]). The main result of that paper is Theorem 9, which is now known as Ellentuck's Theorem 9.5 (see also Matet [16]). However, the aim of Ellentuck's paper was to give a simpler proof for the fact that every analytic set is completely Ramsey — a fact which also follows from Theorem 9.9 (*cf.* Galvin and Prikry [8] and Silver [19]). The proof of Theorem 9.9 is similar to the proof of Jech [12, Theorem 11.18] and is essentially taken from Halbeisen [9, Section 3] (see also Matet [15, Proposition 9.8]).

Related Results

60. *The ideal of completely doughnut null sets*.* In Chapter 2, the doughnut property was introduced. Now, similarly as we defined the ideal $\mathcal{R}_0$ of completely Ramsey-null sets one can define the ideal v_0 of completely doughnut null sets. By Theorem 9.2 we know that $add(\mathcal{R}_0) = cov(\mathcal{R}_0)$, however, it is not known whether we also have $add(v_0) = cov(v_0)$ (see Halbeisen [10, Question 4]). A partial answer to this problem can be found in Kalemba, Plewik, and Wojciechowska [13], where it is shown that $\mathfrak{t} = \min\{\operatorname{cf}(\mathfrak{c}), \mathfrak{r}\}$ implies $add(v_0) = cov(v_0)$.

61. *$\mathcal{R}_0$ and other σ-ideals on $[\omega]^\omega$.* In [5], Corazza compares the ideal of completely Ramsey-null sets with other σ-ideals like the ideal of Lebesgue measure zero, meagre, and Marczewski measure zero sets of reals (see also Louveau [14], Aniszczyk, Frankiewicz, Plewik [1], and Brown [3]).

62. *Ellentuck type theorems.* In [4], Carlson and Simpson survey the interplay between topology and Ramsey Theory. In particular, an abstract version of ELLENTUCK'S THEOREM 9.5 is introduced and discussed. For a further development of this theory see for example Mijares [17].

Let $\beta\omega \setminus \omega$ denote the set of all non-principal ultrafilters over ω. For $A \subseteq \omega$ define

$$A^* = \{\mathscr{U} \in \beta\omega \setminus \omega : A \in \mathscr{U}\},$$

and let $\mathscr{B}^* = \{A^* : A \subseteq \omega\}$. Notice that $\omega^* = \beta\omega \setminus \omega$ and that $A^* = \emptyset$ ***iff*** A is finite. Furthermore, for all $A^*, B^* \in \mathscr{B}^*$ we have

$$A^* \cap B^* = (A \cap B)^* \quad \text{and} \quad A^* \cup B^* = (A \cup B)^*.$$

In particular, $\mathscr{B}^*$ has the property that intersections of sets in $\mathscr{B}^*$ belong to $\mathscr{B}^*$, thus, $\mathscr{B}^*$ is a base for a topology on $\beta\omega \setminus \omega$. The set $\beta\omega \setminus \omega$ with the topology generated by the basic open sets $A^* \in \mathscr{B}^*$ is a topological space which has many interesting properties; the following results can be found for example in Todorčević [20, Section 14].

- $\beta\omega \setminus \omega$ is Hausdorff ([20, Lemma 1]).
- $\beta\omega \setminus \omega$ is compact ([20, Lemma 2]).
- $\beta\omega \setminus \omega$ contains no non-trivial converging sequences ([20, Theorem 2]).

For an introduction to $\beta\omega \setminus \omega$ see van Mill [21], and for combinatorial properties of $\beta\omega \setminus \omega$ we refer the reader to Hindman and Strauss [11].

63. *The minimum height of a tree π-base of $\beta\omega\setminus\omega$.* A family $\mathscr{P} \subseteq \mathscr{B}^*$ of basic open sets is a **π-base** for $\beta\omega \setminus \omega$ if every non-empty element of $\mathscr{B}^*$ contains a member of $\mathscr{P}$. If a π-base $\mathscr{P} \subseteq \mathscr{B}^*$ is a tree when considered as a partially ordered set under reverse inclusion (*i.e.*, for every $A^* \in \mathscr{P}$, $A^*_{\lneq} := \{B^* \in \mathscr{P} : A^* \subsetneq B^*\}$ is well-ordered by "$\supseteq$"), then $\mathscr{P}$ is called a **tree π-base** of $\beta\omega \setminus \omega$. If $\mathscr{P} \subseteq \mathscr{B}^*$ is a tree π-base of $\beta\omega \setminus \omega$, then the height of an element $A^* \in \mathscr{P}$, denoted $h(A^*)$, is the order type of $A^*_{\lneq}$ (well-ordered by "$\supseteq$"), and the **height** of $\mathscr{P}$ is defined by $h(\mathscr{P}) := \bigcup\{h(A^*) : A^* \in \mathscr{P}\}$. Now, the BASE MATRIX LEMMA 2.11 of Balcar, Pelant, and Simon [2] (see Chapter 8 | RELATED RESULT 51) shows that $\mathfrak{h}$ is the minimum height of a tree π-base of $\beta\omega \setminus \omega$, *i.e.*,

$$\mathfrak{h} = \min\{h(\mathscr{P}) : \mathscr{P} \subseteq \mathscr{B}^* \text{ is a tree } \pi\text{-base of } \beta\omega \setminus \omega\}.$$

REFERENCES

1. BOHDAN ANISZCZYK, RYSZARD FRANKIEWICZ, AND SZYMON PLEWIK, *Remarks on (s) and Ramsey-measurable functions*, ***Bulletin of the Polish Academy of Sciences, Mathematics***, vol. 35 (1987), 479–485.
2. BOHUSLAV BALCAR, JAN PELANT, AND PETR SIMON, *The space of ultrafilters on N covered by nowhere dense sets*, ***Fundamenta Mathematicae***, vol. 110 (1980), 11–24.

3. Jack B. Brown, *The Ramsey sets and related sigma algebras and ideals*, ***Fundamenta Mathematicae***, vol. 136 (1990), 179–185.
4. Timothy J. Carlson and Steve G. Simpson, *Topological Ramsey theory*, in ***Mathematics of Ramsey Theory*** (J. Nešetřil and V. Rödl, eds.), [Algorithms and Combinatorics 5], Springer-Verlag, Berlin, 1990, pp. 172–183.
5. Paul Corazza, *Ramsey sets, the Ramsey ideal, and other classes over* R, ***The Journal of Symbolic Logic***, vol. 57 (1992), 1441–1468.
6. Erik Ellentuck, *A new proof that analytic sets are Ramsey*, ***The Journal of Symbolic Logic***, vol. 39 (1974), 163–165.
7. Ryszard Engelking, ***General Topology***, Heldermann Verlag, Berlin, 1989.
8. Fred Galvin and Karel Prikry, *Borel sets and Ramsey's Theorem*, ***The Journal of Symbolic Logic***, vol. 38 (1973), 193–198.
9. Lorenz Halbeisen, *Symmetries between two Ramsey properties*, ***Archive for Mathematical Logic***, vol. 37 (1998), 241–260.
10. ———, *Making doughnuts of Cohen reals*, ***Mathematical Logic Quarterly***, vol. 49 (2003), 173–178.
11. Neil Hindman and Dona Strauss, ***Algebra in the Stone-Čech Compactification: Theory and Applications***, [De Gruyter Expostitions in Mathematics], Walter de Gruyter, New York, 1998.
12. Thomas Jech, ***Set Theory****, The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
13. Piotr Kalemba, Szymon Plewik, and Anna Wojciechowska, *On the ideal* (v_0), ***Central European Journal of Mathematics***, vol. 6 (2008), 218–227.
14. Alain Louveau, *Une méthode topologique pour l'étude de la propriété de Ramsey*, ***Israel Journal of Mathematics***, vol. 23 (1976), 97–116.
15. Pierre Matet, *Happy families and completely Ramsey sets*, ***Archive for Mathematical Logic***, vol. 32 (1993), 151–171.
16. ———, *A short proof of Ellentuck's theorem*, ***Proceedings of the American Mathematical Society***, vol. 129 (2000), 1195–1197.
17. José G. Mijares, *Parametrizing the abstract Ellentuck theorem*, ***Discrete Mathematics***, vol. 307 (2007), 216–225.
18. Szymon Plewik, *On completely Ramsey sets*, ***Fundamenta Mathematicae***, vol. 127 (1986), 127–132.
19. Jack Silver, *Every analytic set is Ramsey*, ***The Journal of Symbolic Logic***, vol. 35 (1970), 60–64.
20. Stevo Todorčević, ***Topics in Topology***, [Lecture Notes in Mathematics 1652], Springer-Verlag, Berlin a.o., 1997.
21. Jan van Mill, *An introduction to* $\beta\omega$, in ***Handbook of Set-Theoretic Topology*** (K. Kunen and J.E. Vaughan, eds.), North-Holland, Amsterdam, 1990, pp. 503–567.

10

Happy Families and their Relatives

A cadence is a certain simultaneous progression of all the voices in a composition accompanying a repose in the harmony or the completion of a meaningful segment of the text.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

In this chapter we shall investigate combinatorial properties of certain families of infinite subsets of ω. In order to do so, we shall use many of the combinatorial tools developed in the preceding chapters. The families we investigate — particularly P-families and Ramsey families — will play a key role in understanding the combinatorial properties of Silver and Mathias forcing notions (see Chapter 22 and Chapter 24 respectively).

Happy Families

The P-families and Ramsey families mentioned above are relatives to the so-called *happy families*. The name "happy families" comes from a children's card game, where the idea of the game is to collect the members of fictional families. The connection to families in Set Theory is that a family $\mathscr{E} \subseteq [\omega]^\omega$ is happy if for every countable decreasing sequence $y_0 \supseteq y_1 \supseteq \cdots$ of elements of $\mathscr{E}$ there is a member of $\mathscr{E}$ which selects certain elements from the sets y_i (*cf.* PROPOSITION 10.6.(b)). This explains why happy families are also called *selective co-ideals* — which is more sober but less amusing.

Firstly recall that a family $\mathscr{F} \subseteq [\omega]^\omega$ is a filter if it is closed under supersets and finite intersections, and that the Fréchet filter is the filter consisting of all co-finite subsets of ω (*i.e.*, all $x \in [\omega]^\omega$ such that $\omega \setminus x$ is finite). To keep the notation short, for $x \subseteq \omega$ define $x^{\mathsf{c}} := \omega \setminus x$. For a filter $\mathscr{F} \subseteq [\omega]^\omega$, $\mathscr{F}^+$

denotes the collection of all sets $x \subseteq \omega$ such that $\omega \setminus x$ does not belong to $\mathscr{F}$, *i.e.*,

$$\mathscr{F}^+ = \{x \subseteq \omega : x^{\mathsf{c}} \notin \mathscr{F}\}.$$

An equivalent definition of $\mathscr{F}^+$ is given by the following

FACT 10.1. *For any filter $\mathscr{F} \subseteq [\omega]^\omega$, $x \in \mathscr{F}^+$ if and only if $x \cap z$ is non-empty whenever $z \in \mathscr{F}$.*

Proof. On the one hand, if, for some $z \in \mathscr{F}$, $x \cap z = \emptyset$, then $x^{\mathsf{c}} \supseteq z$, which implies that $x^{\mathsf{c}} \in \mathscr{F}$ and therefore $x \notin \mathscr{F}^+$. On the other hand, if, for some $x \subseteq \omega$, $x^{\mathsf{c}} \in \mathscr{F}$, then we obviously have $x \cap x^{\mathsf{c}} = \emptyset$, thus, x does not meet every member of $\mathscr{F}$. ⊣

If $\mathscr{U}$ is an ultrafilter and $x \cup y \in \mathscr{U}$, then at least one of x and y belongs to $\mathscr{U}$. In general, this is not the case for filters $\mathscr{F}$, but it holds for $\mathscr{F}^+$.

LEMMA 10.2. *Let $\mathscr{F} \subseteq [\omega]^\omega$ be a filter. If $\mathscr{F}^+$ contains $x \cup y$, then it contains at least one of x and y.*

Proof. If neither x nor y belongs to $\mathscr{F}^+$, then $x^{\mathsf{c}}, y^{\mathsf{c}} \in \mathscr{F}$. Hence, $(x \cup y)^{\mathsf{c}} = x^{\mathsf{c}} \cap y^{\mathsf{c}} \in \mathscr{F}$, and therefore $x \cup y \notin \mathscr{F}^+$. ⊣

Now, a filter $\mathscr{F} \subseteq [\omega]^\omega$ is called a **free filter** if it contains the Fréchet filter. In particular, every ultrafilter on $[\omega]^\omega$ is free. Notice that for a free filter $\mathscr{F}$, $\mathscr{F}^+ = \{x \subseteq \omega : \forall z \in \mathscr{F}(|x \cap z| = \omega)\}$, and that a filter $\mathscr{U} \subseteq [\omega]^\omega$ is an ultrafilter *iff* $\mathscr{U} = \mathscr{U}^+$. Finally, a family $\mathscr{E}$ of subsets of ω is called a **free family** if there is a free filter $\mathscr{F} \subseteq [\omega]^\omega$ such that $\mathscr{E} = \mathscr{F}^+$. In particular, $[\omega]^\omega$ and all ultrafilters on $[\omega]^\omega$ are free families. Notice that a free family does not contain any finite sets and is closed under supersets. Moreover, a free family $\mathscr{E}$ is closed under finite intersections *iff* $\mathscr{E}$ is an ultrafilter on $[\omega]^\omega$.

Recall that $\operatorname{fin}(\omega)$ denotes the set of all finite subsets of ω. To keep the notation short, for $s \in \operatorname{fin}(\omega)$ let $\bar{s} := \bigcup s$, and for $n \in \omega$ let $n^+ := n + 1$ (in other words, n^+ is the successor cardinal of n). In particular, for non-empty sets $s \in \operatorname{fin}(\omega)$ we have $\bar{s} = \max(s)$ and $\bar{s}^+ = \max(s) + 1$.

A set $x \subseteq \omega$ is said to **diagonalise** the set $\{x_s : s \in \operatorname{fin}(\omega)\} \subseteq [\omega]^\omega$ if the following conditions are satisfied:

- $x \subseteq x_\emptyset$;
- for all $s \in \operatorname{fin}(\omega)$, if $\bar{s} \in x$ then $x \setminus \bar{s}^+ \subseteq x_s$.

For $\mathscr{A} \subseteq [\omega]^\omega$ we write $\operatorname{fil}(\mathscr{A})$ for the filter generated by the members of $\mathscr{A}$, *i.e.*, $\operatorname{fil}(\mathscr{A})$ consists of all subsets of ω which are supersets of intersections of finitely many members of $\mathscr{A}$.

Now, a set $\mathscr{E} \subseteq [\omega]^\omega$ is a **happy family** if $\mathscr{E}$ is a free family and whenever $\operatorname{fil}(\{x_s : s \in \operatorname{fin}(\omega)\}) \subseteq \mathscr{E}$, there is an $x \in \mathscr{E}$ which diagonalises the set $\{x_s : s \in \operatorname{fin}(\omega)\}$.

Below, we give two examples of happy families; in the first the family is as large as possible, and in the second the family is of medium size — in the next section we shall see examples of happy families which are as small as possible.

FACT 10.3. *The family* $[\omega]^\omega$ *is happy.*

Proof. Let $\{x_s : s \in \operatorname{fin}(\omega)\} \subseteq [\omega]^\omega$ be a subfamily of $[\omega]^\omega$ and assume that $\operatorname{fil}\big(\{x_s : s \in \operatorname{fin}(\omega)\}\big) \subseteq [\omega]^\omega$, *i.e.*, the intersection of finitely many elements of $\{x_s : s \in \operatorname{fin}(\omega)\}$ is infinite. Let $n_0 := \bigcap x_\emptyset$ and for $k \in \omega$ choose $n_{k+1} > n_k$ such that

$$n_{k+1} \in \bigcap \{x_s : \bar{s}^+ \leq n_k + 1\}.$$

By our assumption, those choices are possible. Let $x = \{n_k : k \in \omega\}$; then $x \subseteq x_\emptyset$, and whenever $\bar{s} = n_k$ (*i.e.*, $\bar{s}^+ \leq n_k + 1$), we get

$$x \setminus \bar{s}^+ \subseteq \bigcap \{x_s : \bar{s}^+ \leq n_k + 1\}.$$

In particular, $x \setminus \bar{s}^+ \subseteq x_s$, as required. ⊣

In order to construct non-trivial examples of happy families, we have to introduce first the following notion: For a *mad* family $\mathscr{A} \subseteq [\omega]^\omega$, let $\mathscr{F}_{\mathscr{A}}$ be the collection of all subsets of ω which are almost contained in supersets of complements of finite unions of members of $\mathscr{A}$.

The goal is to show that $\mathscr{F}_{\mathscr{A}}^+$ is a happy family whenever $\mathscr{A} \subseteq [\omega]^\omega$ is a *mad* family, but for this we have to prove first that $\mathscr{F}_{\mathscr{A}}$ is a free filter.

PROPOSITION 10.4. *If* $\mathscr{A} \subseteq [\omega]^\omega$ *is a mad family, then* $\mathscr{F}_{\mathscr{A}}$ *is a free filter but not an ultrafilter.*

Proof. Let $\mathscr{A} \subseteq [\omega]^\omega$ be a *mad* family and let

$$\mathscr{F}_{\mathscr{A}} = \big\{y \in [\omega]^\omega : \exists x_0 \dots x_n \in \mathscr{A}\big((x_0 \cup \dots \cup x_n)^{\mathsf{c}} \subseteq^* y\big)\big\}.$$

Firstly, $\mathscr{F}_{\mathscr{A}}$ is a free filter: By definition, $\mathscr{F}_{\mathscr{A}}$ is closed under supersets and contains all co-finite sets, and since $\mathscr{A}$ is *mad*, no co-finite set is the union of finitely many members of $\mathscr{A}$, hence, $\mathscr{F}_{\mathscr{A}}$ does not contain any finite set. Further, for any $y, y' \in \mathscr{F}_{\mathscr{A}}$ there are $x_0, \dots, x_n$ and $x'_0, \dots, x'_m$ in $\mathscr{A}$ such that

$$\Big(\bigcup_{i \in n} x_i\Big)^{\mathsf{c}} \subseteq^* y \quad \text{and} \quad \Big(\bigcup_{j \in m} x'_j\Big)^{\mathsf{c}} \subseteq^* y',$$

which shows that

$$\Big(\bigcup_{i \in n} x_i \cup \bigcup_{j \in m} x'_j\Big)^{\mathsf{c}} \subseteq^* y \cap y' \in \mathscr{F}_{\mathscr{A}}.$$

Secondly, $\mathscr{F}_{\mathscr{A}}$ is not an ultrafilter: We have to find a set $z \in [\omega]^\omega$ such that neither z nor z^{c} belongs to $\mathscr{F}_{\mathscr{A}}$. Let $\{x_i : i \in \omega\}$ be distinct elements of $\mathscr{A}$. Notice that it is enough to construct a set $z \in [\omega]^\omega$ such that both z and z^{c} have infinite intersection with each x_i. To construct such a set z, take a strictly increasing sequence $n_0 < \dots < n_k < \dots$ of natural numbers such that for each $k \in \omega$, if $k = 2^l(2m+1)$, then both n_{2k} and n_{2k+1} are in x_m and put $z = \{n_{2k} : k \in \omega\}$. ⊣

Now we are ready to give non-trivial examples of happy families. Even though the proof of the following proposition becomes considerably easier by the characterisation of happy families given by PROPOSITION 10.6.(b), we think it makes sense to have some non-trivial examples of happy families — and to work with the original definition — before giving an equivalent definition of happy families.

PROPOSITION 10.5. *Let $\mathscr{A} \subseteq [\omega]^\omega$ be a mad family. Then $\mathscr{F}_{\mathscr{A}}^+$ is a happy family.*

Proof. Given any family $\{y_t : t \in \operatorname{fin}(\omega)\}$ with $\operatorname{fil}(\{x_s : s \in \operatorname{fin}(\omega)\}) \subseteq \mathscr{F}_{\mathscr{A}}^+$. For $s \in \operatorname{fin}(\omega)$, let $x_s = \bigcap\{y_t : \bar{t} \leq \bar{s}\}$. Then for any $n \in \omega$, $x_{\{n\}} = x_s$ whenever $n = \bar{s}$. We shall construct an $x \in \mathscr{F}_{\mathscr{A}}^+$ which diagonalises $\{y_t : t \in \operatorname{fin}(\omega)\}$ by showing that for all $n \in \omega$, $x \setminus n^+ \subseteq x_{\{n\}}$. For this, let x^0 — constructed as in the proof of FACT 10.3 — diagonalise $\{x_s : s \in \operatorname{fin}(\omega)\}$. We may not assume that x^0 belongs to $\mathscr{F}_{\mathscr{A}}^+$, i.e., there might be a $z \in \mathscr{F}$ such that $x^0 \cap z$ is finite. However, since $\mathscr{A}$ is *mad*, there is a $y^0 \in \mathscr{A}$ such that $x^0 \cap y^0$ is infinite. For each $s \in \operatorname{fin}(\omega)$ define $x_s^1 := x_s \setminus y^0$. Notice that all x_s^1 are infinite and that $\operatorname{fil}(\{x_s^1 : s \in \operatorname{fin}(\omega)\}) \subseteq \mathscr{F}_{\mathscr{A}}^+$, as $y^0 \in \mathscr{A}$. Let x^1 diagonalise $\{x_s^1 : s \in \operatorname{fin}(\omega)\}$ and let $y^1 \in \mathscr{A}$ be such that $x^1 \cap y^1$ is infinite. Since $x^1 \subseteq x_\emptyset^1 \subseteq \omega \setminus y^0$ we get $y^1 \neq y^0$. Further, notice that x^1 also diagonalises $\{x_s : s \in \operatorname{fin}(\omega)\}$. Now, for each $s \in \operatorname{fin}(\omega)$ define $x_s^2 := x_s \setminus (y^0 \cup y^1)$ and proceed as before. After countably many steps we have constructed two sequences of infinite sets, $\langle x^i : i \in \omega\rangle$ and $\langle y^i : i \in \omega\rangle$, such that each y^i belongs to $\mathscr{A}$, $y^i \neq y^j$ whenever $i \neq j$, $x^i \cap y^i$ is infinite (for all $i \in \omega$), and x^i diagonalises $\{x_s : s \in \operatorname{fin}(\omega)\}$. Construct a strictly increasing sequence $n_0 < \ldots < n_k < \ldots$ of natural numbers such that $n_0 \in x_\emptyset$ and for each $k \in \omega$, if $k = 2^i(2m+1)$, then

$$n_k \in y^i \cap x^i \cap x_{\{n_{k-1}\}}\,.$$

Such a sequence of natural numbers exists because all sufficiently large numbers in x^i belong to $x_{\{n_{k-1}\}}$ and since $y^i \cap x^i$ is infinite. Finally, let $x = \{n_k : k \in \omega\}$. Then x diagonalises $\{x_s : s \in \operatorname{fin}(\omega)\}$ and it remains to show that $x \in \mathscr{F}_{\mathscr{A}}^+$, i.e., x has infinite intersection with each member of $\mathscr{F}_{\mathscr{A}}$. By construction, for each $i \in \omega$, $x \cap y^i$ is infinite, and since $\mathscr{A}$ is *mad*, $x \setminus y^i$ is infinite as well. Thus, x has infinite intersection with the complement of any finite union of elements in $\mathscr{A}$, hence, $x \in \mathscr{F}_{\mathscr{A}}^+$. ⊣

After having seen that there are non-trivial happy families, let us give now another characterisation of happy families which will be used later in this chapter.

PROPOSITION 10.6. *For a free family $\mathscr{E}$, the following statements are equivalent:*

(a) $\mathscr{E}$ is happy.

(b) If $y_0 \supseteq y_1 \supseteq \cdots \supseteq y_i \supseteq \cdots$ is a countable decreasing sequence of elements of $\mathscr{E}$, then there is a function $f \in {}^\omega\omega$ such that $f[\omega] \in \mathscr{E}$, $f(0) \in y_0$, and for all $n \in \omega$ we have $f(n+1) \in y_{f(n)}$.

Proof. (a)⇒(b) Assume that $\mathscr{E}$ is happy and let $\{y_i : i \in \omega\} \subseteq \mathscr{E}$ be such that for all $i \in \omega$, $y_{i+1} \subseteq y_i$. For each $s \in \text{fin}(\omega)$ define

$$x_s = \bigcap \{y_i : i \leq \bar{s}\}.$$

Notice that $\text{fil}\big(\{x_s : s \in \text{fin}(\omega)\}\big) \subseteq \mathscr{E}$. Since $\mathscr{E}$ is assumed to be happy there is an x which diagonalises the family $\{x_s : s \in \text{fin}(\omega)\}$. Let $f = f_x$ — recall that $f_x \in {}^\omega\omega$ is the (unique) strictly increasing bijection between ω and x (defined in Chapter 8). For an arbitrary $n \in \omega$ let $s := x \cap \big(f(n)+1\big)$. Then $\bar{s}^+ = f(n)+1$ and $\bar{s} \in x$. As $f(n+1) \in x \setminus \bar{s}^+$ and $x \setminus \bar{s}^+ \subseteq x_s \subseteq y_{f(n)}$, we have $f(n+1) \in y_{f(n)}$, and since n was arbitrary, f has the required properties.

(b)⇒(a) Assume now that $\mathscr{E}$ has property (b) and let $\{x_s : s \in \text{fin}(\omega)\} \subseteq \mathscr{E}$ be such that $\text{fil}\big(\{x_s : s \in \text{fin}(\omega)\}\big) \subseteq \mathscr{E}$. We have to find an $x \in \mathscr{E}$ which diagonalises $\{x_s : s \in \text{fin}(\omega)\}$. For each $i \in \omega$ define

$$y_i = \bigcap \{x_s : \bar{s} \leq i\}.$$

Obviously, for each $i \in \omega$ we have $y_i \in \mathscr{E}$ and $y_{i+1} \subseteq y_i$. By (b) there is a function $f \in {}^\omega\omega$ such that $f[\omega] \in \mathscr{E}$ and for all $n \in \omega$ we have $f(n+1) \in y_{f(n)}$. Let $x := f[\omega]$ and let $s \in \text{fin}(\omega)$ be such that $\bar{s} \in x$. Then there exists an $n \in \omega$ such that $f(n) = \bar{s}$, and for every $k \in x \setminus \bar{s}^+$ we have $k = f(m)$ for some $m > n$, hence, $k \in y_{f(n)}$. Now, $\bar{s}^+ = f(n)+1$, and since $y_{f(n)} \subseteq x_s$ we get $k \in x_s$. Hence, for all $s \in \text{fin}(\omega)$ with $\bar{s} \in x$ we have $x \setminus \bar{s}^+ \subseteq x_s$, which shows that x diagonalises $\{x_s : s \in \text{fin}(\omega)\}$. ⊣

We leave it as an exercise to the reader to find an easier proof of Proposition 10.5 by using the characterisation of happy families given by Proposition 10.6.(b).

Ramsey Ultrafilters

So far we have seen two examples of happy families. In the first example (Fact 10.3), the happy family was as large as possible, and in the second example (Proposition 10.5), the happy families were of medium size. Below, we consider happy families which are as small as possible, *i.e.*, happy families which are ultrafilters.

A free ultrafilter $\mathscr{U} \subseteq [\omega]^\omega$ is a **Ramsey ultrafilter** if for every colouring $\pi : [\omega]^2 \to 2$ there exists an $x \in \mathscr{U}$ which is homogeneous for π, *i.e.*, $\pi|_{[x]^2}$ is constant.

The following result gives two alternative characterisations of Ramsey ultrafilter. The first characterisation of Ramsey ultrafilters is related to P-points and Q-points (introduced below), and the second characterisation show that a Ramsey ultrafilter is an ultrafilter that is also a happy family.

PROPOSITION 10.7. *For every free ultrafilter $\mathscr{U}$, the following conditions are equivalent:*

(a) $\mathscr{U}$ is a Ramsey ultrafilter.

(b) Let $\{u_i \subseteq \omega : i \in \omega\}$ be a partial partition of ω, i.e., $\bigcup\{u_i : i \in \omega\} \subseteq \omega$ and for any distinct $i, j \in \omega$ we have $u_i \cap u_j = \emptyset$. Then either $u_i \in \mathscr{U}$ for a (unique) $i \in \omega$, or there exists an $x \in \mathscr{U}$ such that for each $i \in \omega$, $|x \cap u_i| \leq 1$.

(c) $\mathscr{U}$ is happy.

Proof. (a)⇒(b) Let $\{u_i : i \in \omega\}$ be a partition of ω. With respect to $\{u_i : i \in \omega\}$ define the colouring $\pi : [\omega]^2 \to 2$ as follows:

$$\pi\big(\{n,m\}\big) = \begin{cases} 0 & \text{if there is an } i \in \omega \text{ such that } \{n,m\} \subseteq u_i, \\ 1 & \text{otherwise.} \end{cases}$$

By (a) there is an $x \in \mathscr{U}$ such that $\pi|_{[x]^2}$ is constant. Now, if $\pi|_{[x]^2}$ is constantly zero, then there exists an $i \in \omega$ such that $x \subseteq u_i$, hence, $u_i \in \mathscr{U}$. On the other hand, if $\pi|_{[x]^2}$ is constantly one, then for any distinct $n, m \in x$ and any $i \in \omega$ we get that $\{n,m\} \cap u_i$ has at most one element, hence, for each $i \in \omega$, $x \cap u_i$ has at most one element.

(b)⇒(c) By PROPOSITION 10.6 it is enough to show that for every countable decreasing sequence $y_0 \supseteq y_1 \supseteq \ldots \supseteq y_n \supseteq \ldots$ of elements of $\mathscr{U}$ there is a function $f \in {}^\omega\omega$ such that $f[\omega] \in \mathscr{U}$, $f(0) \in y_0$, and for all $k \in \omega$ we have $f(k+1) \in y_{f(k)}$. If $y = \bigcap_{n\in\omega} y_n \in \mathscr{U}$, then the function $f_y \in {}^\omega\omega$ has the required properties. So, let us assume that $\bigcap_{n\in\omega} y_n \notin \mathscr{U}$ and without loss of generality let us further assume that for all $n \in \omega$, $y_n \setminus y_{n+1} \neq \emptyset$. Consider the partition $\big\{y_0^{\mathsf{c}} \cup \bigcap_{n\in\omega} y_n\big\} \cup \{y_n \setminus y_{n+1} : n \in \omega\}$ and notice that none of the pieces are in $\mathscr{U}$. By (b), there exists a set $x = \{a_n : n \in \omega\} \in \mathscr{U}$ such that for all $n \in \omega$, $x \cap (y_n \setminus y_{n+1}) = \{a_n\}$, in particular, $x \cap \bigcap_{n\in\omega} y_n = \emptyset$. Let $g \in {}^\omega\omega$ be a strictly increasing function such that $g(0) > 0$, $g[\omega] \subseteq x$, and for all $n \in \omega$, $x \setminus g(n) \subseteq y_n$. For $k \in \omega$ let $g^{k+1}(0) := g\big(g^k(0)\big)$, where $g^0(0) := 0$. Further, for $k \in \omega$ let $x_k := x \cap \big[g^{2k}(0), g^{2k+1}(0)\big)$ — recall that $[a,b) = \{i \in \omega : a \leq i < b\}$. Now, by (b) and since $\mathscr{U}$ is an ultrafilter, there exists a set $z = \{c_k : k \in \omega\} \subseteq x$ such that $z \in \mathscr{U}$ and for all $k \in \omega$, $z \cap x_k = \{c_k\}$. Notice that by construction, for each $k \in \omega$ we have $c_{k+2} > g(c_k)$ and $c_{k+2} \in y_{c_k}$. Finally, since $\mathscr{U}$ is an ultrafilter and $\{c_k : k \in \omega\} \in \mathscr{U}$, either $\{c_{2k} : k \in \omega\}$ or $\{c_{2k+1} : k \in \omega\}$ belongs to $\mathscr{U}$. In the former case define $f \in {}^\omega\omega$ by stipulating $f(k) := c_{2k}$, otherwise define $f(k) := c_{2k+1}$. Then f has the required properties.

(c)⇒(a) Let $\mathscr{U}$ be an ultrafilter that is also a happy family, and further let

$\pi : [\omega]^2 \to 2$ be an arbitrary but fixed colouring. We have to find a $y \in \mathscr{U}$ such that $\pi|_{[y]^2}$ is constant. The proof is similar to the proof of PROPOSITION 2.2. First we construct a family $\{x_s : s \in \text{fin}(\omega)\} \subseteq \mathscr{U}$. Let $x_\emptyset = \omega$, and let $x_{\{0\}} \in \mathscr{U}$ be such that $x_{\{0\}} \subseteq \omega \setminus \{0\}$ and for all $k, k' \in x_{\{0\}}$ we have $\pi(\{0,k\}) = \pi(\{0,k'\})$. Notice that since $\mathscr{U}$ is an ultrafilter, $x_{\{0\}}$ exists. In general, if x_s is defined and $n > \bar{s}$, then let $x_{s\cup\{n\}} \in \mathscr{U}$ be such that $x_{s\cup\{n\}} \subseteq x_s \setminus n^+$ and for all $k, k' \in x_{s\cup\{n\}}$ we have $\pi(\{n,k\}) = \pi(\{n,k'\})$. Since $\mathscr{U}$ is happy, there is a $y \in \mathscr{U}$ which diagonalises the family $\{x_s : s \in \text{fin}(\omega)\}$. By construction, for each $n \in y$ and for all $k, k' \in y \setminus n^+$ we have $\pi(\{n,k\}) = \pi(\{n,k'\})$ and we can define the colouring $\tau : x \to 2$ by stipulating

$$\tau(n) = \begin{cases} 0 & \text{if there is a } k \in x \setminus n^+ \text{ such that } \pi(\{n,k\}) = 0, \\ 1 & \text{otherwise.} \end{cases}$$

Since $\mathscr{U}$ is an ultrafilter, there exists a $x \in \mathscr{U}$ such that $x \subseteq y$ and $\tau|_x$ is constant, hence, $\pi|_{[x]^2}$ is constant. ⊣

At a first glance, condition (a) is just related to PROPOSITION 2.2 and not to RAMSEY'S THEOREM. However, the following fact shows that this is not the case. Moreover, even PROPOSITION 2.8 is related to Ramsey ultrafilters (the proofs are left to the reader).

FACT 10.8. *For every free ultrafilter $\mathscr{U}$, the following conditions are equivalent:*

(a) $\mathscr{U}$ is a Ramsey ultrafilter, i.e., for every colouring $\pi : [\omega]^2 \to 2$ there exists an $x \in \mathscr{U}$ which is homogeneous for π.

(b) For any $n \in \omega$, for any positive integer $r \in \omega$, and for every colouring $\pi : [\omega]^n \to r$, there exists an $x \in \mathscr{U}$ which is homogeneous for π.

(c) Let $\{r_k : k \in \omega\}$ and $\{n_k : k \in \omega\}$ be two (possibly finite) sets of positive integers, and for each $k \in \omega$ let $\pi_k : [\omega]^{n_k} \to r_k$ be a colouring. Then there exists an $x \in \mathscr{U}$ which is almost homogeneous for each π_k.

It is time now to address the problem of the existence of Ramsey ultrafilters. On the one hand, it can be shown that there are models of ZFC in which no Ramsey ultrafilters exist (see PROPOSITION 25.11). Thus, the existence of Ramsey ultrafilters is not provable in ZFC. On the other hand, if we assume for example CH (or just $\mathfrak{p} = \mathfrak{c}$), then we can easily construct a Ramsey ultrafilter.

PROPOSITION 10.9. *If $\mathfrak{p} = \mathfrak{c}$, then there exists a Ramsey ultrafilter.*

Proof. Let $\{\pi_\alpha : \alpha \in \mathfrak{c}\}$ be an enumeration of the set of all 2-colourings of $[\omega]^2$, i.e., for every colouring $\pi : [\omega]^2 \to 2$ there exists an $\alpha \in \mathfrak{c}$ such that $\pi = \pi_\alpha$. By transfinite induction we first construct a sequence $\langle x_\alpha : \alpha \in \mathfrak{c}\rangle \subseteq [\omega]^\omega$ such that $\{x_\alpha : \alpha \in \mathfrak{c}\}$ has the finite intersection property and for all $\alpha \in \mathfrak{c}$, $\pi_\alpha|_{[x_{\alpha+1}]^2}$ is constant. Let $x_0 := \omega$ and assume that for some $\alpha \in \mathfrak{c}$ we have already constructed x_β ($\beta \in \alpha$) such that $\{x_\beta : \beta \in \alpha\}$ has the finite intersection property and for all $\gamma+1 \in \alpha$ we have $\pi_\gamma|_{[x_{\gamma+1}]^2}$ is constant. If α is a successor ordinal, say $\alpha = \beta_0+1$, then let $x_\alpha \in [x_{\beta_0}]^\omega$ be such that $\pi_{\beta_0}|_{[x_\alpha]^2}$ is constant (notice that by RAMSEY'S THEOREM 2.1, $x_{\alpha+1}$ exists). If α is a limit ordinal, then let x_α be a pseudo-intersection of $\{x_\beta : \beta \in \alpha\}$ (notice that since $|\alpha| < \mathfrak{p}$, $x_{\alpha+1}$ exists). In either case, the family $\{x_\beta : \beta \in \alpha\}$ has the required properties. In particular, the family $\mathscr{E} = \{x_\alpha : \alpha \in \mathfrak{c}\}$ has the finite intersection property and for each colouring $\pi : [\omega]^2 \to 2$ there is an $x \in \mathscr{E}$ such that $\pi|_{[x]^2}$ is constant. Finally, extend the family $\mathscr{E}$ to an ultrafilter $\mathscr{U}$. Then $\mathscr{U}$ is a Ramsey ultrafilter. ⊣

P-points and *Q*-points

Below, we consider ultrafilters which are weaker than Ramsey ultrafilters, but which share with them some combinatorial properties.

A free ultrafilter $\mathscr{U}$ is a ***P*-point** if for each partition $\{u_n \subseteq \omega : n \in \omega\}$ of ω, either $u_n \in \mathscr{U}$ for a (unique) $n \in \omega$, or there exists an $x \in \mathscr{U}$ such that for each $n \in \omega$, $x \cap u_n$ is finite.

Furthermore, a free ultrafilter $\mathscr{U}$ is a ***Q*-point** if for each partition of ω into finite pieces $\{I_n \subseteq \omega : n \in \omega\}$, (*i.e.*, for each $n \in \omega$, I_n is finite), there exists an $x \in \mathscr{U}$ such that for each $n \in \omega$, $x \cap I_n$ has at most one element.

Comparing these definitions of P-points and Q-points with PROPOSITION 10.7.(b), it is evident that a Ramsey ultrafilter is both, a P-point as well as a Q-point; but also the converse is true:

FACT 10.10. *$\mathscr{U}$ is a Ramsey ultrafilter if and only if $\mathscr{U}$ is a P-point and a Q-point.*

Proof. ($\Rightarrow$) This follows immediately from PROPOSITION 10.7.(b) and the definitions of P-points and Q-points.

($\Leftarrow$) Let $\mathscr{U}$ be a P-point and a Q-point and let $\{u_n \subseteq \omega : n \in \omega\}$ be a partition of ω. We have to show that either $u_n \in \mathscr{U}$ for a (unique) $n \in \omega$, or there exists an $x \in \mathscr{U}$ such that for each $n \in \omega$, $x \cap u_n$ has at most one element. If there is a $u_n \in \mathscr{U}$, then we are done. So, assume that for all $n \in \omega$, $u_n \notin \mathscr{U}$. Since $\mathscr{U}$ is a P-point, there exists a $y_0 \in \mathscr{U}$ such that for each $n \in \omega$, $y_0 \cap u_n$ is finite. For $n \in \omega$ let $I_{2n} := y_0 \cap u_n$. Further, let $\{a_i : i \in \omega\} = \omega \setminus \bigcup_{n\in\omega}\{I_{2n} : n \in \omega\}$ and for $n \in \omega$ let $I_{2n+1} := \{a_n\}$. Then $\{I_n : n \in \omega\}$ is a partition of ω into finite pieces. Since $\mathscr{U}$ is a Q-point, there exists a $y_1 \in \mathscr{U}$ such that for each $n \in \omega$, $y_1 \cap I_n$ has at most one element. Now, let $x = y_0 \cap y_1$. Then $x \in \mathscr{U}$ and for each $n \in \omega$, $x \cap u_n$ has at most one element. ⊣

Below, we give a few other characterisations of P-points and Q-points. The proofs are straightforward and are left to the reader.

FACT 10.11. *For every free ultrafilter $\mathscr{U}$, the following conditions are equivalent:*

(a) $\mathscr{U}$ is a P-point.

(b) For every family $\{x_n : n \in \omega\} \subseteq \mathscr{U}$ there is an $x \in \mathscr{U}$ such that for all $n \in \omega$, $x \subseteq^* x_n$ (i.e., $x \setminus x_n$ is finite).

(c) For every family $\{x_n : n \in \omega\} \subseteq \mathscr{U}$ there is a function $f \in {}^\omega\omega$ and a set $x \in \mathscr{U}$ such that for all $n \in \omega$, $x \setminus f(n) \subseteq x_n$.

FACT 10.12. *For every free ultrafilter $\mathscr{U}$, the following conditions are equivalent:*

(a) $\mathscr{U}$ is a Q-point.

(b) For every family $\{x_n : n \in \omega\} \subseteq \mathscr{U}$ there is an $x \in \mathscr{U}$ such that for all $n \in \omega$, $x \cap (\omega \setminus x_n)$ is finite.

There are also characterisations of P-points which are not so obvious:

PROPOSITION 10.13. *For a free ultrafilter $\mathscr{U}$, the following conditions are equivalent:*

(a) $\mathscr{U}$ is a P-point.

(b) For every family $\{x_n : n \in \omega\} \subseteq \mathscr{U}$ there is an $x \in \mathscr{U}$ such that for infinitely many $n \in \omega$, $x \setminus n \subseteq x_n$.

Proof. Since (b)⇒(a) is obvious, we just prove (a)⇒(b): Since $\mathscr{U}$ is a P-point, by FACT 10.11.(c) there exists a function $f \in {}^\omega\omega$ and a set $y \in \mathscr{U}$ such that for all $n \in \omega$, $y \setminus f(n) \in x_n$. Hence, there exists also a function $g \in {}^\omega\omega$ such that $g(0) = 0$ and for all $k \in \omega$ we have $y \setminus g(k+1) \subseteq x_{g(k)}$. Since $\mathscr{U}$ is an ultrafilter, either $y_0 = \bigcup_{k\in\omega} \big[g(2k+1), g(2k+2)\big)$ or $y_1 = \bigcup_{k\in\omega} \big[g(2k), g(2k+1)\big)$ belongs to $\mathscr{U}$. Let $x = y \cap y_\varepsilon$, where $\varepsilon \in \{0,1\}$ is such that $y_\varepsilon \in \mathscr{U}$. Then for every $k \in \omega$ we have $x \setminus g(2k+\varepsilon) = x \setminus g(2k+\varepsilon+1) \subseteq x_{2k+\varepsilon}$. ⊣

P-points and Q-points, and consequently Ramsey ultrafilters, can also be characterised in terms of functions, but before we have to introduce the notion of finite-to-one functions: A function $f \in {}^\omega\omega$ is **finite-to-one** if for every $k \in \omega$, the set $\{n \in \omega : f(n) = k\}$ is finite.

PROPOSITION 10.14. *Let $\mathscr{U}$ be a free ultrafilter.*

(a) $\mathscr{U}$ is a P-point if and only if for every function $f \in {}^\omega\omega$ there exists an $x \in \mathscr{U}$ such that $f|_x$ is constant or finite-to-one.

(b) $\mathscr{U}$ is a Q-point if and only if for every finite-to-one function $f \in {}^\omega\omega$ there exists an $x \in \mathscr{U}$ such that $f|_x$ is one-to-one.

(c) $\mathscr{U}$ is a Ramsey ultrafilter if and only if for every function $f \in {}^\omega\omega$ there exists an $x \in \mathscr{U}$ such that $f|_x$ is constant or one-to-one.

Proof. Let $f \in {}^\omega\omega$ be an arbitrary but fixed function. For $k \in \omega$ define $u_k := \{n \in \omega : f(n) = k\}$. Then $\{u_k : k \in \omega\}$ is a partition of ω. The proof now follows from FACT 10.10 and the following observations (the details are left to the reader):

- For any $x \in [\omega]^\omega$, $f|_x$ is constant *iff* there is a $k \in \omega$ such that $x \subseteq u_k$.
- For any $x \in [\omega]^\omega$, $f|_x$ is finite-to-one *iff* for all $k \in \omega$ we have $x \cap u_k$ is finite.
- The function f is finite-to-one *iff* each u_k is finite.
- For any $x \in [\omega]^\omega$, $f|_x$ is one-to-one *iff* for all $k \in \omega$, $x \cap u_k$ has at most one element. ⊣

The next result shows that ultrafilters, and especially Q-points, must contain quite "sparse" sets.

PROPOSITION 10.15. *For free families $\mathscr{U} \subseteq [\omega]^\omega$ we have:*

(a) If $\mathscr{U}$ is a free ultrafilter, then the family $\{f_x \in {}^\omega\omega : x \in \mathscr{U}\}$ is unbounded.

(b) If $\mathscr{U}$ is a Q-point, then the family $\{f_x \in {}^\omega\omega : x \in \mathscr{U}\}$ is dominating.

Proof. (a) Let $f \in {}^\omega\omega$ be arbitrary. Define $g(0) = \max\{f(0), 1\}$ and for $k \in \omega$ define $g(k+1) := g(k) + f\big(g(k)\big)$. Further, let $x_0 = \big[0, g(0)\big)$, and in general, for $n \in \omega$ let $x_n = \big[g(2n), g(2n+1)\big)$ and $y_n = \big[g(2n+1), g(2n+2)\big)$. Finally, let $x = \bigcup_{n\in\omega} x_n$ and $y = \bigcup_{n\in\omega} y_n$. We leave it as an exercise to the reader to verify that $f_x \not\leq^* f$ and $f_y \not\leq^* f$. Hence, f dominates neither f_x nor f_y. Now, since $\mathscr{U}$ is an ultrafilter, either x or y belongs to $\mathscr{U}$. Hence, f does not dominate the family $\mathscr{B} = \{f_x \in {}^\omega\omega : x \in \mathscr{U}\}$, and since f was arbitrary, $\mathscr{B}$ is unbounded.

(b) Let $g \in {}^\omega\omega$ be arbitrary. Without loss of generality we may assume that g is strictly increasing. For $n \in \omega$ let $I_n = \big[g(2n), g(2n+2)\big)$. Then $\{I_n : n \in \omega\}$ is a partition of ω into finite pieces. Since $\mathscr{U}$ is a Q-point, there exists an $x \in \mathscr{U}$ such that for each $n \in \omega$, $x \cap I_n$ has at most one element which implies that $g <^* f_x$. Hence, f_x dominates g, and since g was arbitrary, the family $\{f_x \in {}^\omega\omega : x \in \mathscr{U}\}$ is dominating. ⊣

As we have seen above (PROPOSITION 10.9), $\mathfrak{p} = \mathfrak{c}$ implies the existence of a Ramsey ultrafilter. On the other hand, one can show that $\mathfrak{d} = \mathfrak{c}$ is not sufficient to prove the existence of Ramsey ultrafilters (see PROPOSITION 25.11). However, as a consequence of the next result, we get that $\mathfrak{d} = \mathfrak{c}$ is sufficient to prove the existence of P-points — which shows that P-points are easier to get than Ramsey ultrafilters (*cf.* RELATED RESULTS 66 & 67).

THEOREM 10.16. $\mathfrak{d} = \mathfrak{c}$ *if and only if every free filter over a countable set which is generated by less than $\mathfrak{c}$ sets can be extended to a P-point. In particular, $\mathfrak{d} = \mathfrak{c}$ implies the existence of P-points.*

Proof. ($\Leftarrow$) Suppose that $\mathscr{E} \subseteq {}^\omega\omega$ is a family of cardinality less than $\mathfrak{c}$. For $f \in \mathscr{E}$ and $n \in \omega$ define

$$x_f = \big\{\langle n, k\rangle \in \omega \times \omega : f(n) < k\big\} \quad \text{and} \quad x_n = \big\{\langle m, k\rangle \in \omega \times \omega : n \leq m\big\},$$

and let

$$\mathscr{C} = \{x_f : f \in \mathscr{E}\} \cup \{x_n : n \in \omega\} \cup \{z \subseteq \omega \times \omega : (\omega \times \omega) \setminus z \text{ is finite}\}.$$

Notice that $|\mathscr{C}| < \mathfrak{c}$ and that each set in $\mathscr{C}$ is an infinite subsets of the countable set $\omega \times \omega$. Moreover, for any finitely many members $y_0, \dots, y_n \in \mathscr{C}$ we have $y_0 \cap \cdots \cap y_n$ is infinite. Now, the family $\mathscr{C}$ generates a free filter over $\omega \times \omega$, which, by assumption, can be extended to a P-point $\mathscr{U} \subseteq [\omega \times \omega]^\omega$. Consider the partition $\{u_n : n \in \omega\}$ of $\omega \times \omega$, where for $n \in \omega$, $u_n := \{n\} \times \omega$. Notice that no u_n (for $n \in \omega$) belongs to $\mathscr{U}$. Since $\mathscr{U}$ is a P-point, there exists a $y \in \mathscr{U}$ such that for all $n \in \omega$, $y \cap u_n$ is finite. Let us define the function $g \in {}^\omega\omega$ by stipulating $g(n) = \bigcup \{k \in \omega : \langle n, k\rangle \in y \cap u_n\}$. Since $y \in \mathscr{U}$, for all $f \in \mathscr{E}$ we have $y \cap x_f$ is infinite. Hence, for every $f \in \mathscr{E}$ there are infinitely many $n \in \omega$ such that $g(n) > f(n)$. In other words, g is not dominated by any function $f \in \mathscr{E}$, which shows that no family of cardinality less than $\mathfrak{c}$ is dominating.

($\Rightarrow$) The proof is by induction using the following

CLAIM. *Suppose that the free filter $\mathscr{F} \subseteq [\omega]^\omega$ is generated by less than $\mathfrak{d}$ sets and let $\{x_n : n \in \omega\} \subseteq \mathscr{F}$. Then there exists $x \in [\omega]^\omega$ such that for all $n \in \omega$, $x \subseteq^* x_n$, and for all $y \in \mathscr{F}$, $x \cap y$ is infinite.*

Proof of Claim. Without loss of generality we may assume that for all $n \in \omega$, $x_{n+1} \subseteq x_n$. For $y \in \mathscr{F}$ define $g_y \in {}^\omega\omega$ by stipulating $g_y(n) = \bigcap(y \cap x_n)$. Notice that the set $y \cap x_n$ is non-empty, and that if $y \subseteq y'$, then for all $n \in \omega$, $g_{y'}(n) \leq g_y(n)$. Now, since $\mathscr{F}$ is generated by less than $\mathfrak{d}$ sets, and since every free ultrafilter generated by less than $\mathfrak{d}$ sets has a basis of less than $\mathfrak{d}$ sets, there exists a function $f \in {}^\omega\omega$ such that for all $y \in \mathscr{F}$ we have $f \not\leq^* g_y$. Finally let

$$x = \bigcup_{n \in \omega} \big(x_n \cap f(n)\big).$$

We leave it to the reader to verify that x has the required properties. $\dashv_{\text{Claim}}$

By the claim and the assumption that $\mathfrak{d} = \mathfrak{c}$ we inductively construct a P-point as follows: Let $\{X_\alpha \subseteq [\omega]^\omega : |X_\alpha| \leq \omega \wedge \alpha \in \mathfrak{c}\}$ be an enumeration of all countable subsets of $[\omega]^\omega$. Let $\mathscr{F}_0$ be any free filter which is generated by less than $\mathfrak{d}$ sets and assume that we have already constructed $\mathscr{F}_\alpha$ for some $\alpha \in \mathfrak{c}$. If $X_\alpha \cup \mathscr{F}_\alpha$ has the finite intersection property, then we use the claim to obtain a set $x_{\alpha+1}$ such that $\{x_{\alpha+1}\} \cup \mathscr{F}_\alpha$ has the finite intersection property and $x_{\alpha+1}$ is a pseudo-intersection of X_α; and let $\mathscr{F}_{\alpha+1}$ be the filter generated by $\mathscr{F}_\alpha$ and $x_{\alpha+1}$. If $X_\alpha \cup \mathscr{F}_\alpha$ does not have the finite intersection property, then let $\mathscr{F}_{\alpha+1} = \mathscr{F}_\alpha$. Further, if $\alpha \in \mathfrak{c}$ is a limit ordinal and for all $\beta \in \alpha$ we have already constructed $\mathscr{F}_\beta$, then let $\mathscr{F}_\alpha = \bigcup_{\beta \in \alpha} \mathscr{F}_\beta$. Finally, let $\mathscr{F} = \bigcup_{\alpha \in \mathfrak{c}} \mathscr{F}_\alpha$. Then $\mathscr{F}$ is a P-point: Firstly, by construction, $\mathscr{F}$ is a filter, and since the free filter $\mathscr{F}_0$ is contained in $\mathscr{F}$, $\mathscr{F}$ is even a free filter. Secondly, for any $x \in [\omega]^\omega$ there exists a $\beta \in \mathfrak{c}$ such that $X_\beta = \{x\}$. Thus, either $x \in \mathscr{F}_{\beta+1}$ or there is a $y \in \mathscr{F}_\beta$ such that $x \cap y$ is finite, which implies that $x^{\mathsf{c}} \in \mathscr{F}_\beta$. Hence, $\mathscr{F}$ is a free ultrafilter. Finally, for every set $\{x_n : n \in \omega\} \subseteq \mathscr{F}$ there exists a

$\gamma \in \mathfrak{c}$ such that $X_\gamma = \{x_n : n \in \omega\}$. Since $X_\gamma \cup \mathscr{F}_\gamma$ has the finite intersection property, there is an $x_{\gamma+1} \in \mathscr{F}_{\gamma+1}$ such that for all $n \in \omega$, $x_{\gamma+1} \subseteq^* x_n$. $\dashv$

Ramsey families and P-families

Below, we give characterisations of Ramsey ultrafilters and P-points in terms of games, which lead to so-called Ramsey families and P-families respectively.

The two *games* we shall consider are infinite and played between two players. Now, a **run** of an infinite two-player game consists of an infinite sequence $\langle x_0, y_0, x_1, y_1, \ldots \rangle$ which is constructed alternately by the two players. More precisely, the first player starts the game with x_0 and the second player responds with y_0, then the first player plays x_1 and the second player responds with y_1, and so on. Of course, in order to get a proper game we have to introduce also some rules defining legal moves and telling which player wins a particular run of the game.

Before we introduce some further game-theoretical notions, let us illustrate the notion of rules by the following infinite two-player game, played between Death and the Maiden.

Let $\mathscr{E}$ be an arbitrary free family. Associated with $\mathscr{E}$ we define two quite similar games, denoted $\mathcal{G}_{\mathscr{E}}$ and $\mathcal{G}^*_{\mathscr{E}}$, between two players, say Death and the Maiden.

In the game $\mathcal{G}_{\mathscr{E}}$, the Maiden always plays members of $\mathscr{E}$ and then Death responds with an element of Maiden's move. Thus, a run of $\mathcal{G}_{\mathscr{E}}$ can be illustrated as follows:

$$\mathcal{G}_{\mathscr{E}}: \quad \begin{tikzcd}[column sep=small]
\textsc{Maiden} & x_0 \arrow[dr, "\ni"] & \supseteq & x_1 \arrow[dr, "\ni"] & \supseteq & x_2 \arrow[dr, "\ni"] & \supseteq & \\
& & & & & & & \ldots \\
\textsc{Death} & & a_0 \arrow[uur] & < & a_1 \arrow[uur] & < & a_2 \arrow[ur, dash] & <
\end{tikzcd}$$

More formally, the rules for $\mathcal{G}_{\mathscr{E}}$ are as follows: For each $i \in \omega$, $x_i \in \mathscr{E}$ and $a_i \in x_i$. Furthermore, we require that for each $i \in \omega$, $x_{i+1} \subseteq x_i$ and $a_i < a_{i+1}$. Finally, Death wins the game $\mathcal{G}_{\mathscr{E}}$ if and only if $\{a_i : i \in \omega\}$ belongs to the family $\mathscr{E}$.

In the game $\mathcal{G}^*_{\mathscr{E}}$, Death has slightly more freedom, since he can play now finite sequences instead of just singletons. A run of $\mathcal{G}^*_{\mathscr{E}}$ can be illustrated as follows:

$$\mathcal{G}^*_{\mathscr{E}}: \quad \begin{tikzcd}[column sep=small]
\textsc{Maiden} & x_0 \arrow[dr, "\supseteq"] & \supseteq & x_1 \arrow[dr, "\supseteq"] & \supseteq & x_2 \arrow[dr, "\supseteq"] & \supseteq & \\
& & & & & & & \ldots \\
\textsc{Death} & & s_0 \arrow[uur] & & s_1 \arrow[uur] & & s_2 \arrow[ur, dash] &
\end{tikzcd}$$

Again, the sets x_i played by the Maiden must belong to the free family $\mathscr{E}$ and each finite set s_i played by Death must be a subset of the corresponding

x_i. Furthermore, for each $i \in \omega$ we require that $x_{i+1} \subseteq \big(x_i \setminus \bigcup_{j \leq i} s_j\big)$. Notice that the finite sets s_i may be empty. Finally, DEATH wins the game $\mathcal{G}^*_{\mathscr{E}}$ if and only if $\bigcup\{s_i : i \in \omega\}$ belongs to the family $\mathscr{E}$.

Now we define the notion of a strategy for the MAIDEN. Roughly speaking, a **strategy** for the MAIDEN is a "rule" that tells her how to play, for each $n \in \omega$, her n^{th} move x_n, given DEATH' previous moves $m_0, \dots, m_n$. In fact, a strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{E}}$ is a certain mapping from $\operatorname{seq}(\mathscr{E} \cup \omega)$ to $\mathscr{E}$. Intuitively, with respect to $\mathcal{G}_{\mathscr{E}}$, a strategy σ for the MAIDEN works as follows: The MAIDEN starts playing $x_0 \in \mathscr{E}$, where $x_0 = \sigma(\emptyset)$ and then DEATH responds by playing an element $a_0 \in x_0$. Then the MAIDEN plays $x_1 = \sigma(x_0, a_0)$, which — by the rules of the game — is a set in $\mathscr{E}$ and a subset of x_0, and DEATH responds with an element $a_1 \in x_1$ where $a_1 > a_0$. In general, for positive integers n, $x_n = \sigma(x_0, a_0, \dots, x_{n-1}, a_{n-1})$, where $x_n \in \mathscr{E}$, $x_n \subseteq x_{n-1}$, $a_0, \dots, a_{n-1}$ are the moves of DEATH, and $x_0, \dots, x_{n-1}$ are the previous moves of the MAIDEN.

A strategy σ for the MAIDEN is a **winning strategy** if, whenever the MAIDEN follows the strategy σ, she wins the game — no matter how sophisticated DEATH plays. For example, σ is a winning strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{E}}$, if whenever $\{a_n : n \in \omega\} \subseteq \omega$ is such that $a_0 \in \sigma(\emptyset)$ and for all $n \in \omega$, $a_n < a_{n+1}$ and $a_{n+1} \in \sigma(x_0, a_0, \dots, x_{n+1})$, then $\{a_n : n \in \omega\} \notin \mathscr{E}$.

Now, a free family $\mathscr{E}$ is called a **Ramsey family** if the MAIDEN has no winning strategy in the game $\mathcal{G}_{\mathscr{E}}$. In other words, no matter how sophisticated her strategy is, if $\mathscr{E}$ is a Ramsey family, then DEATH can win the game. Ramsey families will play an important role in the investigation of Mathias forcing notions (see Chapter 24).

Furthermore, a free family $\mathscr{E}$ is called a **P-family** if the MAIDEN has no winning strategy in the game $\mathcal{G}^*_{\mathscr{E}}$. P-families will play an important role in the investigation of restricted Silver forcing. In fact, in Chapter 22 it will be shown that Silver forcing restricted to a P-family (called Silver-like forcing) has the same combinatorial properties as unrestricted Silver forcing and as Grigorieff forcing, which is Silver forcing restricted to a P-point.

Obviously, the family $[\omega]^\omega$ is a Ramsey family and every Ramsey family is also a P-family. Now, the reader might guess that $[\omega]^\omega$ is not the only example and that there must be some relation between Ramsey families and Ramsey ultrafilters, as well as between P-families and P-points; this is indeed the case:

THEOREM 10.17. *For free ultrafilters $\mathscr{U} \subseteq [\omega]^\omega$ we have:*

(a) $\mathscr{U}$ is a Ramsey ultrafilter if and only if $\mathscr{U}$ is a Ramsey family.

(b) $\mathscr{U}$ is a P-point if and only if $\mathscr{U}$ is a P-family.

Proof. (a) We have to show that $\mathscr{U} \subseteq [\omega]^\omega$ is a Ramsey ultrafilter *iff* whenever the MAIDEN plays the game $\mathcal{G}_{\mathscr{U}}$ by following a strategy, DEATH can win.

($\Leftarrow$) Under the assumption that the free ultrafilter $\mathscr{U}$ is not Ramsey we construct a winning strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{E}}$. If $\mathscr{U}$ is not a Ramsey ultrafilter, then, by PROPOSITION 10.6, there exists a set $\{x_n : n \in$

$\omega\} \subseteq \mathscr{U}$ such that for each function $f \in {}^\omega\omega$ with $f(0) \in x$ and $f(n+1) \in x_{f(n)}$ we have $f[\omega] \notin \mathscr{U}$. Let $\sigma(\emptyset) := x_0$, and for $n \in \omega$ let $\sigma(x_0, a_0, \dots, x_n, a_n) := x_{a_n}$. By the rules of $\mathcal{G}_{\mathscr{U}}$, $a_{n+1} \in x_{a_n}$. Define $f \in {}^\omega\omega$ by stipulating $f(n) = a_n$. Then $f(0) \in x_0$ and for all $n \in \omega$ we have $f(n+1) \in x_{f(n)}$, and therefore $\{f(n) : n \in \omega\} \notin \mathscr{U}$. Thus, $\{a_n : n \in \omega\} \notin \mathscr{U}$, which shows that DEATH loses the game (*i.e.*, σ is a winning strategy for the MAIDEN), and consequently, $\mathscr{U}$ is not a Ramsey family.

($\Rightarrow$) Under the assumption that the free ultrafilter $\mathscr{U}$ is Ramsey we show that no strategy for the MAIDEN is a winning strategy. Let σ be any strategy for the MAIDEN, let $x_\emptyset := \sigma(\emptyset)$, and for $s = \{c_0, \dots, c_n\} \in \operatorname{fin}(\omega)$ let

$$x_s = \begin{cases} \sigma(x_0, c_0, \dots, x_n, c_n) & \text{if } \forall k \leq n (c_k \in x_k), \\ \omega & \text{otherwise.} \end{cases}$$

Notice that in the first case, $\sigma(x_0, c_0, \dots, x_n, c_n) = x_{n+1}$. If $\mathscr{U}$ is a Ramsey ultrafilter, then $\mathscr{U}$ is happy. Thus, there exists an $x \in \mathscr{U}$ such that $x \subseteq x_\emptyset$ and $x \setminus \bar{s}^+ \subseteq x_s$ whenever $\bar{s} \in x$. In particular, if $x = \{a_n : n \in \omega\}$ with $a_n < a_{n+1}$ (for all $n \in \omega$), then $a_0 \in x_0$ and for all $n \in \omega$, $x \setminus \{a_0, \dots, a_n\} = \{a_{n+1}, a_{n+2}, \dots\} \subseteq x_{\{a_0, \dots, a_n\}} = x_{n+1}$. Hence, for all $n \in \omega$ we have $a_n \in x_n$. In particular, whenever the MAIDEN follows the strategy σ, DEATH wins the game by playing the sequence $\langle a_n : n \in \omega \rangle$. So, σ is not a winning strategy for the MAIDEN, and since σ was arbitrary, the MAIDEN does not have a winning strategy.

(b) The proof is similar to that of (a), *i.e.*, we show that the MAIDEN has a winning strategy in the game $\mathcal{G}^*_{\mathscr{U}}$ *iff* the free ultrafilter $\mathscr{U}$ is not a P-point.

($\Leftarrow$) Suppose that $\mathscr{U}$ is not a P-point. Then, by FACT 10.11.(b), there exists a set $\{y_n : n \in \omega\} \subseteq \mathscr{U}$ such that whenever $y \in [\omega]^\omega$ has the property that for all $n \in \omega$, $y \setminus y_n$ is finite, then $y \notin \mathscr{U}$. Let $\sigma(\emptyset) := y_0$ (*i.e.*, $x_0 = y_0$), and for any $k \in \omega$ and $\{s_0, \dots, s_k\} \subseteq \operatorname{fin}(\omega)$ let $\sigma(x_0, s_0, \dots, x_k, s_k) := \bigcap_{i \leq k} y_i \setminus \bigcup_{i \leq k} s_i$. If the MAIDEN follows that strategy σ and the sequence $\langle s_k : k \in \omega \rangle$ represents the moves of DEATH, then for all $n \in \omega$ we have $\left(\bigcup_{k \in \omega} s_k\right) \setminus x_n$ is finite. Hence, $\bigcup_{k \in \omega} s_k \notin \mathscr{U}$, which shows that DEATH loses the game, or in other words, σ is a winning strategy for the MAIDEN.

($\Rightarrow$) Under the assumption that $\mathscr{U}$ is a P-point we show that no strategy for the MAIDEN is a winning strategy. Let σ be any strategy for the MAIDEN. We have to show that DEATH can win. Define X_n as the family of sets played by the MAIDEN in her first $n+1$ moves, assuming that she is following the strategy σ and DEATH plays in his first n moves only sets $s_k \subseteq n$ (for $k < n$). More formally, $x_0 = \sigma(\emptyset)$, and for positive integers $k \leq n$, $x_k \in X_n$ *iff* there are $s_0, \dots, s_{k-1} \subseteq n$ such that for all $i < k$, $s_i \subseteq x_i \cap n^+$, where $x_{i+1} = \sigma(x_0, s_0, \dots, x_i, s_i)$. Clearly, for every $n \in \omega$, X_n is finite, and since $\mathscr{U}$ is an ultrafilter, $y_n := \bigcap X_n$ belongs to $\mathscr{U}$. Moreover, since $\mathscr{U}$ is a P-point, by FACT 10.11.(c) there is a set $y \in \mathscr{U}$ and a strictly increasing function $f \in {}^\omega\omega$ such that for all $n \in \omega$, $y \setminus f(n) \subseteq y_n$. Let $k_0 := f(0)$, and in general, for $n \in \omega$ let $k_{n+1} := f(k_n)$. Since $\mathscr{U}$ is an ultrafilter, either

$$y_0 = \bigcup_{n\in\omega} \big[k_{2n}, k_{2n+1}\big) \ \text{ or } \ y_1 = \omega \setminus y_0$$

belongs to $\mathscr{U}$. Without loss of generality we may assume that $y_1 \in \mathscr{U}$, in particular, $y_1 \cap y \in \mathscr{U}$. Consider the run

$$\langle x_0, s_0, x_1, s_1, \dots \rangle$$

of the game $\mathcal{G}^*_{\mathscr{U}}$, where the MAIDEN plays according to the strategy σ and DEATH plays

$$s_n = \begin{cases} \big[k_{2j+1}, k_{2j+2}\big) \cap y & \text{if } n = k_{2j} \text{ (for some } j \in \omega), \\ \emptyset & \text{otherwise.} \end{cases}$$

It is clear that the MAIDEN loses the game (*i.e.*, $\bigcup_{n\in\omega} s_n \in \mathscr{U}$). It remains to check that the moves of DEATH are legal (*i.e.*, satisfy the rules of the game $\mathcal{G}^*_{\mathscr{U}}$). Firstly notice that for all positive integers j, $s_{k_{2j-2}} \subseteq k_{2j}$. Thus, if $n = k_{2j}$, then for all $k < n$ we have $s_k \subseteq n$. Now, if $n = k_{2j}$ for some $j \in \omega$, then $s_n = s_{k_{2j}} = \big[k_{2j+1}, k_{2j+2}\big) \cap y$. Further, we have

$$y \setminus k_{2j+1} = y \setminus f(k_{2j}) \subseteq y_{k_{2j}} = \bigcap \big\{x_0, \dots, x_{k_{2j}}\big\},$$

and in particular, for $n = k_{2j}$ we get $s_n = s_{k_{2j}} \subseteq x_{k_{2j}} = x_n$. Hence, for all $n \in \omega$, $s_n \subseteq x_n$. ⊣

Roughly speaking, Ramsey families are a kind of generalised Ramsey ultrafilters and P-families are a kind of generalised P-points.

Let us turn back to happy families and let us compare them with Ramsey families. At a first glance, happy families and Ramsey families look very similar. However, it turns out that the conditions for a Ramsey family are slightly stronger than for a happy family. This is because in the definition of happy families we require that they contain sets which diagonalise certain subfamilies having the finite intersection property. On the other hand, a strategy of the MAIDEN in the game $\mathcal{G}_{\mathscr{E}}$ can be quite arbitrary: Even though the sets played by her in a run of $\mathcal{G}_{\mathscr{E}}$ form a decreasing sequence, the family of possible moves of the MAIDEN does not necessarily have the finite intersection property. Of course, by restricting the set of strategies the MAIDEN can choose from, we could make sure that all happy families are Ramsey. In fact we just have to require that all the moves of the MAIDEN — no matter what DEATH is playing — belong to some family which has the finite intersection property. However, the definition of Ramsey families given above has the advantage that the MAIDEN is able — by a winning strategy — to defeat DEATH in the game $\mathcal{G}_{\mathscr{E}}$ even in some cases when $\mathscr{E}$ is happy (see PROPOSITION 10.19).

Below, we show first that every Ramsey family is happy, and then we show that there are happy families which are not even P-families. Thus, Ramsey families are smaller "clans" (*i.e.*, families who originate from the same family and have the same name) than happy families.

FACT 10.18. *Every Ramsey family is happy.*

Proof. Let $\mathscr{E}$ be a free family which is not happy. Thus, there is exists a set $\mathscr{C} = \{y_s : s \in \mathrm{fin}(\omega)\} \subseteq \mathscr{E}$ such that $\mathrm{fil}(\mathscr{C}) \subseteq \mathscr{E}$ but no $y \in \mathscr{E}$ diagonalises $\mathscr{A}$. Let $\sigma(\emptyset) := x_\emptyset$ and for $n \in \omega$ and $s = \{a_0, \ldots, a_n\} \in \mathrm{fin}(\omega)$ let $\sigma(x_0, a_0, \ldots, x_n, a_n) := \bigcap_{s' \subseteq s} y_s$. It is not hard to verify that in the game $\mathcal{G}_{\mathscr{E}}$, σ is a winning strategy for the MAIDEN. ⊣

By PROPOSITION 10.5 we know that every *mad* family induces a happy family. This type of happy families provides examples of happy families which are not Ramsey families, in fact, which are not even P-families.

PROPOSITION 10.19. *Not every happy family is Ramsey; moreover, not every happy family is a P-family.*

Proof. It is enough to construct a happy family which is not a P-family: Let $\{t_k : k \in \omega\}$ be an enumeration of $\bigcup_{n\in\omega} {}^n\omega$ such that for all $i, j \in \omega$, $t_i \subseteq t_j$ implies $i \leq j$, in particular, $t_0 = \emptyset$. For functions $f \in {}^\omega\omega$ define the set $x_f \in [\omega]^\omega$ by stipulating

$$x_f := \{k \in \omega : \exists n, i, j \in \omega \left(f|_n = t_i \wedge f|_{n+1} = t_j \wedge i \leq k < j \wedge t_i \subseteq t_k\right)\}.$$

Obviously, for any distinct functions $f, g \in {}^\omega\omega$, $x_f \cap x_g$ is finite (compare with the sets constructed in the proof of PROPOSITION 8.6). Now, let $\mathscr{A}_0 := \{x_f : f \in {}^\omega\omega\}$. Then $\mathscr{A}_0 \subseteq [\omega]^\omega$ is a set of pairwise almost disjoint sets which can be extended to a *mad* family, say $\mathscr{A}$. Recall that by PROPOSITION 10.5, $\mathscr{F}^+_{\mathscr{A}}$ is a happy family.

We show that $\mathscr{F}^+_{\mathscr{A}}$ is not a P-family: Let $k_0 := 0$ and let $x_0 := \omega$ be the first move of the MAIDEN, and let s_0 be DEATH' response. In general, if s_n is the n^{th} move of DEATH, then the MAIDEN chooses k_{n+1} such that $k_{n+1} \geq \max(s_n)$, $|t_{k_{n+1}}| = n + 1$, and $t_{k_n} \subseteq t_{k_{n+1}}$, and then she plays

$$x_{n+1} = \{i \in \omega : t_{k_{n+1}} \subseteq s_i\}.$$

Obviously, for every $n \in \omega$ we have $x_{n+1} \subsetneq x_n$. Moreover, all moves of the MAIDEN are legal:

CLAIM. *For every $n \in \omega$, $x_n \in \mathscr{F}^+_{\mathscr{A}}$.*

Proof of Claim. Firstly, for every $n \in \omega$, x_n has infinite intersection with infinitely many members of $\mathscr{A}_0$. Indeed, $x_n \cap x_f$ is infinite whenever $f|_n = t_{k_n}$. Secondly, for every $z \in \mathscr{F}_{\mathscr{A}}$ there are finitely many $y_0, \ldots, y_k \in \mathscr{A}$ such that $(y_0 \cup \ldots \cup y_k)^{\mathsf{c}} \subseteq^* z$. Now, for x_n let $x_f \in \mathscr{A}_0 \setminus \{y_0, \ldots, y_k\}$ such that $x_f \cap x_n$ is infinite. Then, since $x_f \cap (y_0 \cup \ldots \cup y_k)$ is finite, $x_f \subseteq^* z$. Hence, $x_n \cap z$ is infinite which shows that $x_n \in\in \mathscr{F}^+_{\mathscr{A}}$. ⊣$_{\text{Claim}}$

By the MAIDEN's strategy, $\bigcup_{n\in\omega} t_{k_n} = f$ for some particular function $f \in {}^\omega\omega$. Moreover, $\bigcup_{n\in\omega} s_n \subseteq x_f \in \mathscr{A}_0$, and since subsets of members of $\mathscr{A}_0$ do not belong to $\mathscr{F}^+_{\mathscr{A}}$, $\bigcup_{n\in\omega} s_n \notin \mathscr{F}^+_{\mathscr{A}}$. Hence, DEATH loses the game, no matter what he is playing, which shows that the MAIDEN has a winning strategy in the game $\mathcal{G}^*_{\mathscr{F}^+_{\mathscr{A}}}$. In other words, the happy family $\mathscr{F}^+_{\mathscr{A}}$ is not a P-family. ⊣

Notes

Happy families and Ramsey ultrafilters. Happy families were introduced by Mathias [8] in order to investigate the Ramsey property as well as Ramsey ultrafilters. Furthermore, happy families are closely related to *Mathias forcing* — also introduced in [8] — which will be discussed in Chapter 24. FACT 10.3 and PROPOSITION 10.5 are taken from Mathias [8, p. 61 ff.]. PROPOSITION 10.6 is due to Mathias [8, Proposition 0.8] and the characterisation of Ramsey ultrafilters (*i.e.*, PROPOSITION 10.7 and FACT 10.8) is taken from Bartoszyński and Judah [1, Theorem 4.5.2] and Booth [3, Theorem 4.9] (according to Booth [3, p. 19], most of [3, Theorem 4.9] is due to Kunen).

On P-points. A point x of a topological space X is called a ***P*-point** if every intersection of countably many open sets containing x, contains an open set containing x. Now, the ultrafilters we called P-points are in fact the P-points of the topological space $\beta\omega \setminus \omega$ (defined on page 222). The existence of P-points of the space $\beta\omega \setminus \omega$ cannot be shown in ZFC (see RELATED RESULT 68). However, by THEOREM 10.16, which is due to Ketonen [6] (see also Bartoszyński and Judah [1, Theorem 4.4.5]), it follows that P-points exist if we assume CH — which was first proved by Rudin [10].

Ramsey families and P-families. Ramsey families and P-families were first introduced and studied by Laflamme in [7], where the filters associated to a Ramsey family are called *$+$-Ramsey filters*, and the filters associated to a P-family are called *$P+$-filters*. However, THEOREM 10.17 is due to Galvin and Shelah (see Bartoszyński and Judah [1, Theorems 4.5.3 & 4.4.4]), and PROPOSITION 10.19 is a generalisation of Halbeisen [4, Proposition 6.2].

Related Results

64. *On the existence of Ramsey ultrafilters.* Mathias showed that under CH, every happy family contains a Ramsey ultrafilter (see Mathias [8, Proposition 0.11]). In particular, this shows that Ramsey ultrafilters exist if we assume CH (according to Booth [3, p. 23], this was first shown by Galvin). However, by PROPOSITION 10.9 we know that $\mathfrak{p} = \mathfrak{c}$ is sufficient for the existence of Ramsey ultrafilters. With Martin's Axiom in place of $\mathfrak{p} = \mathfrak{c}$, this result is due to Booth [3, Theorem 4.14]. Furthermore, Keisler showed that if we assume CH, then there are $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters (see Blass [2, p. 148]). Finally, by combining the proofs of Keisler and Booth, Blass [2, Theorem 2] showed that $\mathfrak{t} = \mathfrak{c}$ (for $\mathfrak{t}$ see Chapter 8 | RELATED RESULT 52) is enough to get $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters (see PROPOSITION 13.9 for a slightly more general result). On the other hand, we shall see in Chapter 25 that the existence of Ramsey ultrafilters is independent of ZFC (see also Chapter 21 | RELATED RESULT 114).

65. *There may exist a unique Ramsey ultrafilter.* We have seen above that we can have infinitely many Ramsey ultrafilters or none. So, it is natural to ask whether it is also consistent with ZFC that there exists, up to permutations of ω, a unique Ramsey ultrafilter. Now, Shelah [12, VI §5] proved that this is indeed the case.

Moreover, it is even consistent with ZFC that there are, up to permutations of ω, exactly two Ramsey ultrafilters (see Shelah [12, p. 335]).

66. *There may be P-points which are not Ramsey.* Booth [3, Theorem 4.12] showed that if we assume CH (or Martin's Axiom), there are P-points which are not Ramsey (*i.e.*, which are not Q-points). For examples of P-points which are not Q-points see PROPOSITION 25.11.

67. *On the existence of Q-points.* Mathias [Proposition 10][9] showed that $\mathfrak{d} = \omega_1$ implies the existence of Q-points. Recall that by PROPOSITION 10.9, $\mathfrak{p} = \mathfrak{c}$ implies the existence of Ramsey ultrafilters; in particular the existence of P-points and Q-points. Thus, the existence of Q-points is consistent with $\mathfrak{d} > \omega_1$. However, if there are just P-points but no Q-points, then we must have $\mathfrak{d} > \omega_1$.

68. *On the existence of P-points.* P-points were studied by Rudin [10], who proved, assuming CH, that they exist and that any of them can be mapped to any other by a homeomorphism of $\beta\omega \setminus \omega$ onto itself. In particular, CH implies the existence of P-points. Of course, this follows from the fact that CH implies the existence of Ramsey ultrafilters, and Ramsey ultrafilters are P-points. However, as we have seen above, the converse is not true (and there are models of ZFC in which there are P-points but no Ramsey ultrafilters). Now, it is natural to ask whether there are models of ZFC in which there are no P-points. Let us consider how models of ZFC are constructed in which there are no Ramsey ultrafilters. In order to construct a model of ZFC in which there are no Ramsey ultrafilters, one usually makes sure that the model does not contain any Q-points (see for example the proof of PROPOSITION 25.11). To some extent, P-points are weaker than Q-points and therefore it is more difficult to construct a model in which there are no P-points. However, Shelah constructed such a model in [11] (see also Shelah [12, VI §4], Wimmers [14], or Bartoszyński and Judah [1, 4.4.7]). Moreover, like for Ramsey ultrafilters, it is consistent with ZFC that, up to up permutations of ω, there exists a single P-point (see Shelah [12, XVIII §4]).

69. *Simple P_κ-points.* For any regular uncountable cardinal κ, a free ultrafilter $\mathscr{U} \subseteq [\omega]^\omega$ is called a **simple P_κ-point** if $\mathscr{U}$ is generated by an almost decreasing (*i.e.*, modulo finite) κ-sequence of infinite subsets of ω. Clearly, every simple P_κ-point is a P-point. It is conjectured that the existence of both, a simple P_{ω_1}-point and a P_{ω_2}-point, is consistent with ZFC. (For weak P-points and other points in $\beta\omega \setminus \omega$ see for example van Mill [13, Section 4].)

70. *Rapid and unbounded filters.* A free filter $\mathscr{F} \subseteq [\omega]^\omega$ is called a **rapid filter** if for each $f \in {}^\omega\omega$ there exists an $x \in \mathscr{F}$ such that for all $n \in \omega$, $|x \cap f(n)| \leq n$. By definition, if $\mathscr{F}$ is rapid filter, then $\{f_x : x \in \mathscr{F}\}$ is a dominating family. It is not hard to verify that all Q-points are rapid (see FACT 25.10), but the converse does not hold (see for example Bartoszyński and Judah [1, Lemma 4.6.3] and in particular the remark after the proof of that lemma). However, like for P-points or Q-points, the existence of rapid filter is independent of ZFC (see PROPOSITION 25.11). A weaker notion than that of rapid filters is the notion of unbounded filters, where a free filter $\mathscr{F} \subseteq [\omega]^\omega$ is called **unbounded** if the family $\{f_x : x \in \mathscr{F}\}$ is unbounded. Since every free ultrafilter induces an unbounded family (*cf.* PROPOSITION 10.15.(a)), unbounded filters always exist. Furthermore, one can show that every unbounded filter induces a set which does

not have the Ramsey property (for a slightly more general result see Judah [5, Fact 8]).

71. *Another characterisation of Ramsey ultrafilters.* Let $\mathscr{U} \subseteq [\omega]^\omega$ be an ultrafilter. The game $\mathcal{G}'_{\mathscr{U}}$ is defined as follows.

$$\mathcal{G}'_{\mathscr{U}}: \quad \begin{array}{lcccccccc} \text{Maiden} & (a_0,x_0) & & (a_1,x_1) & & (a_2,x_2) & & & \\ & & \searrow \quad \nearrow & & \searrow \quad \nearrow & & \searrow \quad \nearrow & & \cdots \\ \text{Death} & & y_0 & & y_1 & & y_2 & & \end{array}$$

The sets y_i and x_i played by Death and the Maiden respectively must belong to the ultrafilter $\mathscr{U}$, and for each $i \in \omega$, a_{i+1} must be a member of y_i. Furthermore, for each $i \in \omega$ we require that $x_{i+1} \subseteq y_i \subseteq x_i$ and that $a_i < \min(x_i)$. Finally, the Maiden wins the game $\mathcal{G}'_{\mathscr{U}}$ if and only if $\{a_i : i \in \omega\}$ does *not* belong to the ultrafilter $\mathscr{U}$.
In 2002, Claude Laflamme showed me that $\mathscr{U}$ is a Ramsey ultrafilter if and only if the Maiden has no winning strategy in the game $\mathcal{G}'_{\mathscr{U}}$.

72. *On strongly maximal almost disjoint families*.* A *mad* family $\mathscr{A}$ is called **strongly maximal almost disjoint** if given countably many members of $\mathscr{F}^+_{\mathscr{A}}$, then there is a member of $\mathscr{A}$ that meets each of them in an infinite set.
For a free family $\mathscr{E}$, consider the following game: The moves of the Maiden are members of $\mathscr{E}$ and Death responses like in the game $\mathcal{G}_{\mathscr{E}}$. Furthermore, Death wins if and only if the set of integers played by Death belongs to $\mathscr{A}$, but has infinite intersection with each set played by the Maiden.
If $\mathscr{A}$ is a *mad* family, then obviously, in the game described above, the Maiden has a winning strategy if and only if $\mathscr{A}$ is not strongly maximal almost disjoint, which motivates the following question: Is it the case that for a *mad* family $\mathscr{A}$, $\mathscr{F}^+_{\mathscr{A}}$ is Ramsey if and only if $\mathscr{A}$ is strongly maximal almost disjoint?

References

1. Tomek Bartoszyński and Haim Judah, ***Set Theory: on the structure of the real line***, A. K. Peters, Wellesley, 1995.
2. Andreas Blass, *The Rudin-Keisler ordering of p-points*, ***Transactions of the American Mathematical Society***, vol. 179 (1973), 145–166.
3. David Booth, *Ultrafilters on a countable set*, ***Annals of Mathematical Logic***, vol. 2 (1970), 1–24.
4. Lorenz Halbeisen, *A playful approach to Silver and Mathias forcings*, *in* ***Foundations of the Formal Sciences V: Infinite Games*** (Stefan Bold, Benedikt Löwe, Thoralf Räsch, and Johan van Benthem, eds.), Papers of a Conference held in Bonn, November 26–29, 2004, [Studies in Logic, vol. 11], College Publications, London, 2007, pp. 123–142.
5. Jaime I. Ihoda, *Unbounded filters on ω*, *in* ***Logic Colloquium '87, Proceedings of the Colloquium held in Granada, Spain, July 20–25, 1987*** (H.-D. Ebbinghaus, J. Fernandez-Prida, M. Garrido, D. Lascar, and M. Rodriguez Artalejo, eds.), [Studies in Logic and the Foundations of Mathematics 129], North-Holland, Amsterdam, 1989, pp. 105–115.

6. Jussi A. Ketonen, *On the existence of P-points in the Stone-Čech compactification of the integers*, ***Fundamenta Mathematicae***, vol. 92 (1976), 91–94.
7. Claude Laflamme, *Filter games and combinatorial properties of strategies*, in ***Set Theory*** (Tomek Bartoszyński and Marion Scheepers, eds.), Contemporary Mathematics, vol. 192, American Mathematical Society, Providence, RI, 1996, pp. 51–67.
8. Adrian Richard David Mathias, *Happy families*, ***Annals of Mathematical Logic***, vol. 12 (1977), 59–111.
9. ———, $0^{\#}$ *and the p-point problem*, in ***Higher set theory,*** *Proceedings, Oberwolfach, Germany, April 13–23, 1977* (Gert H. Müller and Dana S. Scott, eds.), [Lecture Notes in Mathematics 669], Springer-Verlag, Berlin, 1978, pp. 375–384.
10. Walter Rudin, *Homogeneity problems in the theory of Čech compactifications*, ***Duke Mathematical Journal***, vol. 23 (1956), 409–420.
11. Saharon Shelah, ***Proper Forcing***, [Lecture Notes in Mathematics 940], Springer-Verlag, Berlin, 1982.
12. ———, ***Proper and Improper Forcing***, [Perspectives in Mathematical Logic], Springer-Verlag, Berlin, 1998.
13. Jan van Mill, *An introduction to* $\beta\omega$, in ***Handbook of Set-Theoretic Topology*** (K. Kunen and J.E. Vaughan, eds.), North-Holland, Amsterdam, 1990, pp. 503–567.
14. Edward L. Wimmers, *The Shelah P-point independence theorem*, ***Israel Journal of Mathematics***, vol. 43 (1982), 28–48.

11

Coda: A Dual Form of Ramsey's Theorem

Musicians wanted compositions to end on a perfect consonance, because they correctly say that the perfection of anything depends upon and is judged by its end. Since they found that among consonances no greater perfection could be found than in the octave, they made it a fixed rule that each composition should terminate on the octave or unison and no other interval.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

In this chapter we shall present some results in dual Ramsey Theory, *i.e.*, Ramsey type results dealing with partitions of ω. The word "dual" is motivated by the following fact: Each infinite subset of ω corresponds to the *image* of an *injective* function from ω into ω, whereas each infinite partition of ω corresponds to the set of *pre-images* of elements of ω of a *surjective* function from ω onto ω. Similarly, n-element subsets of ω correspond to images of injective functions from n into ω, whereas n-block partitions of ω correspond to pre-images of surjective functions from ω onto n. Thus, to some extent, subsets of ω and partitions of ω are dual to each other.

The Hales-Jewett Theorem

Since we introduced RAMSEY'S THEOREM in Chapter 2, we have used different forms of this powerful combinatorial tool in various applications. However, RAMSEY'S THEOREM is neither the only nor the earliest Ramsey-type result. In fact, the following theorem is one of the earliest results in Ramsey Theory.

THEOREM 11.1 (VAN DER WAERDEN). *For any positive integers r and n, there is a positive integer N such that for every r-colouring of the set $\{0,1,\ldots,N\}$ we find always a monochromatic (non-constant) arithmetic progression of length n.*

Instead of a proof, let us consider VAN DER WAERDEN'S THEOREM from a more combinatorial point of view: Firstly, for some positive integer l, identify the integers $a \in [0, n^l)$ with the l-tuples $\langle a_0 \ \ldots \ a_{l-1}\rangle$ formed from the base-n representation of a, i.e., $a = \sum_{i\in l} a_i n^i$ and for all $i \in l$, $0 \leq a_i < n$. Concerning arithmetic progressions, notice that for example the l-tuples

$$\begin{array}{lllllllllll}
\langle a_0 & \ldots & a_{i-1} & 0 & a_{i+1} & \ldots & a_{j-1} & 0 & a_{j+1} & \ldots & a_{l-1}\rangle \\
\langle a_0 & \ldots & a_{i-1} & 1 & a_{i+1} & \ldots & a_{j-1} & 1 & a_{j+1} & \ldots & a_{l-1}\rangle \\
\langle a_0 & \ldots & a_{i-1} & 2 & a_{i+1} & \ldots & a_{j-1} & 2 & a_{j+1} & \ldots & a_{l-1}\rangle \\
 & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & \\
\langle a_0 & \ldots & a_{i-1} & n-2 & a_{i+1} & \ldots & a_{j-1} & n-2 & a_{j+1} & \ldots & a_{l-1}\rangle \\
\langle a_0 & \ldots & a_{i-1} & n-1 & a_{i+1} & \ldots & a_{j-1} & n-1 & a_{j+1} & \ldots & a_{l-1}\rangle
\end{array}$$

correspond to an arithmetic progression of length n with common difference $n^i + n^j$. Let us call for the moment arithmetic progressions of length n of that type *special arithmetic progressions*. Notice that not every arithmetic progression of length n is special. However, if we could show that for all positive integers n and r there exists a positive integer l such that for every r-colouring of $[0, n^l)$ we find a monochromatic special arithmetic progression, then this would obviously prove VAN DER WAERDEN'S THEOREM.

Now, identify the set of l-tuples $\langle a_0 \ \ldots \ a_{l-1}\rangle$ with the set of functions f from l to n, denoted ${}^l n$, by stipulating $f(k) = a_k$ (for all $k \in l$). Consequently, we can identify every r-colouring of $[0, n^l)$ with an r-colouring of ${}^l n$. Notice that for a non-empty set $s \subseteq l$ and a function $g : l \setminus s \to r$, the set $\big\{f \in {}^l n : f|_{l\setminus s} = g \wedge f|_s \text{ is constant}\big\}$ corresponds to a special arithmetic progression. In the example of a special arithmetic progression given above we have $s = \{i, j\}$ and $g(m) = a_m$ (for all $m \in l \setminus s$). Hence, in terms of functions from l to n, VAN DER WAERDEN'S THEOREM is just a corollary of the following Ramsey-type theorem.

THEOREM 11.2 (HALES-JEWETT THEOREM). *For all positive integers $n, r \in \omega$ there exists a positive integer $l \in \omega$ such that for any r-colouring of ${}^l n$ there is always a non-empty set $s \subseteq l$ and a function $g : l \setminus s \to n$ such that $\big\{f \in {}^l n : f|_{l\setminus s} = g \wedge f|_s \text{ is constant}\big\}$ is monochromatic.*

For given positive integers $n, r \in \omega$, the **Hales-Jewett function** $HJ(n, r)$ denotes the smallest such integer l. In particular, for all positive integers r, $HJ(1, r) = 1$.

Hales and Jewett proved their theorem almost 40 years after van der Waerden proved his. In the original proof, they used — like van der Waerden — a double induction which led to an extremely fast growing upper bound for the Hales-Jewett function $HJ(n,r)$. The proof of the HALES-JEWETT THEOREM given here — which is due to Shelah and modified by Matet involving the FINITE RAMSEY THEOREM — uses just simple induction on n and provides a much better bound for the associated function $HJ(n,r)$.

Before we can give a proof of the HALES-JEWETT THEOREM, including the bounds for $HJ(n,r)$, we have to introduce a kind of *Ramsey number* (*cf.* Chapter 2 | RELATED RESULT 1): By the FINITE RAMSEY THEOREM 2.3 we know that for any positive integers r, p, and q, where $q \leq p$, there exists a positive integer m such that for every r-colouring $\pi : [m]^q \to r$ we find a p-element set $t \in [m]^p$ such that $\pi|_{[t]^q}$ is constant; let $R^q_r(p)$ denote the least such m.

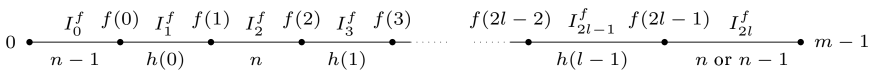
THEOREM 11.3. *For positive integers n and r let $l = HJ(n,r)$, $a = (n+1)^l - n^l$, $k = r^a$, and $m = R^{2l-1}_k(2l)$. Then $HJ(n+1,r) < m$.*

Proof. Let $\mathcal{F}$ be the set of all non-decreasing functions $f \in {}^{2l}m$ (*i.e.*, $f(0) \leq f(1) \leq \ldots \leq f(2l-1)$) such that $2l-1 \leq \big|f[2l]\big|$ (*i.e.*, $f(i) = f(i+1)$ for at most one $i \leq 2l-2$). Let $\mathcal{F}_0 = \big\{f \in \mathcal{F} : \big|f[2l]\big| = 2l\big\}$ and let $\mathcal{F}_1 = \mathcal{F} \setminus \mathcal{F}_0)$. Notice that for each $f \in \mathcal{F}_1$ there exists a unique $i \leq 2l-2$ such that $f(i) = f(i+1)$. So, for every $i \leq 2l-2$ let $F_i = \big\{f \in \mathcal{F}_1 : f(i) = f(i+1)\big\}$. Then $\mathcal{F}_1 = \bigcup_{0 \leq i \leq 2l-2} F_i$.

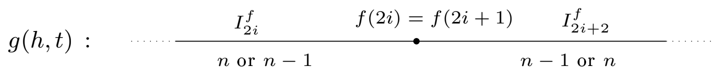
For $f \in \mathcal{F}$ and $i \in [1, 2l-1]$ let $I^f_i = \big[f(i-1), f(i)\big)$, and let $I^f_0 = \big[0, f(0)\big)$ and $I^f_{2l} = \big[f(2l-1), m\big)$. Notice, if $f(0) = 0$ then $I^f_0 = \emptyset$, if $f(2l-1) = m-1$ then $I^f_{2l} = \{m\}$, and if $f \in F_i$, for some $i \leq 2l-2$, then $I^f_{i+1} = \emptyset$. Define $g : {}^l(n+1) \times \mathcal{F} \to {}^{m-1}n+1$ such that for each $j \leq 2l$, $g(h,f)|_{I^f_j}$ is constant, where

$$g(h,f)|_{I^f_j} \text{ is constantly } \begin{cases} n-1 & \text{if } j \equiv 0 \mod 4, \\ n & \text{if } j \equiv 2 \mod 4, \\ h\big((j-1)/2\big) & \text{otherwise.} \end{cases}$$

For $h \in {}^l(n+1)$ and $f \in \mathcal{F}$, $g(h,f)$ is visualised by the following figure:



Notice that for $f \in F_{2i}$ and $h \in \mathcal{H}$ we have the following situation.



For $i \in l$, let $H_i \subseteq {}^l(n+1)$ be the set of all functions $h : l \to (n+1)$ such that $h(i) = n$ and for all $j < n$, $h(j) < n$. Let $\mathcal{H} = \bigcup_{i \in l} H_i$. Notice that $\mathcal{H}$

is the set of all functions $h \in {}^l(n+1)$ such that $h(i) = n$ for some $i \in l$. For each $i \in l$ define a function $g_i : H_i \times [m]^{2l-1} \to {}^{m-1}(n+1)$ by stipulating

$$g_i(h, s) = g(h, f_{s,i}),$$

where $f_{s,i} \in F_{2i}$ is such that $f_{s,i}[2l] = s$.

Fix a colouring $\pi : {}^{(m-1)}(n+1) \to r$. Notice that we can apply π to $g(h, f)$ (where $h \in {}^l(n+1)$ and $f \in \mathcal{F}$) as well as to $g_i(h, s)$ (where $h \in H_i$ and $s \in [m]^{2l-1}$). Recall that we want to show $HJ(n+1, r) \leq m-1$, where $m = R_k^{2l-1}(2l)$. By definition of m, for every colouring $\tau : [m]^{2l-1} \to k$ we find a $2l$-element set $t \in [m]^{2l}$ such that $\tau|_{[t]^{2l-1}}$ is constant. In order to apply the properties of m, we have to find a suitable k-colouring of $[m]^{2l-1}$. Firstly, recall that $k = r^a$, where $a = (n+1)^l - n^l$. Now, $|{}^l(n+1) \setminus \mathcal{H}| = n^l$, and since $|{}^l(n+1)| = (n+1)^l$ we get $|\mathcal{H}| = (n+1)^l - n^l$. Thus, $a = |\mathcal{H}|$, and therefore $k = |{}^{\mathcal{H}}r|$. Now, define the colouring $\tau : [m]^{2l-1} \to {}^{\mathcal{H}}r$ by stipulating

$$\tau(s)(h) = \pi\big(g_i(h, s)\big) \text{ whenever } h \in H_i \text{ for some } i \in l.$$

By definition of m, there exists a $2l$-element set $t \in [m]^{2l}$ such that $\tau|_{[t]^{2l-1}}$ is constant. In particular, for any $s_0, s_1 \in [t]^{2l-1}$ and any $h \in H_i$ we have

$$\pi\big(g_i(h, s_0)\big) = \pi\big(g_i(h, s_1)\big). \qquad (*)$$

Let $f_t \in \mathcal{F}_0$ be such that $f_t[2l] = t$ and define the colouring $\pi' : {}^l n \to r$ by stipulating $\pi'(h) := \pi\big(g(h, f_t)\big)$. Since $l = HJ(n, r)$, there exists a non-empty set $u_0 \subseteq l$ and a function $\tilde{h} : l \setminus u_0 \to n$ such that

$$\hat{H} = \big\{h \in {}^l n : h|_{l \setminus u_0} = \tilde{h} \wedge h|_{u_0} \text{ is constant}\big\}$$

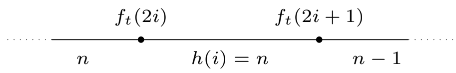
is monochromatic. Notice that $\hat{H} \subseteq {}^l n \subseteq {}^l(n+1)$ and that $\pi|_{\{g(h, f_t) : h \in \hat{H}\}}$ is constant. Let $h_0 \in {}^l(n+1)$ be such that $h_0|_{l \setminus u_0} = \tilde{h}$ and $h_0|_{u_0}$ is constantly n. If we can show that $\{g(h, f_t) : h \in \hat{H} \vee h = h_0\}$ is monochromatic, then we are done. In fact, it is enough to show that $\pi\big(g(h_0, f_t)\big) = \pi\big(g(\hat{h}_0, f_t)\big)$, where $\hat{h}_0 \in \hat{H}$ is such that for all $i \in l$, $\hat{h}_0(i) := \min\big\{h_0(i), n-1\big\}$. This is done by induction on the size of u_0, but first we have to do some preliminary work: For $i \in l$ and $h \in H_i$ define $h' \in {}^l(n+1)$ by stipulating

$$h'(j) = \begin{cases} n-1 & \text{if } j = i, \\ h(j) & \text{otherwise.} \end{cases}$$

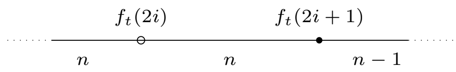
Notice that either $h' \in H_{i'}$ for some $i' > i$, or $h' \in {}^l n$. We show now that for every $h \in H_i$, $\pi\big(g(h, f_t)\big) = \pi\big(g(h', f_t)\big)$. We consider the cases i odd and i even separately.

For i odd and $h \in H_i$ we have the following situation:

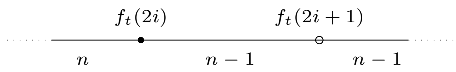
$g(h, f_t)$:



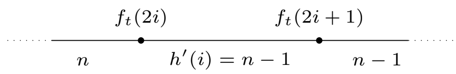
$g_i(h, t \setminus \{f_t(2i)\})$:



$g_i(h, t \setminus \{f_t(2i+1)\})$:

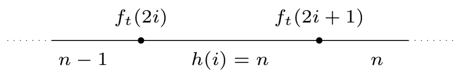


$g(h', f_t)$:

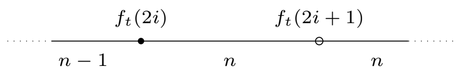


Similarly, for i even and $h \in H_i$ we get:

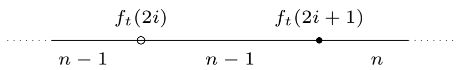
$g(h, f_t)$:



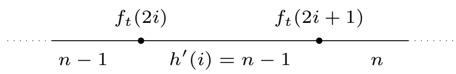
$g_i(h, t \setminus \{f_t(2i+1)\})$:



$g_i(h, t \setminus \{f_t(2i)\})$:



$g(h', f_t)$:



By $(*)$ we have $\pi\big(g_i(h, t \setminus \{f_t(2i)\})\big) = \pi\big(g_i(h, t \setminus \{f_t(2i+1)\})\big)$, and since we obviously have

$$\left.\begin{aligned} g(h, f_t) &= g_i\big(h, t \setminus \{f_t(2i)\}\big) \\ g(h', f_t) &= g_i\big(h, t \setminus \{f_t(2i+1)\}\big) \end{aligned}\right\} \quad \text{if } i \text{ is odd,}$$

and

$$\left.\begin{aligned} g(h, f_t) &= g_i\big(h, t \setminus \{f_t(2i+1)\}\big) \\ g(h', f_t) &= g_i\big(h, t \setminus \{f_t(2i)\}\big) \end{aligned}\right\} \quad \text{if } i \text{ is even,}$$

we get

$$\pi\big(g(h, f_t)\big) = \pi\big(g(h', f_t)\big) .$$

Now we are ready to show that $\pi\big(g(h_0, f_t)\big) = \pi\big(g(\hat{h}_0, f_t)\big)$: For $j < |u_0|$ let $h_{j+1} := h'_j$. Then, by the preceding fact we have

$$\pi\big(g(h_0, f_t)\big) = \pi\big(g(h_1, f_t)\big) = \ \ldots \ = \pi\big(g(h_{|u|}, f_t)\big) ,$$

and since $h_{|u|} = \hat{h}_0$, we finally get $\pi\big(g(h_0, f_t)\big) = \pi\big(g(\hat{h}_0, f_t)\big)$, which completes the proof of THEOREM 11.3 as well as of the HALES-JEWETT THEOREM. $\dashv$

The HALES-JEWETT THEOREM will be used to start the induction in the proof of CARLSON'S LEMMA (see Claim 2), where CARLSON'S LEMMA is the crucial part in the proof of a generalisation of RAMSEY'S THEOREM in terms of partitions — the main result of this chapter which will be called PARTITION RAMSEY THEOREM.

The PARTITION RAMSEY THEOREM is a very strong combinatorial result which implies the HALES-JEWETT THEOREM as well as some other Ramsey-type results like the WEAK HALPERN-LÄUCHLI THEOREM 11.6. However, before we can formulate and prove the PARTITION RAMSEY THEOREM, we have to introduce first the corresponding terminology.

Families of Partitions

Even though partitions have already been used in Chapter 10, let us introduce the notion of partition in a more formal way.

A set $P \subseteq \mathscr{P}(S)$ is a **partition** of the set S, if $\emptyset \notin P$, $\bigcup P = S$, and for all distinct $p_1, p_2 \in P$ we have $p_1 \cap p_2 = \emptyset$. A member of a partition P is called a **block** of P and $\mathrm{Dom}(P) := \bigcup P$ is called the **domain** of P. A partition P is called **infinite**, if $|P|$ is infinite (where $|P|$ denotes the cardinality of the set P); otherwise, the partition P is called **finite**.

If P and Q are two partitions with the same domain, then P is **coarser** than Q, or equivalently Q is **finer** than P, if each block of P is the union of blocks of Q. Notice that the relation "coarser" is a partial ordering on the set of partitions with a given domain, and that there are unique finest and coarsest partitions. For example with respect to partitions of ω, the finest partition is $\{\{n\} : n \in \omega\}$ and the coarsest partition is $\{\omega\}$.

Below, we are mainly interested in infinite partitions of ω, denote by capital letters like $X, Y, Z, \ldots$, as well as in (finite) partitions of natural numbers, usually denoted by capital letters like $S, T, U, \ldots$. So, let $(\omega)^\omega$ denote the set of all infinite partitions of ω and let $(\mathbb{N})$ denote the set of all (finite) partitions S with $\mathrm{Dom}(S) \in \omega$. Notice that $S \in (\mathbb{N})$ *iff* S is a partition of some natural number $n \in \omega$.

The following notation allows us to compare partitions with different domains: For partitions P and Q (*e.g.*, $P \in (\mathbb{N})$ and $Q \in (\omega)^\omega$) we write $P \sqsubseteq Q$ if for all blocks $p \in P$ the set $p \cap \mathrm{Dom}(Q)$ is the union of some sets $q_i \cap \mathrm{Dom}(P)$, where each q_i is a block of Q. Notice that in general, $P \sqsubseteq Q \sqsubseteq P$ does not imply $P = Q$, except when $\mathrm{Dom}(P) = \mathrm{Dom}(Q)$. Furthermore, let $P \sqcap Q$ ($P \sqcup Q$) denote the finest (coarsest) partition R such that $\mathrm{Dom}(R) = \mathrm{Dom}(P) \cup \mathrm{Dom}(Q)$ and R is coarser (finer) than P and Q. In particular, if $\mathrm{Dom}(P) \subseteq \mathrm{Dom}(Q)$ then $P \sqcap Q \sqsubseteq Q \sqsubseteq P \sqcup Q$.

Let $S \in (\mathbb{N})$ and $X \in (\omega)^\omega$. If for each $s \in S$ there exists an $x \in X$ such that $x \cap \mathrm{Dom}(S) = s$, we write $S \preccurlyeq X$. Similarly, for $S, T \in (\mathbb{N})$, where $\mathrm{Dom}(S) \subseteq \mathrm{Dom}(T)$, we write $S \preccurlyeq T$ if for each $s \in S$ there exists a $t \in T$ such that $t \cap \mathrm{Dom}(S) = s$. Roughly speaking, $P \preccurlyeq Q$ is the same as saying "Q

restricted to $\mathrm{Dom}(P)$ is equal to P". Notice that for $S \sqsubseteq X$, where $S \in (\mathbb{N})$ and $X \in (\omega)^\omega$, we have $S \preccurlyeq (S \sqcap X) \sqsubseteq X$.

At a first glance, the set of partitions of ω, with the partitions $\{\omega\}$ and $\big\{\{n\} : n \in \omega\big\}$ and the operations "$\sqcup$" and "$\sqcap$", looks similar to the Boolean algebra $\big(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega\big)$. However, partitions of ω behave differently than subsets of ω. The main difference between partitions and subsets is that partitions do not have proper complements. For example if $x, y, z \in [\omega]^\omega$ are such that $x \cup y = x \cup z = \omega$ and $x \cap y = x \cap z = \emptyset$, then $y = z$. This is not the case for partitions: It is not hard to find partitions $X, Y, Z \in (\omega)^\omega$ such that $X \sqcup Y = X \sqcup Z = Y \sqcup Z = \big\{\{n\} : n \in \omega\big\}$ and $X \sqcap Y = X \sqcap Z = Y \sqcap Z = \{\omega\}$, *e.g.*, let $X = \big\{\{3i, 3i{+}1\} : i \in \omega\big\} \cup \big\{\{3i{+}2\} : i \in \omega\big\}$, $Y = \big\{\{3i{+}1, 3i{+}2\} : i \in \omega\big\} \cup \big\{\{3i\} : i \in \omega\big\}$, and $Z = \big\{\{3i, 3i{+}2\} : i \in \omega\big\} \cup \big\{\{3i{+}1\} : i \in \omega\big\}$. We leave it as an exercise to the reader to construct infinite partitions $X, Y, Z \in (\omega)^\omega$ with the same property but such that all blocks of X, Y, and Z, are infinite.

Now, let us define a topology on $(\omega)^\omega$ which is similar to the Ellentuck topology on $[\omega]^\omega$ (defined on page 216): For $S \in (\mathbb{N})$ and $X \in (\omega)^\omega$ with $S \sqsubseteq X$, let

$$(S, X)^\omega = \big\{ Y \in (\omega)^\omega : S \preccurlyeq Y \sqsubseteq X \big\} .$$

A set $(S, X)^\omega$, where S and X are as above, is usually called a **dual Ellentuck neighbourhood**. We leave it as an exercise to the reader to show that the intersection of finitely many dual Ellentuck neighbourhoods is either empty or a dual Ellentuck neighbourhood. The topology on $(\omega)^\omega$ generated by the dual Ellentuck neighbourhoods is called **dual Ellentuck topology**.

The usual trick to get subsets of ω from partitions is as follows: For a partition P of a subset of ω, *e.g.*, $P \in (\omega)^\omega$ or $P \in (\mathbb{N})$, let

$$\mathrm{Min}(P) = \big\{ \min(p) : p \in P \big\} .$$

Obviously, if $X \in (\omega)^\omega$ then $\mathrm{Min}(X) \in [\omega]^\omega$ and if $S \in (\mathbb{N})$ then $\mathrm{Min}(S) \in \mathrm{fin}(\omega)$. Further we have that for any $X, Y \in (\omega)^\omega$, $X \sqsubseteq Y$ implies $\mathrm{Min}(X) \subseteq \mathrm{Min}(Y)$.

A *non-empty* family $\mathscr{C} \subseteq (\omega)^\omega$ is called **free**, if for every $X \in \mathscr{C}$ there is a $Y \in \mathscr{C}$ such that $Y \sqsubseteq X$, but for all $S \in (\mathbb{N})$, $(S \sqcap X) \not\sqsubseteq Y$.

A family $\mathscr{C} \subseteq (\omega)^\omega$ is **closed under refinement** if $X \sqsubseteq Y$ and $X \in \mathscr{C}$ implies $Y \in \mathscr{C}$, and it is **closed under finite coarsening** if $S \in (\mathbb{N})$ and $X \in \mathscr{C}$ implies $(S \sqcap X) \in \mathscr{C}$. Notice that a family $\mathscr{C} \subseteq (\omega)^\omega$ is closed under refinement and finite coarsening *iff* for all $S \in (\mathbb{N})$ and $Y \in (\omega)^\omega$, $X \sqsubseteq (S \sqcap Y)$ and $X \in \mathscr{C}$ implies $Y \in \mathscr{C}$.

A family $\mathscr{C} \subseteq (\omega)^\omega$ is called **complete**, if $\mathscr{C}$ is free and closed under refinement and finite coarsening.

In order to define the game which plays a key role in the proof of the Partition Ramsey Theorem, we have to introduce the following notation. For $S \in (\mathbb{N})$, let S^* denote the partition $S \cup \big\{\{\mathrm{Dom}(S)\}\big\}$. Notice that $|S^*| = |S| + 1$. Further, notice that whenever $(S^*, X)^\omega$ is a dual Ellentuck neighbourhood, then every $Y \in (S^*, X)^\omega$ has a block y such that $y \cap \mathrm{Dom}(S) = \emptyset$ and $y \cap \mathrm{Dom}(S^*) = \{\mathrm{Dom}(S)\}$.

With respect to a complete family $\mathscr{C} \subseteq (\omega)^\omega$ we define the infinite two-player game $\mathcal{G}_{\mathscr{C}}$ as follows.

$$
\mathcal{G}_{\mathscr{C}} : \quad
\begin{tikzcd}[column sep=small]
\text{MAIDEN} & (S_0, X_0) \arrow[dr] & & (S_1, X_1) \arrow[dr] & & (S_2, X_2) \arrow[dr] & & \cdots \\
\text{DEATH} & & Y_0 \arrow[ur] & & Y_1 \arrow[ur] & & Y_2 \arrow[ur, dash] &
\end{tikzcd}
$$

We require that the first move (S_0, X_0) of the MAIDEN is such that $X_0 \in \mathscr{C}$ and that $(S_0^*, X_0)^\omega$ is a dual Ellentuck neighbourhood. Further, we require that for each $n \in \omega$, the n^{th} move of DEATH Y_n is such that $Y_n \in (S_n^*, X_n)^\omega$ and $Y_n \in \mathscr{C}$, and that the MAIDEN plays (S_{n+1}, X_{n+1}) such that

- $S_n^* \preccurlyeq S_{n+1}$, $|S_{n+1}| = |S_n| + 1$, $S_{n+1}^* \sqsubseteq Y_n$, and
- $X_{n+1} \in (S_{n+1}^*, Y_n)^\omega \cap \mathscr{C}$.

Finally, the MAIDEN wins the game $\mathcal{G}_{\mathscr{C}}$ if and only if $\bigcap_{n \in \omega} (S_n, X_n)^\omega \cap \mathscr{C} = \emptyset$, *i.e.*, the (unique) infinite partition $X \in (\omega)^\omega$ such that $S_n \prec X$ (for all $n \in \omega$) does ***not*** belong to the family $\mathscr{C}$.

Now, a complete family $\mathscr{C} \subseteq (\omega)^\omega$ is called a **Ramsey partition-family** if the MAIDEN has no winning strategy in the game $\mathcal{G}_{\mathscr{C}}$ (compare with the game introduced in Chapter 10 | RELATED RESULT 71).

Obviously, the set $(\omega)^\omega$ is an example for a Ramsey partition-family and it is not hard to construct Ramsey partition-families which are proper subsets of $(\omega)^\omega$, *e.g.*, for any partition $X \in (\omega)^\omega$, $(X)^\omega$ is a Ramsey partition-family. For a non-trivial example of a Ramsey partition-family take a Ramsey ultrafilter $\mathscr{F} \subseteq [\omega]^\omega$ and let $\mathscr{C} = \{X \in (\omega)^\omega : \mathrm{Min}(X) \in \mathscr{F}\}$. Then, by Chapter 10 | RELATED RESULT 71, we get that $\mathscr{C}$ is a Ramsey partition-family (for other non-trivial examples of Ramsey partition-families see Chapter 26).

It turns out that Ramsey partition-families have very strong combinatorial properties, and to some extent, they are proper generalisations of Ramsey families (see also Chapter 26). The combinatorial strength of Ramsey partition-families is used for example in the proof of CARLSON'S LEMMA, which is — as mentioned above — the crucial part in the proof of the PARTITION RAMSEY THEOREM.

Carlson's Lemma and the Partition Ramsey Theorem

Before we formulate and prove the PARTITION RAMSEY THEOREM, let us first consider a few possible generalisations of RAMSEY'S THEOREM in terms of partitions: RAMSEY'S THEOREM states that whenever we colour $[\omega]^n$ (*i.e.*, the n-element subsets of ω) with finitely many colours, then we find an $x \in [\omega]^\omega$ (*i.e.*, an infinite subsets of ω) such that $[x]^n$ is monochromatic (*i.e.*, all whose

n-element subsets have the same colour). If we try to formulate RAMSEY'S THEOREM in terms of partitions, we first have to decide which partitions correspond to the "n-element subsets of ω" and "infinite subsets of ω" respectively. It seems natural that infinite subsets of ω correspond to infinite partitions of ω, *i.e.*, $x \in [\omega]^\omega$ is replaced by $X \in (\omega)^\omega$. Similarly, we could say that n-element subsets of ω correspond to n-block partitions of ω, and therefore we would replace $[\omega]^n$ by $(\omega)^n := \{X \in (\omega)^\omega : |X| = n\}$. This leads to the following first attempt of a generalisation of RAMSEY'S THEOREM in terms of partitions:

Generalisation 1. For every colouring of $(\omega)^n$ with finitely many colours, there exists an infinite partition $X \in (\omega)^\omega$ such that $(X)^n$ is monochromatic, where $(X)^n := \{Y \in (\omega)^n : Y \sqsubseteq X \wedge |Y| = n\}$.

Unfortunately, this generalisation of RAMSEY'S THEOREM fails. In fact, by transfinite induction we can construct a counterexample even for the case when $n = 2$: Firstly notice that for each $X \in (\omega)^\omega$, $|(X)^2| = |(\omega)^\omega| = \mathfrak{c}$. Let $\{X_\alpha : \alpha \in \mathfrak{c}\}$ be an enumeration of $(\omega)^\omega$. For each $\alpha \in \mathfrak{c}$ choose two distinct partitions

$$Y_\alpha^0, Y_\alpha^1 \in \Big((X_\alpha)^2 \setminus \{Y_\beta^0, Y_\beta^1 : \beta \in \alpha\}\Big).$$

Finally, define $\pi : (\omega)^2 \to \{0,1\}$ by stipulating $\pi(Y) = 0$ *iff* there is an $\alpha \in \mathfrak{c}$ such that $Y = Y_\alpha^0$. By construction, for every $X \in (\omega)^\omega$ we find Y^0 and Y^1 in $(X)^2$ such that $\pi(Y^0) = 0$ and $\pi(Y^1) = 1$. Thus, for every $X \in (\omega)^\omega$, $(X)^n$ is dichromatic.

One might ask why is it not possible to construct a similar counterexample for RAMSEY'S THEOREM? The reason is simple: For any partition $X \in (\omega)^\omega$, $(X)^2$ is of cardinality $\mathfrak{c}$, whereas for any $x \in [\omega]^\omega$ and $n \in \omega$, the set $[x]^n$ is countable.

Now, one might ask why are n-element subsets of ω so different from n-block partitions? A reason is that n-element subsets of ω are proper finitary objects, whereas an n-block partition $Y \in (\omega)^n$ necessarily contains infinite sets. Furthermore, every n-element subset of ω is a subset of some $k \in \omega$, which is not the case for partitions $Y \in (\omega)^n$. However, it is true for partitions $S \in (\mathbb{N})$. So, let us replace now $[\omega]^n$ and $[x]^n$ by $(\omega)^{(n)}$ and $(X)^{(n)}$ respectively, where

$$(\omega)^{(n)} = \{S \in (\mathbb{N}) : |S| = n\},$$

and for $X \in (\omega)^\omega$,

$$(X)^{(n)} = \{S \in (\omega)^{(n)} : S \sqsubseteq X\}.$$

Generalisation 2. For every colouring of $(\omega)^{(n)}$ with finitely many colours, there exists an infinite partition $X \in (\omega)^\omega$ such that $(X)^{(n)}$ is monochromatic.

Unfortunately, this generalisation fails as well. Again, we can construct a counterexample even for the case when $n = 2$: For this, consider the colouring $\pi : (\omega)^{(2)} \to \{0,1\}$ defined by stipulating

$$\pi\big(\{s_0, s_1\}\big) = 0 \iff 0 \in s_0 \wedge \max(s_0) < \max(s_1)\,.$$

We leave it as an exercise to the reader to show that for every $X \in (\omega)^\omega$, $(X)^{(n)}$ is dichromatic.

After these two failures, let us now formulate RAMSEY'S THEOREM directly in terms of partitions of subsets of ω: A partition P of a subset of ω is **segmented** if for any distinct $p_0, p_1 \in P$, either $\max(p_0) < \min(p_1)$ or $\max(p_1) < \min(p_0)$. Let $\langle\omega\rangle^\omega$ denote the set of all segmented partitions of ω. Notice that if $P \in \langle\omega\rangle^\omega$, then all blocks P are finite. For the moment let $\dot\omega := \omega \setminus \{0\}$. For an infinite set of positive integers $x = \{k_i : i \in \dot\omega\} \in [\dot\omega]^\omega$, where $k_i < k_{i+1}$ for all $i \in \dot\omega$, we define $P_x \in \langle\omega\rangle^\omega$ by stipulating

$$P_x = \big\{[k_i, k_{i+1}) : i \in \omega\big\}\,,$$

where $k_0 := 0$. Notice that $\langle\omega\rangle^\omega = \big\{P_x : x \in [\dot\omega]^\omega\big\}$. Similarly, for an n-element set $s = \{k_1, \dots, k_n\} \in [\dot\omega]^n$, where $k_i < k_{i+1}$ for $1 \le i \le n$, we define

$$Q_s = \big\{[k_i, k_{i+1}) : i \in n\big\}\,,$$

where again $k_0 = 0$. Notice that for all $s \in \operatorname{fin}(\dot\omega)$, Q_s is a segmented partition with $\operatorname{Dom}(Q_s) = \max(s)$. Now, let $\langle\omega\rangle^{(n)} = \big\{Q_s : s \in [\dot\omega]^n\big\}$ and for $P \in \langle\omega\rangle^\omega$ let

$$\langle P\rangle^{(n)^*} = \big\{Q \in \langle\omega\rangle^{(n)} : Q^* \sqsubseteq P\big\}\,.$$

Recall that for $s \in \operatorname{fin}(\dot\omega)$, $Q_s^* = Q_s \cup \big\{\operatorname{Dom}(Q_s)\big\} = Q_s \cup \big\{\max(s)\big\}$, and notice that for all $x \in [\dot\omega]^\omega$, $\langle P_x\rangle^{(n)^*} = \big\{Q_s^* : s \in [x]^n\big\}$.

Now we are ready to formulate RAMSEY'S THEOREM in terms of segmented partitions — we leave it as an exercise to the reader to show that RAMSEY'S THEOREM is indeed equivalent to the following statement.

Ramsey's Theorem. For every colouring of $\langle\omega\rangle^{(n)}$ with finitely many colours, there exists an infinite segmented partition $P \in \langle\omega\rangle^\omega$ such that $\langle P\rangle^{(n)^*}$ is monochromatic.

So, we finally found a formulation of RAMSEY'S THEOREM in terms of segmented partitions. The next step is to find a general formulation which works for all, and not just for segmented partitions. For this, we only have to replace the angle brackets by round brackets and define the meaning of $(X)^{(n)^*}$: For $n \in \omega$ and $X \in (\omega)^\omega$ let

$$(X)^{(n)^*} = \big\{S \in (\omega)^{(n)} : S^* \sqsubseteq X\big\}\,.$$

Similarly, for a dual Ellentuck neighbourhood $(S, X)^\omega$, where $|S| \le n$, let

$$(S, X)^{(n)^*} = \big\{U \in (\omega)^{(n)} : S \preccurlyeq U \wedge U^* \sqsubseteq X\big\}\,.$$

Now we are ready to state the sought partition form of RAMSEY'S THEOREM:

THEOREM 11.4 (PARTITION RAMSEY THEOREM). *For any Ramsey partition-family $\mathscr{C} \subseteq (\omega)^\omega$ and for any colouring of $(\omega)^{(n)}$ with r colours, where r and n are positive integers, there is an $X \in \mathscr{C}$ such that $(X)^{(n)^*}$ is monochromatic.*

The PARTITION RAMSEY THEOREM will follow from CARLSON'S LEMMA. With respect to Ramsey partition-families, CARLSON'S LEMMA states as follows:

LEMMA 11.5 (CARLSON'S LEMMA). *Let $\mathscr{C} \subseteq (\omega)^\omega$ be an arbitrary but fixed Ramsey partition-family. For any colouring $\pi : (\omega)^{(n)} \to r$, where r and n are positive integers, and for any dual Ellentuck neighbourhood $(S_0, X_0)^\omega$, where $|S_0| = n$ and $X \in \mathscr{C}$, there is a $\bar{X} \in (S_0, X_0)^\omega$ which belongs to $\mathscr{C}$ such that $(S_0, \bar{X})^{(n)^*}$ is monochromatic.*

Proof. Before we begin with the proof, let us first introduce the following notion: For a dual Ellentuck neighbourhood $(S, X)^\omega$ and for a positive integer $m \in \omega$, a set $D \subseteq (\omega)^{(m)}$ is called *$\mathscr{C}$-dense* in $(S, X)^{(m)^*}$ if for all $Y \in (S, X)^\omega \cap \mathscr{C}$, $(S, Y)^{(m)^*} \cap D \neq \emptyset$. Notice that for every colouring $\pi : (\omega)^{(n)} \to r$, there exists a colour $c \in r$ and a partition $X_0' \in (S_0, X_0)^\omega \cap \mathscr{C}$ such that the set $D_c := \{S \in (\omega)^{(n)} : \pi(S) = c\}$ is $\mathscr{C}$-dense in $(S_0, X_0')^{(n)^*}$. Indeed, if D_0 is $\mathscr{C}$-dense in $(S_0, X_0)^{(n)^*}$ then we are done. Otherwise, there exists an $X_1 \in (S_0, X_0)^\omega \cap \mathscr{C}$ such that $(S_0, X_1)^{(n)^*} \cap D_0 = \emptyset$. Now, either D_1 is $\mathscr{C}$-dense in $(S_0, X_1)^{(n)^*}$, or there exists an $X_2 \in (S_0, X_1)^\omega \cap \mathscr{C}$ such that $(S_0, X_2)^{(n)^*} \cap D_1 = \emptyset$. Proceeding this way, we finally find a $c \in r$ such that for all $Y \in (S_0, X_c)^\omega \cap \mathscr{C}$, $(S_0, Y)^{(n)^*} \cap D_c \neq \emptyset$; let $X_0' = X_c$.

After this preliminary remark, we can now begin with the proof: Without loss of generality we may assume that the dual Ellentuck neighbourhood $(S_0, X_0)^\omega$ is such that D_0 is $\mathscr{C}$-dense in $(S_0, X_0)^{(n)^*}$.

The proof is now given in several steps. Firstly we show that there exists an $\tilde{S} \in (\mathbb{N})$ with $S_0 \preccurlyeq \tilde{S} \sqsubseteq X_0$, such that for all $T \in (\mathbb{N})$ with $\tilde{S} \preccurlyeq T \sqsubseteq X_0$, there is a $T' \sqsubseteq T$ such that $\mathrm{Dom}(T') = \mathrm{Dom}(T)$, $|T'| = n$, $S_0 \preccurlyeq T'$, and $T' \in D_0$. To state this in a more formal way, we introduce the following two notations: For $S, T \in (\mathbb{N})$, where $S \preccurlyeq T$ and $|S| \leq m$, let

$$(S, T)^m = \{U \in (\mathbb{N}) : \mathrm{Dom}(U) = \mathrm{Dom}(T) \wedge S \preccurlyeq U \sqsubseteq T \wedge |U| = m\},$$

and for a dual Ellentuck neighbourhood $(U, Z)^\omega$, let

$$(U, Z)^{(<\omega)^*} = \bigcup_{k \in \omega} (U, Z)^{(k)^*}.$$

In other words, $(U, Z)^{(<\omega)^*} = \{S \in (\mathbb{N}) : U \preccurlyeq S^* \sqsubseteq Z\}$ and $(S, T)^m$ is the set of all m-block partitions of $\mathrm{Dom}(T)$ which contain S as a "sub-partition" and are coarser than T.

CLAIM 1. *There is a $Z_0 \in (S_0, X_0)^\omega \cap \mathscr{C}$ and an $\tilde{S} \in (S_0, Z_0)^{(<\omega)^*}$ such that for all $S \in (\tilde{S}, Z_0)^{(<\omega)^*}$, $(S_0, S)^n \cap D_0 \neq \emptyset$.*

Proof of Claim 1. If the claim fails, then for every $Y \in (S_0, X_0)^\omega \cap \mathscr{C}$ and each $T \in (S_0, Y)^{(<\omega)^*}$ there is an $S \in (T, Y)^{(<\omega)^*}$ such that $(S_0, S)^n \cap D_0 = \emptyset$; in particular, there is an $S' \in (T, Y)^{(|T|)^*}$ such that $(S_0, S')^n \cap D_0 = \emptyset$. We define a strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{C}}$. The MAIDEN starts the game with (S_0, X_0) and replies the i^{th} move Y_i of DEATH with (S_{i+1}, X_{i+1}), where $X_{i+1} = Y_i$ and S_{i+1} is constructed as follows: Take any $T_{i+1} \in (S_i^*, Y_i)^{(n+i+1)^*}$ and let $S_{i+1} \in (T_{i+1}, Y_i)^{(n+i+1)^*}$ be such that $(S_0, S_{i+1})^n \cap D_0 = \emptyset$. As $\mathscr{C}$ is a Ramsey-partition family, fix a play where the MAIDEN follows this strategy but DEATH wins. Let $Z \in (\omega)^\omega$ be the unique infinite partition such that for all $i \in \omega$ we have $S_i \prec Z$. Since $\mathscr{C}$ is a Ramsey partition-family, the partition Z belongs to $\mathscr{C}$. By construction, $S_0 \prec Z$ and $(S_0, Z)^{(n)^*} \cap D_0 = \emptyset$. Thus, D_0 is not $\mathscr{C}$-dense in $(S_0, X_0)^{(n)^*}$, a contradiction. $\dashv_{\text{Claim 1}}$

The next step is where the HALES-JEWETT THEOREM comes in:

CLAIM 2. *Let $Z_0 \in (S_0, X_0)^\omega \cap \mathscr{C}$ be as in Claim 1. Then there is a $\tilde{U} \in (S_0, Z_0)^{(n+1)^*}$ such that $(S_0, \tilde{U})^n \subseteq D_0$.*

Proof of Claim 2. Let $\tilde{S} \in (S_0, Z_0)^{(<\omega)^*}$ be as in CLAIM 1, *i.e.*, for all $W \in (\tilde{S}, Z_0)^{(<\omega)^*}$ there is a $W' \in (S_0, W)^n$ such that $W' \in D_0$. Let $m = |\tilde{S}|$, $r_0 = \left|(S_0, \tilde{S})^n\right|$, and let $\{U_k : k \in r_0\}$ be an enumeration of $(S_0, \tilde{S})^n$. By the HALES-JEWETT THEOREM 11.2, or more precisely by a partition form of it, there is a positive integer $l = HJ(m, r_0)$ such that for any $T \in (\tilde{S}, Z_0)^{(m+l)^*}$ and any r_0-colouring of $(\tilde{S}, T)^m$ there is a $W_0 \in (\tilde{S}, T)^{m+1}$ such that $(\tilde{S}, W_0)^m$ is monochromatic (the details are left to the reader). Fix an arbitrary $\tilde{T} \in (\tilde{S}, Z_0)^{(m+l)^*}$. Then, by the choice of $\tilde{S}$, for all $W \in (\tilde{S}, \tilde{T})^m$ there is a $U \in (S_0, W)^n$ such that $U \in D_0$. Moreover, there is a $k \in r_0$ such that $U_k \prec U$, and since $|U_k| = |U| = n$ we have $U = U_k \sqcap W$. Hence, for every $W \in (\tilde{S}, \tilde{T})^m$ there is a $k \in r_0$ such that $U_k \sqcap W \in D_0$. Now, for each $W \in (\tilde{S}, \tilde{T})^m$ let

$$\tau(W) = \min\{k \in r_0 : U_k \sqcap W \in D_0\}.$$

Then τ is an r_0-colouring of $(\tilde{S}, \tilde{T})^m$. Since $\tilde{T} \in (\tilde{S}, Z_0)^{(m+l)^*}$ there is a $W_0 \in (\tilde{S}, \tilde{T})^{m+1}$ such that $(\tilde{S}, W_0)^m$. is monochromatic, say of colour k_0. Thus, for all $W \in (\tilde{S}, W_0)^m$, $U_{k_0} \sqcap W \in D_0$. Finally, let $\tilde{U} = U_{k_0} \sqcap W_0$. Then $\tilde{U} \in (S_0, W_0)^{n+1}$, hence $\tilde{U} \in (S_0, Z_0)^{(n+1)^*}$, and $(S_0, \tilde{U})^n \subseteq D_0$ as required. $\dashv_{\text{Claim 2}}$

As an obvious generalisation of CLAIM 2 we get

CLAIM 2*. *For each $X \in (S_0, X_0)^\omega \cap \mathscr{C}$ there is a $U \in (S_0, X)^{(n+1)^*}$ such that $(S_0, U)^n \subseteq D_0$.*

The next step is crucial in the construction of $\bar{X}$:

CLAIM 3. *Let $Z_0 \in (S_0, X_0)^\omega \cap \mathscr{C}$ be as in Claim 1. Then there are $S \in (S_0, Z_0)^{(n+1)^*}$ and $X \in (S, Z_0)^\omega \cap \mathscr{C}$ such that the set*

$$\left\{T \in (S, X)^{(n+1)^*} : (S_0, T)^n \subseteq D_0\right\}$$

is $\mathscr{C}$-dense in $(S, X)^{(n+1)^*}$.

Proof of Claim 3. Assume towards a contradiction that the claim fails. Then, for any $S \in (S_0, Z_0)^{(n+1)^*}$ and each $Y \in (S, X_0)^\omega \cap \mathscr{C}$ there exists a $Z \in (S, Y)^\omega \cap \mathscr{C}$, such that for all $T \in (S, Z)^{(n+1)^*}$ we have $(S_0, T)^n \nsubseteq D_0$. We define a strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{C}}$. The MAIDEN starts the game with (S_0, Z_0) and replies the i^{th} move Y_i of DEATH with (S_{i+1}, Z_{i+1}), where $Z_{i+1} \in (S_i^*, Y_i)^\omega \cap \mathscr{C}$ and $S_{i+1} \in (S_i^*, Z_{i+1})^{(n+i+1)^*}$ are such that for all $S \in (S_0, S_{i+1})^{n+1}$ and all $T \in (S, Z_{i+1})^{(n+1)^*}$ we have $(S_0, T)^n \nsubseteq D_0$: For $i = 0$, let $S_1 \in (S_0, Y_0)^{(n+1)^*}$ be arbitrary and let $Z_1 \in (S_1^*, Y_0)^\omega \cap \mathscr{C}$ be such that for all $T \in (S_1, Z_1)^{(n+1)^*}$ we have $(S_0, T)^n \nsubseteq D_0$. For $i > 0$, we construct S_{i+1} and Z_{i+1} as follows. Firstly, let $\{T_{i,k} : k \in h_i\}$ be an enumeration of $(S_0, S_i)^{n+1}$. Secondly, let $Z_{i,0} = Y_i$ and for $k \in h_i$ let $Z_{i,k+1} \in (S_i, Z_{i,k})^\omega \cap \mathscr{C}$ be such that for all $T \in (T_{i,k}, Z_{i,k+1})^{(<\omega)^*}$ we have $(S_0, T)^n \nsubseteq D_0$. Finally, let $Z_{i+1} = Z_{i,h_i}$ and let $S_{i+1} \in (S_i^*, Z_{i+1})^{(n+i+1)^*}$. Fix a play where the MAIDEN follows this strategy but DEATH wins. Since $\mathscr{C}$ is a Ramsey partition-family, the unique infinite partition $Z \in (\omega)^\omega$ such that for all $i \in \omega$ we have $S_i \prec Z$ belongs to $\mathscr{C}$. Now, by construction, for any $U \in (S_0, Z)^{(n+1)^*}$ we find a positive integer $i \in \omega$ as well as a $k \in h_i$ such that $U \in (T_{i,k}, Z_{i+1})^{(n+1)^*}$. Thus, for all $U \in (S_0, Z)^{(n+1)^*}$ we have $(S_0, U)^n \nsubseteq D_0$, but since $(S_0, Z)^\omega \subseteq (S_0, Z_0)^\omega$, this contradicts CLAIM 2*. $\dashv_{\text{Claim 3}}$

The following claim is just a generalisation of CLAIM 3:

CLAIM 3*. *Let $(T_0, Y_0)^\omega \subseteq (S_0, X_0)^\omega$ be a dual Ellentuck neighbourhood, where $Y_0 \in \mathscr{C}$ and $|T_0| = m$. If $E \subseteq (\omega)^{(m)}$ is $\mathscr{C}$-dense in $(T_0, Y_0)^{(m)^*}$, then there exist $S \in (T_0, Y_0)^{(m+1)^*}$ and $X \in (S, Y_0)^\omega \cap \mathscr{C}$ such that the set $\{T \in (S, Y_0)^{(m+1)^*} : (T_0, T)^m \subseteq E\}$ is $\mathscr{C}$-dense in $(S, X)^{(m+1)^*}$.*

Proof of Claim 3.* In the proofs of the preceding claims, just replace S_0 by T_0, X_0 by Y_0, and D_0 by E. $\dashv_{\text{Claim 3}^*}$

Now we construct the first piece of the sought partition $\bar{X}$:

CLAIM 4. *There is a $U_0 \in (S_0, X_0)^{(n)^*}$ such that $\pi(U_0) = 0$, i.e., $U_0 \in D_0$, and in addition there is an $X \in (U_0^*, X_0)^\omega \cap \mathscr{C}$ such that the set*

$$\{T \in (U_0, X)^{(n+1)^*} : (S_0, T)^n \subseteq D_0\}$$

is $\mathscr{C}$-dense in $(U_0, X)^{(n+1)^*}$.

Proof of Claim 4. We define a strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{C}}$. The MAIDEN starts the game with (S_0, X_0) and replies the i^{th} move Y_i of DEATH with (S_{i+1}, X_{i+1}), where S_{i+1} and X_{i+1} are constructed as follows: For $i = 0$, let $S_1 \in (S_0, Y_0)^{(n+1)^*}$ and $X_1 \in (S_1, Y_0)^\omega \cap \mathscr{C}$ be such that the set

$$E_1 = \{T \in (S_1, X_1)^{(n+1)^*} : (S_0, T)^n \subseteq D_0\}$$

is $\mathscr{C}$-dense in $(S_1, X_1)^{(n+1)^*}$. Notice that by CLAIM 3*, S_1 and X_1 exist. Similarly, for $i > 0$ let $S_{i+1} \in (S_i, Y_i)^{(n+1)^*}$ and $X_{i+1} \in (S_i, Y_i)^\omega \cap \mathscr{C}$ be such that the set

$$E_{i+1} = \{T \in (S_{i+1}, X_{i+1})^{(n+i+1)^*} : (S_i, T)^{n+i} \subseteq E_i\}$$

is $\mathscr{C}$-dense in $(S_{i+1}, X_{i+1})^{(n+i+1)^*}$. By induction on i one verifies that for all $i \in \omega$ we have

$$E_{i+1} \subseteq \left\{T \in (S_{i+1}, X_{i+1})^{(n+i+1)^*} : (S_0, T)^n \subseteq D_0\right\},$$

where $E_0 := D_0$ (the details are left to the reader). Finally, fix a play where the MAIDEN follows this strategy but DEATH wins, and let $X \in (\omega)^\omega$ be the unique infinite partition such that for all $i \in \omega$ we have $S_i \prec X$. Since $\mathscr{C}$ is a Ramsey partition-family, X belongs to $\mathscr{C}$. Now, since D_0 is $\mathscr{C}$-dense in $(S_0, X_0)^\omega$ and $X \in (S_0, X_0)^\omega \cap \mathscr{C}$, there is a $U_0 \in (S_0, X)^{(n)^*}$ such that $U_0 \in D_0$. Choose $i_0 \in \omega$ large enough such that there is an $S \in (S_0, S_{i_0})^{n+1}$ for which we have $U_0^* \preccurlyeq S$. Since $(S_0, S)^n \subseteq (S_0, S_{i_0})^n$ we get that $\left\{T \in (S, X_{i_0})^{(n+1)^*} : (S_0, T)^n \subseteq D_0\right\}$ is $\mathscr{C}$-dense in $(S, X_{i_0})^{(n+1)^*}$. In particular, the set $\left\{T \in (S, X)^{(n+1)^*} : (S_0, T)^n \subseteq D_0\right\}$ is $\mathscr{C}$-dense in $(S, X)^{(n+1)^*}$, and since $\pi(U_0) = 0$ and $U_0^* \preccurlyeq S$, U_0 has the required properties. $\dashv_{\text{Claim 4}}$

We leave it as an exercise to the reader to prove the following generalisation of CLAIM 4:

CLAIM 4*. *If* $U_i \in (S_0, X_0)^{(n+i)^*}$ *is such that* $(S_0, U_i)^n \subseteq D_0$ *and* $Y \in (U_i^*, X_0)^\omega \cap \mathscr{C}$ *is such that* $\left\{T \in (U_i, Y)^{(n+i+1)^*} : (S_0, T)^n \subseteq D_0\right\}$ *is* $\mathscr{C}$*-dense in* $(U_i, Y)^{(n+1)^*}$*, then there are* $U_{i+1} \in (U_i^*, Y)^{(n+i+1)^*}$ *and* $X \in (U_{i+1}^*, Y)^\omega \cap \mathscr{C}$ *such that*

$$\left\{T \in (U_{i+1}, X)^{(n+i+2)^*} : (S_0, T)^n \subseteq D_0\right\}$$

is $\mathscr{C}$*-dense in* $(U_{i+1}, X)^{(n+1)^*}$ *and* $(S_0, U_{i+1})^n \subseteq D_0$.

Now we are ready to construct an infinite partition $\bar{X} \in (S_0, X_0)^\omega \cap \mathscr{C}$ such that for every $U \in (S_0, \bar{X})^{(n)^*}$ we have $\pi(U) = 0$, *i.e.*, $(S_0, \bar{X})^{(n)^*} \subseteq D_0$: Indeed, by defining a suitable strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{C}}$ (applying CLAIM 4*), we can construct partitions $U_i \in (S_0, X_0)^{(<\omega)^*}$ such that for all $i \in \omega$ we have

$$|U_i| = n + i\,, \quad U_i^* \preccurlyeq U_{i+1}\,, \quad (S_0, U_i)^n \subseteq D_0\,, \tag{$\circledast$}$$

and the unique partition $\bar{X} \in (\omega)^\omega$ such that $U_i \prec \bar{X}$ (for all $i \in \omega$) belongs to the Ramsey partition-family $\mathscr{C}$. By ($\circledast$), for all $U \in (S_0, \bar{X})^{(n)^*}$ we have $(S_0, U)^n \subseteq D_0$, *i.e.*, $(S_0, \bar{X})^{(n)^*}$ is monochromatic, which completes the proof of CARLSON'S LEMMA. $\dashv$

Having CARLSON'S LEMMA at hand, we are now able to prove the main result of this chapter:

Proof of the Partition Ramsey Theorem. The proof is by induction on n. For $n = 1$, the PARTITION RAMSEY THEOREM follows immediately by the Pigeon-Hole Principle. So, let $n, r \in \omega$ be given, where r is positive and $n > 1$, and assume that the PARTITION RAMSEY THEOREM is already proved for all positive integers $n' < n$.

Fix an arbitrary colouring $\pi : (\omega)^n \to r$. Take an arbitrary partition $X_0 \in \mathscr{C}$ and let $S_0 \in (\mathbb{N})$ be such that $|S_0| = n-1$ and $S_0^* \prec X_0$.

We define a strategy for the MAIDEN in the game $\mathcal{G}_{\mathscr{C}}$ and as byproduct we get a partial mapping τ from $(\omega)^{n-1}$ to r. The MAIDEN starts the game with (S_0, X_0) and replies the i^{th} move Y_i of DEATH with (S_{i+1}, X_{i+1}), where S_{i+1} and X_{i+1} are constructed as follows: Let $\{T_k \in (\mathbb{N}) : k \in h_i\}$ be an enumeration of all $T \sqsubseteq S_i$ with $\mathrm{Dom}(T) = \mathrm{Dom}(S_i)$ and $|T| = n-1$. Let $Z_0 := Y_i$, and for each $k \in h_i$, let $Z_{k+1} \in (S_i^*, Z_k)^\omega \cap \mathscr{C}$ be such that $\pi|_{(T_k^*, Z_{k+1})^{(n)^*}}$ is constant and define

$$\tau(T_k) = \pi(U) \text{ for some } U \in (T_k^*, Z_{k+1})^{(n)^*}.$$

Now, the partition $Z_{k+1} \in \mathscr{C}$ we construct by applying first CARLSON'S LEMMA 11.5 with respect to the dual Ellentuck neighbourhood $(T_k^*, Z_k)^\omega$ and then by refining the resulting partition such that it belongs to the dual Ellentuck neighbourhood $(S_i^*, Z_k)^\omega$. Let $X_{i+1} := Z_{h_i}$ and let $S_{i+1} \in (\mathbb{N})$ be such that $S_{i+1}^* \prec X_{i+1}$ and $|S_{i+1}| = (n-1) + (i+1)$. Finally, fix a play where the MAIDEN follows this strategy but DEATH wins, and let $Z \in (\omega)^\omega$ be the unique infinite partition such that for all $i \in \omega$ we have $S_i \prec Z$. Since $\mathscr{C}$ is a Ramsey partition-family, the partition Z belongs to $\mathscr{C}$. For each $T \in (Z)^{(n-1)^*}$ there exist unique numbers $i, k \in \omega$ such that $k \in h_i$ and $T = T_k$. Thus, τ is an r-colouring of $(Z)^{(n-1)^*}$. By the induction hypothesis we find an $X \in (Z)^\omega \cap \mathscr{C}$ such that $\tau|_{(X)^{(n-1)^*}}$ is constant, say $\tau(T) = j$ for all $T \in (X)^{(n-1)^*}$. Now, take any $S \in (X)^{(n)^*}$ and let $\tilde{S}^* \prec S$ be such that $|\tilde{S}| = n-1$. Notice that the domain of $\tilde{S}$ is equal to $\mathrm{Dom}(S_i)$ for some $i \in \omega$. Consider the partition X_{i+1}. By the construction of X_{i+1} we know that $(T^*, X_{i+1})^{(n)^*}$ is monochromatic whenever $T \sqsubseteq S_i$ with $|T| = n-1$ and $\mathrm{Dom}(T) = \mathrm{Dom}(S_i)$, and by the construction of the partition X, $\pi|_{(T^*, X_{i+1})^{(n)^*}}$ is constantly j. In particular, $\pi(U) = j$ whenever $U \in (\tilde{S}^*, X_{i+1})^{(n)^*}$, and since $S \in (\tilde{S}^*, X_{i+1})^{(n)^*}$, we get $\pi(S) = j$, which completes the proof. ⊣

A Weak Form of the Halpern-Läuchli Theorem

One can show that for example the HALES-JEWETT THEOREM, a weakened form of the HALPERN-LÄUCHLI THEOREM, RAMSEY'S THEOREM, as well as the FINITE RAMSEY THEOREM and a partition form of it, are all derivable from the PARTITION RAMSEY THEOREM. Below, we just give the proof of the WEAK HALPERN-LÄUCHLI THEOREM (for the other results see RELATED RESULT 75).

To state this weakened form of the HALPERN-LÄUCHLI THEOREM, we have to give first some notations: A set $T \subseteq \mathrm{seq}(2)$, where $\mathrm{seq}(2) = \bigcup_{n\in\omega} {}^n2$, is a **tree** if for every $s \in T$ and $k \in \mathrm{dom}(s)$ we have $s|_k \in T$. In particular, $\mathrm{seq}(2)$ is a tree. For a tree $T \subseteq \mathrm{seq}(2)$ and $l \in \omega$ let

$$T(l) = \{s \in T : \mathrm{dom}(s) = l\}.$$

For a finite product of trees $\mathscr{T} = T_0 \times \ldots \times T_{d-1} \subseteq \big(\mathrm{seq}(2)\big)^d$ (*i.e.*, for all $k \in d$, where $d \in \omega$, $T_k \subseteq \mathrm{seq}(2)$ is a tree), and for $l \in \omega$, let

$$\mathscr{T}(l) = \big\{s \in \mathscr{T} : s \in T_0(l) \times \ldots \times T_{d-1}(l)\big\}.$$

A tree $T \subseteq \mathrm{seq}(2)$ is **perfect** if for each $s \in T$ there is an $n > \mathrm{dom}(s)$ and two *distinct* functions $t_0, t_1 \in {}^n2 \cap T$ such that $t_0|_{\mathrm{dom}(s)} = t_1|_{\mathrm{dom}(s)} = s$. In other words, for each $s \in T$ there are $t_0, t_1 \in T$ and $k \in \mathrm{dom}(t_0) \cap \mathrm{dom}(t_1)$ such that $t_0|_{\mathrm{dom}(s)} = t_1|_{\mathrm{dom}(s)} = s$ and $t_0(k) = 1 - t_1(k)$.

Now we are ready to state and proof the following result.

THEOREM 11.6 (WEAK HALPERN-LÄUCHLI THEOREM). *For every positive $d \in \omega$ and for every colouring of $\bigcup_{l\in\omega}({}^l2)^d$ with finitely many colours, there exists a product of perfect trees $\mathscr{T} = T_0 \times \ldots \times T_{d-1}$ and an infinite set $H \subseteq \omega$ such that $\bigcup_{l\in H} \mathscr{T}(l)$ is monochromatic.*

Proof. Let d be a fixed positive integer and let $n := 2^d$. Because $|{}^d2| = 2^d$, there exists a one-to-one correspondence ζ between n and ${}^d2$. For any $l \in \omega$, an element $\langle s_0, \ldots, s_{d-1}\rangle \in ({}^l2)^d$ is a sequence of length d of functions $s_i : l \to 2$. For any $l \in \omega$, define the function $\xi : ({}^l2)^d \to ({}^d2)^l$ by stipulating

$$\xi(\langle s_0, \ldots, s_{d-1}\rangle) = \langle t_0, \ldots, t_{l-1}\rangle \text{ where } t_j(i) := s_i(j)\,,$$

in other words, for any function $s : d \to {}^l2$, $\xi(s)(j)(i) = s(i)(j)$. Notice that for each $l \in \omega$, the function ξ is a one-to-one function from $({}^l2)^d$ onto $({}^d2)^l$. Let $S = \{u_k : k \in n\} \in (\omega)^n$ be such that $\min(u_0) < \min(u_1) < \ldots \min(u_{n-1})$. For $j \in u_k$ let $t^S_j(i) := \xi(k)(i)$. Now, define the function $\eta : (\omega)^n \to \big(\mathrm{seq}(2)\big)^d$ by stipulating

$$\eta(S) = \xi^{-1}\big(\langle t^S_0, \ldots, t^S_{\mathrm{Dom}(S)-1}\rangle\big)\,.$$

Notice that for $S \in (\omega)^n$ with $\mathrm{Dom}(S) = l$, $\eta(S) \in ({}^l2)^d$. Finally, for any colouring $\pi : \bigcup_{l\in\omega}({}^l2)^d \to r$, where r is a positive integer, we define the colouring $\tau : (\omega)^n \to r$ by stipulating $\tau(S) := \pi\big(\eta(S)\big)$. Let $X \in (\omega)^\omega$ be as in the conclusion of the PARTITION RAMSEY THEOREM 11.4 (with respect to the colouring τ). Let $S_0^* \prec X$ be such that $|S_0| = n$ and let $H := \mathrm{Min}(X) \setminus \mathrm{Min}(S_0)$. Further, let

$$\mathscr{S} = \big\{S \in (\omega)^n : S \preccurlyeq S_0 \,\vee\, S_0 \preccurlyeq S \sqsubseteq X\big\}$$

and define

$$\mathscr{T} = \big\{s \in \big(\mathrm{seq}(2)\big)^d : \exists S \in \mathscr{S}\big(s = \eta(S)\big)\big\}\,.$$

We leave it as an exercise to the reader to check that $\mathscr{T}$ and H are as desired and that they have the desired properties. ⊣

For the full version of the HALPERN-LÄUCHLI THEOREM see RELATED RESULT 77. However, in many applications the WEAK HALPERN-LÄUCHLI

THEOREM is strong enough. For example the WEAK HALPERN-LÄUCHLI THEOREM is sufficient to prove that a finite product of Sacks forcing does not add splitting reals (see Chapter 22 | RELATED RESULT 121).

NOTES

Van der Waerden's Theorem. The theorem of van der Waerden can be considered as the beginning of Ramsey Theory and it was first proved by van der Waerden in [34]. For a short but not easy proof of VAN DER WAERDEN'S THEOREM see Graham and Rothschild [8], and for a combinatorial proof of a slightly more general result see Pin [22, Chapter 3].For a description of how van der Waerden found his proof we refer the reader to [35].

The Hales-Jewett Theorem. In Graham, Rothschild, and Spencer [9, p. 35 ff.] we can read the following remark: VAN DER WAERDEN'S THEOREM *should be regarded, not as a result dealing with integers, but rather as a theorem about finite sequences formed from finite sets. The* HALES-JEWETT THEOREM *strips* VAN DER WAERDEN'S THEOREM *of its unessential elements and reveals the heart of Ramsey theory.* As mentioned above, the original proof of Hales and Jewett [13] (*cf.* Prömel and Voigt [28, p. 117 f.]) uses a double induction which leads to an extremely fast growing upper bound for the Hales-Jewett function $HJ(n, r)$. In 1987, Shelah [30] found a fundamentally new proof of the HALES-JEWETT THEOREM which just uses simple induction on n and provides a much better bound for $HJ(n, r)$. The proof of the HALES-JEWETT THEOREM (*i.e.*, of THEOREM 11.3) presented here is Shelah's proof modified by Matet [23], who replaced what is sometimes called "Shelah's pigeonhole lemma" by the FINITE RAMSEY THEOREM. For the HALES-JEWETT THEOREM, and in particular for Shelah's proof, see also Graham, Rothschild, and Spencer [9, Chapter 2], Nilli [25], Prömel and Voigt [28, p. 119 ff.], and Jukna [19, Chapter 29].

Carlson's Lemma and the Partition Ramsey Theorem. According to Carlson and Simpson [4, p. 268], Carlson proved Lemma 2.4 of [4] in 1982. In fact, he proved a stronger result involving so-called "special partitions", which are essentially segmented partitions where finitely many blocks may be infinite; and in the proof of LEMMA 11.5 we essentially followed Carlson's proof of that stronger result, which is Theorem 6.3 of [4]. CARLSON'S LEMMA, or more precisely Lemma 2.4 of [4], plays a key role in the proof of the DUAL RAMSEY THEOREM, which is the main result of Carlson and Simpson [4]. The DUAL RAMSEY THEOREM corresponds to our *Generalisation 1* — where the set $(\omega)^n$ is coloured with finitely many colours — except that the set of admissible colours of $(\omega)^n$ is restricted to *Borel colourings*. Thus, the DUAL RAMSEY THEOREM is in a certain sense the dual of RAMSEY'S THEOREM. However, it was natural to seek a partition form (*i.e.*, dual form) of RAMSEY'S THEOREM which works for arbitrary colourings. Such a result we found in the PARTITION RAMSEY THEOREM (see also RELATED RESULT 75). The proof of the PARTITION RAMSEY THEOREM 11.4 is taken from Halbeisen [10, Chapter IV.2] (for the relation between the PARTITION RAMSEY THEOREM and other Ramsey-type results we refer the reader to Halbeisen [10, Chapter IV.4])..

The Halpern-Läuchli Theorem. What we stated as WEAK HALPERN-LÄUCHLI THEOREM 11.6 is just a consequence of the HALPERN-LÄUCHLI THEOREM (see RELATED RESULT 77), which was first proved by Halpern and Läuchli in [15] and later by Halpern in [14] (see also Argyros, Felouzis and Kanellopoulos [1], Todorčević [32, Chapter 3], or Todorčević and Farah [33]). According to Pincus and Halpern [26, p. 549] (*cf.* [16, p. 97]) the original purpose of the HALPERN-LÄUCHLI THEOREM was to show that in ZF, the Prime Ideal Theorem does not imply the Axiom of Choice, which was proved by Halpern and Lévy in [16] (*cf.* THEOREM 7.16, where it is shown that in ZFA, PIT does not imply AC). As mentioned above, in many applications, a weak form or a particular case of the HALPERN-LÄUCHLI THEOREM is sufficient (*e.g.*, Halpern and Lévy [16, p. 97]). The version of the HALPERN-LÄUCHLI THEOREM given above — as well as the idea of proof — is taken from Carlson and Simpson [4, p. 272]. For some applications and other weak forms of the HALPERN-LÄUCHLI THEOREM see RELATED RESULT 77.

RELATED RESULTS

73. *Van der Waerden numbers.* For positive integers r and $l_1, l_2, \ldots, l_r$, the *van der Waerden number* $w(l_1, l_2, \ldots, l_r; r)$ is the least positive integer N such that for every r-colouring of set $\{1, 2, \ldots, N\}$, there is a monochromatic arithmetic progression of length l_i of colour i for some i. In [3], Brown, Landman, and Robertson gave asymptotic lower bounds for $w(l, m; 2)$ for fixed m, as well as for $w(4, 4, \ldots, 4; r)$.

74. *Non-repetitive sequences and van der Waerden's Theorem*.* A finite set of one or more consecutive terms in a sequence is called a *segment* of the sequence. A sequence on a finite set of symbols is called *non-repetitive* if no two adjacent segments are identical, where adjacent means abutting but not overlapping. It is known that there are infinite non-repetitive sequences on three symbols (see Pleasants [27]), and on the other hand, it is obvious that a non-repetitive sequence on two symbols is at most of length 3. Erdős has raised in [6] the question of the maximum length of a sequence on k symbols, such that no two adjacent segments are *permutations* of each other. Such a sequence is called *strongly non-repetitive*. Keränen [20] has shown that four symbols are enough to construct an infinite strongly non-repetitive sequence.
Now, replacing the finite set of symbols of an infinite strongly non-repetitive sequence by different prime numbers, one gets an infinite sequence on a finite set of integers such that no two adjacent segments have the same *product*. It is natural to ask whether one can replace in the statement above "product" by "sum", which leads to the following question: Is it possible to construct an infinite sequence on a finite set of integers such that no two adjacent segments have the same sum? By an application of VAN DER WAERDEN'S THEOREM, it is not hard to show that the answer to this question is negative. Moreover, in any infinite sequence on a finite set of integers we always find arbitrary large finite sets of adjacent segments such that all these segments have the same sum (see Hungerbühler and Halbeisen [11]). However, it is still open whether there exists an infinite sequence on a finite set of integers such that no two adjacent segments *of the same length* have the same sum. It seems that VAN DER WAERDEN'S THEOREM alone is not strong enough to solve this problem.

75. *Corollaries of the Partition Ramsey Theorem.* Below, we present a few corollaries of the PARTITION RAMSEY THEOREM. We would like to mention that these

corollaries — like for example the WEAK HALPERN-LÄUCHLI THEOREM — also follow from the so-called DUAL RAMSEY THEOREM, which is due to Carlson and Simpson [4].

Firstly we derive RAMSEY'S THEOREM from the PARTITION RAMSEY THEOREM: To every r-colouring $\pi : [\omega]^n \to r$ of the n-element subsets of ω we can assign an r-colouring $\tau : (\omega)^n \to r$ by stipulating $\tau(S) := \pi\big(\operatorname{Min}(S^*) \setminus \{0\}\big)$. Now, if $(X)^{(n)^*}$ is monochromatic for τ for some $X \in (\omega)^\omega$, then $\operatorname{Min}(X) \setminus \{0\}$ is monochromatic for π, and since $\operatorname{Min}(X) \in [\omega]^\omega$, this shows that RAMSEY'S THEOREM 2.1 is just a special case of the PARTITION RAMSEY THEOREM. Similarly, the FINITE RAMSEY THEOREM 2.3 as well as the HALES-JEWETT THEOREM 11.2 follows from the following finite version of the PARTITION RAMSEY THEOREM which is originally due to Graham and Rothschild [7, Corollary 10].

GRAHAM-ROTHSCHILD RESULT: *For all $m, n, r \in \omega$, where $r \geq 1$ and $n \leq m$, there exists an $N \in \omega$, where $N \geq m$, such that for every r-colouring of $(N)^n$ there exists a partition $H \in (N)^m$, all of whose n-block coarsenings have the same colour.*

The relation between these results is illustrated by the following figure.

$$
\begin{tikzcd}
\text{PARTITION RAMSEY THEOREM} \arrow[r] \arrow[d] & \text{RAMSEY'S THEOREM} \arrow[d] \\
\text{GRAHAM-ROTHSCHILD RESULT} \arrow[r] \arrow[d] & \text{FINITE RAMSEY THEOREM} \\
\text{HALES-JEWETT THEOREM} &
\end{tikzcd}
$$

As a matter of fact we would like to remind the reader that we used the FINITE RAMSEY THEOREM to prove the HALES-JEWETT THEOREM, that we used the HALES-JEWETT THEOREM to start the induction in the proof of CARLSON'S LEMMA 11.5, and that CARLSON'S LEMMA was crucial in the proof of the PARTITION RAMSEY THEOREM.

76. *A generalisation of the Partition Ramsey Theorem.* By combining CARLSON'S LEMMA with the GRAHAM-ROTHSCHILD RESULT, Halbeisen and Matet [12] proved a result which is even stronger than the PARTITION RAMSEY THEOREM.

77. *The Halpern-Läuchli Theorem.* Before we can state the full HALPERN-LÄUCHLI THEOREM of Halpern and Läuchli [15], we have to introduce some terminology. A set $T \subseteq {}^{<\omega}\omega$, where ${}^{<\omega}\omega = \bigcup_{n\in\omega} {}^n\omega$, is a *finitely branching tree* if T is a tree (*i.e.*, for every $s \in T$ and $k \in \operatorname{dom}(s)$, $s|_k \in T$) such that for all $s \in T$, the set $\big\{t \in T : s \subseteq t \wedge |t| = |s| + 1\big\}$ is finite. An element $s \in T$ of a tree $T \subseteq {}^{<\omega}\omega$ is a *leaf* if $\{t \in T : s \subsetneq t\} = \emptyset\}$. If A and B are subsets of a tree $T \subseteq {}^{<\omega}\omega$, then we say that A *supports* (*dominates*) B if for all $t \in B$ there exists an $s \in A$ such that $s \subseteq t$ ($t \subseteq s$). A subset D of a tree $T \subseteq {}^{<\omega}\omega$ is said to be (h, k)-*dense* if there is an $s \in T$ with $|s| = h$ such that $\big\{t \in T : s \subseteq t \wedge |t| = h + k\big\}$ is dominated by D. Let $\prod_{i\in d} T_i = T_0 \times \ldots \times T_{d-1}$ be a product of trees $T_i \subseteq {}^{<\omega}\omega$.

A product $\prod_{i\in d} A_i \subseteq \prod_{i\in d} T_i$, where each A_i is (h,k)-dense in T_i, is called a (h,k)-*matrix*. Now we can state Theorem 1 of Halpern and Läuchli [15].

HALPERN-LÄUCHLI THEOREM: *Let $\prod_{i\in d} T_i$ be a finite product of finitely branching trees $T_i \subseteq {}^{<\omega}\omega$ without leaves, and let $Q \subseteq \prod_{i\in d} T_i$. Then either*
(a) for each k, Q contains a $(0,k)$-matrix, or
(b) there exists h such that for each k, $\left(\prod_{i\in d} T_i\right) \setminus Q$ contains an (h,k)-matrix.

There exist many reformulations, weakenings, and generalised forms of the HALPERN-LÄUCHLI THEOREM. For example Hans Läuchli proved in a student seminar at the ETH Zürich a weak form of the HALPERN-LÄUCHLI THEOREM in which the trees $T \subseteq {}^{<\omega}\omega$ were replaced by $\bigcup_{n\in\omega}\left\{[\frac{k}{2^n}, \frac{k+1}{2^n}) : k \in 2^n\right\}$, and in which the set $[0,1)^2$ was coloured with two colours. The HALPERN-LÄUCHLI THEOREM is a very strong combinatorial statement and even weak forms of it have interesting applications (see for example Chapter 22 | RELATED RESULT 121, Blass [2, Polarized Theorem], or Milliken [24]). However, there are also some generalisations of the HALPERN-LÄUCHLI THEOREM: For example Laver [21] generalised the perfect tree version of the HALPERN-LÄUCHLI THEOREM to infinite products (see also Ramović [29]), and Shelah [31] replaced the trees $T \subseteq {}^{<\omega}\omega$ of height ω by trees of uncountable height (see also Džamonja, Larson, and Mitchell [5]).

78. *Partition regularity.* A finite or infinite matrix A with rational entries in which there are only a finite number of non-zero entries in each row is called partition regular if, whenever the natural numbers are finitely coloured, there is a monochromatic vector x (*i.e.*, all entries of x have the same colour) with $Ax = 0$. Many of the classical theorems of Ramsey Theory may naturally be interpreted as assertions that particular matrices are partition regular. For example, Schur's Theorem (*i.e.*, COROLLARY 2.5) is the assertion that the 1×3-matrix $(1, 1, -1)$ is partition regular; or VAN DER WAERDEN'S THEOREM is (with the strengthening that we may also choose the common difference of the arithmetic progression to have the same colour) exactly the statement that a certain $(m-1)\times(m+1)$-matrix is partition regular (see Hindman, Leader, and Strauss [18]). While in the finite case partition regularity is well understood, very little is known in the infinite case. For a survey of results on partition regularity of matrices see Hindman [17].

REFERENCES

1. SPIROS A. ARGYROS, VAGGELIS FELOUZIS, AND VASSILIS KANELLOPOULOS, *A proof of Halpern-Läuchli partition theorem*, ***European Journal of Combinatorics***, vol. 23 (2002), 1–10.
2. ANDREAS BLASS, *A partition theorem for perfect sets*, ***Proceedings of the American Mathematical Society***, vol. 82 (1981), 271–277.
3. TOM BROWN, BRUCE M. LANDMAN, AND AARON ROBERTSON, *Bounds on some van der Waerden numbers*, ***Journal of Combinatorial Theory (A)***, vol. 115 (2008), 1304–1309.
4. TIMOTHY J. CARLSON AND STEVE G. SIMPSON, *A dual form of Ramsey's Theorem*, ***Advances in Mathematics***, vol. 53 (1984), 265–290.

5. Mirna Džamonja, Jean A. Larson, and William J. Mitchell, *A partition theorem for a large dense linear order*, ***Israel Journal of Mathematics***, vol. 171 (2009), 237–284.
6. Paul Erdős, *Some unsolved problems*, ***Magyar Tudomanyos Akademia Matematikai Kutató Intezetenek Közlemenyei***, vol. 6 (1961), 221–254.
7. Ronald L. Graham and Bruce L. Rothschild, *Ramsey's Theorem for n-parameter sets*, ***Transactions of the American Mathematical Society***, vol. 159 (1971), 257–292.
8. ———, *A short proof of van der Waerden's Theorem on arithmetic progressions*, ***Proceedings of the American Mathematical Society***, vol. 42 (1974), 385–386.
9. Ronald L. Graham, Bruce L. Rothschild, and Joel H. Spencer, ***Ramsey Theory***, 2nd ed., J. Wiley & Sons, New York, 1980.
10. Lorenz Halbeisen, *Combinatorial properties of sets of partitions*, Habilitationsschrift (2003/2009), University of Bern/Zürich (Switzerland).
11. Lorenz Halbeisen and Norbert Hungerbühler, *An application of van der Waerden's theorem in additive number theory*, ***Integers. Electronic Journal of Combinatorial Number Theory***, vol. 0 (2000), #A07, 5 pp. (electronic).
12. Lorenz Halbeisen and Pierre Matet, *A result in dual Ramsey theory*, ***Journal of Combinatorial Theory (A)***, vol. 100 (2002), 394–398.
13. Alfred W. Hales and Robert I. Jewett, *Regularity and positional games*, ***Transactions of the American Mathematical Society***, vol. 106 (1963), 222–229.
14. James D. Halpern, *Nonstandard combinatorics*, ***Proceedings of the London Mathematical Society, Ser. III***, vol. 30 (1975), 40–54.
15. James D. Halpern and Hans Läuchli, *A partition theorem*, ***Transactions of the American Mathematical Society***, vol. 124 (1966), 360–367.
16. James D. Halpern and Azriel Lévy, *The Boolean prime ideal theorem does not imply the axiom of choice*, in ***Axiomatic Set Theory*** (Dana S. Scott, ed.), [Proceedings of Symposia in Pure Mathematics, Vol. XIII, Part I], American Mathematical Society, Providence, Rhode Island, 1971, pp. 83–134.
17. Neil Hindman, *Partition regularity of matrices*, in ***Combinatorial Number Theory*** (Bruce Landman, Melvyn B. Nathanson, Jaroslav Nešetřil, Richard J. Nowakowski, and Carl Pomerance, eds.), Proceedings of the 'Integers Conference 2005' in Celebration of the 70th Birthday of Ronald Graham. Carrollton, Georgia, USA, October 27–30, 2005, Walter de Gruyter, Berlin, 2007, pp. 265–298.
18. Neil Hindman, Imre Leader, and Dona Strauss, *Open problems in partition regularity*, ***Combinatorics, Probability and Computing***, vol. 12 (2003), 571–583.
19. Stasys Jukna, ***Extremal combinatorics. With applications in computer science***, [Texts in Theoretical Computer Science], Springer-Verlag, Berlin, 2001.
20. Veikko Keränen, *Abelian squares are avoidable on 4 letters*, in ***Automata, languages and programming (Vienna, 1992)*** (A.R.D. Mathias, ed.), [Lecture Notes in Computer Science 623], Springer-Verlag, Berlin, 1992, pp. 41–52.
21. Richard Laver, *Products of infinitely many perfect trees*, ***Journal of the London Mathematical Society (2)***, vol. 29 (1984), 385–396.

22. M. Lothaire, ***Combinatorics on Words***, [Cambridge Mathematical Library], Cambridge University Press, Cambridge, 1997, With a foreword by Roger Lyndon and a preface by Dominique Perrin, Corrected reprint of the 1983 original, with a new preface by Perrin.
23. Pierre Matet, *Shelah's proof of the Hales-Jewett theorem revisited*, ***European Journal of Combinatorics***, vol. 28 (2007), 1742–1745.
24. Keith R. Milliken, *A Ramsey theorem for trees*, ***Journal of Combinatorial Theory (A)***, vol. 26 (1979), 215–237.
25. Alon Nilli, *Shelah's proof of the Hales-Jewett theorem*, in ***Mathematics of Ramsey Theory*** (J. Nešetřil and V. Rödl, eds.), [Algorithms and Combinatorics 5], Springer-Verlag, Berlin, 1990, pp. 150–151.
26. David Pincus and James D. Halpern, *Partitions of products*, ***Transactions of the American Mathematical Society***, vol. 267 (1981), 549–568.
27. Peter A. B. Pleasants, *Non-repetitive sequences*, ***Proceedings of the Cambridge Philosophical Society***, vol. 68 (1970), 267–274.
28. Hans J. Prömel and Bernd Voigt, *Graham-Rothschild parameter sets*, in ***Mathematics of Ramsey Theory*** (J. Nešetřil and V. Rödl, eds.), Springer-Verlag, Berlin, 1990, pp. 113–149.
29. Goran Ramović, *Halpern-Läuchli theorem on the product of infinitely many trees in the version of strongly embedded trees*, ***Univerzitet u Beogradu. Publikacije Elektrotehničkog Fakulteta. Serija Matematika***, vol. 7 (1996), 18–24.
30. Saharon Shelah, *Primitive recursive bounds for the van der Waerden numbers*, ***Journal of the American Mathematical Society***, vol. 1 (1988), 683–697.
31. ———, *Strong partition relations below the power set: consistency; was Sierpiński right? II.*, in ***Sets, Graphs and Numbers (Budapest, 1991)*** (G. Halasz, Laszlo Lovasz, D. Miklos, and T. Szonyi, eds.), Colloquia Mathematica Societatis János Bolyai, vol. 60, North-Holland, Amsterdam, 1992, pp. 637–668.
32. Stevo Todorčević, ***Introduction to Ramsey Spaces***, [Annals of Mathematics Studies 174], Princeton University Press, Princeton (New Jersey), 2010.
33. Stevo Todorčević and Ilijas Farah, ***Some applications of the method of forcing***, [Yenisei Series in Pure and Applied Mathematics], Yenisei, Moscow, 1995.
34. Bartel L. van der Waerden, *Beweis einer Baudetschen Vermutung*, ***Nieuw Archief voor Wiskunde***, vol. 15 (1927), 212–216.
35. ———, *Wie der Beweis der Vermutung von Baudet gefunden wurde*, ***Elemente der Mathematik***, vol. 53 (1998), 139–148.

Part II

From Martin's Axiom to Cohen's Forcing

...changes of genus are brought about not by the introduction of major or minor thirds, divided or undivided, but by a melodic progression through intervals proper to certain genera. It remains to be noted that the change from one genus to another is also accompanied by a change in melodic style.
...a difference of genus may be assumed when a notable divergence in melodic style is heard, with rhythm and words suitably accommodated to it.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

12

The Idea of Forcing

Forcing is a technique — invented by Cohen in the early 1960s — for proving the independence, or at least the consistency, of certain statements relative to ZFC. In fact, starting from a model of ZFC, Cohen constructed in 1962 models of ZF in which the Axiom of Choice fails as well as models of ZFC in which the Continuum Hypothesis fails. On the other hand, starting from a model of ZF, Gödel constructed a model of ZFC in which the Continuum Hypothesis holds (*cf.* Chapter 5). By combining these results we get that the Axiom of Choice is independent of ZF and that the Continuum Hypothesis is independent of ZFC.

Before we discuss Cohen's forcing technique, let us briefly recall what it means for a sentence φ to be independent of ZFC: From a syntactical point of view it means that neither φ nor its negation is provable from ZFC. From a semantical point of view it means that there are models of ZFC in which φ holds and some in which φ fails. Equivalently we can say that φ is independent of ZFC *iff* φ as well as its negation is consistent with ZFC (*i.e.*, $\mathsf{ZFC} + \varphi$ as well as $\mathsf{ZFC} + \neg\varphi$ has a model).

Now, in order to proof that a given sentence φ is consistent with ZFC, we have to show that $\mathsf{ZFC} + \varphi$ is consistent — tacitly assuming the consistency of ZFC. This can be done in different ways: For example one could apply the COMPACTNESS THEOREM 3.7 and show that whenever $\mathsf{ZFC}^* \subseteq \mathsf{ZFC}$ is a finite set of axioms, then $\mathsf{ZFC}^* + \varphi$ has a model (*i.e.*, $\mathsf{ZFC}^* + \varphi$ is consistent); or, starting from a model of ZFC, one could construct directly a model of $\mathsf{ZFC}+\varphi$.

These two approaches correspond to two different ways to look at forcing: In the latter point of view we consider forcing as a technique for extending models of ZFC in such a way that φ holds in the extended model. Except for Chapter 16, we will mainly take this approach which will be demonstrated in Chapter 14. Before we discuss the former approach, let us give two examples how a model of a given theory can be extended.

An example from Group Theory: Consider the group $\mathbf{G} = (\mathbb{Q}^+, \cdot)$ (*i.e.*, $\mathbf{G} \vDash \mathsf{GT}$, the domain of $\mathbf{G}$ is the set of all positive rational numbers with

multiplication as operation), and let φ be the statement $\exists x\,(x \cdot x = 2)$. Obviously we have $\mathbf{G} \nvDash \varphi$.
Now, extend the domain of $\mathbf{G}$ by elements of the form qX, where $q \in \mathbb{Q}^+$, and for all $p, q \in \mathbb{Q}^+$ define:

- $p * q := p \cdot q$
- $p * qX := (p \cdot q)X$
- $pX * q := (p \cdot q)X$
- $pX * qX := 2 \cdot p \cdot q$
- $(pX)^{-1} := \left(\frac{1}{2} \cdot p^{-1}\right)X$

Let $\mathbb{Q}^+[X] = \mathbb{Q}^+ \cup \{pX : p \in \mathbb{Q}^+\}$ and $\mathbf{G}[X] = (\mathbb{Q}^+[X], *)$. We leave it as an exercise to the reader to show that $\mathbf{G}[X] \vDash \mathsf{GT}$. Now, $\mathbf{G}[X] \vDash 1X * 1X = 2$, and therefore, $\mathbf{G}[X] \vDash \varphi$. Thus, the extended model $\mathbf{G}[X]$ is a model of GT and the statement φ, which failed in $\mathbf{G}$, holds in $\mathbf{G}[X]$. So, by extending an existing model we were able to "force" that a given statement became true.

An example from Peano Arithmetic: Assume that PA is consistent and let $\mathbf{N} = (\mathbb{N}, 0, s, +, \cdot\,)$ — where for $n \in \mathbb{N}$, $s(n) := n + 1$ — be a model of PA. Let ψ be the statement $\exists x\,(x + x = 1)$, where $1 := s(0)$. Obviously we have $\mathbf{N} \nvDash \psi$. Now, let us try the same trick as above: So, extend the domain of $\mathbf{N}$ by elements of the form $n + X$, where $n \in \mathbb{N}$, and extend the operation "+" by stipulating $X + X := 1$. Now, the corresponding model $\mathbf{N}[X]$ is surely a model of ψ, but do we also have $\mathbf{N}[X] \vDash \mathsf{PA}$?

By setting $\varphi(x) \equiv (x = \mathsf{0}) \vee \exists y\,\big(x = \mathsf{s}(y)\big)$ in PA_7, we get that each number is either equal to 0 or a successor. Now, since $X \neq 0$, it must be a successor. Thus, there is a y such that $X = y + 1$, and since $X \neq 1$, by PA_2 we get $y \neq 0$. Similarly we can show that there is a z such that $y = z + 1$, and consequently $X = (z + 1) + 1$. Now, $1 = X + X = X + \big((z + 1) + 1\big)$ and by PA_4 we get $X + \big((z+1)+1\big) = \big(X + (z+1)\big) + 1$, which implies (by PA_2) that $X + (z + 1) = 0$. Applying again PA_4 we finally get $(X + z) + 1 = 0$, which contradicts PA_1. Thus, $\mathbf{N}[X]$ is not a model of PA.

This example shows that just extending an existing model of a theory T in order to "force" that a given statement becomes true may result in a model which is no longer a model of T.

Let us now discuss the other approach to forcing (demonstrated in Chapter 16), where one shows that whenever ZFC^* is a finite set of axioms of ZFC, then $\mathsf{ZFC}^* + \varphi$ is consistent (as always, we tacitly assume the consistency of ZFC): Let ZFC^* be an arbitrary finite set of axioms of ZFC and let $\mathbf{V}$ be a model of ZFC (*e.g.*, $\mathbf{V} = \mathbf{L}$). The so-called Reflection Principle (discussed in Chapter 15) tells us that for every **finite fragment** ZFC^* of ZFC (*i.e.*, for every finite set of axioms of ZFC) there is a *set model* $\mathbf{M}$ such that $\mathbf{M} \vDash \mathsf{ZFC}^*$ where the domain of $\mathbf{M}$ is a *set* M in the model $\mathbf{V}$. The goal is now to show that for any finite set Φ of axioms of ZFC, there is a finite fragment ZFC^* of ZFC such that it is possible to extend any set model $\mathbf{M}$ of ZFC^* to a set model $\mathbf{M}[X]$ of $\Phi + \varphi$ (*i.e.*, we "force" that φ as well as the formulae in Φ

become true in $\mathbf{M}[X]$). Then, since Φ was arbitrary, by the COMPACTNESS THEOREM 3.7 we get the consistency of $\mathsf{ZFC} + \varphi$.

The advantage of this approach is that the entire forcing construction can be carried out in the model $\mathbf{V}$: Because M, the domain of $\mathbf{M}$, is a *set* in the model $\mathbf{V}$ (but not in the model $\mathbf{M}$), we can extend the model $\mathbf{M}$ within $\mathbf{V}$ to the desired model $\mathbf{M}[X]$, such that the domain of $\mathbf{M}[X]$ is still a *set* in $\mathbf{V}$. So, all takes place within the model $\mathbf{V}$.

To illustrate this approach let us consider again the group-theoretic example from above: Let us work with the group $\bar{\mathbf{G}} = (\mathbb{R}^+, \cdot\,)$, where $\mathbb{R}^+$ is the set of positive real numbers. Now, the group $\mathbf{G} = (\mathbb{Q}^+, \cdot\,)$ is just a subgroup of $\bar{\mathbf{G}}$ and in $\bar{\mathbf{G}}$ we can extend $\mathbf{G}$ to the group $\mathbf{G}[\sqrt{2}]$ with domain $\mathbb{Q}^+ \cup \{p \cdot \sqrt{2} : p \in \mathbb{Q}^+\}$, which is still a subgroup of $\bar{\mathbf{G}}$.

A difference to the other approach is that we look now at the model $\mathbf{G}$ from the larger model $\bar{\mathbf{G}}$ (*i.e.*, from "outside"), and extend $\mathbf{G}$ within this model. Another difference is that in the former example, the symbol X — at least for people living in $\mathbf{G}$ — is just a symbol with some specified properties, whereas in the latter example, $\sqrt{2}$ — at least for people living in $\bar{\mathbf{G}}$ — is a proper real number. Of course, for people living in $\mathbf{G}$, $\sqrt{2}$ is also just a symbol and is not more real than any other symbol. On the other hand, in the latter example the people living in $\bar{\mathbf{G}}$ know already that $\sqrt{2}$ exists, whereas in the former example there are no such people, since our universe is just $\mathbf{G}$.

Before the notion of forcing is introduced in Chapter 14, we present in the next chapter the so-called Martin's Axiom. We do so because on the one hand, Martin's Axiom is a statement closely related to forcing, involving also partially ordered sets and certain generic filters, but on the other hand, unlike forcing, it does not involve any model-theoretic or even metamathematical arguments. Furthermore, Martin's Axiom is a proper set-theoretical axiom which is widely used in other branches of Mathematics, especially in Topology.

13

Martin's Axiom

In this chapter, we shall introduce a set-theoretic axiom, known as Martin's Axiom, which is independent of ZFC. In the presence of the Continuum Hypothesis, Martin's Axiom becomes trivial, but if the Continuum Hypothesis fails, then Martin's Axiom becomes an interesting combinatorial statement as well as an important tool in Combinatorics. Furthermore, Martin's Axiom provides a good introduction to the forcing technique which will be introduced in the next chapter.

Filters on Partially Ordered Sets

Below, we introduce (and recall respectively) some properties of partially ordered sets, which will play an important role in the development and investigation of forcing constructions.

Let $\mathbb{P} = (P, \leq)$ be a partially ordered set. The elements of P are usually called **conditions**, since in the context of forcing, elements of partially ordered sets are conditions for sentences to be true in generic extensions. Two conditions p_1 and p_2 of P are called **compatible**, denoted $p_1 \mid p_2$, if there exists a $q \in P$ such that $p_1 \leq q \geq p_2$; otherwise they are called **incompatible**, denoted $p_1 \perp p_2$.

A typical example of a partially ordered set is the set of finite partial functions with inclusion as partial ordering: Let I and J be arbitrary sets. Then $\mathrm{Fn}(I, J)$ is the set of all functions p such that

- $\mathrm{dom}(p) \in \mathrm{fin}(I)$, *i.e.*, $\mathrm{dom}(p)$ is a finite subset of I, and
- $\mathrm{ran}(p) \subseteq J$.

For $p, q \in \mathrm{Fn}(I, J)$ define:

$$p \leq q \iff \mathrm{dom}(p) \subseteq \mathrm{dom}(q) \ \wedge\ q|_{\mathrm{dom}(p)} \equiv p$$

If we consider functions as sets of ordered pairs, as we usually do, then $p \leq q$ is just $p \subseteq q$. We leave it as an exercise to the reader to verify that $\big(\mathrm{Fn}(I, J), \subseteq\big)$ is indeed a partially ordered set.

Let $\mathbb{P} = (P, \leq)$ be a partially ordered set, and for the moment let $C \subseteq P$. Then C is called **directed** if for any $p_1, p_2 \in C$ there is a $q \in C$ such that $p_1 \leq q \geq p_2$, C is called **open** if $p \in C$ and $q \geq p$ implies $q \in C$, and C is called **downwards closed** if $p \in C$ and $q \leq p$ implies $q \in C$. Furthermore, C is called **dense** if for every condition $p \in P$ there is a $q \in C$ such that $q \geq p$. For example with respect to $\big(\mathrm{Fn}(I,J), \subseteq\big)$, for every $x \in I$ the set $\big\{p \in \mathrm{Fn}(I,J) : x \in \mathrm{dom}(p)\big\}$ is open and dense. Finally, a non-empty set $F \subseteq P$ is a **filter** (on P) if it is directed and downwards closed. Notice that this definition of "filter" reverses the ordering from the definition given in Chapter 5. Let $\mathscr{D} \subseteq \mathscr{P}(P)$ be a set of open dense subsets of P. A filter $G \subseteq P$ is a **$\mathscr{D}$-generic filter** on P if $G \cap D \neq \emptyset$ for every open dense set $D \in \mathscr{D}$. As an example consider again $\big(\mathrm{Fn}(I,J), \subseteq\big)$: If $\mathscr{F}$ is a filter on $\mathrm{Fn}(I,J)$, then $\bigcup \mathscr{F} : X \to J$ is a function, where X is some (possibly infinite) subset of I.

PROPOSITION 13.1. *If $(P, \leq)$ is a partially ordered set and $\mathscr{D}$ is a countable set of open dense subsets of P, then there exists a $\mathscr{D}$-generic filter on P. Moreover, for every $p \in P$ there exists a $\mathscr{D}$-generic filter G on P which contains p.*

Proof. For $\mathscr{D} = \{D_n : n \in \omega\}$ and $p_{-1} := p$, choose for each $n \in \omega$ a $p_n \in D_n$ such that $p_n \geq p_{n-1}$, which is possible since D_n is dense. Then the set

$$G = \big\{q \in P : \exists n \in \omega\, (q \leq p_n)\big\}$$

is a $\mathscr{D}$-generic filter on P and $p \in G$. $\dashv$

A set $A \subseteq P$ is an **anti-chain** in P if any two distinct elements of A are incompatible. As mentioned in Chapter 5, this definition of "anti-chain" is different from the one used in Order Theory. A partially ordered set $\mathbb{P} = (P, \leq)$ satisfies the **countable chain condition**, denoted *ccc*, if every anti-chain in P is at most countable (*i.e.*, finite or countably infinite).

As a consequence of the following lemma we get that $\mathrm{Fn}(I,J)$ satisfies *ccc* whenever J is countable.

LEMMA 13.2 (Δ-SYSTEM LEMMA). *Let $\mathscr{E}$ be an uncountable family of finite sets. Then there exist an uncountable family $\mathscr{C} \subseteq \mathscr{E}$ and a finite set Δ such that for any distinct elements $x, y \in \mathscr{C}$: $x \cap y = \Delta$.*

Proof. We shall consider two cases.

Case 1: *There exists an uncountable $\mathscr{E}' \subseteq \mathscr{E}$ such that for every $a \in \bigcup \mathscr{E}'$, $\{x \in \mathscr{E}' : a \in x\}$ is countable.* Firstly notice that for such a set $\mathscr{E}'$, $\bigcup \mathscr{E}'$ is uncountable, and that for any countable set $C \subseteq \bigcup \mathscr{E}'$, also the set $\{x \in \mathscr{E}' : x \cap C = \emptyset\}$ must be uncountable. By transfinite induction we construct an uncountable family $\{x_\alpha : \alpha \in \omega_1\} \subseteq \mathscr{E}'$ of pairwise disjoint sets as follows: Let x_0 be any member of $\mathscr{E}'$. If we have already constructed a set $C_\alpha = \{x_\xi : \xi \in \alpha \in \omega_1\} \subseteq \mathscr{E}'$ of pairwise disjoint sets, let $x_\alpha \in \mathscr{E}'$ be such that $x_\alpha \cap \bigcup C_\alpha = \emptyset$. Then $\mathscr{C} = \{x_\alpha : \alpha \in \omega_1\}$ and $\Delta = \emptyset$ are as required.

Case 2: *For every uncountable $\mathscr{E}' \subseteq \mathscr{E}$ there exists an $a \in \bigcup \mathscr{E}'$ such that $\{x \in \mathscr{E}' : a \in x\}$ is uncountable.* In this case, consider the function $\nu : \mathscr{E} \to \omega$, where for all $x \in \mathscr{E}$, $\nu(x) := |x|$. Since $\mathscr{E}$ is uncountable, there is an $n \in \omega$ and an uncountable set $\mathscr{E}' \subseteq \mathscr{E}$ such that $\nu|_{\mathscr{E}'} \equiv n$, *i.e.*, for all $x \in \mathscr{E}'$ we have $\nu(x) = n$.

The proof is now by induction on n: If $n = 1$, then for any two distinct elements $x, y \in \mathscr{E}'$ we have $x \cap y = \emptyset$, thus, $\Delta = \emptyset$ and in this case $\mathscr{C} = \mathscr{E}'$.

Now, let us assume that $\nu|_{\mathscr{E}'} \equiv n + 1$ for some $n \geq 1$ and that the lemma holds for n. Since we are in Case 2, there is an $a \in \bigcup \mathscr{E}'$ such that $\{x \in \mathscr{E}' : a \in x\}$ is uncountable. Thus, we can apply the induction hypothesis to the family $\mathscr{E}'_a := \big\{x \setminus \{a\} : x \in \mathscr{E}' \wedge a \in x\big\}$ and obtain an uncountable family $\mathscr{C}_a \subseteq \mathscr{E}'_a$ and a finite set Δ_a such that for any distinct elements $x, y \in \mathscr{C}_a$ we have $x \cap y = \Delta_a$. Then $\mathscr{C} := \big\{x \cup \{a\} : x \in \mathscr{C}_a\big\}$ and $\Delta := \Delta_a \cup \{a\}$ are as required. ⊣

COROLLARY 13.3. *If I is arbitrary and J is countable, then* $\mathrm{Fn}(I, J)$ *satisfies the countable chain condition.*

Proof. Let $\mathscr{F} \subseteq \mathrm{Fn}(I, J)$ be an uncountable family of partial functions. We have to show that $\mathscr{F}$ is not an anti-chain, *i.e.*, we have to find at least two distinct conditions in $\mathscr{F}$ which are compatible. Let $\mathscr{E} := \big\{\operatorname{dom}(p) : p \in \mathscr{F}\big\}$. Then $\mathscr{E}$ is obviously a family of finite sets. Further, since J is assumed to be countable, for every finite set $K \in \operatorname{fin}(I)$ the set $\big\{p \in \mathscr{E} : \operatorname{dom}(p) = K\big\}$ is countable, and therefore, since $\mathscr{F}$ is uncountable, $\mathscr{E}$ is uncountable as well.

Applying the Δ-SYSTEM LEMMA 13.2 to the family $\mathscr{E}$ yields an uncountable family $\mathscr{C} \subseteq \mathscr{F}$ and a finite set $\Delta \subseteq I$, such that for all distinct $p, q \in \mathscr{C}$, $\operatorname{dom}(p) \cap \operatorname{dom}(q) = \Delta$.

Since J is countable and Δ is finite, uncountably many conditions of $\mathscr{C}$ must agree on Δ, *i.e.*, for some $p_0 \in \mathrm{Fn}(I, J)$ with $\operatorname{dom}(p_0) = \Delta$, the set $\mathscr{C}' = \big\{q \in \mathscr{C} : q|_\Delta = p_0\big\}$ is uncountable. So, $\mathscr{C}'$ is an uncountable subset of $\mathscr{F}$ consisting of pairwise compatible conditions, hence, $\mathscr{F}$ is not an anti-chain. ⊣

The following hypothesis can be regarded as a generalisation of PROPOSITION 13.1 — for the reason why $\mathbb{P}$ must satisfy *ccc* see PROPOSITION 13.4.

> $\mathsf{MA}(\kappa)$: If $\mathbb{P} = (P, \leq)$ is a partially ordered set which satisfies *ccc*, and $\mathscr{D}$ is a set of at most κ open dense subsets of P, then there exists a $\mathscr{D}$-generic filter on P.

On the one hand, $\mathsf{MA}(\omega)$ is just PROPOSITION 13.1, and therefore, $\mathsf{MA}(\omega)$ is provable in ZFC. On the other hand, $\mathsf{MA}(\mathfrak{c})$ is just false as we will see in PROPOSITION 13.5. However, the following statement can neither be proved nor disproved in ZFC and can therefore be considered as a proper axiom of Set Theory (especially when CH fails):

> Martin's Axiom (MA): If $\mathbb{P} = (P, \leq)$ is a partially ordered set which satisfies *ccc*, and $\mathscr{D}$ is a set of less than $\mathfrak{c}$ open dense subsets of P, then there exists a $\mathscr{D}$-generic filter on P. In other words, $\mathsf{MA}(\kappa)$ holds for each cardinal $\kappa < \mathfrak{c}$.

If we assume CH, then $\kappa < \mathfrak{c}$ is the same as saying $\kappa \leq \omega$, thus, by PROPOSITION 13.1, CH implies MA. On the other hand, MA can replace the Continuum Hypothesis in many proofs that use CH; which is important since MA is consistent with $\mathsf{ZFC} + \neg\mathsf{CH}$ (see Chapter 19).

It might be tempting to generalise Martin's Axiom by weakening its premise: Firstly, one might try to omit *ccc*, and secondly, one might try to allow larger families of open dense subsets of P. However, both attempts to generalise MA fail.

PROPOSITION 13.4. *There exist a (non ccc) partially ordered set $\mathbb{P} = (P, \leq)$ and a set $\mathscr{D}$ of cardinality ω_1 of open dense subsets of P such that no filter on P is $\mathscr{D}$-generic.*

Proof. Consider the partially ordered set $\big(\mathrm{Fn}(\omega, \omega_1), \subseteq\big)$. For each $\alpha \in \omega_1$, the set

$$D_\alpha = \big\{p \in \mathrm{Fn}(\omega, \omega_1) : \alpha \in \mathrm{ran}(p)\big\}$$

is an open dense subset of $\mathrm{Fn}(\omega, \omega_1)$: Obviously, D_α is open. To see that D_α is also dense, take any $p \in \mathrm{Fn}(\omega, \omega_1)$. If $\alpha \in \mathrm{ran}(p)$, then $p \in D_\alpha$ and we are done. Otherwise, let $n \in \omega$ be such that $n \notin \mathrm{dom}(p)$ (notice that such an n exists since $\mathrm{dom}(p)$ is finite). Now, let $q := p \cup \{\langle n, \alpha\rangle\}$; then $q \in D_\alpha$ and $q \geq p$. Similarly, for each $n \in \omega$, the set $E_n = \big\{p \in \mathrm{Fn}(\omega, \omega_1) : n \in \mathrm{dom}(p)\big\}$ is open dense.

Let $\mathscr{D} = \{D_\alpha : \alpha \in \omega_1\} \cup \{E_n : n \in \omega\}$; then $|\mathscr{D}| = \omega_1$. Assume that $G \subseteq \mathrm{Fn}(\omega, \omega_1)$ is a $\mathscr{D}$-generic filter on $\mathrm{Fn}(\omega, \omega_1)$. Since for each $n \in \omega$, $G \cap E_n \neq \emptyset$, $f_G = \bigcup G$ is a function from ω to ω_1. Further, since for each $\alpha \in \omega_1$, $G \cap D_\alpha \neq \emptyset$, the function $f_G : \omega \to \omega_1$ is even surjective, which contradicts the definition of ω_1. ⊣

PROPOSITION 13.5. $\mathsf{MA}(\mathfrak{c})$ *is false.*

Proof. Consider the partially ordered set $\big(\mathrm{Fn}(\omega, 2), \subseteq\big)$. Then $\mathrm{Fn}(\omega, 2)$ is countable and consequently satisfies *ccc*. For each $g \in {}^\omega 2$, the set

$$D_g = \big\{p \in \mathrm{Fn}(\omega, 2) : \exists n \in \omega\big(p(n) = 1 - g(n)\big)\big\}$$

is an open dense subset of $\mathrm{Fn}(\omega, 2)$: Obviously, D_g is open, and for $p \notin D_g$ let $q := p \cup \{\langle n, 1 - g(n)\rangle\}$ where $n \notin \mathrm{dom}(p)$. Then $q \in D_g$ and $q \geq p$. Similarly, for each $n \in \omega$, the set $D_n = \big\{p \in \mathrm{Fn}(\omega, 2) : n \in \mathrm{dom}(p)\big\}$ is open dense.

Let $\mathscr{D} = \{D_g : g \in {}^\omega 2\} \cup \{D_n : n \in \omega\}$. Then $|\mathscr{D}| = |{}^\omega 2| = \mathfrak{c}$. Assume that $G \subseteq \mathrm{Fn}(\omega, 2)$ is a $\mathscr{D}$-generic filter on $\mathrm{Fn}(\omega, 2)$. Since for each $n \in \omega$, $G \cap D_n \neq \emptyset$, $f_G = \bigcup G$ is a function from ω to 2. Further, since for each $g \in {}^\omega 2$, $G \cap D_g \neq \emptyset$, $f_G \neq g$. Thus, f_G would be a function from ω to 2 which differs from every function $g \in {}^\omega 2$, which is impossible. ⊣

Weaker Forms of MA

Below, we introduce a few forms of Martin's Axiom which are in fact proper weakenings of MA (*cf.* RELATED RESULT 81).

Let $\mathbb{P} = (P, \leq)$ be a partially ordered set. $\mathbb{P}$ is said to be **countable** if the set P is countable; and $\mathbb{P}$ is said to be **σ-centred** if P is the union of at most countably many centred sets, where a set $Q \subseteq P$ is called **centred**, if any finite set $q_1, \ldots, q_n \in Q$ has an upper bound in Q.

Let $\mathcal{P}$ be any property of partially ordered sets, *e.g.*, $\mathcal{P} = \sigma$-centred, $\mathcal{P} = ccc$, or $\mathcal{P} =$ countable. Then $\mathsf{MA}(\mathcal{P})$ is the following statement.

> $\mathsf{MA}(\mathcal{P})$: If $\mathbb{P} = (P, \leq)$ is a partially ordered set having the property $\mathcal{P}$, and $\mathscr{D}$ is a set of less than $\mathfrak{c}$ open dense subsets of P, then there exists a $\mathscr{D}$-generic filter on P.

Since every countable partially ordered set is σ-centred, and every σ-centred partially ordered set satisfies *ccc*, we obviously get:

$$\mathsf{MA} \Rightarrow \mathsf{MA}(\sigma\text{-centred}) \Rightarrow \mathsf{MA}(\text{countable})$$

Below, we present some consequences of Martin's Axiom for countable and σ-centred partially ordered sets.

Some consequences of $\mathsf{MA}(\boldsymbol{\sigma}\textbf{-centred})$

THEOREM 13.6. $\mathsf{MA}(\sigma\text{-centred})$ *implies* $\mathfrak{p} = \mathfrak{c}$.

Proof. Let $\kappa < \mathfrak{c}$ be an infinite cardinal and let $\mathscr{F} = \{x_\alpha : \alpha \in \kappa\} \subseteq [\omega]^\omega$ be a family with the strong finite intersection property (*i.e.*, intersections of finitely many members of $\mathscr{F}$ are infinite) of cardinality κ. Under the assumption of $\mathsf{MA}(\sigma\text{-centred})$ we construct an infinite pseudo-intersection of $\mathscr{F}$.

Let P be the set of all ordered pairs $\langle s, E\rangle$ such that $s \in [\omega]^{<\omega}$ and $E \in \operatorname{fin}(\kappa)$; and for $\langle s, E\rangle, \langle t, F\rangle \in P$ define

$$\langle s, E\rangle \leq \langle t, F\rangle \iff s \subseteq t \wedge E \subseteq F \wedge (t \setminus s) \subseteq \bigcap \bigl\{x_\alpha \in \mathscr{F} : \alpha \in E\bigr\}.$$

For $s \in [\omega]^{<\omega}$ let $P_s := \bigl\{\langle s, E\rangle \in P : E \in \operatorname{fin}(\kappa)\bigr\}$. Then any finite set $\langle s, E_1\rangle, \ldots, \langle s, E_n\rangle \in P_s$ has an upper bound, namely $\bigl\langle s, \bigcup_{i=1}^n E_i\bigr\rangle$, and since $[\omega]^{<\omega}$ is countable and $P = \bigcup \bigl\{P_s : s \in [\omega]^{<\omega}\bigr\}$, the partially ordered set $(P, \leq)$ is σ-centred. For each $\alpha \in \kappa$ and $n \in \omega$, the set

$$D_{\alpha,n} = \bigl\{\langle s, E\rangle \in P : \alpha \in E \wedge |s| > n\bigr\}$$

is an open dense subset of P. Let $\mathscr{D} = \{D_{\alpha,n} : \alpha \in \kappa \wedge n \in \omega\}$. Then $|\mathscr{D}| = \kappa$, in particular, $|\mathscr{D}| < \mathfrak{c}$. So, by $\mathsf{MA}(\sigma\text{-centred})$ there exists a $\mathscr{D}$-generic filter

G on P. Let $x_G := \bigcup\big\{s \in [\omega]^{<\omega} : \exists E \in \operatorname{fin}(\kappa)\big(\langle s, E\rangle \in G\big)\big\}$. Then, by construction, x_G is infinite. Moreover, for every $\alpha \in \kappa$ there is a condition $\langle s, E\rangle \in G$ such that $\alpha \in E$, which implies that $x_G \setminus s \subseteq x_\alpha$. Hence, for each $\alpha \in \kappa$ we have $x_G \subseteq^* x_\alpha$, and therefore, x_G is an infinite pseudo-intersection of $\mathscr{F}$. ⊣

The key idea in the proof that $\mathsf{MA}(\sigma\text{-centred}) \implies 2^\kappa = \mathfrak{c}$ for all infinite cardinals $\kappa < \mathfrak{c}$ is to encode subsets of an almost disjoint family of cardinality $\kappa < \mathfrak{c}$ by subsets of ω. For the premise of the following lemma — in which the "codes" are constructed — recall that there is always an almost disjoint family of cardinality $\mathfrak{c}$, and therefore of any cardinality $\kappa \leq \mathfrak{c}$ (*cf.* PROPOSITION 8.6).

LEMMA 13.7. *Let $\kappa < \mathfrak{c}$ be an infinite cardinal and let $\mathscr{A} = \{x_\alpha : \alpha \in \kappa\} \subseteq [\omega]^\omega$ be an almost disjoint family of cardinality κ. Furthermore, let $\mathscr{B} \subseteq \mathscr{A}$ be any subfamily of $\mathscr{A}$ and let $\mathscr{C} = \mathscr{A} \setminus \mathscr{B}$. If we assume* $\mathsf{MA}(\sigma\text{-centred})$, *then there exists a set $c \subseteq \omega$ such that for all $x \in \mathscr{A}$:*

$$|c \cap x| = \omega \iff x \in \mathscr{B}$$

Proof. Similar as in the proof of THEOREM 13.6, let P be the set of all ordered pairs $\langle s, E\rangle$ such that $s \in [\omega]^{<\omega}$ and $E \in \operatorname{fin}(\mathscr{C})$; and for $\langle s, E\rangle, \langle t, F\rangle \in P$ define

$$\langle s, E\rangle \leq \langle t, F\rangle \iff s \subseteq t \wedge E \subseteq F \wedge (t \setminus s) \cap \bigcup E = \emptyset\,.$$

Similar as above, one shows that the partially ordered set $(P, \leq)$ is σ-centred.

Now, for each $x_\gamma \in \mathscr{C}$, the set

$$D_{x_\gamma} = \big\{\langle s, E\rangle \in P : x_\gamma \in E\big\}$$

is an open dense subset of P; and for each $x_\beta \in \mathscr{B}$ and each $k \in \omega$, the set

$$D_{x_\beta,k} = \big\{\langle s, E\rangle \in P : |s \cap x_\beta| \geq k\big\}$$

is also an open dense subset of P. Notice that we do not require that $\mathscr{C}$ or $\mathscr{B}$ is non-empty. Finally, let $\mathscr{D} = \{D_{x_\gamma} : x_\gamma \in \mathscr{C}\} \cup \{D_{x_\beta,k} : x_\beta \in \mathscr{B} \wedge k \in \omega\}$. Then $|\mathscr{D}| = \kappa$, and since $\kappa < \mathfrak{c}$ we get $|\mathscr{D}| < \mathfrak{c}$. So, by $\mathsf{MA}(\sigma\text{-centred})$ there exists a $\mathscr{D}$-generic filter G on P. Let $c = \bigcup\big\{s \in [\omega]^{<\omega} : \exists E \in \operatorname{fin}(\mathscr{C})\big(\langle s, E\rangle \in G\big)\big\}$. Then for any $x_\beta \in \mathscr{B}$, $|c \cap x_\beta| = \omega$; and, like in the proof of THEOREM 13.6, for any $x_\gamma \in \mathscr{C}$, $|c \cap x_\gamma| < \omega$. Thus, the set $c \subseteq \omega$ has the required properties. ⊣

Now we are ready to prove the following consequences of $\mathsf{MA}(\sigma\text{-centred})$:

THEOREM 13.8. *If we assume* $\mathsf{MA}(\sigma\text{-centred})$, *then for all infinite cardinals $\kappa < \mathfrak{c}$ we have $2^\kappa = \mathfrak{c}$, and as a consequence we get that $\mathfrak{c}$ is regular.*

Proof. Let $\kappa < \mathfrak{c}$ be an infinite cardinal. We have to show that $2^\kappa = \mathfrak{c}$. For this, fix an almost disjoint family $\mathscr{A} = \{x_\alpha : \alpha \in \kappa\} \subseteq [\omega]^\omega$ of cardinality κ, and for each $u \in \mathscr{P}(\kappa)$ let $\mathscr{B}_u := \{x_\alpha \in \mathscr{A} : \alpha \in u\}$. Then, by LEMMA 13.7, there is a set $c_u \subseteq \omega$ such that for each $x \in \mathscr{A}$ we have $|c_u \cap x| = \omega \iff x \in \mathscr{B}_u$. Notice that for any distinct $u, v \in \mathscr{P}(\kappa)$ we have $c_u \neq c_v$. Indeed, if $u, v \in \mathscr{P}(\kappa)$ are distinct, then without loss of generality we may assume that there exists an $\alpha \in \kappa$ such that $\alpha \in u \setminus v$. So, $c_u \cap x_\alpha$ is infinite, whereas $c_v \cap x_\alpha$ is finite, and hence, $c_u \neq c_v$. Thus, the mapping

$$\begin{array}{ccc} \mathscr{P}(\kappa) & \to & \mathscr{P}(\omega) \\ u & \mapsto & c_u \end{array}$$

is one-to-one, which implies that $2^\kappa \leq \mathfrak{c}$. Now, since $\omega \leq \kappa$, and consequently $\mathfrak{c} \leq 2^\kappa$, we finally get $2^\kappa = \mathfrak{c}$.

To see that $\mathfrak{c}$ is regular assume towards a contradiction that $\kappa = \mathrm{cf}(\mathfrak{c}) < \mathfrak{c}$. Then, by COROLLARY 5.12, $\mathfrak{c} < \mathfrak{c}^\kappa$, but since $\mathfrak{c} = 2^\kappa$ we get that $\mathfrak{c}^\kappa = \left(2^\kappa\right)^\kappa = 2^\kappa = \mathfrak{c}$, a contradiction. ⊣

MA(countable) implies the existence of Ramsey ultrafilters

As a consequence of MA(countable) we get that there are $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters. By Chapter 10 | RELATED RESULT 64, it would be enough to show that MA(countable) implies $\mathfrak{p} = \mathfrak{c}$; however, this is not the case (*cf.* RELATED RESULTS 79–81 and COROLLARY 21.11).

PROPOSITION 13.9. MA(countable) *implies that there exist $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters.*

Proof. Since there are just $\mathfrak{c}$ permutation of ω, in order to get $2^{\mathfrak{c}}$ mutually *non-isomorphic* Ramsey ultrafilters it is enough to find $2^{\mathfrak{c}}$ *distinct* Ramsey ultrafilters. The $2^{\mathfrak{c}}$ mutually distinct Ramsey ultrafilters are constructed by transfinite induction: For every $\gamma : \mathfrak{c} \to 2$ and every $\alpha \in \mathfrak{c}$ we construct a set $\mathscr{F}_{\gamma|_\alpha} = \{x_{\beta,\gamma(\beta)} : \beta \in \alpha\} \subseteq [\omega]^\omega$ with the finite intersection property such that the filter generated by $\bigcup_{\alpha\in\mathfrak{c}} \mathscr{F}_{\gamma|_\alpha}$ is a Ramsey ultrafilter. In addition we make sure that for any two distinct $\gamma, \gamma' \in {}^{\mathfrak{c}}2$, the filters generated by $\bigcup_{\alpha\in\mathfrak{c}} \mathscr{F}_{\gamma|_\alpha}$ and $\bigcup_{\alpha\in\mathfrak{c}} \mathscr{F}_{\gamma'|_\alpha}$ are distinct. In order to get Ramsey ultrafilters at the end, by PROPOSITION 10.7.(b) it is enough to make sure that for every partition $\{Y_n : n \in \omega\}$ of ω, either there is an $n_0 \in \omega$ such that $Y_{n_0} \in \bigcup_{\alpha\in\mathfrak{c}} \mathscr{F}_{\gamma|_\alpha}$, or there exists an $x \in \bigcup_{\alpha\in\mathfrak{c}} \mathscr{F}_{\gamma|_\alpha}$ such that for all $n \in \omega$, $|x \cap Y_n| \leq 1$.

Let $\{\mathscr{P}_\alpha : \alpha \in \mathfrak{c}\}$ be the set of all infinite partitions of ω. Thus, for each $\alpha \in \mathfrak{c}$, $\mathscr{P}_\alpha = \{Y_n^\alpha : n \in \omega\}$ is a set of pairwise disjoint subsets of ω such that $\bigcup \mathscr{P}_\alpha = \omega$. Further, let $x_{0,0} := \{2n : n \in \omega\}$, $x_{0,1} := \{2n+1 : n \in \omega\}$, and for $\delta \in \{0,1\}$ let $\mathscr{F}_{\{\langle 0,\delta\rangle\}} := \{x_{0,\delta}\} \cup \{x \subseteq \omega : |\omega \setminus x| < \omega\}$. Obviously, both sets $\mathscr{F}_{\{\langle 0,0\rangle\}}$ and $\mathscr{F}_{\{\langle 0,1\rangle\}}$ have the finite intersection property. Let $\alpha \in \mathfrak{c}$ and assume that for each $\eta \in {}^\alpha 2$ and each $\beta \in \alpha$ we already have constructed a set $\mathscr{F}_{\eta|_\beta} \subseteq [\omega]^\omega$ with the finite intersection property, and such that for any

$\beta_0 \in \beta_1 \in \alpha$ we have $\mathscr{F}_{\eta|_{\beta_0}} \subseteq \mathscr{F}_{\eta|_{\beta_1}}$. In order to construct $\mathscr{F}_\eta$ we have to consider two cases:

α limit ordinal: If α is a limit ordinal, then let

$$\mathscr{F}_\eta = \bigcup_{\beta\in\alpha} \mathscr{F}_{\eta|_\beta}\,.$$

Since the sets $\mathscr{F}_{\eta|_\beta}$ are increasing and each of these sets has the finite intersection property, $\mathscr{F}_\eta$ has the finite intersection property as well.

α successor ordinal: If α is a successor ordinal, say $\alpha = \beta_0 + 1$, then we proceed as follows: Consider the partition $\mathscr{P}_{\beta_0} = \{Y_n : n \in \omega\}$ and notice that *either* there is an $n_0 \in \omega$ such that $\mathscr{F}_{\eta|_{\beta_0}} \cup \{Y_{n_0}\}$ has the finite intersection property, *or* for every $n \in \omega$, Y_n belongs to the dual ideal of $\mathscr{F}_{\eta|_{\beta_0}}$, *i.e.*, is a subset of the complement of a finite intersection of members of $\mathscr{F}_{\eta|_{\beta_0}}$. We consider the two cases separately:

Case 1: Let $n_0 \in \omega$ be such that $\mathscr{F}_{\eta|_{\beta_0}} \cup \{Y_{n_0}\}$ has the finite intersection property. Let $P_1 = \mathrm{Fn}(Y_{n_0}, 2)$ and for $p, q \in P_1$ let $p \le q \iff p \subseteq q$. Then $(P_1, \le)$ is countable and for every finite set $E \in \mathrm{fin}(\beta_0)$, every $n \in \omega$ and each $\delta \in \{0,1\}$, the set

$$D_{E,n,\delta} = \Bigl\{p \in P_1 : \bigl|p^{-1}(\delta) \cap \bigcap_{\iota\in E} x_{\iota,\eta(\iota)}\bigr| \ge n\Bigr\}$$

is an open dense subset of P_1. Now let $\mathscr{D} = \bigl\{D_{E,n,\delta} : E \in \mathrm{fin}(\beta_0) \wedge n \in \omega \wedge \delta \in \{0,1\}\bigr\}$. Then $|\mathscr{D}| \le \max\{|\alpha|, \omega\} < \mathfrak{c}$ and by MA(countable) there exists a $\mathscr{D}$-generic filter G on P_1. For $\delta \in \{0,1\}$, let

$$x_{\beta_0,\delta} := \bigcup \bigl\{p^{-1}(\delta) : p \in G\bigr\}\,.$$

For $\delta \in \{0,1\}$ we get that $x_{\beta_0,\delta} \in [Y_{n_0}]^\omega$ and that $\mathscr{F}_\eta := \mathscr{F}_{\eta|_{\beta_0}} \cup \{x_{\beta_0,\eta(\beta_0)}\}$ has the finite intersection property. Finally, let $\eta, \eta' \in {}^\alpha 2$ be such that $\eta(\beta_0) = 1 - \eta'(\beta_0)$. Since $x_{\beta_0,0} \cap x_{\beta_0,1} = \emptyset$ we obviously have $\mathscr{F}_\eta \ne \mathscr{F}_{\eta'}$. Moreover, by construction we get that $\mathscr{F}_\eta \cup \mathscr{F}_{\eta'}$ lacks the finite intersection property, and therefore no ultrafilter can extend both $\mathscr{F}_\eta$ and $\mathscr{F}_{\eta'}$.

Case 2: If for each $n \in \omega$, Y_n belongs to the dual ideal of $\mathscr{F}_{\eta|_{\beta_0}}$, then each finite intersection of members of $\mathscr{F}_{\eta|_{\beta_0}}$ meets infinitely many sets of $\mathscr{P}_{\beta_0}$. Let $P_2 \subseteq \mathrm{Fn}(\omega, 2)$ be such that $p \in P_2$ *iff* for every $Y \in \mathscr{P}_{\beta_0}$ we have

$$\max\bigl\{|p^{-1}(0) \cap Y|, |p^{-1}(1) \cap Y|\bigr\} \le 1\,,$$

and for $p, q \in P_2$ let $p \le q \iff p \subseteq q$. Like before, $(P_2, \le)$ is countable and for every finite set $E \in \mathrm{fin}(\beta_0)$, every $n \in \omega$ and each $\delta \in \{0,1\}$, the set

$$D_{E,n,\delta} = \Bigl\{p \in P_2 : \bigl|p^{-1}(\delta) \cap \bigcap_{\iota\in E} x_{\iota,\eta(\iota)}\bigr| \ge n\Bigr\}$$

is an open dense subset of P_2. Let $\mathscr{D} = \{D_{E,n,\delta} : E \in \text{fin}(\beta_0) \wedge n \in \omega \wedge \delta \in \{0,1\}\}$ and let G be a $\mathscr{D}$-generic filter on P_2. Finally, for $\delta \in \{0,1\}$ let $x_{\beta_0,\delta} := \bigcup\{p^{-1}(\delta) : p \in G\}$. Then $\mathscr{F}_\eta := \mathscr{F}_{\eta|\beta_0} \cup \{x_{\beta_0,\eta(\beta_0)}\}$ has the finite intersection property, and in addition there exists a set $x \in \mathscr{F}_\eta$ such that for all $n \in \omega$, $|x \cap Y_n| \leq 1$. Further, for $\eta, \eta' \in {}^{\alpha}2$ with $\eta(\beta_0) = 1 - \eta'(\beta_0)$, no ultrafilter can extend both $\mathscr{F}_\eta$ and $\mathscr{F}_{\eta'}$.

Finally, for each $\gamma \in {}^{\mathfrak{c}}2$, let $\mathscr{F}_\gamma$ be the filter generated by the set $\bigcup_{\alpha\in\mathfrak{c}} \mathscr{F}_{\gamma|\alpha}$. By construction, for any two distinct $\gamma, \gamma' \in {}^{\mathfrak{c}}2$, $\mathscr{F}_\gamma$ and $\mathscr{F}_{\gamma'}$ are two distinct Ramsey ultrafilters, and consequently there exist $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters. ⊣

Notes

Martin's Axiom. MA was first discovered by Martin and Solovay [8]. The paper contains various equivalent formulations of MA and numerous applications (including Theorem 13.8). They also stress the usefulness of MA as a viable alternative to CH and point out that many of the traditional problems solved using CH can be solved using MA. Roughly speaking, this is because under MA, sets of cardinality less than $\mathfrak{c}$ usually behave like countable sets (but of course, there are exceptions).

For equivalents of MA, consequences, weaker forms, history, *et cetera*we refer the reader to Kunen [7, Chapter II, §2–§5], Fremlin [4], Weiss [12], Rudin [10], Blass [2, Section 7], and Jech [6, Chapter 16].

MA(countable) ***and Ramsey ultrafilters.*** Proposition 13.9 is due to Canjar [3] (who actually proved even more), but the proof given above was communicated to me by Michael Hrušák (compare Proposition 13.9 with Chapter 10 | Related Result 64).

The Δ-System Lemma. This useful combinatorial result was first proved by Shanin [11] (see Kunen [7, Chapter II, §1] for a slightly more general result).

Related Results

79. MA(σ-centred) $\iff$ $\mathfrak{p} = \mathfrak{c}$. As we have seen above in Theorem 13.6, MA(σ-centred) implies $\mathfrak{p} = \mathfrak{c}$. On the other hand, also the converse is true, *i.e.*, $\mathfrak{p} = \mathfrak{c}$ implies MA(σ-centred). This somewhat surprising result was first proved by Bell [1] (see also Fremlin [4, 14C] or the proof of Theorem 19.4).

80. MA(countable) $\iff$ $cov(\mathcal{M}) = \mathfrak{c}$. Fremlin and Shelah showed in [5] that MA(countable) is equivalent to $cov(\mathcal{M}) = \mathfrak{c}$, where $cov(\mathcal{M})$ denotes the *covering number* of the meagre ideal (defined in Chapter 21). See also Martin and Solovay [8, §4], Blass [2, Theorem 7.13], and Miller [9] for some further results concerning $cov(\mathcal{M})$.

81. MA(σ-linked). A partially ordered set $(P, \leq)$ is said to be **σ-linked** if we can write $P = \bigcup_{n\in\omega} P_n$, where each set P_n consists of pairwise compatible elements. On the one hand, it is easily verified that

$$\text{MA} \Longrightarrow \text{MA}(\sigma\text{-linked}) \Longrightarrow \text{MA}(\sigma\text{-centred}) \Longrightarrow \text{MA}(\text{countable}),$$

but on the other hand, to show that none of the converse implications hold requires quite sophisticated techniques. For the corresponding references we refer the reader to Fremlin [4, Appendix B1].

References

1. Murray G. Bell, *On the combinatorial principle $P(\mathfrak{c})$*, ***Fundamenta Mathematicae***, vol. 114 (1981), 149–157.
2. Andreas Blass, *Combinatorial Cardinal Characteristics of the Continuum*, in ***Handbook of Set Theory,*** *Volume 1* (Matthew Foreman and Akihiro Kanamori, eds.), Springer-Verlag, Berlin, 2010, pp. 395–490.
3. R. Michael Canjar, *On the generic existence of special ultrafilters*, ***Proceedings of the American Mathematical Society***, vol. 110 (1990), 233–241.
4. David H. Fremlin, ***Consequences of Martin's axiom***, Cambridge Tracts in Mathematics 84, Cambridge University Press, Cambridge, 1984.
5. David H. Fremlin and Saharon Shelah, *On partitions of the real line*, ***Israel Journal of Mathematics***, vol. 32 (1979), 299–304.
6. Thomas Jech, ***Set Theory,*** *The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
7. Kenneth Kunen, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.
8. Donald A. Martin and Robert M. Solovay, *Internal Cohen extensions*, ***Annals of Mathematical Logic***, vol. 2 (1970), 143–178.
9. Arnold W. Miller, *The Baire category theorem and cardinals of countable cofinality*, ***The Journal of Symbolic Logic***, vol. 47 (1982), 275–288.
10. Mary Ellen Rudin, *Martin's axiom*, in ***Handbook of Mathematical Logic*** (J. Barwise, ed.), North-Holland, Amsterdam, 1977, pp. 491–501.
11. Nikolai A. Shanin, *A theorem from the general theory of sets*, ***Comptes Rendus (Doklady) de l'Académie des Sciences de l'URSS (N.S.)***, vol. 53 (1946), 399–400.
12. William Weiss, *Versions of Martin's axiom*, in ***Handbook of Set-Theoretic Topology*** (K. Kunen and J.E. Vaughan, eds.), North-Holland, Amsterdam, 1990, pp. 827–886.

14

The Notion of Forcing

In this chapter we present a general technique, called forcing, for extending models of ZFC. The main ingredients to construct such an extension are a model $\mathbf{V}$ of ZFC (*e.g.*, $\mathbf{V} = \mathbf{L}$), a partially ordered set $\mathbb{P} = (P, \leq)$ contained in $\mathbf{V}$, as well as a special subset G of P which will not belong to $\mathbf{V}$. The extended model $\mathbf{V}[G]$ will then consist of all sets which can be "described" or "named" in $\mathbf{V}$, where the "naming" depends on the set G. The main task will be to prove that $\mathbf{V}[G]$ is a model of ZFC as well as to decide (within $\mathbf{V}$) whether a given statement is true or false in a certain extension $\mathbf{V}[G]$.

To get an idea how this is done, think for a moment that there are people living in $\mathbf{V}$. For these people, $\mathbf{V}$ is the unique set-theoretic universe which contains *all* sets. Now, the key point is that for any statement, these people are able to compute whether the statement is true or false in a particular extension $\mathbf{V}[G]$, even though they have almost no information about the set G (in fact, they would actually deny the existence of such a set).

The Language of Forcing

The notion of forcing notion. In fact, a **forcing notion** is just a partially ordered set $\mathbb{P} = (P, \leq)$ with a smallest element, *i.e.*,

$$\exists p \in P \; \forall q \in P \, (p \leq q) \, .$$

Notice that this condition implies that P is non-empty. Further notice that we do not require that $\mathbb{P}$ is anti-symmetric (*i.e.*, $p \leq q$ and $q \leq p$ does not necessarily imply $p = q$), even though most of the forcing notions considered in this book are actually anti-symmetric. In fact, for every forcing notion $\mathbb{P}$ there exists an *equivalent* forcing notion $\tilde{\mathbb{P}}$ which is anti-symmetric (see FACT 14.5 below).

In order to make sure that forcing with a forcing notion $\mathbb{P}$ yields a non-trivial extension, we require that a forcing notion $\mathbb{P} = (P, \leq)$ has the property that there are incompatible elements above each $p \in P$, *i.e.*,

$$\forall p \in P\, \exists q_1 \in P\, \exists q_2 \in P\, \big(p \le q_1 \wedge p \le q_2 \wedge q_1 \perp q_2\big)\,.$$

Notice that this property implies that there is no maximal element in P, *i.e.*, $\forall p \in P\, \exists q \in P\,(p < q)$. Later on, when we shall be somewhat familiar with forcing, the second condition will be tacitly cancelled in order to allow also trivial forcing notions like for example $\mathbb{P} = \big(\{\emptyset\}, \subseteq\big)$.

Usually, forcing notions are named after the person who investigated first the corresponding partially ordered set in the context of forcing (*e.g.*, the forcing notion defined below is called *Cohen forcing*). As in the previous chapter, the elements of P are called "conditions". Furthermore, if p and q and two conditions and $p \le q$, then we say that p is **weaker** than q, or equivalently, that q is **stronger** than p.

Below, we give two quite different examples of forcing notions. The first one is the forcing notion which is used to prove that $\neg\mathsf{CH}$ is consistent with ZFC, and the second one is a forcing notion which will accompany us — in different forms — throughout this book.

1. Recall that $\mathrm{Fn}(I, J)$ is the set of all finite partial functions from I to J (defined in the previous chapter). Now, for cardinal numbers $\kappa > 0$ define the partially ordered set

$$\mathbb{C}_\kappa = \big(\,\mathrm{Fn}(\kappa \times \omega, 2), \subseteq\,\big)\,,$$

i.e., for $p, q \in \mathrm{Fn}(\kappa\times\omega, 2)$, p is stronger than q *iff* the function p extends q. Obviously, the smallest (*i.e.*, weakest) element of $\mathrm{Fn}(\kappa\times\omega, 2)$ is $\emptyset$ (*i.e.*, the empty function), thus, $\mathbb{C}_\kappa$ has a smallest element. Furthermore, for each condition (*i.e.*, function) $p \in \mathrm{Fn}(\kappa\times\omega, 2)$ there is an ordered pair $\langle\alpha, n\rangle \in \kappa \times \omega$ which does not belong to $\mathrm{dom}(p)$. Now, let $q_1 := p \cup \big\{\big\langle\langle\alpha, n\rangle, 1\big\rangle\big\}$ and $q_2 := p \cup \big\{\big\langle\langle\alpha, n\rangle, 0\big\rangle\big\}$. Obviously, $q_1, q_2 \in \mathrm{Fn}(\kappa \times \omega, 2)$, $q_1 \perp q_2$, and $q_1 \supseteq p \subseteq q_2$. This shows that there are incompatible elements above each $p \in \mathrm{Fn}(\kappa \times \omega, 2)$. Hence, $\mathbb{C}_\kappa$ is a forcing notion. The forcing notion $\mathbb{C}_1$, denoted $\mathbb{C}$, is called **Cohen forcing**, and $\mathbb{C}_\kappa$ is in fact just a kind of product of κ copies of Cohen forcing (*cf.* Chapter 21).

2. A natural example of a partially ordered set is the set of infinite subsets of ω together with the superset relation. However, let us consider a slightly different partially ordered set: Define an equivalence relation on $[\omega]^\omega$ by stipulating

$$x \sim y \iff x \triangle y \text{ is finite}$$

and let $[\omega]^\omega/\,\mathrm{fin} := \big\{[x]^{\tilde{}} : x \in [\omega]^\omega\big\}$. On $[\omega]^\omega/\,\mathrm{fin}$ we define a partial ordering "$\le$" by stipulating

$$[x]^{\tilde{}} \le [y]^{\tilde{}} \iff y \subseteq^* x\,,$$

i.e., $[x]^{\tilde{}} \le [y]^{\tilde{}}$ *iff* $y \setminus x$ is finite, and let

$$\mathbb{U} = \big([\omega]^\omega/\,\mathrm{fin}, \le\,\big)\,.$$

Then $\mathbb{U}$ is a partially ordered. Moreover, $\mathbb{U}$ is a forcing notion: Obviously, the weakest element of $\mathbb{U}$ is $[\omega]^{\tilde{}}$ (the set of all co-finite subsets of ω), thus, $\mathbb{U}$ has a smallest element. Furthermore, for each $x \in [\omega]^\omega$ one easily finds disjoint sets y_1 and y_2 in $[x]^\omega$. This shows that there are incompatible elements above any condition $[x]^{\tilde{}}$. This forcing notion — which does not have an established name — we shall call **ultrafilter forcing** (the name is motivated by PROPOSITION 14.18).

Making names for sets. Let $\mathbf{V}$ be a model of ZFC and let $\mathbb{P} = (P, \leq)$ be a forcing notion which belongs to $\mathbf{V}$, *i.e.*, the set P as well as the relation "$\leq$" (which is a subset of $P \times P$) belongs to the model $\mathbf{V}$. The goal is to extend the so-called ground model $\mathbf{V}$, by adding a certain subset $G \subseteq P$ to $\mathbf{V}$, and then construct a model $\mathbf{V}[G]$ of ZFC which contains $\mathbf{V}$. In order to get a proper extension of $\mathbf{V}$, the set G — even though it is a subset of P — must not belong to $\mathbf{V}$. However, this seemingly paradoxical property of G does not affect the construction of the model $\mathbf{V}[G]$.

Roughly speaking, $\mathbf{V}[G]$ consists of all sets which can be constructed from G by applying set-theoretic processes definable in $\mathbf{V}$. In fact each set in the extension will have a *name* in $\mathbf{V}$, which tells how it has been constructed from G. We use symbols like $\underset{\sim}{x}$, $\underset{\sim}{y}$, $\underset{\sim}{f}$, $\underset{\sim}{X}$, *et cetera* for ordinary names, but also $\underset{\cdot}{x}$, $\underset{\cdot}{y}$, $\underset{\cdot}{c}$, $\underset{\cdot}{G}$, *et cetera* for some special names (*e.g.*, names for sets in $\mathbf{V}$).

Informally, a **name**, or more precisely a $\mathbb{P}$**-name**, is a possibly empty set of ordered pairs of the form $\langle \underset{\sim}{x}, p\rangle$, where $\underset{\sim}{x}$ is a $\mathbb{P}$-name and $p \in P$. The *class* of all $\mathbb{P}$-names is denoted by $\mathbf{V}^{\mathbb{P}}$.

Formally, $\mathbf{V}^{\mathbb{P}}$ is defined by transfinite induction (similar to the cumulative hierarchy of sets defined in Chapter 3):

$$\begin{aligned} \mathrm{V}_0^{\mathbb{P}} &= \emptyset \\ \mathrm{V}_\alpha^{\mathbb{P}} &= \textstyle\bigcup_{\beta\in\alpha} \mathrm{V}_\beta^{\mathbb{P}} \qquad \textit{if } \alpha \textit{ is a limit ordinal} \\ \mathrm{V}_{\alpha+1}^{\mathbb{P}} &= \mathscr{P}\big(\mathrm{V}_\alpha^{\mathbb{P}} \times P\big) \end{aligned}$$

and let

$$\mathbf{V}^{\mathbb{P}} = \bigcup_{\alpha\in\Omega} \mathrm{V}_\alpha^{\mathbb{P}} .$$

Notice that $\mathbf{V}^{\mathbb{P}}$ is a proper subclass of $\mathbf{V}$. The formal definition of $\mathbf{V}^{\mathbb{P}}$ allows to define a *rank-function* on the class of names: For $\mathbb{P}$-names $\underset{\sim}{x} \in \mathbf{V}^{\mathbb{P}}$ let

$$\mathrm{rk}(\underset{\sim}{x}) := \bigcup \big\{ \mathrm{rk}(\underset{\sim}{y}) + 1 : \exists p \in P \left(\langle \underset{\sim}{y}, p\rangle \in \underset{\sim}{x}\right) \big\} .$$

Consider for example the three $\mathbb{U}$-conditions $u_1 = [\omega]^{\tilde{}}$, $u_2 = [\{2n : n \in \omega\}]^{\tilde{}}$, and $u_3 = [\{3n : n \in \omega\}]^{\tilde{}}$, as well as the three $\mathbb{U}$-names $\underset{\sim}{x} = \big\{\langle\emptyset, u_2\rangle, \langle\emptyset, u_3\rangle\big\}$, $\underset{\sim}{y} = \big\{\langle \underset{\sim}{x}, u_2\rangle, \langle\emptyset, u_1\rangle\big\}$, and $\underset{\sim}{z} = \big\{\langle \underset{\sim}{y}, u_1\rangle, \langle \underset{\sim}{x}, u_2\rangle, \langle\emptyset, u_2\rangle, \langle\emptyset, u_3\rangle, \langle \underset{\sim}{y}, u_3\rangle\big\}$. Then $\mathrm{rk}(\underset{\sim}{x}) = 1$, $\mathrm{rk}(\underset{\sim}{y}) = 2$, and $\mathrm{rk}(\underset{\sim}{z}) = 3$.

Making sets from names. Names are objects in $\mathbf{V}$ intended to designate sets in the extension $\mathbf{V}[G]$ (where G is a certain subset of P). In other words, names are special sets in $\mathbf{V}$ which stand for sets in the extension. So, the next step in the construction of $\mathbf{V}[G]$ is to transform the names to the sets they stand for: Let G be a subset of P (later, G will always be a *generic filter*). Then by transfinite recursion on $\mathbb{P}$-names $\underset{\sim}{x}$ we define

$$\underset{\sim}{x}[G] = \bigl\{\underset{\sim}{y}[G] : \exists q \in G\,(\langle \underset{\sim}{y}, q\rangle \in \underset{\sim}{x})\bigr\}\,,$$

and in general let

$$\mathbf{V}[G] = \bigl\{\underset{\sim}{x}[G] : \underset{\sim}{x} \in \mathbf{V}^{\mathbb{P}}\bigr\}\,.$$

Notice that if $G = \emptyset$, then $\mathbf{V}[G] = \emptyset$. For example let us consider again the three $\mathbb{U}$-names $\underset{\sim}{x}$, $\underset{\sim}{y}$, $\underset{\sim}{z}$, and the three $\mathbb{U}$-conditions u_1, u_2, u_3, from above and let $G_1 = \{u_1\}$, $G_{1,2} = \{u_1, u_2\}$, and $G_3 = \{u_3\}$. Then $\underset{\sim}{x}[G_1] = 0$, $\underset{\sim}{x}[G_{1,2}] = 1$, $\underset{\sim}{x}[G_3] = 1$, $\underset{\sim}{y}[G_1] = 1$, $\underset{\sim}{y}[G_{1,2}] = 2$, $\underset{\sim}{y}[G_3] = 0$, $\underset{\sim}{z}[G_1] = \{1\}$, $\underset{\sim}{z}[G_{1,2}] = 3$, $\underset{\sim}{z}[G_3] = 2$ (recall that $0 = \emptyset$, $1 = \{0\}$, $2 = \{0,1\}$, *et cetera*).

A saucerful of names. Since $\mathbf{V}[G]$ is supposed to be an *extension* of $\mathbf{V}$, we have to show that $\mathbf{V}$ is in general a subclass of $\mathbf{V}[G]$. Furthermore, G should belong to $\mathbf{V}[G]$, no matter whether G belongs to $\mathbf{V}$ or not.
Firstly, let us show that $\mathbf{V}$ is a subclass of $\mathbf{V}[G]$ whenever $G \subseteq P$ is non-empty. Below, we always assume that G contains $\mathbf{0}$ where $\mathbf{0}$ denotes the smallest element of P. For every set $x \in \mathbf{V}$ there is a **canonical name** $\underset{\cdot}{x} \in \mathbf{V}[G]$ such that $\underset{\cdot}{x}[G] = x$: By transfinite recursion define

$$\underset{\cdot}{x} = \bigl\{\langle \underset{\cdot}{y}, \mathbf{0}\rangle : y \in x\bigr\}\,.$$

For example $\underset{\cdot}{\emptyset} = \emptyset$, $\underset{\cdot}{1} = \bigl\{\langle \underset{\cdot}{\emptyset}, \mathbf{0}\rangle\bigr\}$, $\underset{\cdot}{2} = \bigl\{\langle \underset{\cdot}{\emptyset}, \mathbf{0}\rangle, \langle \underset{\cdot}{1}, \mathbf{0}\rangle\bigr\}$, *et cetera*. Notice that since $\mathbf{0} \in G$, for all $x \in \mathbf{V}$ we have $\underset{\cdot}{x}[G] = \bigl\{\underset{\cdot}{y}[G] : y \in x\bigr\}$. It remains to show that for each $x \in \mathbf{V}$ we have $\underset{\cdot}{x}[G] = x$.

FACT 14.1. *If $G \subseteq P$ with $\mathbf{0} \in G$, then for every $x \in \mathbf{V}$ we have $\underset{\cdot}{x}[G] = x$.*

Proof. The proof is by transfinite induction on $\mathrm{rk}(\underset{\cdot}{x})$. If $\mathrm{rk}(\underset{\cdot}{x}) = 0$, then $\underset{\cdot}{x} = \underset{\cdot}{\emptyset} = \emptyset$, and

$$\underset{\cdot}{\emptyset}[G] = \bigl\{\underset{\cdot}{y}[G] : y \in \emptyset)\bigr\} = \emptyset\,.$$

Now let $\mathrm{rk}(\underset{\cdot}{x}) = \alpha$ and assume that $\underset{\cdot}{y}[G] = y$ for all $\mathbb{P}$-names $\underset{\cdot}{y}$ with $\mathrm{rk}(\underset{\cdot}{y}) \in \alpha$. Then

$$\underset{\cdot}{x}[G] = \bigl\{\underset{\cdot}{y}[G] : y \in x\bigr\} = \bigl\{y : y \in x\bigr\} = x$$

which completes the proof. ⊣

In order to make sure that G belongs to $\mathbf{V}[G]$, we need a $\mathbb{P}$-name $\underset{\sim}{G}$ for G such that $\underset{\sim}{G}[G] = G$. For example define

$$\underset{\sim}{G} = \bigl\{\langle \underset{\cdot}{p}, p\rangle : p \in P\bigr\}\,.$$

As an immediate consequence of Fact 14.1 we get the following

FACT 14.2. *For every $G \subseteq P$ which contains $\mathbf{0}$ we have $\underset{\sim}{G}[G] = G$.*

Proof. We just have to evaluate the $\mathbb{P}$-name $\underset{\sim}{G}$:

$$\underset{\sim}{G}[G] = \big\{\underset{\cdot}{p}[G] : \exists q \in G\,\big(\langle \underset{\cdot}{p}, q\rangle \in \underset{\sim}{G}\big)\big\} = \big\{\underset{\cdot}{p}[G] : p \in G\big\} = \big\{p : p \in G\big\} = G$$

$\dashv$

Hence, for *any* subset $G \subseteq P$ we have $G = \underset{\sim}{G}[G]$. Thus, the name $\underset{\sim}{G}$, usually denoted $\underset{\cdot}{G}$, is the canonical name for G. Furthermore, we see that $G \in \mathbf{V}[G]$, no matter whether G — belonging to some set-theoretic universe — belongs to $\mathbf{V}$.

We can also define names for unordered and ordered pairs of sets: For $\mathbb{P}$-names $\underset{\sim}{x}$ and $\underset{\sim}{y}$ define

$$\mathrm{up}(\underset{\sim}{x}, \underset{\sim}{y}) = \big\{\langle \underset{\sim}{x}, \mathbf{0}\rangle, \langle \underset{\sim}{y}, \mathbf{0}\rangle\big\}$$

and

$$\mathrm{op}(\underset{\sim}{x}, \underset{\sim}{y}) = \big\{\big\langle\{\langle \underset{\sim}{x}, \mathbf{0}\rangle\}, \mathbf{0}\big\rangle, \big\langle\{\langle \underset{\sim}{x}, \mathbf{0}\rangle, \langle \underset{\sim}{y}, \mathbf{0}\rangle\}, \mathbf{0}\big\rangle\big\}\,.$$

We leave it as an exercise to the reader to verify that for every $G \subseteq P$ with $\mathbf{0} \in G$ we have $\mathrm{up}(\underset{\sim}{x}, \underset{\sim}{y})[G] = \big\{\underset{\sim}{x}[G], \underset{\sim}{y}[G]\big\}$ and $\mathrm{op}(\underset{\sim}{x}, \underset{\sim}{y})[G] = \big\langle \underset{\sim}{x}[G], \underset{\sim}{y}[G]\big\rangle$.

The forcing language. We are now ready to introduce a kind of logical language, the so-called **forcing language**. A sentences ψ of the forcing language is like a first-order sentence, except that the parameters appearing in ψ are some names in $\mathbf{V}^{\mathbb{P}}$, *i.e.*, specific sets in $\mathbf{V}$. Sentences of the forcing language use the names in $\mathbf{V}^{\mathbb{P}}$ to assert something about $\mathbf{V}[G]$ (for certain $G \subseteq P$). The people living in the ground model $\mathbf{V}$ may not know whether a given sentence ψ is true in $\mathbf{V}[G]$. The truth or falsity of ψ in $\mathbf{V}[G]$ will in general depend on the set $G \subseteq P$. For example consider the $\mathbb{U}$-name $\underset{\sim}{x} = \big\{\langle \underset{\cdot}{\emptyset}, p_0\rangle\big\}$ with $p_0 = [\{2n : n \in \omega\}]^{\tilde{}}$, and the sentence $\psi \equiv \exists y(y \in \underset{\sim}{x})$ of the forcing language which asserts that $\underset{\sim}{x}$ is non-empty. Now, ψ is true in $\mathbf{V}[G]$ if and only if $\mathbf{V}[G] \vDash \exists y\big(y \in \underset{\sim}{x}[G]\big)$, which is the case if and only if $p_0 \in G$. Hence, depending on $G \subseteq [\omega]^\omega$, ψ becomes true or false in $\mathbf{V}[G]$.

However, even though people living in $\mathbf{V}$ do not know whether $\mathbf{V}[G] \vDash \psi$, they know that $\mathbf{V}[G] \vDash \psi$ *iff* $p_0 \in G$. Thus, in order to decide whether $\mathbf{V}[G] \vDash \psi$ they just need to know whether G contains the condition p_0.

This leads to one of the key features of forcing: By knowing whether a certain condition p belongs to $G \subseteq P$, people living in $\mathbf{V}$ can figure out whether a given sentence of the forcing language is true or false in $\mathbf{V}[G]$. Moreover, it will turn out that people living in $\mathbf{V}$ are able to verify that in certain models $\mathbf{V}[G]$ *all* axioms of ZFC remain true. In the following section we shall see how this is done.

Generic Extensions

Let again $\mathbb{P} = (P, \leq)$ be an arbitrary forcing notion which belongs to a model $\mathbf{V}$ of ZFC. Below, we define first the notion of a *generic filter* (which is a special subset $G \subseteq P$) and the corresponding *generic model* $\mathbf{V}[G]$; then we introduce the *forcing relation* and show how people in $\mathbf{V}$ can decide whether a given sentence is true or false in a particular generic model. Finally we construct a generic model in which the Continuum Hypothesis fails and discuss the existence of generic filters.

Generic filters and generic models. Let us briefly recall some definitions from the previous chapter: A set $D \subseteq P$ is **open dense** if $p \in D$ and $q \geq p$ implies $q \in D$ (*open*), and if for every $p \in P$ there is a $q \in D$ such that $q \geq p$ (*dense*). A set $A \subseteq P$ is an **anti-chain** in P if any two distinct elements of A are incompatible, and it is maximal if it is not properly contained in any anti-chain in P. A non-empty set $G \subseteq P$ is a **filter** (on P) if $p \in G$ and $q \leq p$ implies $q \in G$ (*downwards closed*), and if for any $p_1, p_2 \in G$ there is a $q \in G$ such that $p_1 \leq q \geq p_2$ (*directed*).

Now, a filter $G \subseteq P$ is said to be **$\mathbb{P}$-generic over V** if $G \cap D \neq \emptyset$ for every open dense set $D \subseteq P$ which belongs to $\mathbf{V}$ (compare with the notion of a $\mathscr{D}$-generic filter, which was introduced in the previous chapter). In other words, a filter G on P is $\mathbb{P}$-generic over $\mathbf{V}$ if it meets every open dense subset of P *which belongs to* $\mathbf{V}$. The restriction that the open dense subsets have to belong to $\mathbf{V}$ — which at a first glance seems to be superficial — is in fact crucial.

Equivalent forcing notions. It may happen that two different forcing notions $\mathbb{P} = (P, \leq_P)$ and $\mathbb{Q} = (Q, \leq_Q)$ yield the same generic models, in which case we say that $\mathbb{P}$ and $\mathbb{Q}$ are **equivalent**, denoted $\mathbb{P} \approx \mathbb{Q}$.z More precisely, $\mathbb{P} \approx \mathbb{Q}$ if for every $G \subseteq P$ which is $\mathbb{P}$-generic over $\mathbf{V}$, there exists an $H \subseteq Q$ which is $\mathbb{Q}$-generic over $\mathbf{V}$ such that $\mathbf{V}[G] = \mathbf{V}[H]$, and vice versa, for every $\mathbb{Q}$-generic H there is a $\mathbb{P}$-generic G such that $\mathbf{V}[H] = \mathbf{V}[G]$. Notice that "$\approx$" is indeed an equivalence relation on the class of forcing notions.

In order to prove that two forcing notions $\mathbb{P} = (P, \leq_P)$ and $\mathbb{Q} = (Q, \leq_Q)$ are equivalent, it is sufficient to show the existence of a so-called dense embedding from P to Q (or vice versa), where a function $h : P \to Q$ is called a **dense embedding** if it satisfies the following conditions:

- $\forall p_0, p_1 \in P \big(p_0 \leq_P p_1 \leftrightarrow h(p_0) \leq_Q h(p_1)\big)$
- $\forall q \in Q\, \exists p \in P \big(q \leq_Q h(p)\big)$

Notice that the function h is not necessarily surjective, in particular, h is in general not an isomorphism. However, it is not hard to verify that the forcing notions $\mathbb{P}$ and $\mathbb{Q}$ are equivalent whenever there exists a dense embedding $h : P \to Q$. The proof of the following fact is left to the reader.

FACT 14.3. *Let $\mathbb{P} = (P, \leq)$ and $\mathbb{Q} = (Q, \leq)$ be any forcing notions. If there exists a dense embedding $h : P \to Q$, then $\mathbb{P}$ and $\mathbb{Q}$ are equivalent. In fact, if $G \subseteq P$ is $\mathbb{P}$-generic over $\mathbf{V}$, then the set*

$$H = \{q \in Q : \exists p \in G\,(q \leq h(p))\}$$

is $\mathbb{Q}$-generic over $\mathbf{V}$ and $\mathbf{V}[G] = \mathbf{V}[H]$. Conversely, if a set $H \subseteq Q$ is $\mathbb{Q}$-generic over $\mathbf{V}$, then the set

$$G = \{p \in P : h(p) \in H\}$$

is $\mathbb{P}$-generic over $\mathbf{V}$ and $\mathbf{V}[H] = \mathbf{V}[G]$.

The preceding fact implies that it is enough to consider forcing notions of the form $(\kappa, \leq, \emptyset)$, where κ is a cardinal number, "$\leq$" is a partial ordering on κ, and $\emptyset$ is the smallest element (with respect to $\leq$) in κ. More precisely, we get the following

FACT 14.4. *Every forcing notion $\mathbb{P} = (P, \leq, \mathbf{0})$, where $\mathbf{0}$ is a smallest element in P, is equivalent to some forcing notion $(\kappa, \preccurlyeq, \emptyset)$, where $\kappa = |P|$. In particular, we may always identify the smallest element of a forcing notion with the empty set.*

Proof. Let $h : P \to \kappa$ be a bijection, where $h(\mathbf{0}) = \emptyset$, and let

$$h(p) \preccurlyeq h(q) \iff p \leq q\,.$$

Then h is obviously a dense embedding. $\dashv$

As another consequence of FACT 14.3 we get that every forcing notion is equivalent to some anti-symmetric forcing notion.

FACT 14.5. *Let $\mathbb{P} = (P, \leq)$ be any forcing notion and let $\tilde{\mathbb{P}} := (\tilde{P}, \leq^{\sim})$, where $p \sim q \iff p \leq q \wedge q \leq p$, $\tilde{P} = \{[p]^{\sim} : p \in P\}$, and $[p]^{\sim} \leq^{\sim} [q]^{\sim} \iff p \leq q$. Then $\tilde{\mathbb{P}}$ is anti-symmetric and equivalent to $\mathbb{P}$.*

Proof. Firstly notice that $\tilde{\mathbb{P}}$ is a forcing notion. Now define $h : P \to \tilde{P}$ by stipulating $h(p) := [p]^{\sim}$. Then h is obviously a dense embedding and therefore $\mathbb{P} \approx \tilde{\mathbb{P}}$. Finally, if we have $[p]^{\sim} \leq^{\sim} [q]^{\sim}$ and $[q]^{\sim} \leq^{\sim} [p]^{\sim}$, then $[p]^{\sim} = [q]^{\sim}$, which shows that $\tilde{\mathbb{P}}$ is anti-symmetric. $\dashv$

Alternative definitions of generic filters. It is sometimes useful to have a few alternative definitions of $\mathbb{P}$-generic filters at hand which are sometimes easier to apply.

FACT 14.6. *Let $\mathbb{P} = (P, \leq)$ be a forcing notion which belongs to a model $\mathbf{V}$ of* ZFC*. Then, for a filter G on P, the following statements are equivalent:*

(a) G is $\mathbb{P}$-generic over $\mathbf{V}$.

(b) G meets every maximal anti-chain in P which belongs to $\mathbf{V}$.

(c) G meets every dense subset of P which belongs to $\mathbf{V}$.

Proof. (a)⇒(b) Let $A \subseteq P$ be a maximal anti-chain in P which belongs to $\mathbf{V}$. Then $D_A := \{p \in P : \exists q \in A\,(p \geq q)\}$ is open dense in P: D_A is obviously open, and since A is a maximal anti-chain in P, for every $p_0 \in P$ there is a condition $q_0 \in A$ such that p_0 and q_0 are compatible, *i.e.*, there is a $p \in D_A$ such that $q_0 \leq p \geq p_0$, which implies that D_A is dense. Now, if G is $\mathbb{P}$-generic over $\mathbf{V}$, then G meets D_A, and since G is downwards closed, it meets the maximal anti-chain A.

(b)⇒(c) Let $D \subseteq P$ be a dense subset of P which belongs to $\mathbf{V}$. Then by Kurepa's Principle (introduced in Chapter 5) there is a maximal anti-chain A in D. Since D is dense in P, A is also a maximal anti-chain in P (otherwise, there would be a condition $p \in P$ which is incompatible with all conditions of D, contradicting the fact that D is dense in P). Now, if G meets every maximal anti-chain in P (which belongs to $\mathbf{V}$), then G meets A, and since A is a subset of D, it meets the dense set D.

(c)⇒(a) If G meets every dense subset of P which belongs to $\mathbf{V}$, then it obviously meets also every open dense subset of P which belongs to $\mathbf{V}$. ⊣

Let $p \in P$; then a set $D \subseteq P$ is **dense above** p if for any $p' \geq p$ there is a $q \in D$ such that $q \geq p'$. Notice that if $D \subseteq P$ is dense above p (for some $p \in P$) and $q \geq p$, then D is also dense above q.

The proof of the following characterisation of $\mathbb{P}$-generic filters is left to the reader.

FACT 14.7. *Let $\mathbb{P} = (P, \leq)$ be a forcing notion which belongs to a model $\mathbf{V}$ of* ZFC*, and let $G \subseteq P$ be a filter on P which contains the condition p. Then G is $\mathbb{P}$-generic over $\mathbf{V}$ if and only if G meets every set $D \subseteq P$ which is dense above p.*

If the filter $G \subseteq P$ is $\mathbb{P}$-generic over $\mathbf{V}$, then the class $\mathbf{V}[G]$ is called a **generic extension** of $\mathbf{V}$, or just a **generic model**.

ZFC in Generic Models

In order to prove that a generic model $\mathbf{V}[G]$ is indeed a model of ZFC, we first have to develop a technique which allows us to verify within $\mathbf{V}$ that all axioms of ZFC remain true in $\mathbf{V}[G]$.

The forcing relationship. In this section, we shall define a relationship, denoted $\Vdash_{\mathbb{P}}$, between conditions $p \in P$ and sentences ψ of the forcing language. Even though the relationship "$\Vdash_{\mathbb{P}}$" involves formulae and is therefore not expressible in the language of First-Order Logic, we write $p \Vdash_{\mathbb{P}} \psi$ (*"p forces ψ"*) to mean that *if G is $\mathbb{P}$-generic over $\mathbf{V}$ and contains p, then ψ is true in* $\mathbf{V}[G]$, where we tacitly assume that for every $p \in P$ there is a $\mathbb{P}$-generic filter over $\mathbf{V}$ which contains p. Surprisingly, the definition of the relationship "$\Vdash_{\mathbb{P}}$" takes place in the model $\mathbf{V}$ without actually knowing any $\mathbb{P}$-generic filter.

DEFINITION 14.8. Let $p_0 \in P$ be a condition, let $\psi(x_1, \ldots, x_n)$ be a first-order formula with all free variables shown, and let $\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n \in \mathbf{V}^{\mathbb{P}}$ be any $\mathbb{P}$-names. The relationship $p_0 \Vdash_{\mathbb{P}} \psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ is essentially defined by induction on the complexity of ψ. However, for atomic formulae ψ we have to use a double induction on the ranks of the names that are substituted for the variables in ψ:

(a) $p_0 \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$ if and only if

(α) for all $\langle \underset{\sim}{y}_1, s_1 \rangle \in \underset{\sim}{x}_1$, the set

$$\big\{q \geq p_0 : q \geq s_1 \to \exists \langle \underset{\sim}{y}_2, s_2 \rangle \in \underset{\sim}{x}_2 \big(q \geq s_2 \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2\big)\big\}$$

is dense above p_0, and

(β) for all $\langle \underset{\sim}{y}_2, s_2 \rangle \in \underset{\sim}{x}_2$, the set

$$\big\{q \geq p_0 : q \geq s_2 \to \exists \langle \underset{\sim}{y}_1, s_1 \rangle \in \underset{\sim}{x}_1 \big(q \geq s_1 \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2\big)\big\}$$

is dense above p_0.

(b) $p_0 \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 \in \underset{\sim}{x}_2$ if and only if the set

$$\big\{q \geq p_0 : \exists \langle \underset{\sim}{y}, s \rangle \in \underset{\sim}{x}_2 \big(q \geq s \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y} = \underset{\sim}{x}_1\big)\big\}$$

is dense above p_0.

(c) $p_0 \Vdash_{\mathbb{P}} \neg\varphi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ if and only if for all $q \geq p_0$ we have

$$q \nVdash_{\mathbb{P}} \varphi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)\,,$$

i.e., for no $q \geq p_0$ we have $q \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$.

(d) $p_0 \Vdash_{\mathbb{P}} \varphi_1(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) \wedge \varphi_2(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ if and only if

$$p_0 \Vdash_{\mathbb{P}} \varphi_1(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) \quad \text{and} \quad p_0 \Vdash_{\mathbb{P}} \varphi_2(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)\,.$$

(e) $p_0 \Vdash_{\mathbb{P}} \exists z \varphi(z, \underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ if and only if the set

$$\big\{q \geq p_0 : \exists \underset{\sim}{z} \in \mathbf{V}^{\mathbb{P}} \big(q \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{z}, \underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)\big)\big\}$$

is dense above p_0.

As an immediate consequence of DEFINITION 14.8 we get the following

FACT 14.9. *For any sentence ψ of the forcing language we have:*

(a) If $p \Vdash_{\mathbb{P}} \psi$ and $q \geq p$, then $q \Vdash_{\mathbb{P}} \psi$.

(b) The set $\Delta_\psi := \big\{p \in P : (p \Vdash_{\mathbb{P}} \psi) \vee (p \Vdash_{\mathbb{P}} \neg\psi)\big\}$ is open dense in P.

Proof. Part (a) is obvious. For (b) notice that for every $p \in P$, either there is a $q \geq p$ such that $q \Vdash_{\mathbb{P}} \psi$, or for all $q \geq p$ we have $q \nVdash_{\mathbb{P}} \psi$. In the former case, $q \in \Delta_\psi$, and in the latter case we get $p \Vdash_{\mathbb{P}} \neg\psi$ and consequently $p \in \Delta_\psi$. ⊣

Until now, we did not prove that the forcing relationship is doing what we want, *e.g.*, $p \Vdash_{\mathbb{P}} \psi$ should imply $p \nVdash_{\mathbb{P}} \neg\psi$. However, this follows implicitly from the proof of the FORCING THEOREM 14.10, which is the core result of forcing.

The Forcing Theorem. In order to prove that ZFC holds in every generic extension of any model $\mathbf{V}$ of ZFC, we need a tool which allows us to decide within $\mathbf{V}$ whether a given first-order formula is true or false in a certain generic model. The following theorem is the required tool.

THEOREM 14.10 (FORCING THEOREM). *Let $\psi(x_1, \ldots, x_n)$ be a first-order formula with all free variables shown, i.e.,* $\operatorname{free}(\psi) \subseteq \{x_1, \ldots, x_n\}$. *Let $\mathbf{V}$ be a model of* ZFC, *let $\mathbb{P} = (P, \leq)$ be a forcing notion which belongs to $\mathbf{V}$, let $\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n \in \mathbf{V}^{\mathbb{P}}$ be any $\mathbb{P}$-names, and let $G \subseteq P$ be $\mathbb{P}$-generic over $\mathbf{V}$.*

(1) If $p \in G$ and $p \Vdash_{\mathbb{P}} \psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$, then $\mathbf{V}[G] \vDash \psi\big(\underset{\sim}{x}_1[G], \ldots, \underset{\sim}{x}_n[G]\big)$.

(2) If $\mathbf{V}[G] \vDash \psi\big(\underset{\sim}{x}_1[G], \ldots, \underset{\sim}{x}_n[G]\big)$, then $\exists p \in G\big(p \Vdash_{\mathbb{P}} \psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)\big)$.

Proof. The proof is by induction on the complexity of $\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)\big)$. So, we first prove (1) and (2) for atomic formulae ψ.

$\boldsymbol{\psi(\underset{\sim}{x}_1, \underset{\sim}{x}_2) \equiv (\underset{\sim}{x}_1 = \underset{\sim}{x}_2)}$: When $\psi(\underset{\sim}{x}_1, \underset{\sim}{x}_2)$ is $\underset{\sim}{x}_1 = \underset{\sim}{x}_2$, the proof is by transfinite induction on $\underline{\operatorname{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2) := \max\{\operatorname{rk}(\underset{\sim}{x}_1), \operatorname{rk}(\underset{\sim}{x}_2)\}$, using clause (a) of DEFINITION 14.8: If $\underline{\operatorname{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2) = 0$, then $\underset{\sim}{x}_1 = \underset{\sim}{x}_2 = \emptyset$. Now, $\emptyset[G] = \emptyset$, which implies (1), and for all $p \in P$ we have $p \Vdash_{\mathbb{P}} \emptyset = \emptyset$, which implies (2). For $\underline{\operatorname{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2) > 0$ we shall check (1) and (2) separately.

(1) : Assume that $p \in G$ and $p \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$, and that (1) holds for all names $\underset{\sim}{y}_1, \underset{\sim}{y}_2$ with $\underline{\operatorname{rk}}(\underset{\sim}{y}_1, \underset{\sim}{y}_2) < \underline{\operatorname{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2)$. We show $\underset{\sim}{x}_1[G] = \underset{\sim}{x}_2[G]$ by proving that $\underset{\sim}{x}_1[G] \subseteq \underset{\sim}{x}_2[G]$ using (α) of DEFINITION 14.8.(a); the proof of $\underset{\sim}{x}_2[G] \subseteq \underset{\sim}{x}_1[G]$ using (β) is the same. Every element of $\underset{\sim}{x}_1[G]$ is of the form $\underset{\sim}{y}_1[G]$, where $\langle \underset{\sim}{y}_1, s_1 \rangle \in \underset{\sim}{x}_1$ for some $s_1 \in G$. We must show that $\underset{\sim}{y}_1[G] \in \underset{\sim}{x}_2[G]$. Since G is directed, there is an $r \in G$ with $s_1 \leq r \geq p$. By FACT 14.9.(a), $r \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$, and by DEFINITION 14.8.(a).(α) and FACT 14.7, there is a $q \in G$ such that $q \geq r$ (in particular $q \geq s_1$) and

$$\exists \langle \underset{\sim}{y}_2, s_2 \rangle \in \underset{\sim}{x}_2 \big(q \geq s_2 \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2\big)\,. \tag{$\exists$}$$

Fix $\langle \underset{\sim}{y}_2, s_2 \rangle \in \underset{\sim}{x}_2$ as in ($\exists$), then $\underline{\operatorname{rk}}(\underset{\sim}{y}_1, \underset{\sim}{y}_2) < \underline{\operatorname{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2)$ and by our assumption we get $\underset{\sim}{y}_1[G] = \underset{\sim}{y}_2[G]$. Further, since $q \geq s_2$ and G is downwards closed we have $s_2 \in G$ which implies $\underset{\sim}{y}_2[G] \in \underset{\sim}{x}_2[G]$, and consequently we get $\underset{\sim}{y}_1[G] \in \underset{\sim}{x}_2[G]$.

(2) : To check (2), assume $\underset{\sim}{x}_1[G] = \underset{\sim}{x}_2[G]$, and that (2) holds for all names $\underset{\sim}{y}_1, \underset{\sim}{y}_2$ with $\underline{\operatorname{rk}}(\underset{\sim}{y}_1, \underset{\sim}{y}_2) < \underline{\operatorname{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2)$. Let $D_{\underset{\sim}{x}_1, \underset{\sim}{x}_2} \subseteq P$ be the set of all conditions $r \in P$ such that either $r \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$, or we are at least in one of the following two cases:

(α') there exists a name $\langle \underset{\sim}{y}_1, s_1\rangle \in \underset{\sim}{x}_1$ such that $r \geq s_1$ and

$$\forall\langle \underset{\sim}{y}_2, s_2\rangle \in \underset{\sim}{x}_2 \forall q \in P\big((q \geq s_2 \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2) \to q \perp r\big)\,,$$

(β') there exists a name $\langle \underset{\sim}{y}_2, s_2\rangle \in \underset{\sim}{x}_2$ such that $r \geq s_1$ and

$$\forall\langle \underset{\sim}{y}_1, s_1\rangle \in \underset{\sim}{x}_1 \forall q \in P\big((q \geq s_1 \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2) \to q \perp r\big)\,.$$

First we show that no condition $r \in G$ can satisfy (α') or (β'): Indeed, if $r \in G$ and $\langle \underset{\sim}{y}_1, s_1\rangle \in \underset{\sim}{x}_1$ as in (α'), then $s_1 \in G$ and therefore $\underset{\sim}{y}_1[G] \in \underset{\sim}{x}_1[G] = \underset{\sim}{x}_2[G]$ (by our assumption). Now, fix $\langle \underset{\sim}{y}_2, s_2\rangle \in \underset{\sim}{x}_2$ with $s_2 \in G$ and $\underset{\sim}{y}_1[G] = \underset{\sim}{y}_2[G]$. Since $\underline{\mathrm{rk}}(\underset{\sim}{y}_1, \underset{\sim}{y}_2) < \underline{\mathrm{rk}}(\underset{\sim}{x}_1, \underset{\sim}{x}_2)$ there is a condition $q_0 \in G$ such that $q_0 \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2$, and since G is directed there is a $q \in G$ such that $q_0 \leq q \geq s_2$. By FACT 14.9.(a) we have $q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2$, and hence by ($\alpha'$) we get $q \perp r$, which contradicts the fact that G is directed.

If there is no $r \in G$ such that $r \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$, then $D_{\underset{\sim}{x}_1,\underset{\sim}{x}_2} \cap G = \emptyset$. We would be done if we could show that $D_{\underset{\sim}{x}_1,\underset{\sim}{x}_2}$ is dense in P since this would contradict the fact that G meets every dense set in $\mathbf{V}$: Fix an arbitrary condition $p \in P$. Either $p \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$, or otherwise, ($\alpha$) or ($\beta$) of DEFINITION 14.8.(a) fails. If (α) fails, then there are $\langle \underset{\sim}{y}_1, s_1\rangle \in \underset{\sim}{x}_1$ and $r \geq p$ such that $r \geq s_1$ and for all $q \geq r$ we have:

$$\forall\langle \underset{\sim}{y}_2, s_2\rangle \in \underset{\sim}{x}_2\big(\neg(q \Vdash_{\mathbb{P}} \underset{\sim}{y}_1 = \underset{\sim}{y}_2) \wedge q \geq s_2\big) \qquad (\forall)$$

If $\langle \underset{\sim}{y}_2, s_2\rangle \in \underset{\sim}{x}_2$, $q \geq s_2$, and $q \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 = \underset{\sim}{x}_2$, then $q \perp r$, since a common extension q' of q and r would contradict ($\forall$). Thus, $r \geq p$ and r satisfies (α'), in particular $r \in D_{\underset{\sim}{x}_1,\underset{\sim}{x}_2}$. Likewise, if ($\beta$) fails then there is a condition $r \geq p$ which satisfies (β').

$\boldsymbol{\psi(\underset{\sim}{x}_1, \underset{\sim}{x}_2) \equiv (\underset{\sim}{x}_1 \in \underset{\sim}{x}_2)}$: When $\psi(\underset{\sim}{x}_1, \underset{\sim}{x}_2)$ is $\underset{\sim}{x}_1 \in \underset{\sim}{x}_2$ we check again (1) and (2) separately.

(1) : Assume that there is a condition $p \in G$ such that $p \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 \in \underset{\sim}{x}_2$. Then, by DEFINITION 14.8.(b), the set

$$D_p = \big\{q \in P : \exists\langle \underset{\sim}{y}, s\rangle \in \underset{\sim}{x}_2\big(q \geq s \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y} = \underset{\sim}{x}_1\big)\big\}$$

is dense above p. Fix a condition $q \in G \cap D_p$ and a $\mathbb{P}$-name $\langle \underset{\sim}{y}, s\rangle \in \underset{\sim}{x}_2$ such that $q \geq s$ and $q \Vdash_{\mathbb{P}} \underset{\sim}{y} = \underset{\sim}{x}_1$. Since $s \in G$ and $\langle \underset{\sim}{y}, s\rangle \in \underset{\sim}{x}_2$ we get $\underset{\sim}{y}[G] \in \underset{\sim}{x}_2[G]$, and since $q \in G$ and $q \Vdash_{\mathbb{P}} \underset{\sim}{y} = \underset{\sim}{x}_1$, by (1) applied to $\underset{\sim}{y} = \underset{\sim}{x}_1$ we also get $\underset{\sim}{y}[G] = \underset{\sim}{x}_1[G]$. Thus, we have $\underset{\sim}{y}[G] \in \underset{\sim}{x}_2[G]$ as well as $\underset{\sim}{y}[G] = \underset{\sim}{x}_1[G]$, which obviously implies that $\underset{\sim}{x}_1[G] \in \underset{\sim}{x}_2[G]$.

(2) : Assume now $\underset{\sim}{x}_1[G] \in \underset{\sim}{x}_2[G]$. By definition of $\underset{\sim}{x}_2[G]$ there is a name $\langle \underset{\sim}{y}, s\rangle \in \underset{\sim}{x}_2$ such that $s \in G$ and $\underset{\sim}{y}[G] = \underset{\sim}{x}_1[G]$. By (1) for $\underset{\sim}{y}[G] = \underset{\sim}{x}_1[G]$, there is an $r \in G$ such that

$$r \Vdash_{\mathbb{P}} \underset{\sim}{y} = \underset{\sim}{x}_1\,.$$

Finally, let $p \in G$ be such that $s \leq p \geq r$. Then

$$\forall q \geq p\big(q \geq s \wedge q \Vdash_{\mathbb{P}} \underset{\sim}{y} \in \underset{\sim}{x}_2\big)\,,$$

and consequently $p \Vdash_{\mathbb{P}} \underset{\sim}{x}_1 \in \underset{\sim}{x}_2$.

This concludes the proof of (1) and (2) for atomic formulae. The proofs for non atomic formulae are much easier than the preceding proofs, but even though it is enough to prove (1) and (2) for formulae ψ of the form $\neg\varphi$, $\varphi_1 \wedge \varphi_2$, and $\exists x \varphi(x)$, there are still six cases to be checked.

$\boldsymbol{\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) \equiv \neg\varphi}$: Let $\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ be a negated formula, *i.e.*, of the form $\neg\varphi$ for some formula φ.

(1) : We assume (2) for φ and conclude (1) for $\neg\varphi$. Assume $p \in G$ and $p \Vdash_{\mathbb{P}} \neg\varphi$. We have to show that $\mathbf{V}[G] \vDash \neg\varphi$: If $\mathbf{V}[G] \vDash \varphi$, then by (2) for φ there is a $q \in G$ such that $q \Vdash_{\mathbb{P}} \varphi$. Since G is directed, there is an $r \in G$ such that $q \leq r \geq p$ and by FACT 14.9.(a) we would have $r \Vdash_{\mathbb{P}} \varphi$, contradicting the definition of $p \Vdash_{\mathbb{P}} \neg\varphi$.

(2) : We assume (1) for φ and conclude (2) for $\neg\varphi$. Assume that $\mathbf{V}[G] \vDash \neg\varphi$. We have to show that there is a condition $p \in G$ such that $p \Vdash_{\mathbb{P}} \neg\varphi$. Consider the set $\Delta_\varphi := \{r \in P : (r \Vdash_{\mathbb{P}} \varphi) \vee (r \Vdash_{\mathbb{P}} \neg\varphi)\}$. By FACT 14.9.(b), Δ_φ is open dense in P and therefore $\Delta_\varphi \cap G \neq \emptyset$. Fix a condition $p \in \Delta_\varphi \cap G$. If $p \Vdash_{\mathbb{P}} \neg\varphi$, then we are done; and if $p \Vdash_{\mathbb{P}} \varphi$, then by (1) for φ we have $\mathbf{V}[G] \vDash \varphi$, a contradiction.

$\boldsymbol{\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) \equiv \varphi_1 \wedge \varphi_2}$: Let $\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ be of the form $\varphi_1 \wedge \varphi_2$ for some formulae φ_1 and φ_2.

(1) : We assume (1) for φ_1 and φ_2 and conclude (1) for $\varphi_1 \wedge \varphi_2$. Assume $p \in G$ and $p \Vdash_{\mathbb{P}} \varphi_1 \wedge \varphi_2$. Then $p \Vdash_{\mathbb{P}} \varphi_1$ and $p \Vdash_{\mathbb{P}} \varphi_2$, hence, by (1) for φ_1 and φ_2 we have $\mathbf{V}[G] \vDash \varphi_1$ and $\mathbf{V}[G] \vDash \varphi_2$ which implies $\mathbf{V}[G] \vDash \varphi_1 \wedge \varphi_2$.

(2) : We assume (2) for φ_1 and φ_2 and conclude (2) for $\varphi_1 \wedge \varphi_2$. Assume $\mathbf{V}[G] \vDash \varphi_1 \wedge \varphi_2$. By (2) for φ_1 and φ_2 there are $p_1, p_2 \in G$ such that $p_1 \Vdash_{\mathbb{P}} \varphi_1$ and $p_2 \Vdash_{\mathbb{P}} \varphi_2$. Let $r \in G$ be such that $p_1 \leq r \geq p_2$. Then $r \Vdash_{\mathbb{P}} \varphi_1$ and $r \Vdash_{\mathbb{P}} \varphi_2$, hence, $r \Vdash_{\mathbb{P}} \varphi_1 \wedge \varphi_2$.

$\boldsymbol{\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n) \equiv \exists x \varphi(x)}$: Let $\psi(\underset{\sim}{x}_1, \ldots, \underset{\sim}{x}_n)$ be an existential formula of the form $\exists x \varphi(x)$ for some formula φ.

(1) : We assume (1) for $\varphi(\underset{\sim}{x})$ and conclude (1) for $\exists x \varphi(x)$. Assume $p \in G$ and $p \Vdash_{\mathbb{P}} \exists x \varphi(x)$. Then the set

$$\{r \in P : \exists \underset{\sim}{x} (r \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{x}))\}$$

is dense above p. So, we find a $q \in G$ and a $\mathbb{P}$-name $\underset{\sim}{x}_0 \in \mathbf{V}^{\mathbb{P}}$ such that $q \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{x}_0)$. By (1) for $\varphi(\underset{\sim}{x}_0)$ we get $\mathbf{V}[G] \vDash \varphi(\underset{\sim}{x}_0[G])$, and therefore $\mathbf{V}[G] \vDash \exists x \varphi(x)$.

(2) : We assume (2) for $\varphi(\underset{\sim}{x}[G])$ and conclude (2) for $\exists x \varphi(x)$. Assume $\mathbf{V}[G] \vDash \exists x \varphi(x)$. Then there exists an $x_0 \in \mathbf{V}[G]$ such that $\mathbf{V}[G] \vDash \varphi(x_0)$ and let $\underset{\sim}{x}_0$ be such that $\mathbf{V}[G] \vDash \underset{\sim}{x}_0[G] = x_0$. By (2) for $\varphi(\underset{\sim}{x}_0[G])$ there is a $p \in G$ such that $p \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{x}_0)$. Then for all $r \geq p$ we have $r \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{x}_0)$, which implies that $p \Vdash_{\mathbb{P}} \exists x \varphi(x)$. ⊣

One might be tempted to prove the following result (which is to some extent the converse of the FORCING THEOREM 14.10): *If for all $\mathbb{P}$-generic filters*

$G \subseteq P$ containing a certain $\mathbb{P}$-condition p we have $\mathbf{V}[G] \vDash \psi$ (for a given sentence ψ), then $p \Vdash_{\mathbb{P}} \psi$. For the proof we notice first that $p \not\Vdash_{\mathbb{P}} \psi$ would imply that there exists a condition $q > p$ such that $q \Vdash_{\mathbb{P}} \neg\psi$. Now, if we could show that there exists a $\mathbb{P}$-generic filter G containing q we would have $\mathbf{V}[G] \vDash \neg\psi$, which contradicts our assumption. However, as we shall see below, the existence of a $\mathbb{P}$-generic filter G (no matter if it contains q or not) cannot be proved within ZFC.

However, assume for the moment — as we shall later always do — that for any condition q there exists a generic filter containing q. As an application of the FORCING THEOREM 14.10 we prove the following lemma, which is one of the standard results about forcing.

LEMMA 14.11. *Let $\mathbb{P} = (P, \leq)$ be a forcing notion, let G be $\mathbb{P}$-generic over $\mathbf{V}$, and let $p \in G$.*

(a) If $p \Vdash_{\mathbb{P}} \underset{\sim}{z} \in \underset{\sim}{y}$, then there exist a $\mathbb{P}$-name $\underset{\sim}{x}$ with $\mathrm{rk}(\underset{\sim}{x}) < \mathrm{rk}(\underset{\sim}{y})$ and a $\mathbb{P}$-condition $q \geq p$ in G such that $q \Vdash_{\mathbb{P}} \underset{\sim}{z} = \underset{\sim}{x}$.

(b) If $p \Vdash_{\mathbb{P}} \underset{\sim}{f} \in {}^{\underset{\sim}{A}}\underset{\sim}{B} \wedge \underset{\sim}{x}_0 \in \underset{\sim}{A}$, then there is a $\mathbb{P}$-name $\langle \underset{\sim}{y}, r\rangle \in \underset{\sim}{B}$ with $r \in G$ and a condition $q \geq p$ in G such that $q \Vdash_{\mathbb{P}} \underset{\sim}{f}(\underset{\sim}{x}_0) = \underset{\sim}{y}$.

Proof. (a) Since $p \in G$, $\mathbf{V}[G] \vDash \underset{\sim}{z}[G] \in \underset{\sim}{y}[G]$, and since $\underset{\sim}{y}[G] = \big\{\underset{\sim}{x}[G] : \underset{\sim}{x} \in \underset{\sim}{y}\big\}$, there is a name $\langle \underset{\sim}{x}_0, r\rangle \in \underset{\sim}{y}$ with $r \in G$ such that $\underset{\sim}{x}_0[G] = \underset{\sim}{z}[G]$. In particular, $\mathrm{rk}(\underset{\sim}{x}_0) < \mathrm{rk}(\underset{\sim}{y})$. Now, since $\mathbf{V}[G] \vDash \underset{\sim}{x}_0[G] = \underset{\sim}{z}[G]$, there is a condition $p' \in G$ such that $p' \Vdash_{\mathbb{P}} \underset{\sim}{z} = \underset{\sim}{x}_0$. Further, since G is directed, there is a $q \in G$ such that $p \leq q \geq p'$. Thus, $q \Vdash_{\mathbb{P}} \underset{\sim}{z} = \underset{\sim}{x}_0$.

(b) Since $p \in G$, there is a set $z \in \mathbf{V}[G]$ such that

$$\mathbf{V}[G] \vDash z \in \underset{\sim}{B}[G] \wedge \big\langle \underset{\sim}{x}_0[G], z\big\rangle \in \underset{\sim}{f}[G]\,.$$

Let $\underset{\sim}{z}$ be a $\mathbb{P}$-name in $\mathbf{V}$ for z (i.e., $\underset{\sim}{z}[G] = z$). By the proof of (a) there is a $\mathbb{P}$-name $\langle \underset{\sim}{y}, r\rangle \in \underset{\sim}{B}$ with $r \in G$ and a $p' \in G$ such that $p' \Vdash_{\mathbb{P}} \underset{\sim}{y} = \underset{\sim}{z} \wedge \underset{\sim}{y} \in \underset{\sim}{B}$. Since G is directed, there is a $q \in G$ such that $p \leq q \geq p'$. Thus, we have $q \Vdash_{\mathbb{P}} \mathrm{op}(\underset{\sim}{x}_0, \underset{\sim}{y}) \in \underset{\sim}{f}$, or in other words, $q \Vdash_{\mathbb{P}} \underset{\sim}{f}(\underset{\sim}{x}_0) = \underset{\sim}{y}$. ⊣

The Generic Model Theorem. With the FORCING THEOREM 14.10 we would now be able to prove that generic extensions of models of ZFC are also models of ZFC (however, we omit most of the quite tedious proof).

THEOREM 14.12 (GENERIC MODEL THEOREM). *Let $\mathbf{V}$ be a transitive standard model of ZFC (i.e., a transitive model with the standard membership relation), let $\mathbb{P} = (P, \leq)$ be a forcing notion which belongs to $\mathbf{V}$, and let $G \subseteq P$ be $\mathbb{P}$-generic over $\mathbf{V}$. Then $\mathbf{V}[G] \vDash$ ZFC. Moreover, the class $\mathbf{V}$ is a subclass of $\mathbf{V}[G]$, $G \in \mathbf{V}[G]$, and every transitive standard model of ZFC containing $\mathbf{V}$ as a subclass and G as an element also contains $\mathbf{V}[G]$ (i.e., $\mathbf{V}[G]$ is the smallest standard model of ZFC containing $\mathbf{V}$ as a subclass and G as a set). Furthermore, $\Omega^{\mathbf{V}[G]} = \Omega^{\mathbf{V}}$, i.e., every ordinal in $\mathbf{V}[G]$ belongs to $\mathbf{V}$, and vice versa.*

Instead of the full Generic Model Theorem, let us just prove the following four partial results.

Fact 14.13. *If* $\mathbf{V} \vDash \mathsf{ZFC}$ *and* G *is* $\mathbb{P}$*-generic over* $\mathbf{V}$*, then* $\mathbf{V}[G]$ *satisfies the* Axiom of Pairing.

Proof. Let G be an arbitrary $\mathbb{P}$-generic filter and let $\underset{\sim}{x}$ and $\underset{\sim}{y}$ be $\mathbb{P}$-names for some sets x and y in $\mathbf{V}[G]$ (*i.e.*, $\underset{\sim}{x}[G] = x$ and $\underset{\sim}{y}[G] = y$ respectively). Because G is downwards closed we have $\mathbf{0} \in G$ and therefore we get

$$\mathrm{up}(\underset{\sim}{x}, \underset{\sim}{y})[G] = \big\{\underset{\sim}{x}[G], \underset{\sim}{y}[G]\big\} = \{x, y\}\,.$$

Thus, if x and y belong to $\mathbf{V}[G]$, then also $\{x, y\}$ belongs to $\mathbf{V}[G]$. ⊣

Proposition 14.14. *If* $\mathbf{V} \vDash \mathsf{ZFC}$ *and* G *is* $\mathbb{P}$*-generic over* $\mathbf{V}$*, then* $\mathbf{V}[G] \vDash \mathsf{AC}$.

Proof. Let $x \in \mathbf{V}[G]$ be an arbitrary set. Since the Well-Ordering Principle implies AC, it is enough to prove that in $\mathbf{V}[G]$ there exists an injective function from x into Ω (notice that the empty function is injective). Let $\underset{\sim}{x}$ be a $\mathbb{P}$-name in $\mathbf{V}$ for x and let

$$\bar{y} = \big\{\underset{\sim}{y} : \exists p \in P\,(\langle \underset{\sim}{y}, p\rangle \in \underset{\sim}{x})\big\}\,.$$

Obviously, $\bar{y}$ is a set of $\mathbb{P}$-names which belongs to $\mathbf{V}$. By the Axiom of Choice, which holds in $\mathbf{V}$, we can write $\bar{y} = \{\underset{\sim}{y}_\alpha : \alpha \in \kappa\}$, where $\kappa = |\bar{y}|$ is a cardinal in $\mathbf{V}$. Now let

$$\underset{\sim}{R} = \big\{\,\mathrm{op}(\underset{.}{\alpha}, \underset{\sim}{y}_\alpha) : \alpha \in \kappa\big\} \times \big\{\mathbf{0}\big\}$$

which is a $\mathbb{P}$-name in $\mathbf{V}$ for a set of ordered pairs in $\mathbf{V}[G]$. Since $\mathbf{0} \in G$, $\underset{\sim}{R}[G]$ induces a surjection from $\big\{\alpha \in \kappa : \exists p \in G(\langle \underset{\sim}{y}_\alpha, p\rangle \in \underset{\sim}{x})\big\} \subseteq \kappa$ onto the set $x = \underset{\sim}{x}[G] = \big\{\underset{\sim}{y}_\alpha[G] : \exists p \in G(\langle \underset{\sim}{y}_\alpha, p\rangle \in \underset{\sim}{x})\big\}$, and consequently the set $x \in \mathbf{V}[G]$ can be well-ordered. Hence, since x was arbitrary, $\mathbf{V}[G] \vDash \mathsf{AC}$. ⊣

Fact 14.15. *If* $\mathbf{V} \vDash \mathsf{ZFC}$ *and* G *is* $\mathbb{P}$*-generic over* $\mathbf{V}$*, then* $G \in \mathbf{V}[G]$ *and* $\mathbf{V}$ *is a subclass of* $\mathbf{V}[G]$.

Proof. Let G be an arbitrary $\mathbb{P}$-generic filter. By definition of $\underset{.}{G}$, $\underset{.}{G}[G] = G$, and hence, by definition of $\mathbf{V}[G]$, $G \in \mathbf{V}[G]$. Further, G is downwards closed and therefore contains $\mathbf{0}$ (the smallest element of P). Hence, for each $x \in \mathbf{V}$ we have $\underset{.}{x}[G] = x$ and consequently $x \in \mathbf{V}[G]$. ⊣

Proposition 14.16. *Let* $\mathbf{V} \vDash \mathsf{ZFC}$*, let* $\mathbb{P}$ *be a forcing notion in* $\mathbf{V}$*, and let* G *be* $\mathbb{P}$*-generic over* $\mathbf{V}$*; then* $\Omega^{\mathbf{V}[G]} = \Omega^{\mathbf{V}}$.

Proof. Since $\mathbf{V} \subseteq \mathbf{V}[G]$, we obviously have $\Omega^{\mathbf{V}} \subseteq \Omega^{\mathbf{V}[G]}$. On the other hand, assume towards a contradiction that there exists an ordinal in $\mathbf{V}[G]$ which does not belong to $\mathbf{V}$. Since the class $\Omega^{\mathbf{V}[G]}$ is well-ordered in $\mathbf{V}[G]$ by $\in$, there is a smallest ordinal in $\mathbf{V}[G]$, say γ, which does not belong to $\mathbf{V}$. Let $\underset{\sim}{\gamma}$ be a $\mathbb{P}$-name for γ, *i.e.*, $\gamma = \underset{\sim}{\gamma}[G]$. Then $\big\{\underset{\sim}{x} : \exists p(\langle \underset{\sim}{x}, p\rangle \in \underset{\sim}{\gamma})\big\}$ is a *set* in $\mathbf{V}$, hence, the collection of all ordinals $\alpha \in \gamma$ is in fact a set in $\mathbf{V}$. This implies that γ belongs to $\mathbf{V}$ and contradicts our assumption. ⊣

Until now we did not show that generic filters exist, but let us postpone this topic until the end of this chapter and let us show first how a statement (*e.g.*, "there are Ramsey ultrafilters") can be forced to become true in a certain generic model.

Forcing notions which do not add reals. In this section, we shall see that the forcing notion $\mathbb{U}$ adds a Ramsey ultrafilter to the ground model $\mathbf{V}$. In fact we shall see that whenever G is $\mathbb{U}$-generic over $\mathbf{V}$, then G induces a filter over ω such that for any colouring $\pi : [\omega]^2 \to 2$ in $\mathbf{V}$ there is an $x \in G$ such that $\pi|_{[x]^2}$ is constant. However, in order to make this approach work we have to show that forcing with $\mathbb{U}$ does not add any new reals (*i.e.*, subsets of ω or functions $[\omega]^2 \to 2$) to $\mathbf{V}$; if $\mathbb{U}$ would add new reals to $\mathbf{V}$, there might be a colouring $\rho : [\omega]^2 \to 2$ in $\mathbf{V}[G]$ such that no set $x \in G$ is homogeneous for ρ, and consequently, $\big\{x \in [\omega]^\omega : \exists y \in G(y \subseteq x)\big\}$ would just be a filter in $\mathbf{V}[G]$.

So, let us first prove that whenever G is $\mathbb{U}$-generic over $\mathbf{V}$, then $[\omega]^\omega \cap \mathbf{V} = [\omega]^\omega \cap \mathbf{V}[G]$, *i.e.*, every subset of ω which is in $\mathbf{V}[G]$ is also in $\mathbf{V}$, and vice versa.

A forcing notion $\mathbb{P} = (P, \leq)$ is said to be σ**-closed** if whenever $\langle p_n : n \in \omega\rangle$ is an increasing sequence of elements of P (*i.e.*, $m < k \to p_m \leq p_k$), then there exists a condition $q \in P$ such that for all $n \in \omega$, $q \geq p_n$.

By the proof of the fact that $\mathfrak{p}$ is uncountable (*cf.* THEOREM 8.1) we get that the forcing notion $\mathbb{U}$ is σ-closed.

The next result shows that forcing with a σ-closed forcing notion does not add new reals to the ground model.

LEMMA 14.17. *Let $\mathbb{P} = (P, \leq)$ be a σ-closed forcing notion, G a $\mathbb{P}$-generic filter over $\mathbf{V}$, X a set in $\mathbf{V}$, and $f : \omega \to X$ a function in $\mathbf{V}[G]$, i.e., $\mathbf{V}[G] \vDash f \in {}^\omega X$; then f belongs to $\mathbf{V}$.*

Proof. Let $f \in {}^\omega X$ be a function in $\mathbf{V}[G]$ and let $\underset{\sim}{f}$ be a $\mathbb{P}$-name for f. Assume towards a contradiction that $\underset{\sim}{f}[G] \notin \mathbf{V}$. By the FORCING THEOREM 14.10.(2) there is a condition $q \in P$ (in fact, $q \in G$) such that

$$q \Vdash_{\mathbb{P}} \underset{\sim}{f} \in \underset{\sim}{{}^\omega X} \wedge \underset{\sim}{f} \notin \underset{\bullet}{{}^\omega X}\,.$$

Notice the difference between $\underset{\sim}{{}^\omega X}$ (which is a $\mathbb{P}$-name for the set ${}^\omega X \in \mathbf{V}[G]$) and $\underset{\bullet}{{}^\omega X}$ (which is the canonical $\mathbb{P}$-name for the set ${}^\omega X \in \mathbf{V}$). By LEMMA 14.11.(b), let $p_0 \geq q$ be such that $p_0 \Vdash_{\mathbb{P}} \underset{\sim}{f}(\underset{\cdot}{0}) = \underset{\cdot}{x}_0$ (for some $x_0 \in X$), and for $n \in \omega$ let $p_{n+1} \geq p_n$ be such that $p_{n+1} \Vdash_{\mathbb{P}} \underset{\sim}{f}(\underset{\cdot}{n} + \underset{\cdot}{1}) = \underset{\cdot}{x}_{n+1}$ (for some $x_{n+1} \in X$). Notice that by LEMMA 14.11.(b), p_0 and p_{n+1} exist and that the construction can be carried out in $\mathbf{V}$. Finally, let $p \in P$ be such that for all $n \in \omega$, $p \geq p_n$. Then, by FACT 14.9.(a), for all $n \in \omega$ there is an $x_n \in X$ such that $p \Vdash_{\mathbb{P}} \underset{\sim}{f}(\underset{\cdot}{n}) = \underset{\cdot}{x}_n$. Thus,

$$p \Vdash_{\mathbb{P}} \underset{\sim}{f} \in \underset{\bullet}{{}^\omega X}\,,$$

which is a contradiction to our assumption. ⊣

Since $\mathbb{U}$ is σ-closed and every real $x \in [\omega]^\omega$ corresponds to a function $f_x \in {}^\omega 2$ (stipulating $f_x(n) = 1 \iff n \in x$), by LEMMA 14.17, ultrafilter forcing $\mathbb{U}$ does not add any new reals to the ground model $\mathbf{V}$. In other words, if G is $\mathbb{U}$-generic over $\mathbf{V}$, then $[\omega]^\omega \cap \mathbf{V} = [\omega]^\omega \cap \mathbf{V}[G]$. With this observation we are ready to prove the following result.

PROPOSITION 14.18. *If G is $\mathbb{U}$-generic over $\mathbf{V}$. Then $\bigcup G$ is a Ramsey ultrafilter in $\mathbf{V}[G]$ which is different from all ultrafilters in $\mathbf{V}$, i.e., ultrafilter forcing $\mathbb{U}$ adds a new Ramsey ultrafilter to $\mathbf{V}$. In particular, $\mathbf{V}[G]$ contains a Ramsey ultrafilter.*

Proof. Firstly we show that $\bigcup G = \{x \in [\omega]^\omega : [x]^{\tilde{}} \in G\}$ is an ultrafilter over ω which is different from all ultrafilters in $\mathbf{V}$: Since G is downwards closed, directed, and meets every maximal anti-chain in $[\omega]^\omega/\operatorname{fin}$ which belongs to $\mathbf{V}$ (in particular all anti-chains of the form $\{[z]^{\tilde{}}, [\omega \setminus z]^{\tilde{}}\}$ for co-infinite sets $z \in [\omega]^\omega$), and since forcing with $\mathbb{U}$ does not add reals, $\bigcup G$ is an ultrafilter over ω. Let now $\mathscr{U} \in \mathbf{V}$ be an arbitrary ultrafilter over ω. Then

$$D_{\mathscr{U}} = \{[x]^{\tilde{}} \in [\omega]^\omega : x \notin \mathscr{U}\}$$

is an open dense subset of $[\omega]^\omega/\operatorname{fin}$. Thus, $G \cap D_{\mathscr{U}} \neq \emptyset$ which implies $\bigcup G \neq \mathscr{U}$, and since $\mathscr{U}$ was arbitrary, the ultrafilter $\bigcup G$ is different from all ultrafilters in $\mathbf{V}$.

Secondly we show that $\bigcup G$ is a Ramsey ultrafilter: Let $\pi : [\omega]^2 \to 2$ be an arbitrary colouring in $\mathbf{V}[G]$. Since forcing with $\mathbb{U}$ does not add reals, $\pi \in \mathbf{V}$. Now the set

$$D_\pi := \{[x]^{\tilde{}} \in [\omega]^\omega : \pi|_{[x]^2} \textit{ is constant}\}$$

is an open dense subset of $[\omega]^\omega/\operatorname{fin}$. Thus, $G \cap D_\pi \neq \emptyset$ which implies that there exists an $[x]^{\tilde{}} \in G$ such that $\pi|_{[x]^2}$ is constant, and since π was arbitrary, $\bigcup G$ is a Ramsey ultrafilter. ⊣

The preceding theorem is a typical example how to force the existence of a certain set whose existence cannot be proved in ZFC: By the same forcing construction as above we shall see in Chapter 24 that there may be a Ramsey ultrafilter even in the case when $\mathfrak{p} < \mathfrak{c}$.

Forcing notions which do not collapse cardinals. Now we consider the forcing notion $\mathbb{C}_\kappa$ (for an arbitrary cardinal κ) and show that the forcing notion $\mathbb{C}_\kappa$ adds κ reals to the ground model $\mathbf{V}$. As a consequence we get that whenever G is $\mathbb{C}_\kappa$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \vDash \mathfrak{c} \geq \kappa$ (where $\mathfrak{c}$ denotes the cardinality of the continuum). In particular, for $\kappa > \omega_1$ we get $\mathbf{V}[G] \vDash \neg\mathsf{CH}$. However, in order to make this approach work we have to show that κ is the same cardinal in $\mathbf{V}[G]$ as it is in $\mathbf{V}$. Let us explain this problem in greater detail: Let $\mathbb{P}$ be a forcing notion and let G be $\mathbb{P}$-generic over $\mathbf{V}$. Further, let κ be an arbitrary infinite cardinal in $\mathbf{V}$. By definition, κ is an ordinal such that there is no bijection between κ and any of its elements (recall that the elements of ordinal are ordinals). Since $\mathbf{V}$ and $\mathbf{V}[G]$ contain the same ordinals, κ is an ordinal number in $\mathbf{V}[G]$. However, since $\mathbf{V}[G]$ is an extension of $\mathbf{V}$, there might be an injective function in $\mathbf{V}[G]$ which maps κ to one of its elements. In other words, the ordinal number κ, which is a cardinal in $\mathbf{V}$, might become an ordinary ordinal in $\mathbf{V}[G]$, *i.e.*, we might have $\mathbf{V} \vDash |\kappa| = \kappa$ but $\mathbf{V}[G] \vDash |\kappa| \in \kappa$. If this is the case, then we say that $\mathbb{P}$ **collapses** κ; otherwise, we say that $\mathbb{P}$ **preserves** κ. If $\mathbb{P}$ preserves all cardinal numbers, *i.e.*, $|\kappa|^{\mathbf{V}[G]} = \kappa$ whenever $|\kappa|^{\mathbf{V}} = \kappa$, then we simply say that $\mathbb{P}$ **preserves cardinalities**. Notice that all finite cardinals are preserved by any forcing notion, and consequently also ω must be preserved, *i.e.*, we always have $|\omega|^{\mathbf{V}} = |\omega|^{\mathbf{V}[G]} = \omega$. On the other hand, any uncountable cardinal number can be collapsed; moreover, any uncountable cardinal can be forced to become a countable ordinal.

Now, let us prove that the forcing notion $\mathbb{C}_\kappa$ preserves cardinals, but first we prove a slightly more general result.

Recall that a forcing notion $\mathbb{P} = (P, \leq)$ is said to satisfy the **countable chain condition**, denoted *ccc*, if every anti-chain in P is at most countable — in which case we usually just say "$\mathbb{P}$ satisfies *ccc*". For example, by COROLLARY13.3 we know that the forcing notion $\mathbb{C}_\kappa$ satisfies *ccc*.

In order to show that a forcing notion which satisfies *ccc* does not collapse any cardinal, we shall show the slightly more general result that a forcing notion which preserves cofinalities also preserves cardinalities: A forcing notion $\mathbb{P}$ **preserves cofinalities** if whenever G is $\mathbb{P}$-generic over $\mathbf{V}$ and κ is a cardinal in $\mathbf{V}$, then $\mathrm{cf}(\kappa)^{\mathbf{V}} = \mathrm{cf}(\kappa)^{\mathbf{V}[G]}$.

LEMMA 14.19. *If $\mathbb{P}$ preserves cofinalities, then $\mathbb{P}$ preserves cardinalities.*

Proof. Assume $\mathbb{P}$ preserves cofinalities and let G be $\mathbb{P}$-generic over $\mathbf{V}$.

Firstly, let κ be a regular cardinal in $\mathbf{V}$, *i.e.*, $\mathbf{V} \vDash \mathrm{cf}(\kappa) = \kappa$. Then, since $\mathbb{P}$ preserves cofinalities, the ordinal $\mathrm{cf}(\kappa)^{\mathbf{V}}$ is equal to the ordinal $\mathrm{cf}(\kappa)^{\mathbf{V}[G]}$. Thus, $\mathbf{V}[G] \vDash \kappa = \mathrm{cf}(\kappa)$ which shows that the ordinal κ, which is a regular cardinal in $\mathbf{V}$, is still a regular cardinal in $\mathbf{V}[G]$.

Secondly, if $\lambda > \omega$ is a limit cardinal in $\mathbf{V}$, then the set of cardinals $\mathcal{C} = \{\kappa < \lambda : \kappa \textit{ regular}\}$ is cofinal in λ (recall that by PROPOSITION 5.10 successor cardinals are regular), and since the cardinals in $\mathcal{C}$ remain (regular) cardinals in $\mathbf{V}[G]$, $\mathcal{C}^{\mathbf{V}} = \mathcal{C}^{\mathbf{V}[G]}$ and consequently λ is a cardinal (in fact a limit cardinal) in $\mathbf{V}[G]$ as well. ⊣

LEMMA 14.20. *If $\mathbb{P} = (P, \leq)$ is a forcing notion which satisfies ccc, then $\mathbb{P}$ preserves cofinalities as well as cardinals.*

Proof. Let $\mathbb{P} = (P, \leq)$ be a forcing notion which satisfies *ccc* and which belongs to some model $\mathbf{V}$ of ZFC, and let G be $\mathbb{P}$-generic over $\mathbf{V}$. By LEMMA 14.19 it is enough to prove that $\mathbb{P}$ preserves cofinalities. Let κ be an infinite cardinal in $\mathbf{V}$ and let $\underset{\sim}{S}$ be a $\mathbb{P}$-name for a strictly increasing sequence of length $\lambda = \mathrm{cf}(\kappa)$ in $\mathbf{V}[G]$ which is cofinal in κ, *i.e.*, we have $\underset{\sim}{S}[G] : \lambda \to \kappa$ with $\bigcup\{\underset{\sim}{S}[G](\alpha) : \alpha \in \lambda\} = \kappa$. Thus, there is a $\mathbb{P}$-condition $p \in G$ such that

$$p \Vdash_{\mathbb{P}} \underset{\sim}{\mathcal{S}} \in {}^{\check{\lambda}}\check{\kappa} \wedge \bigcup\{\underset{\sim}{\mathcal{S}}(\check{\alpha}) : \check{\alpha} \in \check{\lambda}\} = \check{\kappa}\,.$$

Work for a moment in the ground model $\mathbf{V}$: For each $\alpha \in \lambda$ let

$$D_\alpha = \{q \geq p : \exists y (q \Vdash_{\mathbb{P}} \underset{\sim}{\mathcal{S}}(\check{\alpha}) = y)\}\,.$$

Then, by FACT 14.9.(b), D_α is open dense above p. For each $\alpha \in \lambda$ define

$$Y_\alpha = \{\gamma \in \kappa : \exists q \in D_\alpha (q \Vdash_{\mathbb{P}} \underset{\sim}{\mathcal{S}}(\check{\alpha}) = \check{\gamma})\}\,.$$

Then, for every $\alpha \in \lambda$, the set $Y_\alpha \subseteq \kappa$ is in $\mathbf{V}$, and since $\mathbb{P}$ satisfies *ccc*, $|Y_\alpha| \leq \omega$. Indeed, if $q_1 \Vdash_{\mathbb{P}} \underset{\sim}{\mathcal{S}}(\check{\alpha}) = \check{\gamma}_1$ and $q_2 \Vdash_{\mathbb{P}} \underset{\sim}{\mathcal{S}}(\check{\alpha}) = \check{\gamma}_2$, where $\gamma_1 \neq \gamma_2$, then $q_1 \perp q_2$.

Let us turn back to the model $\mathbf{V}[G]$: For every $\alpha \in \lambda$ let A_α be a maximal anti-chain in D_α. By FACT 14.6.(b) and FACT 14.7, G meets every set A_α, which implies that for every $\alpha \in \lambda$, $\underset{\sim}{\mathcal{S}}[G](\alpha) \in Y_\alpha$. Let $Y := \bigcup\{Y_\alpha : \alpha \in \lambda\}$; then $Y \subseteq \kappa$ is a set in $\mathbf{V}$ such that $\bigcup Y = \kappa$. Since the cardinal λ is infinite we get $|Y| \leq \lambda \cdot \omega = \lambda$, which implies that $\mathrm{cf}(\kappa)^{\mathbf{V}} \leq \lambda$. Thus, since $\lambda = \mathrm{cf}(\kappa)^{\mathbf{V}[G]} \leq \mathrm{cf}(\kappa)^{\mathbf{V}}$, we have $\mathrm{cf}(\kappa)^{\mathbf{V}} = \mathrm{cf}(\kappa)^{\mathbf{V}[G]}$. ⊣

Independence of CH: The Gentle Way

Since $\mathbb{C}_\kappa$ satisfies *ccc*, in order to prove the following result we just have to show that forcing with $\mathbb{C}_\kappa$ adds κ different real numbers to the ground model $\mathbf{V}$, *i.e.*, the continuum in $\mathbf{V}[G]$ is at least of cardinality κ.

THEOREM 14.21. *If $\mathbf{V} \vDash \mathsf{ZFC}$ and G is $\mathbb{C}_\kappa$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \vDash \mathfrak{c} \geq \kappa$. In particular, if $\kappa > \omega_1$, then $\mathbf{V}[G] \vDash \neg\mathsf{CH}$.*

Proof. Let G be $\mathbb{C}_\kappa$-generic over $\mathbf{V}$. Since $\mathbb{C}_\kappa$ satisfies *ccc*, by LEMMA 14.20 it is enough to prove that with G one can construct κ different real numbers. To keep the notation short let $C_\kappa := \mathrm{Fn}(\kappa \times \omega, 2)$.

Firstly we show that $\bigcup G$ is a function from $\kappa \times \omega$ to 2: For $\alpha \in \kappa$ and $n \in \omega$ let

$$D_{\alpha,n} = \{p \in C_\kappa : \langle \alpha, n\rangle \in \mathrm{dom}(p)\}\,.$$

Then for any $\alpha \in \kappa$ and $n \in \omega$, $D_{\alpha,n}$ is an open dense subset of C_κ and therefore $G \cap D_{\alpha,n} \neq \emptyset$. Thus, for every $\alpha \in \kappa$ and for every $n \in \omega$ there is a $p \in G$ such that p is defined on $\langle \alpha, n\rangle$, and since G is directed, $\bigcup G$ is a function with $\mathrm{dom}\left(\bigcup G\right) = \kappa \times \omega$.

Secondly we show how to construct κ different real numbers from G: For each $\alpha \in \kappa$ define $r_\alpha \in {}^\omega 2$ by stipulating $r_\alpha(n) := \bigcup G(\langle \alpha, n\rangle)$ (for all $n \in \omega$). Now, for $\alpha, \beta \in \kappa$ let

$$D_{\alpha,\beta} = \{p \in C_\kappa : \exists n \in \omega (\{\langle \alpha, n\rangle, \langle \beta, n\rangle\} \subseteq \mathrm{dom}(p) \wedge p(\langle \alpha, n\rangle) \neq p(\langle \beta, n\rangle))\}\,.$$

Then for any distinct ordinals $\alpha, \beta \in \kappa$, $D_{\alpha,\beta}$ is an open dense subset of C_κ and therefore $G \cap D_{\alpha,\beta} \neq \emptyset$. Thus, for any distinct $\alpha, \beta \in \kappa$ there is an $n \in \omega$ and a $p \in G$ such that $p(\langle \alpha, n\rangle) \neq p(\langle \beta, n\rangle)$, and therefore $r_\alpha(n) \neq r_\beta(n)$.

We can even show that G adds κ new reals to the ground model $\mathbf{V}$: To see this, let $f : \omega \to 2$ be an arbitrary function in $\mathbf{V}$, and for any $\alpha \in \kappa$ let

$$D_{f,\alpha} = \left\{ p \in C_\kappa : \exists n \in \omega \big(\langle \alpha, n\rangle \in \operatorname{dom}(p) \wedge p(\langle \alpha, n\rangle) \neq f(n) \big) \right\}.$$

Since $D_{f,\alpha}$ is obviously open dense in C_κ, $r_\alpha \neq f$, and since the function $f \in \mathbf{V}$ was arbitrary, for each $\alpha \in \kappa$ we have $r_\alpha \notin \mathbf{V}$. ⊣

Now we show that for each ordinal α, the statement $2^{\omega_\alpha} = \omega_{\alpha+1}$ is consistent with ZFC. In particular, for $\alpha = 0$ we get the relative consistency of the Continuum Hypothesis; but first we have to introduce some notations.

Let κ be an infinite cardinal. We say that a forcing notion $\mathbb{P} = (P, \leq)$ is **κ-closed** if whenever $\gamma < \kappa$ and $\{p_\xi : \xi \in \gamma\}$ is an increasing sequence of elements of P (*i.e.*, $\xi_0 < \xi_1 \to p_{\xi_0} \leq p_{\xi_1}$), then there exists a condition $q \in P$ such that for all $\xi \in \gamma$, $q \geq p_\xi$. In particular, ω_1-closed is the same as σ-closed.

The following fact is just a generalisation of LEMMA 14.17 and we leave the proof as an exercise to the reader.

FACT 14.22. *Let $\mathbb{P} = (P, \leq)$ be a κ-closed forcing notion, λ an ordinal in κ, G a $\mathbb{P}$-generic filter over $\mathbf{V}$, X a set in $\mathbf{V}$, and $f : \lambda \to X$ a function in $\mathbf{V}[G]$; then f belongs to $\mathbf{V}$.*

For ordinals α let K_α be the set of all functions p from a subset of $\omega_{\alpha+1}$ to $\mathscr{P}(\omega_\alpha)$ such that $\left|\operatorname{dom}(p)\right| < \omega_{\alpha+1}$ (*i.e.*, $\left|\operatorname{dom}(p)\right| \leq \omega_\alpha$), and let $\mathbb{K}_\alpha := (K_\alpha, \subseteq)$. Since $\omega_{\alpha+1}$ is an infinite successor cardinal, it is regular, and therefore $\mathbb{K}_\alpha$ is $\omega_{\alpha+1}$-closed. Thus, by FACT 14.22, for each ordinal β, every function from ω_α to β in a $\mathbb{K}_\alpha$-generic extension belongs to the ground model. As a consequence we get that the forcing notion $\mathbb{K}_\alpha$ preserves all cardinals $\leq \omega_{\alpha+1}$ and does not add new subsets of ω_α.

With the forcing notion $\mathbb{K}_\alpha$ we can now easily construct a generic model in which $2^{\omega_\alpha} = \omega_{\alpha+1}$.

THEOREM 14.23. *If $\mathbf{V} \vDash$ ZFC and G_α is $\mathbb{K}_\alpha$-generic over $\mathbf{V}$, then $\mathbf{V}[G_\alpha] \vDash 2^{\omega_\alpha} = \omega_{\alpha+1}$. In particular we get $\mathbf{V}[G_0] \vDash$ CH*

Proof. We shall show that $\bigcup G_\alpha$ is a surjective function from $\omega_{\alpha+1}$ onto $\mathscr{P}(\omega_\alpha)$. Work in $\mathbf{V}$. For $\xi \in \omega_{\alpha+1}$ and $x \in \mathscr{P}(\omega_\alpha)$ let

$$D_{\xi,x} = \left\{ p \in \mathbb{K}_\alpha : \xi \in \operatorname{dom}(p) \wedge x \in \operatorname{ran}(p) \right\}.$$

Then for every $\xi \in \omega_{\alpha+1}$ and every $x \in \mathscr{P}(\omega_\alpha)$, $D_{\xi,x}$ is an open dense subset of K_α and therefore $G_\alpha \cap D_{\xi,x} \neq \emptyset$. Thus, for all $\xi \in \omega_{\alpha+1}$ and $x \in \mathscr{P}(\omega_\alpha)$ there is a $p \in G_\alpha$ such that $\xi \in \operatorname{dom}(p)$ and $x \in \operatorname{ran}(p)$, and since G_α is directed, this implies that the set $\bigcup G_\alpha$ (in $\mathbf{V}[G]$) is indeed a surjective function from $\omega_{\alpha+1}$ onto $\mathscr{P}(\omega_\alpha)$. Hence, $\mathbf{V}[G_\alpha] \vDash \left|\mathscr{P}(\omega_\alpha)\right| \leq \omega_{\alpha+1}$, and since $2^{\omega_\alpha} \geq \omega_{\alpha+1}$ we finally get $\mathbf{V}[G_\alpha] \vDash 2^{\omega_\alpha} = \omega_{\alpha+1}$. ⊣

By the two preceding theorems it follows that there are models of ZFC in which the Continuum Hypothesis holds as well as some in which it fails, and as a consequence we get that CH is independent of ZFC. However, the construction of the corresponding generic models relied on the existence of the corresponding generic filters, and it is now time to discuss this issue.

On the Existence of Generic Filters

Let $\mathbf{V}$ be again a model of ZFC and let $\mathbb{P} = (P, \leq)$ be a forcing notion which belongs to $\mathbf{V}$. We know from Chapter 5 that if ZF is consistent, then so is ZFC and that there is a smallest standard model of ZFC containing the ordinals, namely Gödel's constructible universe $\mathbf{L}$. So, we can assume $\mathbf{V} = \mathbf{L}$ (in fact we have no other choice because $\mathbf{L}$ is the only model of ZFC we know of). Now assume that the set $G \subseteq P$ is $\mathbb{P}$-generic over $\mathbf{V}$, where $\mathbb{P}$ belongs to $\mathbf{V}$ and $\mathbf{V}$ is a model of ZFC (*e.g.*, $\mathbf{V} = \mathbf{L}$). We first show that G does not belong to the model $\mathbf{V}$.

FACT 14.24. *If $\mathbf{V}$ is a model of ZFC, $\mathbb{P} = (P, \leq)$ a forcing notion in $\mathbf{V}$, and $G \subseteq P$ is $\mathbb{P}$-generic over $\mathbf{V}$, then the set G does not belong to $\mathbf{V}$.*

Proof. Let $D_G = P \setminus G$ and let $p \in P$ be an arbitrary $\mathbb{P}$-condition. Since $\mathbb{P}$ is a forcing notion, there are incompatible elements above p, *i.e.*, $\exists q_1, q_2 \in P \big(p \leq q_1 \wedge p \leq q_2 \wedge q_1 \perp q_2\big)$. Now, since G is directed, at most one of these two elements belongs to G, or in other words, at least one of these two elements belongs to D_G. Therefore, D_G is dense in P and since G is downwards closed, D_G is also open. Hence, D_G is an open dense subset of P. If G belongs to $\mathbf{V}$, then D_G belongs to $\mathbf{V}$ as well, but obviously $G \cap D_G = \emptyset$ which implies that G is not $\mathbb{P}$-generic over $\mathbf{V}$. ⊣

This leads to the following question: *If $\mathbb{P}$-generic filters do not belong to the ground model $\mathbf{V}$, why do we know that $\mathbb{P}$-generic filters exist?* Informally, people living in $\mathbf{V}$ may ask: Is there life beyond $\mathbf{V}$?

Unfortunately, one cannot prove within ZFC that $\mathbb{P}$-generic filters exist, but at least, this one can prove: Consider the constructible universe $\mathbf{L}$. All sets in $\mathbf{L}$ are constructible, and vice versa, all constructible sets are in $\mathbf{L}$. If we add the statement *all sets are constructible*, denoted $\mathbf{V} = \mathbf{L}$, as a kind of axiom to ZFC, then there exists just a single transitive standard model of ZFC + $\mathbf{V} = \mathbf{L}$ containing all the ordinals, namely $\mathbf{L}$ (at the same time we get that $\mathbf{V} = \mathbf{L}$ is consistent with ZFC). Thus, as a consequence of $\mathbf{V} = \mathbf{L}$ we get that there are no $\mathbb{P}$-generic filters whatsoever.

Let us now explain how to get around this difficulty: Firstly construct a small (*i.e.*, countable) model $\mathbf{M}$ of a large enough fragment of ZFC inside $\mathbf{V}$, and then extend $\mathbf{M}$ within $\mathbf{V}$ to a suitable generic model $\mathbf{M}[G]$. For example to show that $\neg$CH is consistent with ZFC, by the COMPACTNESS THEOREM 3.7

it is enough to show that whenever Φ is a finite set of axioms of ZFC, then $\Phi + \neg\mathsf{CH}$ has a model. Let $\Phi \subseteq \mathsf{ZFC}$ be an arbitrary but fixed finite set of axioms. Now, take a countable set $\mathbf{M} \in \mathbf{V}$ such that $\mathbf{M}$ can be extended in $\mathbf{V}$ to a *set model* $\mathbf{M}[G]$ (still in $\mathbf{V}$) such that $\mathbf{M}[G] \vDash \Phi$ but also $\mathbf{M}[G] \vDash \neg\mathsf{CH}$. Because Φ was arbitrary, this shows that $\neg\mathsf{CH}$ is consistent with ZFC.

In the next chapter we show how to construct countable models for arbitrary finite fragments of ZFC and in Chapter 16 we finally show how to get proper independence proofs. However, in later chapters we shall skip this quite tedious construction and just work with the — in fact equivalent — approach presented here.

Notes

The creation of forcing. The notion of forcing and of generic sets were introduced by Paul Cohen [1] in 1963 to prove that $\neg\mathsf{AC}$ is consistent with ZF and that $\neg\mathsf{CH}$ is consistent with ZFC, and since Gödel's constructible universe $\mathbf{L}$ is a model of $\mathsf{ZF} + \mathsf{AC} + \mathsf{CH}$, this implies that AC and CH are even independent of ZF and ZFC respectively. Cohen's original approach and notation were modified for example by Scott, who defined essentially the forcing relationship given in Definition 14.8 and introduced the corresponding forcing symbol "$\Vdash$" (this definition of forcing and the corresponding symbol were first published in Feferman [6, p. 328 f.]). Notice the similarity between "$\Vdash$" and "$\vdash$", and compare the Forcing Theorem 14.10 with Gödel's Completeness Theorem 3.4. For a description of how Cohen had come to forcing we refer the reader to Cohen [5], and a history of the origins and the early development of forcing can be found in Moore [9] and Kanamori [7] (but see also Cohen [1, 2, 3, 4]).

The approach taken here. The way we introduced forcing was motivated by Kunen [8, Chapter VII, §§2–5], from where for example Definition 14.8 as well as the proof of the Forcing Theorem 14.10 were taken, and where one can also find a complete proof of the Generic Model Theorem 14.12 (*cf.* [8, Chapter VII, Theorem 4.2]). However, Kunen considers generic extensions of countable transitive models of *finite fragments* of ZFC (whereas we considered generic extensions of models of *full* ZFC). This way he gets model-theoretic theorems whereas we just get results in the metatheory.

References

1. Paul J. Cohen, *The independence of the continuum hypothesis I.*, ***Proceedings of the National Academy of Sciences (U.S.A.)***, vol. 50 (1963), 1143–1148.
2. ______, *The independence of the continuum hypothesis II.*, ***Proceedings of the National Academy of Sciences (U.S.A.)***, vol. 51 (1964), 105–110.
3. ______, *Independence results in set theory*, in ***The Theory of Models,*** *Proceedings of the 1963 International Symposium at Berkeley* (J.W. Addison, L. Henkin, and A. Tarski, eds.), [Studies in Logic and the Foundation of Mathematics], North-Holland, Amsterdam, 1965, pp. 39–54.

4. ______, ***Set Theory and the Continuum Hypothesis***, Benjamin, New York, 1966.
5. ______, *The discovery of forcing*, Proceedings of the Second Honolulu Conference on Abelian Groups and Modules (Honolulu, HI, 2001), vol. 32, 2002, pp. 1071–1100.
6. Solomon Feferman, *Some applications of the notions of forcing and generic sets*, ***Fundamenta Mathematicae***, vol. 56 (1964/1965), 325–345.
7. Akihiro Kanamori, *Cohen and set theory*, ***The Bulletin of Symbolic Logic***, vol. 14 (2008), 351–378.
8. Kenneth Kunen, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.
9. Gregory H. Moore, *The origins of forcing*, in ***Logic Colloquium '86,*** *Proceedings of the Colloquium held in Hull, U.K., July 13–19, 1986* (F.R. Drake and J.K. Truss, eds.), [Studies in Logic and the Foundation of Mathematics 124], North-Holland, Amsterdam, 1988, pp. 143–173.

15

Models of finite fragments of Set Theory

In this chapter we summarise the model-theoretic facts which will be used in the next chapter in which the independence of the Continuum Hypothesis will be proved. Most of the following statements are classical results and are stated without proper proofs (for which we refer the reader to standard textbooks in axiomatic Set Theory like Jech [4] or Kunen [5]).

Basic Model-Theoretical Facts

Let $\mathscr{L}$ be an arbitrary but fixed language. Two $\mathscr{L}$-structures $\mathbf{M}$ and $\mathbf{N}$ with domain A and B respectively are called **isomorphic** if there is a bijection $f: A \to B$ between A and B such that:

- $f(c^{\mathbf{M}}) = c^{\mathbf{N}}$ (for each constant symbol $c \in \mathscr{L}$)
- $R^{\mathbf{M}}(a_1, \dots, a_n) \iff R^{\mathbf{N}}(f(a_1), \dots, f(a_n))$ (for each n-ary relation symbol $R \in \mathscr{L}$)
- $f(F^{\mathbf{M}}(a_1, \dots, a_n)) = F^{\mathbf{N}}(f(a_1), \dots, f(a_n))$ (for each n-ary function symbol $F \in \mathscr{L}$)

If the $\mathscr{L}$-structures $\mathbf{M}$ and $\mathbf{N}$ are isomorphic and $f: A \to B$ is the corresponding bijection, then for all $a_1, \dots, a_n \in A$ and each formula $\varphi(x_1, \dots, x_n)$ we have:

$$\mathbf{M} \vDash \varphi(a_1, \dots, a_n) \iff \mathbf{N} \vDash \varphi(f(a_1), \dots, f(a_n))$$

This shows that isomorphic $\mathscr{L}$-structures are essentially the same, except that their elements have different "names", and therefore, isomorphic structures are usually identified. For example the *dihedral group* of order six and S_3 (*i.e.*, the *symmetric group* of order six) are isomorphic; whereas C_6 (*i.e.*, the *cyclic group* of order six) is not isomorphic to S_3 (*e.g.*, consider $\varphi(x_1, x_2) \equiv x_1 \circ x_2 = x_2 \circ x_1$).

If $\mathbf{M}$ and $\mathbf{N}$ are $\mathscr{L}$-structures and $B \subseteq A$, then $\mathbf{N}$ is said to be an **elementary substructure** of $\mathbf{M}$, denoted $\mathbf{N} \prec \mathbf{M}$, if for every formula $\varphi(x_1, \dots, x_n)$ and every $b_1, \dots, b_n \in B$:

$$\mathbf{N} \vDash \varphi(b_1, \dots, b_n) \iff \mathbf{M} \vDash \varphi(b_1, \dots, b_n)$$

For example the linearly ordered set $(\mathbb{Q}, <)$ is an elementary substructure of $(\mathbb{R}, <)$. On the other hand, $(\mathbb{Z}, <)$ is not an elementary substructure of $(\mathbb{Q}, <)$, *e.g.*, $\forall x \forall y \big(x < y \rightarrow \exists z(x < z < y)\big)$ is false in $(\mathbb{Z}, <)$ but true in $(\mathbb{Q}, <)$.

The key point in construction of elementary substructures of a given structure $\mathbf{M}$ with domain A is the following fact: A structure $\mathbf{N}$ with domain $B \subseteq A$ is an elementary substructure of $\mathbf{M}$ if and only if for every formula $\varphi(u, x_1, \dots, x_n)$ and all $b_1, \dots, b_n \in B$:

$$\exists a \in A: \ \mathbf{M} \vDash \varphi(a, b_1, \dots, b_n) \iff \exists b \in B: \ \mathbf{M} \vDash \varphi(b, b_1, \dots, b_n)$$

Notice that the implication from the right to the left is obviously true (since $B \subseteq A$). Equivalently we get that $\mathbf{N} \prec \mathbf{M}$ if for every formula $\varphi(u, x_1, \dots, x_n)$ and all $b_1, \dots, b_n \in B$:

$$\forall a \in A: \ \mathbf{M} \vDash \varphi(a, b_1, \dots, b_n) \iff \forall b \in B: \ \mathbf{M} \vDash \varphi(b, b_1, \dots, b_n)$$

Notice that in this case, the implication from the left to the right is obviously true.

The following theorem is somewhat similar to COROLLARY 15.5 below, even though it goes beyond ZFC (see RELATED RESULT 86). However, it is not used later, but it is a nice consequence of the characterisation of elementary submodels given above.

THEOREM 15.1 (LÖWENHEIM-SKOLEM THEOREM). *Every infinite model for a countable language has a countable elementary submodel. In particular, every model of* ZFC *has a countable elementary submodel.*

The Reflection Principle

Instead of aiming for a *set model* of all of ZFC, we can restrict our attention to **finite fragments** of ZFC (*i.e.*, to finite sets of axioms of ZFC), denoted by ZFC*.

We will see that for every finite fragment ZFC* of ZFC, there is a *set* which is a model of ZFC*, but before we can state this result we have to give some further notions from model theory.

Let $\mathbf{V} \vDash$ ZFC, let $M \in \mathbf{V}$ be any set, and let $\mathbf{M} = (M, \in)$ be an $\in$-structure with domain M. An $\in$-structure $\mathbf{M} = (M, \in)$, where $M \in \mathbf{V}$ is a set, is called a **set model**. Notice that this definition of *model* is slightly different to the one given in Chapter 3, where we defined models with respect to a set of formulae. For any formula φ we define $\varphi^{\mathbf{M}}$, the **relativisation** of φ to $\mathbf{M}$, by induction on the complexity of the formula φ:

- $(x = y)^{\mathbf{M}}$ is $x = y$.
- $(x \in y)^{\mathbf{M}}$ is $x \in y$.
- $(\psi_1 \wedge \psi_2)^{\mathbf{M}}$ is $\psi_1^{\mathbf{M}} \wedge \psi_2^{\mathbf{M}}$.
- $(\neg\psi)^{\mathbf{M}}$ is $\neg(\psi^{\mathbf{M}})$.
- $(\exists x\, \psi)^{\mathbf{M}}$ is $\exists x\, (x \in M \wedge \psi^{\mathbf{M}})$.

In other words, $\varphi^{\mathbf{M}}$ is the formula obtained from φ by replacing the quantifiers "$\exists x$" by "$\exists x \in M$". If $\varphi(x_1, \ldots, x_n)$ is a formula and $x_1, \ldots, x_n \in M$, then $\varphi^{\mathbf{M}}(x_1, \ldots, x_n)$ is the same as $\varphi(x_1, \ldots, x_n)$ except that the bound variables of φ range over M. (For $x_1, \ldots, x_n$ not all in M, the interpretation of $\varphi^{\mathbf{M}}(x_1, \ldots, x_n)$ is irrelevant.) Notice that in the definition of $\varphi^{\mathbf{M}}$, the interpretation of the non-logical symbol "$\in$" remains unchanged. Further, notice that also the sets themselves remain unchanged (which will not be the case for example when we apply MOSTOWSKI'S COLLAPSING THEOREM 15.4).

For a formula φ and a set model $\mathbf{M}$, $\mathbf{M} \vDash \varphi$ means $\varphi^{\mathbf{M}}$ (where the free variables take arbitrary values in M). Similarly, for a set of formulae Φ, $\mathbf{M} \vDash \Phi$ means $\mathbf{M} \vDash \varphi$ for each formula $\varphi \in \Phi$. If $\mathbf{M} = (M, \in)$ and for all formulae $\varphi \in \Phi$ we have

$$\mathbf{M} \vDash \varphi \iff \mathbf{V} \vDash \varphi\,,$$

then we say that M **reflects** Φ.

The following theorem shows that if ZFC is consistent, then any finite fragment of ZFC has a set model.

THEOREM 15.2 (REFLECTION PRINCIPLE). *Assume that* ZFC *has a model, say* $\mathbf{V}$, *let* $M_0 \in \mathbf{V}$ *be an arbitrary set, and let* $\mathsf{ZFC}^* \subseteq \mathsf{ZFC}$ *be an arbitrarily large finite fragment of* ZFC. *Then we have:*

(a) There is a set $M \supseteq M_0$ *in* $\mathbf{V}$ *such that* M *reflects* ZFC^*. *In other words, there is a set* $M \supseteq M_0$ *such that for* $\mathbf{M} = (M, \in)$ *we have*

$$\mathbf{M} \vDash \mathsf{ZFC}^*\,.$$

(b) There is even a transitive set $M \supseteq M_0$ *that reflects* ZFC^* *(recall that a set* x *is transitive if* $z \in y \in x$ *implies* $z \in x$*).*

(c) Moreover, there is a limit ordinal λ *such that* $\mathrm{V}_\lambda \supseteq M_0$ *and the set* V_λ *reflects* ZFC^*.

(d) There is an $M \supseteq M_0$ *such that* M *reflects* ZFC^* *and* $|M| \leq \max\{|M_0|, \omega\}$. *In particular, for* $M_0 = \{\emptyset\}$, *there is a countable set* M *that reflects* ZFC^*.

The crucial point in the proof of the REFLECTION PRINCIPLE 15.2 is to show that for any existential formula $\exists x \varphi(x, y)$ and any set M_0 there exists a set

$M \supseteq M_0$ with the property that whenever $\mathbf{V}$ contains a so-called *witness* for $\exists x \varphi(x,y)$, *i.e.*, a set $a \in \mathbf{V}$ such that for all $b \in \mathbf{M}$, $\mathbf{V} \vDash \varphi(a,b)$, then there is already a witness for $\exists x \varphi(x,y)$ in M:

LEMMA 15.3. *Let $\mathbf{V}$ be a model of* ZFC *and let $\varphi(x, y_1, \dots, y_n)$ be a formula with $\{x, y_1, \dots, y_n\} \subseteq \mathrm{free}(\varphi)$. For each non-empty set M_0 there is a set $M \supseteq M_0$ (where $M \in \mathbf{V}$) such that for all $c_1, \dots c_n \in M$ we have:*

$$\mathbf{V} \vDash \exists x\, \varphi(x, c_1, \dots, c_n) \to \exists a \in M\, \varphi(a, c_1, \dots, c_n)$$

Moreover, we can construct $M' \supseteq M_0$ such that $|M'| \leq \max\{|M_0|, \omega\}$, in particular, if M_0 is countable, then M' is countable as well.

Proof. Let $\mathbf{V} \vDash$ ZFC and let M_0 be any non-empty set, *e.g.*, $M_0 = \{\emptyset\}$. Firstly, define in $\mathbf{V}$ the class function $H : \mathbf{V}^n \to \mathbf{V}$ as follows:
If $\mathbf{V} \vDash \exists x\, \varphi(x, u_1, \dots, u_n)$ for some $u_1, \dots, u_n \in \mathbf{V}$, then let

$$H(u_1, \dots, u_n) = \bigcap \big\{ \mathrm{V}_\alpha : \alpha \in \Omega \wedge \exists x \in \mathrm{V}_\alpha\, \varphi(x, u_1, \dots, u_n) \big\},$$

otherwise, $H(u_1, \dots, u_n) := \{\emptyset\}$.
Now, we construct the set $M \supseteq M_0$ by induction: For $i \in \omega$ let

$$M_{i+1} = M_i \cup \bigcup \big\{ H(c_1, \dots, c_n) : c_1, \dots, c_n \in M_i \big\}$$

and let

$$M = \bigcup_{i \in \omega} M_i\,.$$

If $c_1, \dots, c_n \in M$, then there is an $i \in \omega$ such that $c_1, \dots, c_n \in M_i$, and consequently, if $\mathbf{V} \vDash \exists x\, \varphi(x, c_1, \dots, c_n)$, then there is an $a \in M$ such that $\mathbf{V} \vDash \varphi(a, c_1, \dots, c_n)$.

By AC, fix a well-ordering $<$ of M, and define the partial function $h(c_1, \dots, c_n) : M^n \to M$ as follows: If $H(c_1, \dots, c_n) = \{\emptyset\}$, then let $h(c_1, \dots, c_n) := \emptyset$; otherwise, let $a \in M$ be the $<$-minimal element of $H(c_1, \dots, c_n) \subseteq M$ and let $h(c_1, \dots, c_n) := a$. We construct the set $M' \supseteq M_0$ again by induction: For $i \in \omega$ let

$$M'_{i+1} = M'_i \cup \big\{ h(c_1, \dots, c_n) : c_1, \dots, c_n \in M'_i \big\}$$

and let

$$M' = \bigcup_{i \in \omega} M'_i\,.$$

For all $i \in \omega$ we have $|M'_{i+1}| \leq |\mathrm{seq}(M'_i)| = \max\{|M'_i|, \omega\}$, and therefore, $|M'| \leq \max\{|M_0|, \omega\}$. ⊣

Proof of Theorem 15.2 (Sketch). Let ZFC^* be an arbitrary finite fragment of ZFC. Let $\varphi_1, \dots, \varphi_l$ be the finite list of all subformulae of formulae contained in ZFC^*. We may assume that the formulae $\varphi_1, \dots, \varphi_l$ are written in the set-theoretic language $\{\in\}$ and that no universal quantifier occurs in these formulae (*i.e.*, replace "$\forall x$" by "$\neg\exists x \neg$").

Applying the proof of LEMMA 15.3 to all these formulae simultaneously, yields a set M such that for each i with $1 \leq i \leq l$ we have:

$$\mathbf{V} \vDash \exists x \, \varphi_i \to \exists x \in M \, \varphi_i$$

A formula $\varphi(x_1, \dots, x_n)$ is said to be **absolute** for $\mathbf{M} = (M, \in)$ and $\mathbf{V}$, if for all $a_1, \dots, a_n \in M$ we have $\mathbf{V} \vDash \varphi(a_1, \dots, a_n) \iff \mathbf{M} \vDash \varphi(a_1, \dots, a_n)^{\mathbf{M}}$. The proof is now by induction on the complexity of the formulae $\varphi_1, \dots, \varphi_l$: Let i, j, k be such that $1 \leq i, j, k \leq l$. If φ_i is atomic, *i.e.*, φ_i is equivalent to $x = y$ or $x \in y$, then φ_i is obviously absolute for $\mathbf{M}$ and $\mathbf{V}$. If φ_i is of the form $\neg\varphi_j$, $\varphi_j \vee \varphi_k$, $\varphi_j \wedge \varphi_i$, or $\varphi_j \to \varphi_k$, where φ_j and φ_i are absolute for $\mathbf{M}$ and $\mathbf{V}$, then φ_i is absolute for $\mathbf{M}$ and $\mathbf{V}$ too. Finally, if $\varphi_i \equiv \exists x \, \varphi_j$, then by construction of M, φ_i is absolute for $\mathbf{M}$ and $\mathbf{V}$.

Hence, $M \supseteq M_0$, and the model $\mathbf{M} = (M, \in)$ has the desired properties. ⊣

The REFLECTION PRINCIPLE 15.2 can be considered as a kind of ZFC-version of the LÖWENHEIM-SKOLEM THEOREM 15.1, and even though it is weaker than that theorem, it has many interesting consequences and important applications, especially in consistency proofs.

Some remarks:

(1) If we compare (b) with (d) we see that we may require that the set M is transitive or that $|M| \leq \max\{|M_0|, \omega\}$, but in general *not* both.

For example let ZFC^* be rich enough to define ω_1 as the smallest uncountable ordinal and assume that $\mathbf{M} = (M, \in)$ reflects ZFC^*. If M is countable, then M cannot be transitive; and if M is transitive, then M must be uncountable.

(2) As a consequence of the REFLECTION PRINCIPLE 15.2 and of GÖDEL'S SECOND INCOMPLETENESS THEOREM 3.9, it follows that ZFC is not finitely axiomatisable (*i.e.*, there is no way to replace the two axiom schemata by just finitely many single axioms).

On the other hand, by the REFLECTION PRINCIPLE 15.2 we get that for each finite fragment ZFC^* of ZFC, there is a proof in ZFC that ZFC^* has a set model, whereas by GÖDEL'S SECOND INCOMPLETENESS THEOREM 3.9 the existence of a model of ZFC is not provable within ZFC.

(3) Let ZFC^* be a finite fragment of ZFC and assume that $\mathsf{ZFC}^* \vdash \varphi$ (for some sentence φ). Further, assume that M reflects ZFC^* and let $\mathbf{M} = (M, \in)$. Then, in the model-theoretic sense, $\mathbf{M} \vDash \mathsf{ZFC}^*$, and consequently, $\mathbf{M} \vDash \varphi$.

As we will see later, this is the first step in order to show that a given sentence φ is consistent with ZFC: By the COMPACTNESS THEOREM 3.7 it is enough to show that whenever $\Phi \subseteq$ ZFC is a finite fragment of ZFC, then $\Phi+\varphi$ has a model. Let Φ be an arbitrary but fixed finite set of axioms of ZFC. Now, let $\mathbf{M} \in \mathbf{V}$ be a set model of Ψ, where Ψ is a certain finite fragment of ZFC which makes sure that the model $\mathbf{M}$ can be extended to a set model $\mathbf{M}[X]$ such that $\mathbf{M}[X] \vDash \Phi+\varphi$. Thus, since Φ was arbitrary, this shows that φ is consistent with ZFC. (This method is used and explained again in Chapter 16.)

Countable Transitive Models of Finite Fragments of ZFC

As mentioned above, a set model $\mathbf{M} = (M, \in)$ of a finite fragment of ZFC can be taken to be countable or transitive, but in general not both. However, as a consequence of MOSTOWSKI'S COLLAPSING THEOREM 15.4 we can get also a transitive set model which is isomorphic to M. This is done by reinterpreting the elements of M and as a result we get a model which is countable and transitive, but which is not a submodel of $\mathbf{M}$. Before we can state MOSTOWSKI'S COLLAPSING THEOREM 15.4, we have to introduce some notions.

Let M be an arbitrary set. For a binary relation $E \subseteq M \times M$ on M and each $x \in M$ let

$$\mathrm{ext}_E(x) = \{z \in M : z\,E\,x\}$$

be the **extension** of x.

A binary relation E on M is said to be **well-founded** if every non-empty subset of M has an E-minimal element (*i.e.*, for each non-empty $A \subseteq M$ there is an $x_0 \in A$ such that $\mathrm{ext}_E(x_0) \cap A = \emptyset$).

A well-founded binary relation E on M is **extensional** if for all $x, y \in M$ we have

$$\mathrm{ext}_E(x) = \mathrm{ext}_E(y) \to x = y\,.$$

In other words, E is extensional *iff* (M, E) satisfies the Axiom of Extensionality (with respect to the binary relation E).

The following result shows that for every structure (M, E) which satisfies the Axiom of Extensionality, there exists a transitive set N such that (M, E) and $(N, \in)$ are isomorphic.

THEOREM 15.4 (MOSTOWSKI'S COLLAPSING THEOREM). *If E is a well-founded and extensional binary relation on a set M, then there exists a unique transitive set N and an isomorphism π between (M, E) and $(N, \in)$, i.e., $\pi : M \to N$ is a bijection and for all $x, y \in M$, $y\,E\,x \leftrightarrow \pi(y) \in \pi(x)$.*

Proof (Sketch). Let $x_0 \in M$ be an E-minimal element of M. Since E is extensional, x_0 is unique. Define $\pi(x_0) := \emptyset$ and let $A_0 = \{x_0\}$. If, for some $\alpha \in \Omega$, A_α is already defined and $M \setminus A_\alpha \neq \emptyset$, then let X_α be the set of all E-minimal elements of $M \setminus A_\alpha$, let $A_{\alpha+1} := A_\alpha \cup X_\alpha$, and for each $x \in X_\alpha$

define $\pi(x) := \{\pi(y) : y \, E \, x\}$. Now, $M = \bigcup_{\alpha\in\lambda} A_\alpha$ (for some $\lambda \in \Omega$) and we define $N := \pi[M]$. We leave it as an exercise to the reader to show that π and $(N, \in)$ have the required properties and that $(N, \in)$ is unique. $\dashv$

It is worth mentioning that not just the set N, but also the isomorphism π is unique. We also would like to mention that MOSTOWSKI'S COLLAPSING THEOREM 15.4 is a ZFC result and that π is just a mapping between two sets.

As an immediate consequence of MOSTOWSKI'S COLLAPSING THEOREM 15.4 we get

COROLLARY 15.5. *Let* $\mathbf{V}$ *be a model of* ZFC *and let* $\mathbf{M} = (M, \in)$ *be a countable set model in* $\mathbf{V}$. *If* ZFC^* *is a finite fragment of* ZFC *containing the* Axiom of Extensionality *and* $\mathbf{M} \vDash \mathsf{ZFC}^*$, *then there is a countable transitive set* N *in* $\mathbf{V}$ *such that* $\mathbf{N} = (N, \in)$ *is a set model in* $\mathbf{V}$ *which is isomorphic to* $\mathbf{M}$ *(in particular,* $\mathbf{N} \vDash \mathsf{ZFC}^*$*).*

Proof. Let $\mathbf{M} = (M, \in)$ be a countable set model of ZFC^*. Because M is a set, the relation "$\in$" is obviously a well-founded and extensional binary relation on M. Thus, by MOSTOWSKI'S COLLAPSING THEOREM 15.4, there is a transitive set N such that $\mathbf{M} = (M, \in)$ and $\mathbf{N} = (N, \in)$ are isomorphic, and since $\pi : M \to N$ is a bijection, N is countable. $\dashv$

Let ZFC^* be any finite fragment of ZFC and let $\mathbf{V}$ be a model of ZFC. Then, by the REFLECTION PRINCIPLE 15.2.(d), there is a countable set M in $\mathbf{V}$ that reflects ZFC^* and for $\mathbf{M} = (M, \in)$ we have $\mathbf{M} \vDash \mathsf{ZFC}^*$. Thus, by COROLLARY 15.5, there is a countable transitive set N that reflects ZFC^*. In other words, for any finite fragment $\mathsf{ZFC}^* \subsetneq \mathsf{ZFC}$ there is a **countable transitive model** $\mathbf{N}$ in $\mathbf{V}$ such that $\mathbf{N} \vDash \mathsf{ZFC}^*$.

Let us briefly discuss the preceding constructions: We start with a model $\mathbf{V}$ of ZFC and an arbitrary large but finite set of axioms $\mathsf{ZFC}^* \subsetneq \mathsf{ZFC}$. By the REFLECTION PRINCIPLE 15.2.(d) there is a countable set M in $\mathbf{V}$ such that $\mathbf{M} = (M, \in)$ is a model of ZFC^*. By applying MOSTOWSKI'S COLLAPSING THEOREM 15.4 to $(M, \in)$ we obtain a countable transitive model $\mathbf{N} = (N, \in)$ in $\mathbf{V}$ such that the models $\mathbf{N} = (N, \in)$ and $\mathbf{M}$ are isomorphic, and consequently, $\mathbf{N}$ is a model of ZFC^*.

It is worth mentioning that the model $\mathbf{M} = (M, \in)$ is a genuine submodel of $\mathbf{V}$ and therefore contains the real sets of $\mathbf{V}$. For example if

$$\mathbf{M} \vDash \text{"}\lambda \text{ is the least uncountable ordinal"}$$

then $\lambda = \omega_1$, *i.e.*, $\omega_1 \in M$. However, since the set M is countable in $\mathbf{V}$, there are countable ordinals in $\mathbf{V}$ which do not belong to the set M, and therefore not to the model $\mathbf{M}$ (which implies that M is not transitive). In other words,

$$\mathbf{V} \vDash \lambda = \omega_1 \wedge \omega_1 \in M \wedge |\lambda \cap M| = \omega\,.$$

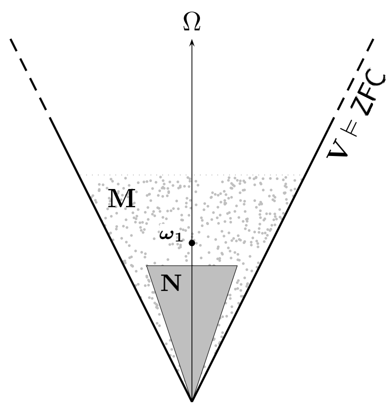
On the one hand, the model $\mathbf{N} = (N, \in)$ is in general not a submodel of $\mathbf{V}$ and just contains a kind of copies of countably many set of $\mathbf{V}$. For example if

$$\mathbf{N} \vDash \text{“}\lambda \text{ is the least uncountable ordinal”}$$

then λ, which corresponds to ω_1 in $\mathbf{N}$, is just a countable ordinal in $\mathbf{V}$. However, since N is transitive, every ordinal in $\mathbf{V}$ which belongs to λ also belongs to the set N, and therefore to the model $\mathbf{N}$. In other words,

$$\mathbf{V} \vDash \lambda \in \omega_1 \wedge \lambda \in N \wedge \lambda \cap N = \lambda\,.$$

The relationships between the three models $\mathbf{V}$, $\mathbf{M}$, and $\mathbf{N}$, are illustrated by the following figure:



As we shall see in the next chapter, countable transitive models of finite fragments of ZFC play a key role in consistency and independence proofs.

Notes

For concepts of model theory and model-theoretical terminology we refer the reader to Hodges [3] or to Chang and Keisler [1]. However, the preceding results (including proofs) can also be found in Jech [4, Chapter 12].

The Löwenheim-Skolem Theorem 15.1 was already discussed in the notes of Chapter 3; the Reflection Principle 15.2 was introduced by Montague [7] (see also Lévy [6]); and the transitive collapse was defined by Mostowski [8].

Related Results

82. *A model of* ZF − Inf *and the consistency of* PA. $V_\omega \vDash \mathsf{ZF} - \mathsf{Inf}$, where Inf denotes the Axiom of Infinity, and moreover, we even have $\mathrm{Con}(\mathsf{PA}) \iff \mathrm{Con}(\mathsf{ZF} - \mathsf{Inf})$ (see Jech [4, Exercise 12.9] and Kunen [5, Chapter IV, Exercise 30]).

83. *Models of* Z. Let Z be ZF without the Axiom Schema of Replacement. For every limit ordinal $\lambda > \omega$ we have $V_\lambda \vDash \mathsf{Z}$ (see Jech [4, Exercise 12.7] or Kunen [5, Chapter IV, Exercise 6]).

For every infinite regular cardinal κ let $\mathrm{H}_\kappa := \{x : |\mathrm{TC}(x)| < \kappa\}$. The elements of H_κ are said to be **hereditarily** of cardinality $< \kappa$. In particular, H_ω — which coincides with V_ω — is the set of hereditarily finite sets and H_{ω_1} is the set of hereditarily countable sets.

84. *Models of* $\mathsf{ZFC} - \mathsf{P}$. If AC holds in $\mathbf{V}$, then for all cardinals $\kappa > \omega$ we have $\mathrm{H}_\kappa \vDash \mathsf{Z} - \mathsf{P}$, where P denotes the Axiom of Power Set. Moreover, for regular cardinals $\kappa > \omega$ we even have $\mathrm{H}_\kappa \vDash \mathsf{ZFC} - \mathsf{P}$ (see Kunen [5, Chapter IV, Exercise 7] and Kunen [5, Chapter IV, Theorem 6.5]).

An uncountable regular cardinal κ is said to be **inaccessible** if for all $\lambda < \kappa$, $2^\lambda < \kappa$. The inaccessible cardinals owe their name to the fact that they cannot be obtained (or accessed) from smaller cardinals by the usual set-theoretical operations. To some extent, an inaccessible cardinal is to smaller cardinals what ω is to finite cardinals and what is reflected by the fact that $\mathrm{H}_\omega \vDash \mathsf{ZFC} - \mathsf{Inf}$ (*cf.* Jech [4, Exercise 12.9]). Notice that by CANTOR'S THEOREM 3.25, every inaccessible cardinal is a regular *limit* cardinal. One cannot prove in ZFC that inaccessible cardinals exist; moreover, one cannot even prove that uncountable regular limit cardinals exist (see Kunen [5, Chapter VI, Corollary 4.13] but also Hausdorff's remark [2, p. 131]).

85. *Models of* ZFC. If κ is inaccessible, then $\mathrm{H}_\kappa \vDash \mathsf{ZFC}$ (*cf.* Kunen [5, Chapter IV, Theorem 6.6]). Let us show that if ZFC is consistent, then $\mathsf{ZFC} \nvdash \mathsf{Inacc}$, where Inacc denotes the axiom "$\exists\kappa\,(\kappa$ *is inaccessible*$)$". Since $\mathrm{H}_\kappa \vDash \mathsf{ZFC}$ (if κ is inaccessible), it is provable from $\mathsf{ZFC} + \mathsf{Inacc}$ that ZFC has a model which is equivalent to saying that ZFC is consistent. Now, if $\mathsf{ZFC} \vdash \mathsf{Inacc}$, then we consequently get that ZFC proves its own consistency, which is impossible by GÖDEL'S SECOND INCOMPLETENESS THEOREM 3.9 (unless ZFC is inconsistent).

86. *The Löwenheim-Skolem Theorem.* Even though the LÖWENHEIM-SKOLEM THEOREM 15.1 for ZFC — which says that every model of ZFC has a countable elementary submodel — is somewhat similar to COROLLARY 15.5, it can neither be formulated in First-Order Logic nor can it be proved in ZFC: Firstly, notice that ZFC consists of infinitely many axioms. Thus, we cannot write these axioms as a single formula as we have done above in order to prove the REFLECTION PRINCIPLE 15.2. Furthermore, even in the case when we would work in higher order Logic, if every model $\mathbf{V}$ of ZFC would have a countable elementary submodel $\mathbf{V}'$, then the set of ordinals in $\mathbf{V}'$ (*i.e.*, $\Omega^{\mathbf{V}} \cap \mathbf{V}'$) would be countable in $\mathbf{V}$ (but not in $\mathbf{V}'$, of course). Now, in $\mathbf{V}$ we can build the sequence $\alpha_0 := \bigcup \Omega^{\mathbf{V}} \cap \mathbf{V}'$, $\alpha_1 := \bigcup \Omega^{\mathbf{V}'} \cap \mathbf{V}''$, and so on. This would result in an infinite, strictly decreasing sequence $\alpha_0 \ni \alpha_1 \ni \ldots$ of ordinals in $\mathbf{V}$, which is a contradiction to the Axiom of Foundation.

REFERENCES

1. CHEN CHUNG CHANG AND H. JEROME KEISLER, ***Model Theory***, 2nd ed., [Studies in Logic and the Foundations of Mathematics 73], North-Holland, Amsterdam, 1977.
2. FELIX HAUSDORFF, ***Grundzüge der Mengenlehre***, de Gruyter, Leipzig, 1914 [reprint: Chelsea, New York, 1965].

3. Wilfried Hodges, ***Model Theory***, Cambridge University Press, Cambridge, 1993.
4. Thomas Jech, ***Set Theory****, The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
5. Kenneth Kunen, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.
6. Azriel Lévy, *Axiom schemata of strong infinity in axiomatic set theory*, ***Pacific Journal of Mathematics***, vol. 10 (1960), 223–238.
7. Richard Montague, *Fraenkel's addition to the axioms of Zermelo*, in ***Essays on the Foundations of Mathematics***, Magnes Press, Hebrew University, Jerusalem, 1961, pp. 91–114.
8. Andrzej Mostowski, *An undecidable arithmetical statement*, ***Fundamenta Mathematicae***, vol. 36 (1949), 143–164.

16

Proving Unprovability

Consistency and Independence Proofs: The Proper Way

We have seen in Chapter 14 how we could extend models of ZFC to models in which for example CH fails — supposed we have suitable generic filters at hand. On the other hand, we have also seen in Chapter 14 that there is no way to prove that generic filters exist.

However, in order to show that for example CH is independent of ZFC we have to show that ZFC + CH as well as ZFC + ¬CH has a model. In other words we are not interested in the generic filters themselves, but rather in the sentences which are true in the corresponding generic models; on the other hand, if there are no generic filters, then there are also no generic models.

The trick to avoid generic filters (over models of ZFC) is to carry out the whole forcing construction within a given model $\mathbf{V}$ of ZFC — or alternatively in ZFC: In $\mathbf{V}$ we first construct a countable model $\mathbf{N}$ of a suitable finite fragment of ZFC. Then we define a kind of "mini-forcing" $\mathbb{P}$ which belongs to the model $\mathbf{N}$ and show that there is a set G in $\mathbf{V}$ which is $\mathbb{P}$-generic over $\mathbf{N}$. From the point of view of $\mathbf{N}$, $\mathbf{N}[G]$ is a proper generic extension of $\mathbf{N}$, and since G is a set in $\mathbf{V}$, also $\mathbf{N}[G]$ belongs to $\mathbf{V}$. This shows that certain generic extensions exist, in particular generic extensions of countable models of finite fragments of ZFC.

What we gain with this approach is that the whole construction takes place in the model $\mathbf{V}$, but the price we pay is that neither $\mathbf{N}$ nor $\mathbf{N}[G]$ is a model of ZFC; but now it is time to describe the proper way for obtaining consistency and independence results in greater detail:

0. *The goal*: Suppose we would like to show that a given sentence φ is consistent with ZFC, *i.e.*, we have to show that Con(ZFC) implies Con(ZFC + φ). By GÖDEL'S COMPLETENESS THEOREM 3.4 this is equivalent to showing that ZFC + φ has a model whenever there is a model $\mathbf{V}$ of ZFC.

1. *Getting started*: By the Compactness Theorem 3.7, $\mathsf{ZFC}+\varphi$ is consistent if and only if for every finite set of axioms Φ of ZFC, $\Phi + \varphi$ is consistent, *i.e.*, $\Phi + \varphi$ has a model. Below, we show how to construct a model of $\Phi_0 + \varphi$, where Φ_0 is an arbitrary but fixed finite set of axioms of ZFC.

2. *A suitable forcing notion* $\mathbb{P}$: In the model $\mathbf{V}$ define a forcing notion $\mathbb{P} = (P, \leq)$ which has the property that there is a condition $p_0 \in P$ such that $p_0 \Vdash_{\mathbb{P}} \varphi$. For example if φ is $\neg\mathsf{CH}$, then by the methods presented in Chapter 14, $\mathbb{C}_{\omega_2}$ would have the required properties.

3. *Choosing a suitable finite set of axioms*: Let $\mathsf{ZFC}^* \subsetneq \mathsf{ZFC}$ be a finite fragment of ZFC such that:
   (a) Each axiom of Φ_0 belongs to ZFC^*.
   (b) ZFC^* is strong enough to define the forcing notion $\mathbb{P}$, the existence of the condition p_0, as well as some properties of $\mathbb{P}$ like satisfying *ccc*, being σ-closed, *et cetera*.
   (c) ZFC^* is strong enough to prove that every sentence in Φ_0 is forced to be true in any $\mathbb{P}$-generic extension of $\mathbf{V}$.
   (d) ZFC^* is strong enough to prove that various concepts like "finite", "partial ordering and dense sets", *et cetera*, are absolute for all countable transitive models.

   The properties (b)–(d) of ZFC^* are necessary to prove Theorem 16.1; however, we will omit most of the quite tedious and technical proof of that theorem.

4. *The corresponding countable transitive model* $\mathbf{N}$: Let $M_0 = \{p_0, P, R_{\leq}\}$, where $R_{\leq} = \big\{\langle p, q\rangle \in P \times P : p \leq q\big\}$. By the Reflection Principle 15.2 there is a countable set $M \supseteq M_0$ in $\mathbf{V}$ such that M reflects ZFC^*, *i.e.*, for $\mathbf{M} = (M, \in)$ we have $\mathbf{M} \vDash \mathsf{ZFC}^*$. By Corollary 15.5 and Mostowski's Collapsing Theorem 15.4, there is a countable transitive model $\mathbf{N} = (N, \in)$ in $\mathbf{V}$ such that $\mathbf{N} \vDash \mathsf{ZFC}^*$, and in addition there is a bijection $\pi : M \to N$ such that for all $x, y \in M$, $y \in x \leftrightarrow \pi(y) \in \pi(x)$. Define $P^{\mathbf{N}} := \pi[P]$ and $\leq^{\mathbf{N}} := \pi[R_{\leq}]$. Notice that for all $p, q \in P^{\mathbf{N}}$, $\mathbf{N} \vDash p \leq^{\mathbf{N}} q$ *iff* $\pi^{-1}(p) \leq \pi^{-1}(q)$.

5. *Relativisation of* $\mathbb{P}$*-generic filters to* $\mathbf{N}$: For a set $G \subseteq P^{\mathbf{N}}$ let
   $$\mathbf{N}[G] = \{\underset{\sim}{x}[G] : \underset{\sim}{x} \text{ is a } \mathbb{P}\text{-name in } \mathbf{N}\}.$$
   A set $G \subseteq P^{\mathbf{N}}$ is $\mathbb{P}^{\mathbf{N}}$-generic over $\mathbf{N}$ if it meets every open dense subset $D \subseteq P^{\mathbf{N}}$ which is in $\mathbf{N}$.

6. *Relativisation of the Generic Model Theorem*: There is even a relativisation of the Generic Model Theorem 14.12 which states as follows.

   Theorem 16.1. *Let $\mathbf{V}$ be a model of ZFC, let $\mathbb{P} = (P, \leq)$ be a forcing notion in $\mathbf{V}$ and let p_0 be an arbitrary condition in P. Furthermore, let Φ_0 and ZFC^* be as above and let $\mathbf{N} = (N, \in)$ be a countable transitive* *model in* $\mathbf{V}$ *such that* $\mathbf{N} \vDash \mathsf{ZFC}^*$. *Then there is a set* $G \subseteq P^{\mathbf{N}}$ *in* $\mathbf{V}$ *which contains* p_0 *and which is* $\mathbb{P}^{\mathbf{N}}$*-generic over* $\mathbf{N}$. *Moreover,* $\mathbf{N}[G] = (N[G], \in)$ *is a countable transitive model in* $\mathbf{V}$ *and* $\mathbf{N}[G] \vDash \Phi_0$.

Proof (Sketch). Firstly, let us show that there exists a set $G \subseteq P^{\mathbf{N}}$ in $\mathbf{V}$ which is $\mathbb{P}^{\mathbf{N}}$-generic over $\mathbf{N}$ and contains p_0: Because the model $\mathbf{N}$ is countable in $\mathbf{V}$, from the point of view of $\mathbf{V}$, the model $\mathbf{N}$ contains just countably many sets which are open dense subsets of $P^{\mathbf{N}}$. Let $\{D_n : n \in \omega\}$ be this countable set. Since D_0 is dense, we can take a condition $q_0 \in D_0$ such that $q_0 \geq p_0$; and in general, for $n \in \omega$ take $q_{n+1} \in D_{n+1}$ such that $q_{n+1} \geq q_n$. Finally let

$$G = \left\{p \in P^{\mathbf{N}} : \exists n \in \omega(p \leq q_n)\right\}.$$

Then $G \subseteq P^{\mathbf{N}}$ is a set in $\mathbf{V}$ which contains p_0 and meets every open dense subset of $P^{\mathbf{N}}$ which belongs to $\mathbf{N}$, and hence, G is $\mathbb{P}^{\mathbf{N}}$-generic over $\mathbf{N}$. Notice that even though each q_n belongs to the model $\mathbf{N}$, the sequence $\{q_n : n \in \omega\}$ — and consequently the set G — does not belong to $\mathbf{N}$. Notice also that since $\mathbf{N}$ is countable in $\mathbf{V}$, there are only countably many names in $\mathbf{N}$ and consequently $N[G]$ is countable in $\mathbf{V}$.
Secondly, let us show that $\mathbf{N}[G] \vDash \Phi_0$: By the choice of ZFC^* (in step 3) we can show in $\mathbf{N}$, by using the technique introduced in Chapter 14, that whenever G is $\mathbb{P}^{\mathbf{N}}$-generic over $\mathbf{N}$ and contains p_0, then $\mathbf{N}[G] \vDash \Phi_0$. ⊣

7. *The final step*: In step 2 we assumed that $\mathbf{V}[G] \vDash \varphi$ whenever G is $\mathbb{P}$-generic over $\mathbf{V}$ and contains p_0. Thus, by THEOREM 16.1, we get that

$$\mathbf{N}[G] \vDash \varphi$$

whenever G is $\mathbb{P}^{\mathbf{N}}$-generic over $\mathbf{N}$ and $p_0 \in G$. On the other hand, by the choice of the set of axioms ZFC^* and since $\mathbf{N} \vDash \mathsf{ZFC}^*$ we get $\mathbf{N}[G] \vDash \Phi_0$, hence,

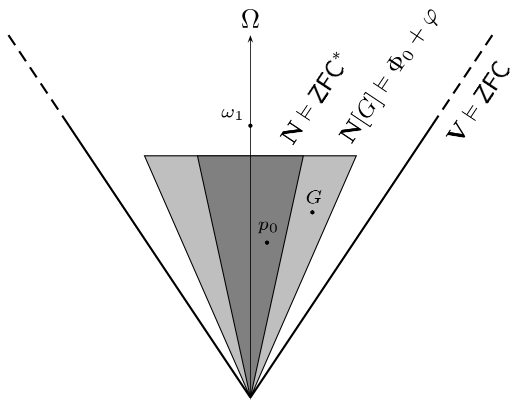
$$\mathbf{N}[G] \vDash \Phi_0 + \varphi$$

which shows that $\Phi_0 + \varphi$ is consistent.

8. *Conclusion*: Since the finite set of axioms Φ_0 we have chosen in step 1 was arbitrary, $\Phi + \varphi$ is consistent for *every* finite set of axioms Φ of ZFC, and consequently we get that φ is consistent with ZFC. This is what we were aiming for and what is summarised by the following result.

PROPOSITION 16.2. *Let* φ *be an arbitrary sentence in the language of Set Theory. If there is a forcing notion* $\mathbb{P} = (P, \leq)$ *and a condition* $p \in P$ *such that* $p \Vdash_{\mathbb{P}} \varphi$, *then* φ *is consistent with* ZFC.

The model-theoretic part of the above construction is illustrated by the following figure:



The most inelegant part in the proof of the consistency of φ is surely step 3, where we have to find a finite set of axioms $\mathsf{ZFC}^* \subsetneq \mathsf{ZFC}$ which is strong enough to prove that whenever $\mathbf{N} \vDash \mathsf{ZFC}^*$ and G is $\mathbb{P}$-generic over $\mathbf{N}$, then $\mathbf{N}[G] \vDash \Phi_0$. On the other hand, for a consistency proof it is not necessary to display explicitly the axioms in ZFC^*; it is sufficient to know that such a finite set of axioms exists.

The crucial point in the proof of the consistency of φ is step 2, where we have to find (or define) a forcing notion $\mathbb{P}$ such that there is a $\mathbb{P}$-condition p_0 which forces φ. In fact it will turn out that p_0 is always equal to $\mathbf{0}$, in which case we say that $\mathbb{P}$ *forces* φ, *i.e.*, φ is true in *all* $\mathbb{P}$-generic extensions of $\mathbf{V}$. For example $\mathbb{K}_0$ and $\mathbb{C}_{\omega_2}$ (both defined in Chapter 14) force CH and $\neg\mathsf{CH}$ respectively.

Now, let us turn our attention to independence results: Firstly recall that a sentence φ is independent of ZFC if φ as well as $\neg\varphi$ is consistent with ZFC. So, in order to show that a sentence φ is independent of ZFC we would have to go twice through the procedure described above. However, since the only crucial point in the proof is step 2, all what we have to do is to find two suitable forcing notions:

> In order to show that a given set-theoretic sentence φ is independent of ZFC, we have to show that there are two forcing notions such that one forces φ and the other one forces $\neg\varphi$.

As a first example let us consider the case when φ is CH.

THEOREM 16.3. CH *is independent of* ZFC.

Proof. On the one hand, by THEOREM 14.21 we get that whenever G is $\mathbb{C}_\kappa$-generic over $\mathbf{V}$ and $\kappa > \omega_1$, then $\mathbf{V}[G] \vDash \neg\mathsf{CH}$, and therefore we get that

Con(ZFC) $\Rightarrow$ Con(ZFC + $\neg$CH). On the other hand, by THEOREM 14.23 we get that whenever G is $\mathbb{K}_0$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \vDash \mathsf{CH}$, which shows that Con(ZFC) $\Rightarrow$ Con(ZFC + CH). $\dashv$

The Cardinality of the Continuum

Until now we just have seen that for each infinite cardinal κ there is a model in which $\mathfrak{c} \geq \kappa$, but we did not give any estimate how large $\mathfrak{c}$ actually is in such a model. Of course, since $\mathfrak{c}^\omega = \mathfrak{c}$, $\mathfrak{c} = \kappa$ implies that κ must also satisfy $\kappa^\omega = \kappa$. Surprisingly, this is the only demand for κ to make it possible to force that $\mathfrak{c} = \kappa$.

THEOREM 16.4. *For every cardinal κ which satisfies $\kappa^\omega = \kappa$ we have:*

$$\mathrm{Con}(\mathsf{ZFC}) \Rightarrow \mathrm{Con}(\mathsf{ZFC} + \mathfrak{c} = \kappa)$$

Proof. Let $\mathbf{V} \vDash \mathsf{ZFC}$ and let κ be a cardinal in $\mathbf{V}$ which satisfies $\kappa^\omega = \kappa$. Consider the forcing notion $\mathbb{C}_\kappa = \big(\mathrm{Fn}(\kappa \times \omega, 2), \subseteq\big)$. For convenience, we write C_κ instead of $\mathrm{Fn}(\kappa \times \omega, 2)$. If G is $\mathbb{C}_\kappa$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \vDash \mathfrak{c} \geq \kappa$ (*cf.* THEOREM 14.21). Thus, it remains to show that $\mathbf{V}[G] \vDash \mathfrak{c} \leq \kappa$.

Firstly we investigate $\mathbb{C}_\kappa$-names for subsets of ω: Let $\underset{\sim}{x}$ be an arbitrary $\mathbb{C}_\kappa$-name for a subset of ω. For each $n \in \omega$ let

$$\Delta_{\underset{\cdot}{n} \in \underset{\sim}{x}} = \big\{p \in C_\kappa : (p \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{n} \in \underset{\sim}{x}) \vee (p \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{n} \notin \underset{\sim}{x})\big\}\,.$$

By FACT 14.9.(b), for each $n \in \omega$ the set $\Delta_{\underset{\cdot}{n} \in \underset{\sim}{x}}$ is open dense in C_κ. For each $n \in \omega$ choose a maximal anti-chain A_n in $\Delta_{\underset{\cdot}{n} \in \underset{\sim}{x}}$ and define

$$\underset{\cdot}{x} = \big\{\langle \underset{\cdot}{n}, p\rangle : p \in A_n \wedge p \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{n} \in \underset{\sim}{x}\big\}\,.$$

A name for a subset of ω of the form like $\underset{\cdot}{x}$ is called a **nice name** (*i.e.*, nice names are a special kind of names for subsets of ω). Now we show that $\mathbf{0} \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{x} = \underset{\sim}{x}$ by showing that for each $n \in \omega$ the set

$$D_n = \big\{q \in C_\kappa : q \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{n} \in \underset{\cdot}{x} \leftrightarrow \underset{\cdot}{n} \in \underset{\sim}{x}\big\}$$

is dense in C_κ. Fix $n \in \omega$ and let p be an arbitrary $\mathbb{C}_\kappa$-condition. Since $\Delta_{\underset{\cdot}{n} \in \underset{\sim}{x}}$ is dense in C_κ there is a $p_0 \supseteq p$ such that $p_0 \in \Delta_{\underset{\cdot}{n} \in \underset{\sim}{x}}$, and since A_n is a maximal anti-chain in $\Delta_{\underset{\cdot}{n} \in \underset{\sim}{x}}$, there is a $q_0 \in A_n$ such that p_0 and q_0 are compatible. Thus, there is a $q \in C_\kappa$ such that $p_0 \subseteq q \supseteq q_0$. By construction we get

$$q \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{n} \in \underset{\cdot}{x} \leftrightarrow \underset{\cdot}{n} \in \underset{\sim}{x}\,,$$

and since $p \subseteq q$ and p was arbitrary this shows that D_n is dense in C_κ. In particular we get that for every $\mathbb{C}_\kappa$-name $\underset{\sim}{x}$ for a subset of ω there exists a nice name $\underset{\cdot}{x}$ such that $\mathbf{0} \Vdash_{\mathbb{C}_\kappa} \underset{\cdot}{x} = \underset{\sim}{x}$.

Secondly we compute the cardinality of the set of nice names: Since κ is infinite, $\left|[\kappa \times \omega \times 2]^{<\omega}\right| = \kappa$ (*cf.* COROLLARY 5.8), and consequently $|C_\kappa| = \kappa$ (we leave the details as an exercise to the reader). Recall that $\mathbb{C}_\kappa$ satisfies *ccc*, *i.e.*, every anti-chain in C_κ is at most countable. Now, every nice name is the countable union of at most countable sets of ordered pairs, where each ordered pair is of the form $\langle \underset{\sim}{n}, p\rangle$ for some $n \in \omega$ and $p \in C_\kappa$. Thus, there are at most

$$\left((\omega \cdot \kappa)^\omega\right)^\omega = \kappa^{\omega \cdot \omega} = \kappa^\omega = \kappa$$

nice names for subsets of ω. Now, because each set $x \subseteq \omega$ which is in $\mathbf{V}[G]$ has a $\mathbb{C}_\kappa$-name in $\mathbf{V}$, and because every $\mathbb{C}_\kappa$-name for a subset of ω corresponds to a nice name, there are at most κ subsets of ω in $\mathbf{V}[G]$. Hence, $\mathbf{V}[G] \vDash \mathfrak{c} \leq \kappa$ and we finally get $\mathbf{V}[G] \vDash \mathfrak{c} = \kappa$. ⊣

NOTES

Approaches to forcing. There are different ways of presenting the forcing technique, and even though they all yield precisely the same consistency proofs, they can be quite different in their metamathematical conception. The approach to forcing presented in this chapter is essentially taken from Kunen [4, Chapter VII]. Another approach — taken for example by Jech in [3, Chapter 14] and in [2, Part I, Section 1] — uses Boolean-valued models. For a discussion of different approaches, as well as for some historical background, we refer the reader to Kunen [4, Chapter VII, §9].

RELATED RESULTS

87. *The κ-chain condition.* Let κ be a regular cardinal. We say that a forcing notion $\mathbb{P} = (P, \leq)$ satisfies the **κ-chain condition**, denoted κ-*cc*, if every anti-chain in P has cardinality $<\kappa$ (*i.e.*, strictly less than κ). In particular, ω_1-*cc* is equivalent to *ccc*.
   One can show that if a forcing notion $\mathbb{P}$ satisfies the κ-*cc*, then forcing with $\mathbb{P}$ preserves all cardinals $\geq\kappa$ (see for example Kunen [4, Chapter VII, Lemma 6.9] or Jech [2, Part I, Section 2]).

88. *On the consistency of $2^{\omega_\alpha} > \omega_{\alpha+1}$.* With essentially the same construction as in the proof of THEOREM 16.4, but replacing the *ccc* forcing notion by a similar one satisfying the $\omega_{\alpha+1}$-chain condition, one can show that $2^{\omega_\alpha} = \kappa$ is consistent with ZFC whenever $\operatorname{cf}(\kappa) > \omega_\alpha$. Notice that by COROLLARY 5.12, the condition $\operatorname{cf}(\kappa) > \omega_\alpha$ is necessary. A more general result is obtained using *Easton forcing* (see Easton [1] or Chapter 18 | RELATED RESULT 100).

REFERENCES

1. WILLIAM B. EASTON, *Powers of regular cardinals*, ***Annals of Pure and Applied Logic***, vol. 1 (1970), 139–178.

2. Thomas Jech, ***Multiple Forcing***, [Cambridge Tracts in Mathematics], Cambridge University Press, Cambridge, 1986.
3. ———, ***Set Theory***, *The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
4. Kenneth Kunen, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.

17

Models in which AC fails

In Chapter 7 we have constructed models of Set Theory in which the Axiom of Choice failed. However, these models were models of Set Theory with *atoms*, denoted ZFA, where atoms are objects which do not have any elements but are distinct from the empty set. In this chapter we shall demonstrate how one can construct models of Zermelo-Fraenkel Set Theory (*i.e.*, models of ZF) in which AC fails. Moreover, we shall also see how we can embed arbitrary large fragments of permutation models (*i.e.*, models of ZFA) into models of ZF.

Symmetric Submodels of Generic Extensions

Let $\mathbf{V}$ be a model of ZFC and let $\mathbb{P} = (P, \leq)$ be a forcing notion which is defined in $\mathbf{V}$ with smallest element $\mathbf{0}$. A mapping $\alpha : P \to P$ is called an **automorphism** of $\mathbb{P}$ if α is a one-to-one mapping from P onto P such that for all $p, q \in P$:

$$\alpha p \leq \alpha q \iff p \leq q\,.$$

In particular we get $\alpha\mathbf{0} = \mathbf{0}$. If α is an automorphism of $\mathbb{P}$, then we define, by induction on $\operatorname{rk}(\underset{\sim}{x})$, an automorphism of the class of $\mathbb{P}$-names $\mathbf{V}^{\mathbb{P}}$ by stipulating

$$\alpha\underset{\sim}{x} = \big\{\langle \alpha\underset{\sim}{y}, \alpha p\rangle : \langle \underset{\sim}{y}, p\rangle \in \underset{\sim}{x}\big\}\,.$$

Notice that in particular we have $\alpha\emptyset = \emptyset$. Moreover, if $\underset{\cdot}{x} = \big\{\langle \underset{\cdot}{y}, \mathbf{0}\rangle : y \in x\big\}$ is the canonical $\mathbb{P}$-name for a set $x \in \mathbf{V}$ and α is an arbitrary automorphism of $\mathbb{P}$, then $\alpha\underset{\cdot}{x} = \underset{\cdot}{x}$. Furthermore, with respect to the forcing relationship "$\Vdash_{\mathbb{P}}$" we have

$$p \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{x}_1, \dots, \underset{\sim}{x}_n) \iff \alpha p \Vdash_{\mathbb{P}} \varphi(\alpha\underset{\sim}{x}_1, \dots, \alpha\underset{\sim}{x}_n)$$

where $\varphi(x_1, \dots, x_n)$ is a first-order formula with all free variables shown and $\underset{\sim}{x}_1, \dots, \underset{\sim}{x}_n \in \mathbf{V}^{\mathbb{P}}$ are arbitrary $\mathbb{P}$-names.

Let now $\mathscr{G}$ be an arbitrary but fixed group of automorphisms of $\mathbb{P}$. In other words, let $\mathscr{G}$ be an arbitrary subgroup of the automorphism group of $\mathbb{P}$.

For each $\mathbb{P}$-name $\underset{\sim}{x}$ we define the symmetry group $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x}) \subseteq \mathscr{G}$ of $\underset{\sim}{x}$ by stipulating

$$\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x}) = \{\alpha \in \mathscr{G} : \alpha\underset{\sim}{x} = \underset{\sim}{x}\}\,.$$

In particular, if $\overset{\cdot}{x}$ is the canonical $\mathbb{P}$-name for a set $x \in \mathbf{V}$, then $\operatorname{sym}_{\mathscr{G}}(\overset{\cdot}{x}) = \mathscr{G}$. Further, if $\beta \in \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x})$ and α is an arbitrary automorphisms of $\mathbb{P}$, then $(\alpha\beta\alpha^{-1})(\alpha\underset{\sim}{x}) = \alpha\underset{\sim}{x}$, and therefore

$$\operatorname{sym}_{\mathscr{G}}(\alpha\underset{\sim}{x}) = \alpha\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x})\,\alpha^{-1}\,,$$

which shows that $\beta \in \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x})$ *iff* $\alpha\beta\alpha^{-1} \in \operatorname{sym}_{\mathscr{G}}(\alpha\underset{\sim}{x})$.

A set $\mathscr{F}$ of subgroups of $\mathscr{G}$ is a **normal filter** on $\mathscr{G}$ if for all subgroups H, K of $\mathscr{G}$ we have:

- $\mathscr{G} \in \mathscr{F}$
- if $H \in \mathscr{F}$ and $H \subseteq K$, then $K \in \mathscr{F}$
- if $H \in \mathscr{F}$ and $K \in \mathscr{F}$, then $H \cap K \in \mathscr{F}$
- if $\alpha \in \mathscr{G}$ and $H \in \mathscr{F}$, then $\alpha H\alpha^{-1} \in \mathscr{F}$

Let $\mathscr{F}$ be an arbitrary but fixed normal filter on $\mathscr{G}$. Then $\underset{\sim}{x} \in \mathbf{V}^{\mathbb{P}}$ is said to be **symmetric** if $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x}) \in \mathscr{F}$. In particular, canonical $\mathbb{P}$-names $\overset{\cdot}{x}$ for sets $x \in \mathbf{V}$ are symmetric (since $\operatorname{sym}_{\mathscr{G}}(\overset{\cdot}{x}) = \mathscr{G}$ and $\mathscr{G} \in \mathscr{F}$), and if $\underset{\sim}{x}$ is symmetric and $\alpha \in \mathscr{G}$, then also $\alpha\underset{\sim}{x}$ is symmetric (since $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x}) \in \mathscr{F}$ *iff* $\operatorname{sym}_{\mathscr{G}}(\alpha\underset{\sim}{x}) \in \mathscr{F}$).

The class **HS** of **hereditarily symmetric** names is defined by induction on $\operatorname{rk}(\underset{\sim}{x})$:

$$\underset{\sim}{x} \in \mathbf{HS} \iff \underset{\sim}{x} \textit{ is symmetric} \text{ and } \{\underset{\sim}{y} : \exists p \in P(\langle \underset{\sim}{y}, p\rangle \in \underset{\sim}{x})\} \subseteq \mathbf{HS}.$$

Since for all $x \in \mathbf{V}$ and each automorphism α of $\mathbb{P}$ we have $\alpha\overset{\cdot}{x} = \overset{\cdot}{x}$, all *canonical* names for sets in $\mathbf{V}$ are in $\mathbf{HS}$. Furthermore, if a $\mathbb{P}$-name $\underset{\sim}{x}$ is hereditarily symmetric and $\alpha \in \mathscr{G}$, then also $\alpha\underset{\sim}{x}$ is hereditarily symmetric. Thus, for all $\alpha \in \mathscr{G}$ we have $\alpha\underset{\sim}{x} \in \mathbf{HS}$ *iff* $\underset{\sim}{x} \in \mathbf{HS}$.

Now, for any $G \subseteq P$ which is $\mathbb{P}$-generic over $\mathbf{V}$ define

$$\hat{\mathbf{V}} = \{\underset{\sim}{x}[G] : \underset{\sim}{x} \in \mathbf{HS}\}\,.$$

In other words, $\hat{\mathbf{V}}$ is the subclass of $\mathbf{V}[G]$ which contains all elements of $\mathbf{V}[G]$ that have a hereditarily symmetric $\mathbb{P}$-name. Since $\mathbb{P}$-names for $\mathbb{P}$-generic filters are in general not symmetric, the set G, which belongs to $\mathbf{V}[G]$, is in general *not* a member of $\hat{\mathbf{V}}$. However, $\hat{\mathbf{V}}$ is a transitive model of ZF which is called **symmetric submodel** of $\mathbf{V}[G]$.

Proposition 17.1. *Every symmetric submodel $\hat{\mathbf{V}}$ of $\mathbf{V}[G]$ is a transitive model of ZF which contains $\mathbf{V}$, i.e., $\mathbf{V} \subseteq \hat{\mathbf{V}} \subseteq \mathbf{V}[G]$ and $\hat{\mathbf{V}} \vDash \mathsf{ZF}$.*

Proof (Sketch). Like for the GENERIC MODEL THEOREM 14.12, we shall prove just a few facts; the remaining parts of the proof are left as an exercise to the reader.

The heredity of the class $\mathbf{HS}$ implies that the class $\hat{\mathbf{V}}$ is transitive, and by the definition of $\hat{\mathbf{V}}$ we get $\hat{\mathbf{V}} \subseteq \mathbf{V}[G]$. Further, since $\underset{\sim}{x} \in \mathbf{HS}$ for every $x \in \mathbf{V}$, we get $\mathbf{V} \subseteq \hat{\mathbf{V}}$.

As a consequence of the transitivity of $\hat{\mathbf{V}}$ we get that $\hat{\mathbf{V}}$ satisfies the Axiom of Extensionality as well as the Axiom of Foundation.

To see that the Axiom of Empty Set and the Axiom of Infinity are valid in $\hat{\mathbf{V}}$, just notice that the canonical $\mathbb{P}$-names for $\emptyset$ and ω respectively are hereditarily symmetric.

For the Axiom of Pairing, let x_0 and x_1 be arbitrary sets in $\hat{\mathbf{V}}$ and let $\underset{\sim}{x}_0, \underset{\sim}{x}_1 \in \mathbf{HS}$ be $\mathbb{P}$-names for x_0 and x_1 respectively. Let $\underset{\sim}{y} := \big\{\langle \underset{\sim}{x}_0, \mathbf{0}\rangle, \langle \underset{\sim}{x}_1, \mathbf{0}\rangle\big\}$. Then $\underset{\sim}{y}[G] = \{x_0, x_1\}$, and since $\underset{\sim}{y} \in \mathbf{HS}$ we get $\{x_0, x_1\} \in \hat{\mathbf{V}}$.

For the Axiom Schema of Separation, let $\varphi(x, y_1, \ldots, y_n)$ be a first-order formula with $\operatorname{free}(\varphi) \subseteq \{x, y_1, \ldots, y_n\}$. Let $u, a_1, \ldots, a_n$ be sets in $\hat{\mathbf{V}}$ and let $\underset{\sim}{u}, \underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_n$ be the corresponding hereditarily symmetric $\mathbb{P}$-names for these sets. We have to find a hereditarily symmetric $\mathbb{P}$-name for the set

$$w = \big\{v \in u : \varphi(v, a_1, \ldots, a_n)\big\}\,.$$

For this, let $\bar{\underset{\sim}{u}} := \big\{\langle \underset{\sim}{v}, p\rangle : \exists q \in P\,\big(q \le p \wedge \langle \underset{\sim}{v}, q\rangle \in \underset{\sim}{u}\big)\big\}$ and let

$$\underset{\sim}{w} = \big\{\langle \underset{\sim}{v}, p\rangle \in \bar{\underset{\sim}{u}} : p \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{v}, \underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_n)\big\}\,.$$

Obviously we have $\underset{\sim}{w}[G] = w$ and it remains to show that $\underset{\sim}{w} \in \mathbf{HS}$. Since $\underset{\sim}{u} \in \mathbf{HS}$, also $\bar{\underset{\sim}{u}} \in \mathbf{HS}$, and it is enough to show that $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{w}) \in \mathscr{F}$. Let $I := \operatorname{sym}_{\mathscr{G}}(\bar{\underset{\sim}{u}}) \cap \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{a}_1) \cap \cdots \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{a}_n)$. Then I, as the intersection of finitely many groups in $\mathscr{F}$, belongs to $\mathscr{F}$. For any $\alpha \in I$ we have $\alpha\bar{\underset{\sim}{u}} = \bar{\underset{\sim}{u}}$ and for every $1 \le i \le n$ we have $\alpha\underset{\sim}{a}_i = \underset{\sim}{a}_i$ Further we have

$$\begin{aligned}
\alpha\underset{\sim}{w} &= \big\{\langle \alpha\underset{\sim}{v}, \alpha p\rangle : \langle \underset{\sim}{v}, p\rangle \in \underset{\sim}{w}\big\} \\
&= \big\{\langle \alpha\underset{\sim}{v}, \alpha p\rangle : \langle \underset{\sim}{v}, p\rangle \in \bar{\underset{\sim}{u}} \wedge p \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{v}, \underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_n)\big\} \\
&= \big\{\langle \alpha\underset{\sim}{v}, \alpha p\rangle : \langle \alpha\underset{\sim}{v}, \alpha p\rangle \in \bar{\underset{\sim}{u}} \wedge \alpha p \Vdash_{\mathbb{P}} \varphi(\alpha\underset{\sim}{v}, \alpha\underset{\sim}{a}_1, \ldots, \alpha\underset{\sim}{a}_n)\big\} \\
&= \big\{\langle \alpha\underset{\sim}{v}, \alpha p\rangle \in \bar{\underset{\sim}{u}} : \alpha p \Vdash_{\mathbb{P}} \varphi(\alpha\underset{\sim}{v}, \underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_n)\big\} \\
&= \big\{\langle \underset{\sim}{v}, p\rangle \in \bar{\underset{\sim}{u}} : p \Vdash_{\mathbb{P}} \varphi(\underset{\sim}{v}, \underset{\sim}{a}_1, \ldots, \underset{\sim}{a}_n)\big\} = \underset{\sim}{w}
\end{aligned}$$

Thus, $I \subseteq \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{w}) \in \mathscr{F}$ and we finally have $\underset{\sim}{w} \in \mathbf{HS}$. $\dashv$

As we shall see in the following examples, $\hat{\mathbf{V}}$ does in general not satisfy the Axiom of Choice. Thus, in general we have $\hat{\mathbf{V}} \nvDash \mathsf{ZFC}$, even though $\mathbf{V}$ as well as $\mathbf{V}[G]$ are models of ZFC.

Examples of Symmetric Models

A model in which the reals cannot be well-ordered

In this section we shall construct a symmetric model $\hat{\mathbf{V}}$ in which there exists an *infinite* set A of real numbers (*i.e.*, $A \subseteq [\omega]^\omega$) such that A is *Dedekind-finite* in $\hat{\mathbf{V}}$, *i.e.*, there is no injection in $\hat{\mathbf{V}}$ which maps ω into A.

Consider the forcing notion $\mathbb{C}_\omega = \big(\mathrm{Fn}(\omega \times \omega, 2), \subseteq\big)$ consisting of finite partial functions from $\omega \times \omega$ to $\{0, 1\}$. To keep the notation short let $C_\omega := \mathrm{Fn}(\omega \times \omega, 2)$. Recall that the smallest element of $\mathbb{C}_\omega$ is $\emptyset$ and for $p, q \in C_\omega$, p is stronger than q *iff* the function p extends q.

Before we construct the symmetric model $\hat{\mathbf{V}}$, let us define a $\mathbb{C}_\omega$-name $\underset{\sim}{A}$ for a set of reals. For each $n \in \omega$ define the $\mathbb{C}_\omega$-name $\underset{\sim}{a}_n$ by stipulating

$$\underset{\sim}{a}_n = \big\{\langle \underset{\cdot}{k}, p\rangle : k \in \omega \wedge p \in C_\omega \wedge p\big(\langle n, k\rangle\big) = 1\big\}$$

and let

$$\underset{\sim}{A} = \big\{\langle \underset{\sim}{a}_n, \emptyset\rangle : n \in \omega\big\}\,.$$

First we show that $\underset{\sim}{A}[G]$ is an infinite set in $\mathbf{V}[G]$ whenever G is $\mathbb{C}_\omega$-generic over some model $\mathbf{V}$ of ZFC. For this, let $G \subseteq C_\omega$ be an arbitrary $\mathbb{C}_\omega$-generic filter over $\mathbf{V}$. Then we obviously have $\underset{\sim}{A}[G] = \big\{\underset{\sim}{a}_n[G] : n \in \omega\big\}$. Since for any integers $n, l \in \omega$ the set

$$\big\{p \in C_\omega : \exists k \in \omega (k \geq l \wedge \langle \underset{\cdot}{k}, p\rangle \in \underset{\sim}{a}_n)\big\}$$

is open dense in C_ω we get $\mathbf{V}[G] \vDash \underset{\sim}{a}_n[G] \in [\omega]^\omega$. Furthermore, for any distinct integers $n, m \in \omega$, also

$$\big\{p \in C_\omega : \exists k \in \omega\big(\langle n, k\rangle \in \mathrm{dom}(p) \wedge \langle m, k\rangle \in \mathrm{dom}(p) \wedge p(\langle n, k\rangle) \neq p(\langle m, k\rangle)\big)\big\}$$

is open dense in C_ω and therefore

$$\mathbf{V}[G] \vDash \text{“}\underset{\sim}{A}[G] \textit{ is infinite”}. \qquad (\infty)$$

Now we construct a symmetric submodel $\hat{\mathbf{V}}$ of $\mathbf{V}[G]$ in which $\underset{\sim}{A}[G]$ is Dedekind-finite. If π is a permutation of ω (*i.e.*, π is a one-to-one mapping from ω onto ω), then π induces an automorphism α_π of $\mathbb{C}_\omega$ by stipulating

$$\alpha_\pi p = \big\{\big\langle\langle \pi n, k\rangle, i\big\rangle : \big\langle \langle n, k\rangle, i\big\rangle \in p\big\}\,,$$

i.e., $\alpha_\pi p\big(\langle \pi n, k\rangle\big) = p\big(\langle n, k\rangle\big)$.

Let $\mathscr{G}$ be the group of all automorphisms of $\mathbb{C}_\omega$ that are induced by permutations of ω, *i.e.*,

$$\mathscr{G} = \{\alpha_\pi : \pi \textit{ is a permutation of } \omega\}\,.$$

For every finite set $E \in \operatorname{fin}(\omega)$ let

$$\operatorname{fix}_{\mathscr{G}}(E) = \big\{ \alpha_\pi \in \mathscr{G} : \pi n = n \textit{ for each } n \in E \big\} .$$

Let $\mathscr{F}$ be the filter on $\mathscr{G}$ generated by the subgroups $\big\{ \operatorname{fix}_{\mathscr{G}}(E) : E \in \operatorname{fin}(\omega) \big\}$, *i.e.*, a subgroup $H \subseteq \mathscr{G}$ belongs to $\mathscr{F}$ *iff* there is an $E \in \operatorname{fin}(\omega)$ such that $\operatorname{fix}_{\mathscr{G}}(E) \subseteq H$. Then $\mathscr{F}$ is a normal filter (notice for example that $\alpha_\pi \operatorname{fix}_{\mathscr{G}}(E) \alpha_\pi^{-1} = \operatorname{fix}_{\mathscr{G}}(\pi E)$ or see Chapter 7).

Finally, let **HS** be the class of all hereditarily symmetric $\mathbb{C}_\omega$-names and let $\hat{\mathbf{V}}$ be the corresponding symmetric submodel of $\mathbf{V}[G]$.

In order to see that the set $\underset{\sim}{A}[G]$ belongs to $\hat{\mathbf{V}}$ we have to verify that $\underset{\sim}{A} \in$ **HS**. Firstly notice that each automorphism α_π corresponds to a permutation of the set $\{\underset{\sim}{a}_n : n \in \omega\}$. In fact, for each $n \in \omega$ we have

$$\begin{aligned} \alpha_\pi \underset{\sim}{a}_n &= \big\{ \langle \alpha_\pi \underset{\cdot}{k}, \alpha_\pi p \rangle : \langle \underset{\cdot}{k}, p \rangle \in \underset{\sim}{a}_n \big\} \\ &= \big\{ \langle \underset{\cdot}{k}, \alpha_\pi p \rangle : \alpha_\pi p\big(\langle \pi n, k \rangle\big) = 1 \big\} \\ &= \big\{ \langle \underset{\cdot}{k}, q \rangle : q\big(\langle \pi n, k \rangle\big) = 1 \big\} = \underset{\sim}{a}_{\pi n} . \end{aligned}$$

In particular, $\alpha_\pi \underset{\sim}{a}_n = \underset{\sim}{a}_n$ *iff* $\pi n = n$. Thus, for each $n \in \omega$, $\operatorname{fix}_{\mathscr{G}}\big(\{n\}\big) = \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{a}_n)$, and since $\big\{ \underset{\cdot}{k} : \exists p \in C_\omega\big(\langle \underset{\cdot}{k}, p \rangle \in \underset{\sim}{a}_n\big) \big\} \subseteq$ **HS**, each $\underset{\sim}{a}_n$ belongs to **HS**. Furthermore, for each $\alpha_\pi \in \mathscr{G}$ we have

$$\begin{aligned} \alpha_\pi \underset{\sim}{A} &= \big\{ \langle \alpha_\pi \underset{\sim}{a}_n, \alpha_\pi \emptyset \rangle : \langle \underset{\sim}{a}_n, \emptyset \rangle \in \underset{\sim}{A} \big\} \\ &= \big\{ \langle \underset{\sim}{a}_{\pi n}, \emptyset \rangle : \langle \underset{\sim}{a}_n, \emptyset \rangle \in \underset{\sim}{A} \big\} = \underset{\sim}{A} , \end{aligned}$$

which shows that $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{A}) = \mathscr{G}$. Thus, $\underset{\sim}{A} \in$ **HS** which implies that $\underset{\sim}{A}[G]$ belongs to $\hat{\mathbf{V}}$. In fact, by (∞), $\underset{\sim}{A}[G]$ is an infinite set of reals which belongs to the model $\hat{\mathbf{V}}$, *i.e.*,

$$\hat{\mathbf{V}} \vDash \text{“}\underset{\sim}{A}[G] \subseteq [\omega]^\omega \textit{ and } \underset{\sim}{A}[G] \textit{ is infinite”}.$$

On the other hand we shall see that

$$\hat{\mathbf{V}} \vDash \text{“}\underset{\sim}{A}[G] \textit{ is } \text{D-}\textit{finite”}.$$

Assume towards a contradiction that the function $f : \omega \hookrightarrow \underset{\sim}{A}[G]$ is an injection which belongs to the model $\hat{\mathbf{V}}$. Then there is a hereditarily symmetric $\mathbb{C}_\omega$-name $\underset{\sim}{f} \in$ **HS** for f and a condition $p \in C_\omega$ such that

$$p \Vdash_{\mathbb{C}_\omega} \underset{\sim}{f} : \underset{\cdot}{\omega} \hookrightarrow \underset{\sim}{A} .$$

Let the finite set $E_0 \in \operatorname{fin}(\omega)$ be such that $\operatorname{fix}_{\mathscr{G}}(E_0) \subseteq \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{f})$. Since $\underset{\sim}{f}$ is an injective function with $\operatorname{dom}(\underset{\sim}{f}) = \omega$, there is an $n_0 \in \omega \setminus E_0$, a $k \in \omega$, and a condition $p_0 \geq p$ such that

$$p_0 \Vdash_{\mathbb{C}_\omega} \underset{\sim}{f}(\underset{\cdot}{k}) = \underset{\sim}{a}_{n_0} .$$

Let now π be a permutation of ω such that $\alpha_\pi \in \mathrm{fix}_{\mathscr{G}}(E_0)$, $\pi n_0 \neq n_0$, but $\alpha_\pi p_0$ and p_0 are compatible (*i.e.*, there is an $r \in C_\omega$ such that $\alpha_\pi p_0 \leq r \geq p_0$). Then the corresponding automorphism $\alpha_\pi \in \mathscr{G}$ belongs to $\mathrm{sym}_{\mathscr{G}}(\underset{\sim}{f})$, in particular $\alpha_\pi \underset{\sim}{f} = \underset{\sim}{f}$. Recall that $\alpha_\pi \underset{\cdot}{k} = \underset{\cdot}{k}$ (for all $k \in \omega$). If $r \in C_\omega$ is such that $\alpha_\pi p_0 \leq r \geq p_0$, then we have

$$r \Vdash_{\mathbb{C}_\omega} \underset{\sim}{f}(\underset{\cdot}{k}) = \underset{\sim}{a}_{n_0}\,,$$

because $r \geq p_0$, as well as

$$r \Vdash_{\mathbb{C}_\omega} \underset{\sim}{f}(\underset{\cdot}{k}) = \underset{\sim}{a}_{\pi n_0}\,,$$

because $r \geq \alpha_\pi p_0$. Hence, $r \Vdash_{\mathbb{C}_\omega} \underset{\sim}{a}_{n_0} = \underset{\sim}{a}_{\pi n_0}$, but this contradicts the fact that $n_0 \neq \pi n_0 \to \underset{\sim}{a}_{n_0}[G] \neq \underset{\sim}{a}_{\pi n_0}[G]$. Obviously, this shows that there is no hereditarily symmetric name for an injection $f : \omega \hookrightarrow \underset{\sim}{A}[G]$, in other words, $\hat{\mathbf{V}} \vDash$ "$\underset{\sim}{A}[G]$ *is* D-*finite*".

Conclusion: Starting from a model $\mathbf{V}$ of ZFC we constructed a symmetric model $\hat{\mathbf{V}}$ of ZF in which there exists an infinite but D-finite set of reals. Thus, there is a model of ZF in which the reals cannot be well-ordered. In particular, the Well-Ordering Principle is not provable in ZF.

A model in which every ultrafilter over ω is principal

The following construction of a symmetric model $\hat{\mathbf{V}}$ in which every ultrafilter over ω is principal is essentially the same as in the example above, except that the set $\{\underset{\sim}{a}_n[G] : n \in \omega\}$ will not belong to the model $\hat{\mathbf{V}}$. Thus, let $\mathbf{V}$ be a model of ZFC and consider again the forcing notion $\mathbb{C}_\omega = (\mathrm{Fn}(\omega \times \omega, 2), \subseteq)$.
For each $n \in \omega$ let $\underset{\sim}{a}_n = \{\langle \underset{\cdot}{k}, p\rangle : k \in \omega \wedge p \in C_\omega \wedge p(\langle n, k\rangle) = 1\}$, and let $G \subseteq C_\omega$ be $\mathbb{C}_\omega$-generic over $\mathbf{V}$; then $\mathbf{V}[G] \vDash \underset{\sim}{a}_n[G] \in [\omega]^\omega$.
For every $X \subseteq \omega \times \omega$ we define an automorphism α_X of $\mathbb{C}_\omega$ by stipulating

$$\begin{aligned} \alpha_X\, p :\ & \mathrm{dom}(p) \longrightarrow \{0,1\} \\ & \langle n, m\rangle \longmapsto \begin{cases} p(\langle n,m\rangle) & \text{if } \langle n,m\rangle \notin X, \\ 1 - p(\langle n,m\rangle) & \text{if } \langle n,m\rangle \in X. \end{cases} \end{aligned}$$

Let $\mathscr{G}$ be the group of all automorphisms α_X, where $X \subseteq \omega \times \omega$, and let $\mathscr{F}$ be the normal filter on $\mathscr{G}$ generated by $\{\mathrm{fix}_{\mathscr{G}}(E \times \omega) : E \in \mathrm{fin}(\omega)\}$, where

$$\mathrm{fix}_{\mathscr{G}}(E \times \omega) = \{\alpha_X : X \cap (E \times \omega) = \emptyset\}\,.$$

Finally, let **HS** be the class of all hereditarily symmetric names and let $\hat{\mathbf{V}}$ be the corresponding symmetric model.
Below, we show that whenever $\mathscr{U} \in \hat{\mathbf{V}}$ is an ultrafilter over ω, then $\mathscr{U}$ is

principal, *i.e.*, $\mathscr{U}$ contains a finite set. Let $\underset{\sim}{\mathscr{U}} \in \mathbf{HS}$ be a name for $\mathscr{U}$ and let $p \in G$ be such that

$$p \Vdash_{\mathbb{C}_\omega} \text{“}\underset{\sim}{\mathscr{U}} \text{ is an ultrafilter over } \underset{\cdot}{\omega}\text{”}.$$

Let $E_0 \in \operatorname{fin}(\omega)$ be such that $\operatorname{fix}_{\mathscr{G}}(E_0 \times \omega) \subseteq \operatorname{sym}_{\mathscr{G}}\big(\underset{\sim}{\mathscr{U}}\big)$ and fix an natural number $l \notin E_0$. Then there is a $q \geq p$ such that $q \in \Delta_{\underset{\sim}{a}_l \in \underset{\sim}{\mathscr{U}}} \cap G$, *i.e.*, $q \in G$ and q decides whether or not $\underset{\sim}{a}_l \in \underset{\sim}{\mathscr{U}}$. Let us assume that $q \Vdash_{\mathbb{C}_\omega} \underset{\sim}{a}_l \notin \underset{\sim}{\mathscr{U}}$ (the case when $q \Vdash_{\mathbb{C}_\omega} \underset{\sim}{a}_l \in \underset{\sim}{\mathscr{U}}$ is similar). Let m_0 be such that for all integers $m \geq m_0$ we have $\langle l, m\rangle \notin \operatorname{dom}(q)$ and let

$$X_0 = \big\{\langle l, m\rangle : m \geq m_0\big\} \subseteq \omega \times \omega\,.$$

Let $\mathscr{U} := \underset{\sim}{\mathscr{U}}[G]$, $a_l := \underset{\sim}{a}_l[G]$, and for $\underset{\sim}{b}_l := \alpha_{X_0}\, \underset{\sim}{a}_l$ let $b_l := \underset{\sim}{b}_l[G]$. Then, for each $m \geq m_0$, $m \in a_l \leftrightarrow m \notin b_l$, which implies that $(\omega \setminus a_l) \cap (\omega \setminus b_l)$ is finite. Notice that since $q \Vdash_{\mathbb{C}_\omega} \underset{\sim}{a}_l \notin \underset{\sim}{\mathscr{U}}$, $\alpha_{X_0}\, q \Vdash_{\mathbb{C}_\omega} \alpha_{X_0}\, \underset{\sim}{a}_l \notin \alpha_{X_0}\, \underset{\sim}{\mathscr{U}}$. By definition of X_0 we further have $\alpha_{X_0} \in \operatorname{fix}_{\mathscr{G}}(E_0 \times \omega) \subseteq \operatorname{sym}_{\mathscr{G}}\big(\underset{\sim}{\mathscr{U}}\big)$ and therefore $\alpha_{X_0}\, \underset{\sim}{\mathscr{U}} = \underset{\sim}{\mathscr{U}}$, and since $\alpha_{X_0}\, q = q$ and $\alpha_{X_0}\, \underset{\sim}{a}_l = \underset{\sim}{b}_l$ we have $q \Vdash_{\mathbb{C}_\omega} \underset{\sim}{b}_l \notin \underset{\sim}{\mathscr{U}}$. Thus, since $q \in G$, we get that neither a_l nor b_l belongs to $\mathscr{U}$. Because $\mathscr{U}$ is an ultrafilter, $\omega \setminus a_l$ as well as $\omega \setminus b_l$ belongs to $\mathscr{U}$, and therefore $(\omega \setminus a_l) \cap (\omega \setminus b_l) \in \mathscr{U}$. Hence, $\mathscr{U}$ contains a finite set, or in other words, $\mathscr{U}$ is principal.

Conclusion: Starting from a model $\mathbf{V}$ of ZFC we constructed a symmetric model $\hat{\mathbf{V}}$ of ZF in which every ultrafilter over ω is principal. Thus, there is a model of ZF in which for example the Fréchet ideal cannot be extended to a prime ideal. In particular we get that the Prime Ideal Theorem is not provable in ZF.

A model with a paradoxical decomposition of the real line

Below, we shall construct a model of ZF in which the real line $\mathbb{R}$ can be partitioned into a family $\mathscr{R}$, such that $|\mathscr{R}| > |\mathbb{R}|$. (Recall that $\mathscr{R}$ is a partition of $\mathbb{R}$ if $\mathscr{R} \subseteq \mathscr{P}(\mathbb{R})$ such that $\bigcup \mathscr{R} = \mathbb{R}$ and for any distinct $x, y \in \mathscr{R}$, $x \cap y = \emptyset$.)

By COROLLARY 4.13 it is enough to construct a model in which the set of reals $\mathscr{P}(\omega)$ is a countable union of countable sets.

In order to construct a symmetric model in which $\mathscr{P}(\omega)$ is a countable union of countable sets we start with a model $\mathbf{V}$ of ZFC such that for each $n \in \omega$, $\mathbf{V} \vDash 2^{\omega_n} = \omega_{n+1}$. Such a model is for example Gödel's constructible universe $\mathbf{L}$. Alternatively, such a model is also obtained by an iterated application of THEOREM 14.23, or more precisely, by iterating the forcing notions of THEOREM 14.23 using the iteration technique given in Chapter 18 (see also RELATED RESULT 100 of that chapter).

Now, let

$$P = \big\{p \in \operatorname{Fn}(\omega \times \omega, \omega_\omega) : \forall \langle n, m\rangle \in \operatorname{dom}(p)\, \big(p(\langle n, m\rangle) \in \omega_n\big)\big\}\,.$$

Then $\mathbb{P} := (P, \subseteq)$ is a forcing notion.

Let $G \subseteq P$ be $\mathbb{P}$-generic over $\mathbf{V}$. We construct a symmetric submodel $\hat{\mathbf{V}}$ of $\mathbf{V}[G]$ such that in $\hat{\mathbf{V}}$, the set of reals is a countable union of countable sets. For this, let $\mathscr{G}$ be the group of all permutations π of $\omega \times \omega$ such that

$$\pi\langle n, i\rangle = \langle m, j\rangle \rightarrow n = m\,.$$

Now, for each $\pi \in \mathscr{G}$ and every $n \in \omega$ let π_n be the permutation of ω such that for every $i \in \omega$,

$$\pi\langle n, i\rangle = \langle n, \pi_n i\rangle\,.$$

Every $\pi \in \mathscr{G}$ induces an automorphism α_π of $\mathbb{P}$ by stipulating

$$\alpha_\pi p = \bigl\{\bigl\langle\langle n, \pi_n i\rangle, \alpha\bigr\rangle : \bigl\langle\langle n, i\rangle, \alpha\bigr\rangle \in p\bigr\}\,.$$

For every $n \in \omega$, let H_n be the group of all $\pi \in \mathscr{G}$ such that for all $k \in n$, the corresponding permutation π_k is the identity, and let $\mathscr{F}$ be the filter on $\mathscr{G}$ generated by the subgroups $\{H_n : n \in \omega\}$. We leave it as an exercise to the reader to verify that $\mathscr{F}$ is a normal filter. Finally, let $\hat{\mathbf{V}}$ be the symmetric submodel of $\mathbf{V}[G]$ which is determined by $\mathscr{F}$.

Now, we show that there are countably many countable sets of reals R_n in $\hat{\mathbf{V}}$ such that $\hat{\mathbf{V}} \vDash \mathscr{P}(\omega) = \bigcup_{n\in\omega} R_n$. Firstly we construct canonical names for reals in $\hat{\mathbf{V}}$: Let $\underset{\sim}{x} \in \mathbf{HS}$ be a name for a real (*i.e.*, for a subset of ω), or more precisely, let $\underset{\sim}{x} \subseteq \bigl\{\langle \underset{\sim}{k}, p\rangle : \underset{\sim}{k} \in \mathbf{HS} \wedge p \in P\bigr\}$ be such that for each $\langle \underset{\sim}{k}, p\rangle \in \underset{\sim}{x}$, $p \Vdash_{\mathbb{P}} \underset{\sim}{k} \in \omega$ (notice that we also have $p \Vdash_{\mathbb{P}} \underset{\sim}{k} \in \underset{\sim}{x}$). Since $\underset{\sim}{x} \in \mathbf{HS}$ there is an $n_0 \in \omega$ such that $H_{n_0} \subseteq \operatorname{sym}_{\mathscr{G}}(\underset{\sim}{x})$, which implies that for all $\alpha_\pi \in H_{n_0}$ we have

$$\underset{\sim}{x} = \bigl\{\langle \underset{\sim}{k}, p\rangle : \langle \underset{\sim}{k}, p\rangle \in \underset{\sim}{x}\bigr\} = \bigl\{\langle \alpha_\pi \underset{\sim}{k}, \alpha_\pi p\rangle : \langle \underset{\sim}{k}, p\rangle \in \underset{\sim}{x}\bigr\} = \alpha_\pi \underset{\sim}{x}\,.$$

With respect to $\underset{\sim}{x}$, the canonical name $\underset{\cdot}{x} \in \mathbf{HS}$ is defined as follows:

$$\underset{\cdot}{x} = \bigl\{\langle \underset{\cdot}{m}, q\rangle : \exists\langle \underset{\sim}{k}, p\rangle \in \underset{\sim}{x}\, \exists r \geq p\, \bigl(q = r|_{n_0\times\omega} \wedge r \Vdash_{\mathbb{P}} \underset{\cdot}{m} = \underset{\sim}{k}\bigr)\bigr\}$$

Claim. $\mathbf{V}[G] \vDash \underset{\cdot}{x}[G] = \underset{\sim}{x}[G]$.

Proof of Claim. First we show that $\underset{\cdot}{x}[G] \subseteq \underset{\sim}{x}[G]$: Let $\langle \underset{\cdot}{m}, q\rangle$ be an arbitrary but fixed element of $\underset{\cdot}{x}$ such that $q \in G$. In particular, $\underset{\cdot}{m}[G] \in \underset{\cdot}{x}[G]$. We show that $\underset{\cdot}{m}[G] \in \underset{\sim}{x}[G]$. By definition of $\underset{\cdot}{x}$, there is a $\langle \underset{\sim}{k}, p\rangle \in \underset{\sim}{x}$ and a condition $r_0 \geq p$ such that $q = r_0|_{n_0\times\omega}$ and $r_0 \Vdash_{\mathbb{P}} \underset{\cdot}{m} = \underset{\sim}{k} \wedge \underset{\sim}{k} \in \underset{\sim}{x}$. Now, for every condition $r' \geq q$ we can find an automorphism $\alpha_\pi \in H_{n_0}$ and a condition r such that $r' \leq r \geq \alpha_\pi r_0$, which implies that $r \Vdash_{\mathbb{P}} \underset{\cdot}{m} = \alpha_\pi \underset{\sim}{k} \wedge \alpha_\pi \underset{\sim}{k} \in \underset{\sim}{x}$ (recall that $\alpha_\pi \underset{\sim}{x} = \underset{\sim}{x}$ and that for all $\pi \in \mathscr{G}$, $\alpha_\pi \underset{\cdot}{m} = \underset{\cdot}{m}$). Since $\alpha_\pi \in H_{n_0}$ we get $\alpha_\pi r|_{n_0\times\omega} = r|_{n_0\times\omega} = q$ and therefore the set $\bigl\{r \geq q : r \Vdash_{\mathbb{P}} \underset{\cdot}{m} \in \underset{\sim}{x}\bigr\}$ is dense above q. Thus, $\underset{\cdot}{m}[G] \in \underset{\sim}{x}[G]$, and since $\langle \underset{\cdot}{m}, q\rangle \in \underset{\cdot}{x}$ was arbitrary (with the property that $q \in G$), we get $\mathbf{V}[G] \vDash \underset{\cdot}{x}[G] \subseteq \underset{\sim}{x}[G]$.

Now we show that $\underset{\sim}{x} \subseteq \underset{\cdot}{x}$: If $\mathbf{V}[G] \vDash m \in \underset{\sim}{x}[G]$, then there exist an $r \in G$ and a name $\langle \underset{\sim}{k}, p\rangle \in \underset{\sim}{x}$ such that $r \geq p$ and $r \Vdash_{\mathbb{P}} \underset{\cdot}{m} = \underset{\sim}{k} \in \underset{\sim}{x}$, which implies that $\langle \underset{\cdot}{m}, r|_{n_0\times\omega}\rangle \in \underset{\cdot}{x}$ and shows that $\mathbf{V}[G] \vDash \underset{\sim}{x}[G] \subseteq \underset{\cdot}{x}[G]$. $\dashv_{\text{Claim}}$

Thus, each real $x \in \hat{\mathbf{V}}$ (*i.e.*, each subset of ω in $\hat{\mathbf{V}}$) has a canonical name $\underset{\cdot}{x}$ which is a subset of $\big\{\langle \underset{\cdot}{m}, q\rangle : m \in \omega \wedge q \in P_{n_0}\big\}$, where $n_0 \in \omega$ and $P_{n_0} := \big\{p \in P : \forall \langle n, m\rangle \in \operatorname{dom}(p)\,\big(n \in n_0\big)\big\}$. If $\underset{\cdot}{x}$ is a canonical name for a real $x \in \hat{\mathbf{V}}$ with $Q_x \subseteq P_n$, where $Q_x = \big\{q \in P : \exists \underset{\cdot}{m}(\langle \underset{\cdot}{m}, q\rangle \in \underset{\cdot}{x})\big\}$, then $\operatorname{sym}_{\mathscr{G}}(\underset{\cdot}{x}) \supseteq H_n$ and since $\underset{\cdot}{m} \in \mathbf{HS}$ for any $m \in \omega$, $\underset{\cdot}{x} \in \mathbf{HS}$. Moreover, for every $\alpha \in \mathscr{G}$, if $\underset{\cdot}{x}$ is a canonical name for a real then also $\alpha\underset{\cdot}{x}$ is a canonical name for a real. To see this, let $\underset{\sim}{x} \in \mathbf{HS}$ be a name for some real $x \in \hat{\mathbf{V}}$, let $\underset{\cdot}{x}$ be the canonical name for x which corresponds to $\underset{\sim}{x}$, and let $\alpha \in \mathscr{G}$. Then $\alpha\underset{\sim}{x}$ is a hereditarily symmetric name for a real in $\hat{\mathbf{V}}$ with corresponding canonical name $\alpha\underset{\cdot}{x}$.

Now, for each $n \in \omega$ let

$$\underset{\sim}{R}_n = \big\{\langle \underset{\cdot}{x}, \emptyset\rangle : \underset{\cdot}{x} \textit{ is a canonical name for a real } x \textit{ with } Q_x \subseteq P_n\big\}\,.$$

Notice that $\underset{\sim}{R}_n$ is in $\mathbf{V}$ and that for each $n \in \omega$ and all $\alpha \in \mathscr{G}$ we have $\alpha\underset{\sim}{R}_n = \underset{\sim}{R}_n$, which shows that $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{R}_n) = \mathscr{G}$, and since $\operatorname{sym}_{\mathscr{G}}(\underset{\cdot}{x}) \supseteq H_n$ for all $\underset{\cdot}{x} \in \underset{\sim}{R}_n$, we even have $\underset{\sim}{R}_n \in \mathbf{HS}$, *i.e.*, $\underset{\sim}{R}_n[G] \in \hat{\mathbf{V}}$. Moreover, also the function which maps each $n \in \omega$ to $\underset{\sim}{R}_n[G]$ belongs to $\hat{\mathbf{V}}$ (notice that the name $\big\{\langle \operatorname{op}(\underset{\cdot}{n}, \underset{\sim}{R}_n), \emptyset\rangle : n \in \omega\big\}$ is hereditarily symmetric). Further, the set $\bigcup\{\underset{\sim}{R}_n[G] : n \in \omega\}$ contains all reals in $\hat{\mathbf{V}}$. So, in order to prove that the set of reals in $\hat{\mathbf{V}}$ can be written as a countable union of countable sets, it is enough to prove that each $\underset{\sim}{R}_n[G]$ is countable in $\hat{\mathbf{V}}$, which is done in two steps:

Firstly recall that $\mathbf{V} \vDash 2^{\omega_n} = \omega_{n+1}$ for each $n \in \omega$. Now, by counting (in the ground model $\mathbf{V}$) the canonical names which belong to $\underset{\sim}{R}_n$ we get that for each $n \in \omega$, $\big|\underset{\sim}{R}_n\big| = (\omega_{n+1})^{\mathbf{V}}$.

Secondly, for each $n \in \omega$ define

$$\underset{\sim}{f}_n = \big\{\langle \operatorname{op}(\underset{\cdot}{k}, \underset{\cdot}{\alpha}), p\rangle : p \in P_{n+1} \wedge \langle n, k\rangle \in \operatorname{dom}(p) \wedge p\big(\langle n, k\rangle\big) = \alpha\big\}\,.$$

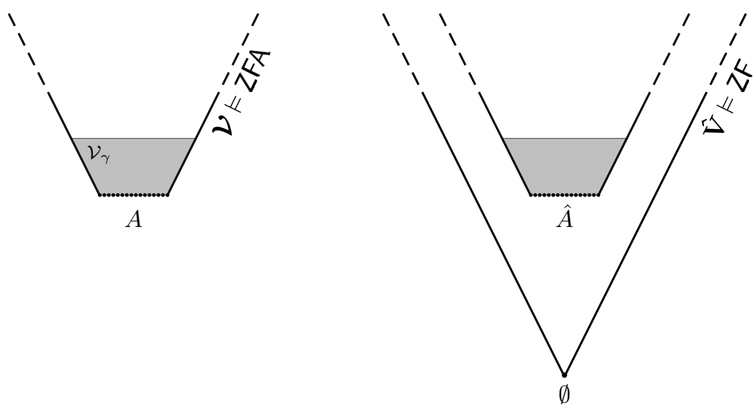
Then, for every $n \in \omega$, $\underset{\sim}{f}_n$ is a name for a function from ω to ω_n, $\operatorname{sym}_{\mathscr{G}}(\underset{\sim}{f}_n) \supseteq H_{n+1}$, and $\underset{\sim}{f}_n \in \mathbf{HS}$, hence $\underset{\sim}{f}_n[G] \in \hat{\mathbf{V}}$. Moreover, $\underset{\sim}{f}_n[G] : \omega \twoheadrightarrow \omega_n^{\mathbf{V}}$ is surjective which implies that $\omega_n^{\mathbf{V}}$ is countable in $\hat{\mathbf{V}}$. Now, since $\big|\underset{\sim}{R}_n\big| = (\omega_{n+1})^{\mathbf{V}}$ (for each $n \in \omega$), each $\underset{\sim}{R}_n[G]$ is countable in $\hat{\mathbf{V}}$ — whereas $\bigcup\big\{\underset{\sim}{R}_n[G] : n \in \omega\big\} = \mathscr{P}(\omega)^{\hat{\mathbf{V}}}$ is uncountable in $\hat{\mathbf{V}}$.

Conclusion: Starting from a model $\mathbf{V}$ of $\mathsf{ZFC} + \forall n \in \omega\,(2^{\omega_n} = \omega_{n+1})$ we constructed a symmetric model $\hat{\mathbf{V}}$ of ZF in which the set of reals is a countable union of countable sets. In particular, this shows that without some form of AC we cannot prove that countable unions of countable sets are countable. Furthermore, we get that in the absence of AC it might be possible that the real line $\mathbb{R}$ can be partitioned into a family $\mathscr{R}$, such that $|\mathscr{R}| > |\mathbb{R}|$. Moreover, by FACT 4.3 we know that $\big|[0,1]^2\big| = \big|\mathbb{R}\big|$ is provable in ZF only, and therefore we get that in the absence of AC, it might be possible to decompose a square into more parts than there are points on the square.

Simulating Permutation Models by Symmetric Models

The following theorem provides a method which enables us to embed an arbitrarily large fragment of a given permutation model (*i.e.*, a model of ZFA) into a well-founded model of ZF. In particular, if φ is a statement which holds in a given permutation model and whose validity depends only on a certain fragment of that model, then there is a well-founded model of ZF in which φ holds as well. For example assume that there are two sets R and S in some permutation model $\boldsymbol{\mathcal{V}}$ of ZFA such that $\boldsymbol{\mathcal{V}} \vDash |R| < |S| \wedge |S| \leq^* |R|$, *i.e.*, there is an injection from R into S, a surjection from R onto S, but no bijection between the two sets (*cf.* THEOREM 4.21 and PROPOSITION 7.14). Notice that the surjection from R onto S induces a partition $\mathscr{R}$ of R of cardinality $|S|$, *i.e.*, $|\mathscr{R}| > |R|$. Now, the validity of the sentence $\exists R\, \exists S\big(|R| < |S| \wedge |S| \leq^* |R|\big)$, which holds in $\boldsymbol{\mathcal{V}}$, depends only on a certain fragment of that model, and thus, by the following theorem, there is a well-founded model of ZF in which we find sets $\hat{R}$ and $\hat{S}$ such that $|\hat{R}| < |\hat{S}| \wedge |\hat{S}| \leq^* |\hat{R}|$.

THEOREM 17.2 (JECH-SOCHOR EMBEDDING THEOREM). *Let $\boldsymbol{\mathcal{V}} \vDash$ ZFA be a permutation model in which* AC *holds in the kernel of $\boldsymbol{\mathcal{V}}$. Furthermore, let A be the set of all atoms of $\boldsymbol{\mathcal{V}}$, let γ be an arbitrary but fixed ordinal number, and let $\mathcal{V}_\gamma := \mathscr{P}^\gamma(A) \cap \boldsymbol{\mathcal{V}}$. Then there exist a symmetric model $\hat{\mathbf{V}}$ (i.e., a model of* ZF*) and an embedding $x \mapsto \hat{x}$ of $\boldsymbol{\mathcal{V}}$ into $\hat{\mathbf{V}}$ whose restriction to $\mathcal{V}_\gamma$ is an $\in$-isomorphism between the sets $\mathcal{V}_\gamma$ and $\mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}}$, where $f : S \to T$ is an $\in$-isomorphism between S and T if f is a bijection and for all $x, y \in S$, $x \in y \iff f(x) \in f(y)$. In other words, one can simulate arbitrarily large fragments of permutation models by symmetric models, which is visualised by the following figure:*



Proof. Let $\boldsymbol{\mathcal{M}}$ be a model of ZFA + AC and let $\mathbf{V} := \mathscr{P}^\infty(\emptyset) \subseteq \boldsymbol{\mathcal{M}}$ be the kernel of $\boldsymbol{\mathcal{M}}$; then $\mathbf{V} \vDash$ ZFC. Let A_0 be the set of all atoms of $\boldsymbol{\mathcal{M}}$. We consider a group $\mathscr{G}_0$ of permutations of A_0 and a normal filter $\mathscr{F}_0$ on $\mathscr{G}_0$, and let $\boldsymbol{\mathcal{V}} \subseteq \boldsymbol{\mathcal{M}}$ be the permutation model (*i.e.*, a model of ZFA) given by $\mathscr{G}_0$ and $\mathscr{F}_0$. Further, let γ be an arbitrary but fixed ordinal number and let $\mathcal{V}_\gamma := \mathscr{P}^\gamma(A) \cap \boldsymbol{\mathcal{V}}$.

In order to construct a symmetric submodel of a generic extension, we have to work in a ground model of ZFC. So, we shall work in the model $\mathbf{V}$ and first construct a generic extension $\mathbf{V}[G]$ of $\mathbf{V}$: Let $\bar{A}$ be a set in $\mathbf{V}$ such that $\boldsymbol{\mathcal{M}} \vDash |\bar{A}| = |A_0|$ and fix in $\boldsymbol{\mathcal{M}}$ a bijection $\iota : A_0 \to \bar{A}$. Let κ be a regular cardinal (in $\mathbf{V}$) such that $\kappa > \bigl|\mathscr{P}^\gamma(\bar{A})\bigr|$. The set P of forcing conditions consists of functions $p : \operatorname{dom}(p) \to \{0,1\}$ such that $\operatorname{dom}(p) \subseteq (\bar{A} \times \kappa) \times \kappa$ and $|\operatorname{dom}(p)| < \kappa$. As usual let $p \leq q \iff p \subseteq q$. Then, by the choice of κ, $\mathbb{P} = (P, \leq)$ is a κ-closed forcing notion. Below, for $p \in P$ and $\bigl\langle \langle \bar{a}, \xi \rangle, \eta \bigr\rangle \in \operatorname{dom}(p)$ we shall write $p(\bar{a}, \xi, \eta)$ instead of $p\bigl(\bigl\langle \langle \bar{a}, \xi \rangle, \eta \bigr\rangle\bigr)$. For each $a \in A_0$ and each $\xi \in \kappa$ let

$$\underset{\cdot}{x}_{a\xi} = \bigl\{ \langle \underset{\cdot}{\eta}, p \rangle : p(\iota a, \xi, \eta) = 1 \bigr\},$$

and for each $a \in A_0$ define

$$\underset{\cdot}{a} = \bigl\{ \langle \underset{\cdot}{x}_{a\xi}, \emptyset \rangle : \xi \in \kappa \bigr\}$$

and let $\underset{\cdot}{A} = \{\underset{\cdot}{a} : a \in A_0\}$. Having now defined $\underset{\cdot}{a}$ for each $a \in A_0$, by transfinite recursion we define $\underset{\cdot}{x}$ for each $x \in \boldsymbol{\mathcal{M}}$ by stipulating

$$\underset{\cdot}{x} = \bigl\{ \langle \underset{\cdot}{y}, \emptyset \rangle : \boldsymbol{\mathcal{M}} \vDash y \in x \bigr\}.$$

Claim 1. *If G is $\mathbb{P}$-generic over $\mathbf{V}$, then for all $x, y \in \boldsymbol{\mathcal{M}}$:*

$$\begin{aligned} \boldsymbol{\mathcal{M}} \vDash y \in x &\iff \mathbf{V}[G] \vDash \underset{\cdot}{y}[G] \in \underset{\cdot}{x}[G] \\ \boldsymbol{\mathcal{M}} \vDash y = x &\iff \mathbf{V}[G] \vDash \underset{\cdot}{y}[G] = \underset{\cdot}{x}[G] \end{aligned}$$

Proof of Claim 1. Notice first that $\underset{\cdot}{x}_{a\xi}[G] \neq \underset{\cdot}{x}_{a'\xi'}[G]$ whenever $\langle a, \xi \rangle \neq \langle a', \xi' \rangle$, that $\underset{\cdot}{x}_{a\xi}[G] \neq \underset{\cdot}{x}[G]$ whenever $x \in \mathbf{V}$, and that for all $x \in \boldsymbol{\mathcal{M}}$ and $a \in A_0$, $\underset{\cdot}{x}[G] \notin \underset{\cdot}{a}[G]$. Consequently we have $\underset{\cdot}{a}[G] \neq \underset{\cdot}{a}'[G]$ whenever $a \neq a'$ are atoms and that the atoms do not contain any elements of the form $\underset{\cdot}{x}[G]$. Further, for all $a \in A_0$, all $\xi \in \kappa$, and every $x \in \boldsymbol{\mathcal{M}}$, we have $\underset{\cdot}{x}[G] \neq \underset{\cdot}{x}_{a,\xi}[G]$. To see this, notice that on the one hand, for all $x \in \mathbf{V}$ we have $\underset{\cdot}{x}[G] = \underset{\cdot}{x}[G]$ and therefore $\underset{\cdot}{x}[G] \neq \underset{\cdot}{x}_{a,\xi}[G]$; on the other hand, if $x \in \boldsymbol{\mathcal{M}} \setminus \mathbf{V}$ then $\mathrm{TC}(x)$ (*i.e.*, the transitive closure of x) contains an atom $a_0 \in A_0$, and hence, $\underset{\cdot}{x}_{a_0\zeta}[G] \in \mathrm{TC}\bigl(\underset{\cdot}{x}[G]\bigr)$ (for every $\zeta \in \kappa$), whereas for example $\underset{\cdot}{x}_{a_0 0}[G] \notin \mathrm{TC}\bigl(\underset{\cdot}{x}_{a\xi}[G]\bigr)$.

Now we can prove the claim simultaneously for "$\in$" and "$=$" by induction on rank, where, for a set x, $\mathrm{rk}_{\boldsymbol{\mathcal{M}}}(x)$ is the least $\alpha \in \Omega$ such that $x \in \mathscr{P}^\alpha(A_0)$. Notice that $\mathrm{rk}_{\boldsymbol{\mathcal{M}}}(\emptyset) = 1$, whereas $\mathrm{rk}_{\boldsymbol{\mathcal{M}}}(a) = 0$ for all atoms $a \in A_0$. Assume that the claim is valid for $y \in z$ and $y = z$ whenever $\mathrm{rk}_{\boldsymbol{\mathcal{M}}}(z) < \mathrm{rk}_{\boldsymbol{\mathcal{M}}}(x)$; we shall show that the claim is also valid for $y \in x$ and $y = x$.

$(\in)$: If $\boldsymbol{\mathcal{M}} \vDash y \in x$, then $\mathbf{V}[G] \vDash \underset{\cdot}{y}[G] \in \underset{\cdot}{x}[G]$ follows by definition of $\underset{\cdot}{x}$.Conversely, if $\mathbf{V}[G] \vDash \underset{\cdot}{y}[G] \in \underset{\cdot}{x}[G]$, then $\underset{\cdot}{x}$ can neither be the name for an atom nor for the empty set, since otherwise we would have $p \Vdash_{\mathbb{P}} \dot{y} \in \underset{\sim}{x}$ (for some $p \in P$), which is obviously impossible. Hence, $\mathbf{V}[G] \models \underset{\sim}{y}[G] = \underset{\sim}{z}[G]$ for some $\underset{\sim}{z} \in \underset{\sim}{x}$ (i.e., $z \in x$), and we have $\mathcal{M} \models y = z$ by the induction hypothesis, thus $\mathcal{M} \models y \in x$.

$(=)$: Obviously, if $\mathcal{M} \models y = x$, then $\mathbf{V}[G] \models \underset{\sim}{y}[G] = \underset{\sim}{x}[G]$. Conversely, if $\mathcal{M} \models y \neq x$, then either both x and y are atoms or the empty set and then $\mathbf{V}[G] \models \underset{\sim}{y}[G] \neq \underset{\sim}{x}[G]$; or for example x contains some z which is not in y, and then, by the $\in$ part already proved, $\mathbf{V}[G] \models \underset{\sim}{z}[G] \in \underset{\sim}{x}[G] \setminus \underset{\sim}{y}[G]$, hence, $\mathbf{V}[G] \models \underset{\sim}{y}[G] \neq \underset{\sim}{x}[G]$. $\dashv_{\text{Claim 1}}$

Notice that the proof of CLAIM 1 does not depend on the particular $\mathbb{P}$-generic filter G.

The next step is to construct a symmetric submodel $\hat{\mathbf{V}}$ of $\mathbf{V}[G]$ which reflects to some extent the model $\mathcal{V}$: We define a group $\bar{\mathscr{G}}$ of automorphisms of $\mathbb{P}$ and a normal filter $\bar{\mathscr{F}}$ on $\bar{\mathscr{G}}$ as follows. For every permutation σ of A_0, let $\bar{\sigma}$ be the set of all permutations π of $\bar{A} \times \kappa$ such that for all $a \in A_0$ and all $\xi \in \kappa$:

$$\pi\langle \iota a, \xi\rangle = \big\langle \iota\sigma(a), \xi'\big\rangle \text{ for some } \xi' \in \kappa\,.$$

One can visualise the set $\bar{A} \times \kappa$ as a set $\bar{A}$ of pairwise disjoint blocks, each block consisting of κ elements. Every permutation σ of A_0 induces a permutation σ' of the blocks and every $\pi \in \bar{\sigma}$ permutes the elements of $\bar{A} \times \kappa$ in such a way that π acts on the blocks exactly as σ' does.

Let

$$\bar{\mathscr{G}} = \bigcup \big\{\bar{\sigma} : \sigma \in \mathscr{G}_0\big\}$$

and for every subgroup H of $\mathscr{G}_0$ let $\bar{H} = \bigcup\{\bar{\sigma} : \sigma \in H\}$. Since every permutation π of $\bar{A} \times \kappa$ corresponds to an automorphism of $\mathbb{P}$ by stipulating

$$\pi p\big(\pi\langle \bar{a}, \xi\rangle, \eta\big) := p(\bar{a}, \xi, \eta)\,,$$

we consider $\bar{\mathscr{G}}$ as well as its subgroups as groups of automorphisms of $\mathbb{P}$. For every finite $E \in \operatorname{fin}(\bar{A} \times \kappa)$ let

$$\operatorname{fix}_{\bar{\mathscr{G}}}(E) = \big\{\pi \in \bar{\mathscr{G}} : \pi x = x \textit{ for each } x \in E\big\}\,.$$

We let $\bar{\mathscr{F}}$ be the filter on $\bar{\mathscr{G}}$ generated by

$$\big\{\bar{H} : H \in \mathscr{F}_0\big\} \cup \big\{\operatorname{fix}_{\bar{\mathscr{G}}} : E \in \operatorname{fin}(\bar{A} \times \kappa)\big\}\,.$$

We leave it as an exercise to the reader to check that $\bar{\mathscr{F}}$ is a normal filter.

Now, let **HS** be the class of all hereditarily symmetric names (with respect to $\bar{\mathscr{G}}$ and $\bar{\mathscr{F}}$), let G be $\mathbb{P}$-generic over $\mathbf{V}$, and let $\hat{\mathbf{V}} = \big\{\underset{\sim}{x}[G] : \underset{\sim}{x} \in \mathbf{HS}\big\}$ be the corresponding symmetric submodel of $\mathbf{V}[G]$. As an immediate consequence of the definition of $\bar{\mathscr{F}}$ we have:

- $\underset{\sim}{x}_{a\xi}[G] \in \hat{\mathbf{V}}$ for all $a \in A_0$ and $\xi \in \kappa$, because $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\sim}{x}_{a\xi}) = \operatorname{fix}_{\bar{\mathscr{G}}}\big(\{\langle \iota a, \xi\rangle\}\big)$.

- $\underset{\cdot}{a}[G] \in \hat{\mathbf{V}}$ for all $a \in A_0$, because $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{a}) = \overline{\operatorname{sym}_{\mathscr{G}_0}(a)}$, *i.e.*, for every $\sigma \in \operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{a})$, $\bar{\sigma} \subseteq \overline{\operatorname{sym}_{\mathscr{G}_0}(\underset{\cdot}{a})}$.
- $\underset{\cdot}{A}[G] \in \hat{\mathbf{V}}$, because $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{A}) = \bar{\mathscr{G}}$.

Below, we shall write $\hat{x}$ for $\underset{\cdot}{x}[G]$. So, in particular we have $\hat{a} \in \hat{\mathbf{V}}$ and $\hat{A} \in \hat{\mathbf{V}}$, *i.e.*, the "atoms" (more precisely, the surrogates of atoms introduced by the forcing) as well as the set of all "atoms" belongs to the model $\hat{\mathbf{V}}$.

The next task is to show that $x \in \boldsymbol{\mathcal{V}}$ *iff* $\hat{x} \in \hat{\mathbf{V}}$, which is done in the following two steps.

Claim 2. *For all* $x \in \boldsymbol{\mathcal{M}}$: $x \in \boldsymbol{\mathcal{V}} \iff \underset{\cdot}{x} \in \mathbf{HS}$.

Proof of Claim 2. It suffices to show that

$$\operatorname{sym}_{\mathscr{G}_0}(x) \in \mathscr{F}_0 \iff \operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{x}) \in \bar{\mathscr{F}}\,.$$

If $\sigma \in \mathscr{G}_0$ and $\pi \in \bar{\sigma}$, then $\alpha_\pi \underset{\cdot}{x}$ is the canonical name for σx, and therefore $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{x}) = \overline{\operatorname{sym}_{\mathscr{G}_0}(x)}$. Thus, if $\operatorname{sym}_{\mathscr{G}_0}(x) \in \mathscr{F}_0$, then $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{x}) \in \bar{\mathscr{F}}$. On the other hand, if $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\cdot}{x}) \in \bar{\mathscr{F}}$, then $\overline{\operatorname{sym}_{\mathscr{G}_0}(x)} \supseteq \bar{H} \cap \operatorname{fix}_{\bar{\mathscr{G}}}(E)$ for some $H \in \mathscr{F}_0$ and a finite set $E \in \operatorname{fin}(\bar{A} \times \kappa)$. Let $E|A_0 = \big\{a \in A_0 : \exists \xi(\langle \iota a, \xi\rangle \in E)\big\}$. Then $\operatorname{sym}_{\mathscr{G}_0}(x) \supseteq H \cap \operatorname{fix}_{\mathscr{G}_0}(E|A_0)$, and since $\mathscr{F}_0$ is a normal filter on $\mathscr{G}_0$ we have $\operatorname{fix}_{\mathscr{G}_0}(E|A_0) \in \mathscr{F}_0$ and hence $\operatorname{sym}_{\mathscr{G}_0}(x) \in \mathscr{F}_0$. $\dashv_{\text{Claim 2}}$

Claim 3. *For all* $x \in \boldsymbol{\mathcal{M}}$: $x \in \boldsymbol{\mathcal{V}} \iff \hat{x} \in \hat{\mathbf{V}}$.

Proof of Claim 3. By Claim 2, it suffices to show that if $\hat{x} \in \hat{\mathbf{V}}$, then $x \in \boldsymbol{\mathcal{V}}$. Assume towards a contradiction that there exists an $x \in \boldsymbol{\mathcal{M}}$ such that $\hat{x} \in \hat{\mathbf{V}}$ and $x \notin \boldsymbol{\mathcal{V}}$, but for all $y \in x$, $y \in \boldsymbol{\mathcal{V}}$. Thus $x \subseteq \boldsymbol{\mathcal{V}}$, and since $\hat{x} \in \hat{\mathbf{V}}$, there exist a name $\underset{\sim}{z} \in \mathbf{HS}$ and a condition $p_0 \in G$ such that $p_0 \Vdash_{\mathbb{P}} \underset{\sim}{z} = \underset{\cdot}{x}$. In other words, $\underset{\cdot}{x} \notin \mathbf{HS}$ but there exists a name $\underset{\sim}{z} \in \mathbf{HS}$ such that $\hat{x} = \underset{\sim}{z}[G]$, and consequently $\hat{x} \in \hat{\mathbf{V}}$. Since we have $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\sim}{z}) \in \bar{\mathscr{F}}$, there is a group $H_0 \in \mathscr{F}_0$ and a finite set $E_0 \in \operatorname{fin}(\bar{A} \times \kappa)$ such that $\operatorname{sym}_{\bar{\mathscr{G}}}(\underset{\sim}{z}) \supseteq \bar{H}_0 \cap \operatorname{fix}_{\bar{\mathscr{G}}}(E_0)$. Assume there are permutations $\sigma \in \mathscr{G}_0$ and $\pi \in \bar{\sigma}$ such that

(a) $\pi \in \bar{H}_0 \cap \operatorname{fix}_{\bar{\mathscr{G}}}(E_0)$,

(b) $\sigma x \neq x$, and

(c) πp_0 and p_0 are compatible.

Then we have $\pi \underset{\sim}{z} = \underset{\sim}{z}$ by (a), $p_0 \Vdash_{\mathbb{P}} \pi \underset{\cdot}{x} \neq \underset{\cdot}{x}$ by (b) and Claim 1, and since $\pi p_0 \Vdash_{\mathbb{P}} \pi \underset{\sim}{z} = \pi \underset{\cdot}{x}$, by (c) there is a $q_0 \in P$ such that $\pi p_0 \leq q_0 \geq p_0$ and

$$q_0 \Vdash_{\mathbb{P}} (\underset{\sim}{z} = \underset{\cdot}{x}) \wedge (\underset{\cdot}{x} \neq \pi \underset{\cdot}{x}) \wedge (\pi \underset{\cdot}{x} = \underset{\sim}{z})\,,$$

a contradiction. To see that permutations σ and π with the above properties exist, notice first that since x is not symmetric (*i.e.*, $x \notin \boldsymbol{\mathcal{V}}$), there exists a $\sigma \in H_0 \cap \operatorname{fix}_{\mathscr{G}_0}(E_0|A_0)$ such that $\sigma x \neq x$. Since $|\operatorname{dom}(p)| < \kappa$, there is a $\delta \in \kappa$ such that

$$\big\{\langle a, \xi\rangle : a \in A_0 \wedge \delta \in \xi \in \kappa\big\} \cap (\operatorname{dom}(p) \cup E_0) = \emptyset$$

and we define $\pi \in \bar{\sigma}$ as follows.

- If $a \in E_0|A_0$, then for all $\xi \in \kappa$:

$$\pi\langle \iota a, \xi\rangle = \langle \iota a, \xi\rangle \,.$$

- If $a \notin E_0|A_0$ and $\xi \in \delta$, then

$$\begin{aligned}\pi\langle \iota a, \xi\rangle &= \langle \iota(\sigma a), \delta+\xi\rangle \\ \pi\langle \iota a, \delta+\xi\rangle &= \langle \iota(\sigma a), \xi\rangle \,.\end{aligned}$$

- If $a \notin E_0|A_0$ and $\delta \in \xi+1 \in \kappa$, then

$$\pi\langle \iota a, \delta+\xi\rangle = \langle \iota(\sigma a), \delta+\xi\rangle \,.$$

By definition it follows that $\pi \in \bar{H}_0 \cap \mathrm{fix}_{\mathscr{G}}(E_0)$ and that πp_0 and p_0 are compatible. $\dashv_{\text{Claim 3}}$

The final step in the proof of THEOREM 17.2 is to show that the embedding $x \mapsto \hat{x}$ is a bijection between $\mathcal{V}_\gamma$ and $\mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}}$.

CLAIM 4. $\{\hat{x} : x \in \mathcal{V}_\gamma\} = \mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}}$

Proof of Claim 4. By CLAIM 3, the left-hand side is included in the right-hand side; thus, it suffices to show that $\mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}} \subseteq \{\hat{x} : x \in \mathcal{V}_\gamma\}$, which will be done by transfinite recursion: Let $x \in \mathcal{V}_\gamma$ and let $y \in \hat{\mathbf{V}}$ be such that $\hat{\mathbf{V}} \vDash y \in \hat{x}$. We have to show that $y = \hat{z}$ for some $z \in \boldsymbol{\mathcal{V}}$. Let $\underset{\sim}{y}$ be a $\mathbb{P}$-name for y. Since $\mathbb{P}$ is κ-closed and $\kappa > |x|$ (since $\kappa > \big|\mathscr{P}^\gamma(\bar{A})\big|$), there is a $p \in G$ which decides $\underset{\cdot}{u} \in \underset{\sim}{y}$ for all $u \in x$; more formally, $p \in G \cap \bigcap_{u\in x} \Delta_{\underset{\cdot}{u}\in \underset{\sim}{y}}$. Hence, $y = \hat{z}$, where $z = \{u \in x : p \Vdash_{\mathbb{P}} \underset{\cdot}{u} \in \underset{\sim}{y}\}$, and since $\hat{z} \in \hat{\mathbf{V}}$, by CLAIM 3 we get $z \in \boldsymbol{\mathcal{V}}$. $\dashv_{\text{Claim 4}}$

Finally, by CLAIM 4 we get that the embedding $x \mapsto \hat{x}$ of $\boldsymbol{\mathcal{V}}$ into $\hat{\mathbf{V}}$ is such that $\{\hat{x} : x \in \mathcal{V}_\gamma\} = \mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}}$, and for all $x, y \in \mathcal{V}_\gamma$ we have $\boldsymbol{\mathcal{V}} \vDash y \in x$ *iff* $\hat{\mathbf{V}} \vDash \hat{y} \in \hat{x}$, which shows that $\mathcal{V}_\gamma$ and $\mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}}$ are indeed $\in$-isomorphic, *i.e.*, the embedding $x \mapsto \hat{x}$ restricted to $\mathcal{V}_\gamma$ is an $\in$-isomorphism between $\mathcal{V}_\gamma$ and $\mathscr{P}^\gamma(\hat{A})^{\hat{\mathbf{V}}}$. $\dashv$

COROLLARY 17.3. *Let ν be an ordinal and let φ be a sentence of the form $\exists X\psi(X,\nu)$, where the only quantifiers we allow in ψ are the restricted quantifiers $\exists u \in \mathscr{P}^\nu(X)$ and $\forall u \in \mathscr{P}^\nu(X)$. If $\boldsymbol{\mathcal{V}} \vDash$ ZFA is a permutation model in which* AC *holds in the kernel and $\boldsymbol{\mathcal{V}} \vDash \varphi$, then there exists a symmetric model $\hat{\mathbf{V}} \vDash$* ZF *such that $\hat{\mathbf{V}} \vDash \varphi$.*

Proof. Let $X \in \boldsymbol{\mathcal{V}}$ be such that $\boldsymbol{\mathcal{V}} \vDash \psi(X,\nu)$ and let $\gamma \in \Omega$ be such that $\mathscr{P}^\nu(X) \subseteq \mathscr{P}^\gamma(A)$, where A is the set of atoms of $\boldsymbol{\mathcal{V}}$. By the JECH-SOCHOR EMBEDDING THEOREM 17.2 there exists a symmetric model $\hat{\mathbf{V}}$ of ZF such that $\mathcal{V}_\gamma$ and $\mathscr{P}^\gamma(\hat{A})$ are $\in$-isomorphic. Now, by the choice of γ and since $\boldsymbol{\mathcal{V}} \vDash \psi(X,\nu)$ we have $(\mathcal{V}_\gamma, \in) \vDash \psi(X,\nu)$, and therefore $(\mathcal{V}_\gamma, \in) \vDash \varphi$. Hence, $\big(\mathscr{P}^\gamma(\hat{A}), \in\big) \vDash \varphi$ which shows that $\hat{\mathbf{V}} \vDash \varphi$. $\dashv$

Applications: Most of the results of Chapter 7 — obtained by permutation models — can now be transferred to proper models of ZF. For example the existence of a set X, such that $|X^2| < |[X]^2|$ is consistent with ZF (*cf.* PROPOSITION 7.18), or in other words, $\mathsf{ZF} \nvdash \forall X\big(|X^2| \nless |[X]^2|\big)$. Similarly we can show that $\mathsf{ZF} \nvdash \forall X\big(|\operatorname{seq}(X)| \nless |\operatorname{fin}(X)|\big)$ (*cf.* PROPOSITION 7.17).

NOTES

Symmetric submodels of generic extensions. The idea of using symmetry arguments to construct models in which the Axiom of Choice fails goes back to Fraenkel [6]. Cohen incorporated the symmetry arguments into his method and constructed for example the model given above in which the reals are not well-orderable. The formulation of Cohen's method in terms of symmetric submodels of generic extensions is due to Scott and Jech (*cf.* Jech [11, Chapter 15]).

Three examples of symmetric models. The first model (*i.e.*, the one in which the reals are not well-orderable) is due to Cohen (*cf.* [3, Chapter IV, §9]) and is sometimes called the **basic Cohen model** (*cf.* Jech [9, Chapter 5, §3]); the second model we presented (*i.e.*, the one in which every ultrafilter over ω is principal) is due to Feferman [4]; and the third model (*i.e.*, the one in which the set of reals is a countable union of countable sets) is due to Feferman and Lévy [5]. However, the constructions can also be found in Jech [11, Chapter 15], and in greater detail in Jech [10, Chapter 3, Section 21] and [9, Chapter 10, §1] respectively.

Simulating permutation models by symmetric models. The JECH-SOCHOR EMBEDDING THEOREM 17.2 is due to Jech and Sochor [12, 13], where numerous applications of the theorem are given in the second paper [13] (see also Jech [9, Theorem 6.1] and [11, Chapter 15]). The limits of the JECH-SOCHOR EMBEDDING THEOREM 17.2 are discussed in RELATED RESULT 93.

RELATED RESULTS

89. *Choice principles in the basic Cohen model.* We have seen that in the basic Cohen model — the model in which the reals cannot be well-ordered — there is an infinite set of reals which does not contain a countable infinite subset and thus, the Axiom of Choice fails in that model. On the other hand, the following choice principles are still valid in the basic Cohen model:
    - If X is infinite, then $\mathscr{P}(X)$ is transfinite, *i.e.*, $\aleph_0 \leq |\mathscr{P}(X)|$ (see Jech [9, p. 81, Problem 20]).
    - For every family $\mathscr{F}$ of sets, each containing at least two elements, there is a function F such that for each set $S \in \mathscr{F}$, $\emptyset \neq F(S) \subsetneq S$ (see Jech [9, p. 82, Problem 21]).
    - Every family of non-empty well-orderable sets has a choice function (see Jech [9, p. 82, Problem 22] and compare with Chapter 7 | RELATED RESULT 48).

90. *A model in which every ultrafilter is principal.* Blass constructed in [1] a model — similar to Feferman's model given above — in which *every* ultrafilter (and not just ultrafilters over ω) is principal.

91. ω_1 *can be singular.* It is provable in ZF that there exists a surjection from the reals onto ω_1 (*cf.* THEOREM 4.11). Hence, in the model in which the set of reals is a countable union of countable sets, ω_1 is a limit of a countable sequence of countable ordinals, and therefore ω_1 is singular in that model (compare with PROPOSITION 5.10 where it is shown that in the presence of AC, successor cardinals are always regular).

92. ω_1 *can be even measurable.* An uncountable aleph κ is called a **measurable cardinal** if there exists a non-principal ultrafilter $\mathscr{U}$ over κ which is κ-complete, *i.e.*, if $\alpha \in \kappa$ and $\{x_\xi : \xi \in \alpha\} \subseteq \mathscr{U}$, then

$$\bigcap \{x_\xi : \xi \in \alpha\} \in \mathscr{U} .$$

In the presence of AC, measurable cardinals are extremely large, even much larger than *inaccessible cardinals*, on which Hausdorff [7, p. 131] wrote that already the smallest of those cardinals — if they exist — is of an *exorbitant magnitude.* However, under the assumption that there is a measurable cardinal in the ground model, Jech constructed in [8] a symmetric model of ZF in which ω_1 is measurable (see also Jech [9, Chapter 12, §1]).

93. *Nontransferable statements.* Not every statement which hold in a permutation model (*i.e.*, in a model of ZFA) can be transferred into ZF. There are even statements which imply AC in ZF but are weaker than AC in ZFA. For example Multiple Choice and Kurepa's Principle are such statements (see THEOREM 5.4 and Jech [9, Theorem 9.2]).

94. *Bases in vector spaces and the Axiom of Choice**. In Chapter 5 we have seen that the Axiom of Choice follows in ZF from the assertion that every vector space has a basis (*cf.* THEOREM 5.4). However, it is still open whether the Axiom of Choice is deducible in ZFA from the assertion that every vector space has a basis, or at least from the assertion that in every vector space every independent set is included in a basis.

95. *Inaccessible cardinals in* ZF. In [2], Blass, Dimitriou, and Löwe introduce and investigate definitions for inaccessible cardinals (see page 315) in the absence of AC. They produce four possible definitions that are equivalent in ZFC but not in ZF, and provide a complete implication diagram (in ZF) for these four different concepts.

REFERENCES

1. ANDREAS BLASS, *A model without ultrafilters*, ***Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques***, vol. 25 (1977), 329–331.
2. ANDREAS BLASS, IOANNA DIMITRIOU, AND LÖWE BENEDIKT, *Inaccessible cardinals without the axiom of choice*, ***Fundamenta Mathematicae***, vol. 194 (2007), 179–189.
3. PAUL J. COHEN, ***Set Theory and the Continuum Hypothesis***, Benjamin, New York, 1966.
4. SOLOMON FEFERMAN, *Some applications of the notions of forcing and generic sets*, ***Fundamenta Mathematicae***, vol. 56 (1964/1965), 325–345.

5. Solomon Feferman and Azriel Lévy, *Independence results in set theory by Cohen's method II*, ***Notices of the American Mathematical Society***, vol. 10 (1963), 593.
6. Adolf Fraenkel, *Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre*, ***Mathematische Annalen***, vol. 86 (1922), 230–237.
7. Felix Hausdorff, ***Grundzüge der Mengenlehre***, de Gruyter, Leipzig, 1914 [reprint: Chelsea, New York, 1965].
8. Thomas Jech, *ω_1 can be measurable*, ***Israel Journal of Mathematics***, vol. 6 (1968), 363–367.
9. ———, ***The Axiom of Choice***, Studies in Logic and the Foundations of Mathematics 75, North-Holland, Amsterdam, 1973.
10. ———, ***Set Theory***, [Pure and Applied Mathematics], Academic Press, London, 1978.
11. ———, ***Set Theory**, The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
12. Thomas Jech and Antonín Sochor, *On θ-model of the set theory*, ***Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques***, vol. 14 (1966), 297–303.
13. ———, *Applications of the θ-model*, ***Bulletin de l'Académie Polonaise des Sciences, Série des Sciences Mathématiques, Astronomiques et Physiques***, vol. 14 (1966), 351–355.

18

Combining Forcing Notions

In this chapter we shall investigate how one can combine various forcing notions. For this we first consider just two (not necessarily distinct) forcing notions, say $\mathbb{P} = (P, \leq_P)$ and $\mathbb{Q} = (Q, \leq_Q)$.

The simplest way to combine $\mathbb{P}$ and $\mathbb{Q}$ is to form the disjoint union of $\mathbb{P}$ and $\mathbb{Q}$ (where conditions of $\mathbb{P}$ are incomparable with those of $\mathbb{Q}$). Obviously, a generic filter of the disjoint union is either $\mathbb{P}$-generic or $\mathbb{Q}$-generic, and therefore, this construction is useless for independence proofs.

Another way to combine $\mathbb{P}$ and $\mathbb{Q}$ is to build the *product* $\mathbb{P} \times \mathbb{Q} = (P \times Q, \leq_{P \times Q})$. Since the forcing notion $\mathbb{P} \times \mathbb{Q}$ belongs to $\mathbf{V}$, forcing with $\mathbb{P} \times \mathbb{Q}$ is in fact just a one-step extension of $\mathbf{V}$. Products of forcing notions will be investigated in the first part of this chapter, where the focus will be on products of Cohen forcing notions.

A more sophisticated way to combine $\mathbb{P}$ and $\mathbb{Q}$ is to *iterate* $\mathbb{P}$ and $\mathbb{Q}$, *i.e.*, we first force with $\mathbb{P}$ and then — in the $\mathbb{P}$-generic extension — by $\mathbb{Q}$. In this case, the forcing notion $\mathbb{Q}$ does not necessarily belong to $\mathbf{V}$. To see this, let G be $\mathbb{P}$-generic over $\mathbf{V}$ and let $\mathbb{Q} = \big(\mathrm{Fn}(G, 2), \subseteq\big)$. Obviously, the forcing notion $\mathbb{Q}$ does not belong to $\mathbf{V}$. However, since $\mathbb{Q}$ belongs to $\mathbf{V}[G]$, there is a $\mathbb{P}$-name $\underset{\sim}{\mathbb{Q}}$ in $\mathbf{V}$ such $\underset{\sim}{\mathbb{Q}}[G] = \mathbb{Q}$. Two-step iterations of this type are denoted by $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$. In the second part of this chapter we shall see how to transform a two-step iteration into a one-step forcing extension. Furthermore, we shall see different ways to define general iterations of forcing notions.

From now on, a *forcing notion* is just a partially ordered set $\mathbb{P} = (P, \leq)$ with a smallest element; in particular, we no longer require that there are incompatible conditions above each $p \in P$.

Products

General Products of Forcing Notions

Before we investigate products of Cohen forcing notions — which will be the most frequently used product of forcing notions — we consider first the general case.

For two forcing notions $\mathbb{P}_0 = (P_0, \leq_0, \mathbf{0}_0)$ and $\mathbb{P}_1 = (P_1, \leq_1, \mathbf{0}_1)$, the product forcing notion

$$\mathbb{P}_0 \times \mathbb{P}_1 = (P_0 \times P_1, \leq, \mathbf{0})$$

is defined by stipulating $\mathbf{0} := \langle \mathbf{0}_0, \mathbf{0}_1 \rangle$ and

$$\langle p_0, p_1 \rangle \leq \langle q_0, q_1 \rangle \iff p_0 \leq q_0 \wedge p_1 \leq q_1 .$$

We leave it as an exercise to the reader to show that $\mathbb{P}_0 \times \mathbb{P}_1 = (P_0 \times P_1, \leq, \mathbf{0})$ is indeed a forcing notion.

In general, if κ is a non-zero cardinal number and $\langle \mathbb{P}_\alpha : \alpha \in \kappa \rangle$ is a sequence of forcing notions, where for all $\alpha \in \kappa$, $\mathbb{P}_\alpha = (P_\alpha, \leq_\alpha, \mathbf{0}_\alpha)$, then we define the product forcing notion

$$\prod_{\alpha \in \kappa} \mathbb{P}_\alpha = \Big(\prod_{\alpha \in \kappa} P_\alpha,\ \leq,\ \mathbf{0} \Big)$$

by stipulating $\mathbf{0} := \langle \mathbf{0}_\alpha : \alpha \in \kappa \rangle$ and

$$\langle p_\alpha : \alpha \in \kappa \rangle \leq \langle q_\alpha : \alpha \in \kappa \rangle \iff \forall \alpha \in \kappa \, (p_\alpha \leq_\alpha q_\alpha) .$$

Let us now have a closer look at the product $\prod_{\alpha \in \kappa} \mathbb{P}_\alpha$ for some $\kappa \geq 2$. If G is $\prod_{\alpha \in \kappa} \mathbb{P}_\alpha$-generic over $\mathbf{V}$, then $G \subseteq \prod_{\alpha \in \kappa} P_\alpha$. Thus, each $p \in G$ is of the form $p = \big\langle p(\alpha) : \alpha \in \kappa \big\rangle$. For each $\alpha \in \kappa$ let $G(\alpha) := \big\{ p(\alpha) : p \in G \big\}$; in particular, $G \subseteq \prod_{\alpha \in \kappa} G(\alpha)$. Obviously, for each $\alpha \in \kappa$, $G(\alpha)$ is $\mathbb{P}_\alpha$-generic over $\mathbf{V}$. Moreover, we have $G = \prod_{\alpha \in \kappa} G(\alpha)$, which implies that $\mathbf{V}[G] = \mathbf{V}\big[\prod_{\alpha \in \kappa} G(\alpha)\big] = \mathbf{V}\big[\langle G(\alpha) : \alpha \in \kappa \rangle\big]$ (the details are left as an exercise to the reader). In fact, we can prove even more:

LEMMA 18.1. *Let κ be a cardinal, let $\prod_{\alpha \in \kappa} \mathbb{P}_\alpha$ be a product of forcing notions $\mathbb{P}_\alpha = (P_\alpha, \leq_\alpha, \mathbf{0}_\alpha)$, and let G be $\prod_{\alpha \in \kappa} \mathbb{P}_\alpha$-generic over $\mathbf{V}$. Then, for each $\gamma \in \kappa$, $G(\gamma)$ is $\mathbb{P}_\gamma$-generic over $\mathbf{V}\big[\langle G(\alpha) : \alpha \in \kappa \setminus \{\gamma\} \rangle\big]$.*

Proof. The cases when $\kappa = 0$ or $\kappa = 1$ are trivial. For the other cases, notice first that it is enough to prove the result just in the case when $\kappa = 2$, for we can always consider the product $\mathbb{P} \times \mathbb{Q}$ where $\mathbb{P} := \mathbb{P}_\gamma$ and $\mathbb{Q} := \prod_{\alpha \in \kappa \setminus \{\gamma\}} \mathbb{P}_\alpha$. So, let $G(0)$ be $\mathbb{P}$-generic over $\mathbf{V}$, where $\mathbb{P} = (P, \leq, \mathbf{0}_P)$. We have to show that $G(1)$ is $\mathbb{Q}$-generic over $\mathbf{V}\big[G(0)\big]$, where $\mathbb{Q} = (Q, \leq, \mathbf{0}_Q)$. Let $D \subseteq Q$ be an open dense set which belongs to the model $\mathbf{V}\big[G(0)\big]$ — notice that D

does not necessarily belong to $\mathbf{V}$. In $\mathbf{V}$ there exist a $\mathbb{P}$-name $\underset{\sim}{D}$ for D and a $\mathbb{P}$-condition $p_0 \in G(0)$ such that

$$\mathbf{V} \models p_0 \Vdash_{\mathbb{P}} \text{“}\underset{\sim}{D} \textit{ is an open dense subset of } \dot{Q}\text{”}.$$

In other words, for every $r \in Q$ there exists a $\mathbb{P}$-name $\underset{\sim}{q}$ for a condition in Q such that $p_0 \Vdash_{\mathbb{P}} \underset{\sim}{q} \geq r \wedge \underset{\sim}{q} \in \underset{\sim}{D}$. Now, let

$$D_1' = \big\{\langle p, q\rangle \in P \times Q : p \geq p_0 \ \wedge\ p \Vdash_{\mathbb{P}} \dot{q} \in \underset{\sim}{D}\big\} \subseteq P \times Q\,.$$

We leave it as an exercise to the reader to show that D_1' is dense above $\langle p_0, \mathbf{0}_Q\rangle$. Since $p_0 \in G(0)$ and $G(1)$ is $\mathbb{Q}$-generic over $\mathbf{V}$, by FACT 14.7 there are conditions $p' \in P$ and $q' \in Q$ such that $\langle p', q'\rangle \in D_1' \cap \big(G(0) \times G(1)\big)$. In particular we have $p' \in G(0)$ and $p' \Vdash_{\mathbb{P}} \dot{q}' \in \underset{\sim}{D}$, which implies that $\mathbf{V}\big[G(0)\big] \models q' \in \underset{\sim}{D}[G(0)]$. Finally, since $q' \in G(1)$ and $\underset{\sim}{D}[G(0)] = D$, we get $q' \in D \cap G(1)$, *i.e.*, $D \cap G(1)$ is non-empty. ⊣

We now introduce the notion of *support* of a condition — a notion which we shall meet again in the definition of iterated forcing.

Let $p = \big\langle p(\alpha) : \alpha \in \kappa\big\rangle$ be a $\prod_{\alpha\in\kappa} \mathbb{P}_\alpha$-condition, *i.e.*, for each $\alpha \in \kappa$ we have $p(\alpha) \in P_\alpha$, where $\mathbb{P}_\alpha = (P_\alpha, \leq_\alpha, \mathbf{0}_\alpha)$. Then the set $\big\{\alpha \in \kappa : p(\alpha) \neq \mathbf{0}_\alpha\big\}$ is called the **support** of p and is denoted by $\operatorname{supp}(p)$. Notice that for any $\prod_{\alpha\in\kappa} \mathbb{P}_\alpha$-conditions p and q, $p \leq q$ implies $\operatorname{supp}(p) \subseteq \operatorname{supp}(q)$. A **finite support product** of forcing notions is a product of forcing notions consisting of those conditions that have finite support.

Products of Cohen Forcing

In this section we show that a finite support product of countably many Cohen forcing notions is essentially the same as Cohen forcing.

For this, let us first consider Cohen forcing $\mathbb{C} = \big(\mathrm{Fn}(\omega, 2), \subseteq\big)$, as it was defined in Chapter 14. If G is $\mathbb{C}$-generic over some ground model $\mathbf{V}$, then $c := \bigcup G$ is a function in $\mathbf{V}[G]$ from ω to $\{0, 1\}$ (*i.e.*, $c \in {}^{\omega}2$) which has the property that the set $\big\{p \in \mathrm{Fn}(\omega, 2) : p \subseteq c\big\}$ is $\mathbb{C}$-generic over $\mathbf{V}$. A real $c \in {}^{\omega}2$ (in some model $\mathbf{V}'$) with this property is called a **Cohen real** over $\mathbf{V}$. Obviously, every $\mathbb{C}$-generic filter over $\mathbf{V}$ corresponds to a Cohen real, and vice versa, every Cohen real over $\mathbf{V}$ corresponds to a $\mathbb{C}$-generic filter over $\mathbf{V}$.

Sometimes it is convenient to consider a Cohen real, defined as an element of ${}^{\omega}2$, as a function from ω to ω. Of course, there exist natural mappings between the sets ${}^{\omega}2$ and ${}^{\omega}\omega$. However, there is a more elegant way to get Cohen reals $c \in {}^{\omega}\omega$: Consider again Cohen forcing $\mathbb{C} = \big(\mathrm{Fn}(\omega, 2), \subseteq\big)$, and for the moment let $\bar{\mathbb{C}} := \big(\bigcup_{n\in\omega} {}^{n}2, \subseteq\big)$, $\mathbb{C}(\omega) := \big(\mathrm{Fn}(\omega, \omega), \subseteq\big)$, and $\bar{\mathbb{C}}(\omega) := \big(\bigcup_{n\in\omega} {}^{n}\omega, \subseteq\big)$.

We shall show that the forcing notions $\bar{\mathbb{C}}$, $\mathbb{C}(\omega)$, and $\bar{\mathbb{C}}(\omega)$, are all equivalent to Cohen forcing $\mathbb{C}$, *i.e.*, no matter whether we force (over some ground model $\mathbf{V}$) with $\mathbb{C}$ or with one of $\bar{\mathbb{C}}$, $\mathbb{C}(\omega)$, or $\bar{\mathbb{C}}(\omega)$, we always get the same generic extension.

PROPOSITION 18.2. $\mathbb{C} \approx \bar{\mathbb{C}} \approx \mathbb{C}(\omega) \approx \bar{\mathbb{C}}(\omega)$.

Proof. In order to prove that two forcing notions $\mathbb{P} = (P, \leq)$ and $\mathbb{Q} = (Q, \leq)$ are equivalent, it is enough to show that there exists a dense embedding $h : P \to Q$ (see FACT 14.3).

$\mathbb{C} \approx \bar{\mathbb{C}}$ *and* $\mathbb{C}(\omega) \approx \bar{\mathbb{C}}(\omega)$: The identities $\iota_1 : \bigcup_{n\in\omega} {}^n 2 \to \mathrm{Fn}(\omega, 2)$ and $\iota_\omega : \bigcup_{n\in\omega} {}^n\omega \to \mathrm{Fn}(\omega, \omega)$ are obviously dense embeddings.

$\bar{\mathbb{C}}(\omega) \approx \bar{\mathbb{C}}$: We shall define a dense embedding $h : \bigcup_{n\in\omega} {}^n\omega \to \bigcup_{n\in\omega} {}^n 2$. For this, take an arbitrary function $p : n_0 \to \omega$. If $n_0 = 0$, then $h(p) := \emptyset$. Otherwise, by induction on n_0 we first define integers b_k such that for all $k \in n_0$ we have

$$b_k = \begin{cases} p(0) & \text{if } k = 0, \\ b_{k-1} + p(k) + 1 & \text{if } k > 0. \end{cases}$$

Let $x_p := \{b_k : k \in n_0\}$ and define the function $h(p) : b_{n_0 - 1} + 1 \to 2$ by stipulating

$$h(p)(j) = \begin{cases} 1 & \text{if } j \in x_p, \\ 0 & \text{if } j \notin x_p. \end{cases}$$

Notice that we always have $h(p)(b_{n_0-1}) = 1$. On the other hand, if the function $q : k_0 + 1 \to 2$ is such that $q(k_0) = 1$, then there exists a $p : l \to \omega$, where $l = \big|\{m \in k_0 + 1 : q(m) = 1\}\big|$, such that $h(p) = q$. In fact, $h(p)$ is the sequence of $p(0)$ zeros, a single 1, $p(1)$ zeros, a single 1, *et cetera*. We leave it as an exercise to the reader to verify that h is indeed a dense embedding. $\dashv$

Since the forcing notions $\mathbb{C}$, $\bar{\mathbb{C}}$, $\mathbb{C}(\omega)$, $\bar{\mathbb{C}}(\omega)$, are all equivalent, we shall not distinguish between these four forcing notions, and in order to simplify the terminology, each of these four forcing notions is called **Cohen forcing** and is denoted by $\mathbb{C}$.

Let us now consider products of Cohen forcing: For any ordinal $\lambda \in \Omega$ let $\mathbb{C}_\lambda = \big(\mathrm{Fn}(\omega \times \lambda, 2), \subseteq\big)$ and let $\mathbb{C}^\lambda$ denote the *finite support* product of λ copies of Cohen forcing $\mathbb{C} = \big(\mathrm{Fn}(\omega, 2), \subseteq\big)$. We shall show that for any ordinal λ, $\mathbb{C}_\lambda \approx \mathbb{C}^\lambda$, and in addition, if λ is a non-zero countable ordinal, then both forcing notions are equivalent to Cohen forcing $\mathbb{C}$.

PROPOSITION 18.3. *For every ordinal λ we have $\mathbb{C}_\lambda \approx \mathbb{C}_{|\lambda|} \approx \mathbb{C}^{|\lambda|} \approx \mathbb{C}^\lambda$, and for every non-zero countable ordinal γ we have $\mathbb{C} \approx \mathbb{C}_\gamma \approx \mathbb{C}^\gamma$.*

Proof. It is sufficient to show that for every non-zero countable ordinal γ we have $\mathbb{C} \approx \mathbb{C}_\gamma$, and that for every ordinal λ we have $\mathbb{C}_\lambda \approx \mathbb{C}_{|\lambda|}$, $\mathbb{C}^\lambda \approx \mathbb{C}^{|\lambda|}$, and $\mathbb{C}_\lambda \approx \mathbb{C}^\lambda$.

$\mathbb{C} \approx \mathbb{C}_\gamma$: Let $\xi : \omega \times \gamma \to \omega$ be a bijection and let $h : \mathrm{Fn}(\omega \times \gamma, 2) \to \mathrm{Fn}(\omega, 2)$ be such that for each $p \in \mathrm{Fn}(\omega \times \gamma, 2)$, $\mathrm{dom}\big(h(p)\big) = \xi[\mathrm{dom}(p)]$ and for all $j \in \xi[\mathrm{dom}(p)]$ we have $h(p)(j) = p\big(\xi^{-1}(j)\big)$. Then h is obviously a dense embedding; in fact, h is even an isomorphism.

$\mathbb{C}^\lambda \approx \mathbb{C}_\lambda$: Since $\mathbb{C}^\lambda$ is a finite support product, for every $\mathbb{C}^\lambda$-condition $p = \big\langle p(\beta) : \beta \in \lambda \big\rangle$, the set $\operatorname{supp}(p) = \big\{ \beta \in \lambda : p(\beta) \neq \mathbf{0} \big\}$ is finite. Now, for every $\mathbb{C}^\lambda$-condition p let $h(p) \in \operatorname{Fn}(\omega \times \lambda, 2)$ be such that

$$\operatorname{dom}\big(h(p)\big) = \big\{ \langle \beta, n \rangle \in \operatorname{supp}(p) \times \omega : n \in \operatorname{dom}\big(p(\beta)\big) \big\}$$

and $h(p)\big(\langle \beta, n \rangle\big) = p(\beta)(n)$. Then h is obviously a dense embedding; in fact, it is even an isomorphism.

Finally, let $\zeta : \lambda \to |\lambda|$ be a bijection. Then ζ induces a bijection between $\omega \times \lambda$ and $\omega \times |\lambda|$, as well as a bijection between the set of $\mathbb{C}^\lambda$-conditions and the set of $\mathbb{C}^{|\lambda|}$-conditions, which shows that $\mathbb{C}_\lambda \approx \mathbb{C}_{|\lambda|}$ and that $\mathbb{C}^\lambda \approx \mathbb{C}^{|\lambda|}$. $\dashv$

As an immediate consequence of Proposition 18.3 we get that for every non-zero countable ordinal λ, each $\mathbb{C}^\lambda$-generic filter can be encoded by a single Cohen real. Roughly speaking, adding one Cohen real is the same as adding countably many Cohen reals. Since this is one of the main features of Cohen forcing, we state it in a more formal way.

Fact 18.4. *If G is $\mathbb{C}^\lambda$-generic over $\mathbf{V}$ and G' is $\mathbb{C}_\lambda$-generic over $\mathbf{V}$, where λ is a non-zero countable ordinal, then there are Cohen reals c and c' over $\mathbf{V}$ such that $\mathbf{V}[G] = \mathbf{V}[c]$ and $\mathbf{V}[G'] = \mathbf{V}[c']$.*

A Model in which $\mathfrak{a} < \mathfrak{c}$

As a first application of a product of Cohen forcing we shall construct a model of ZFC in which $\mathfrak{c}$ is large and $\mathfrak{a}$ is small. Recall that $\mathfrak{a}$ is the least cardinality of an infinite, maximal almost disjoint family (called *mad* family), where a family $\mathscr{F} \subseteq [\omega]^\omega$ is almost disjoint if any two distinct elements of $\mathscr{F}$ have finite intersection (see Chapter 8).

Proposition 18.5. *$\omega_1 = \mathfrak{a} < \mathfrak{c}$ is consistent with* ZFC.

Proof. Let $\mathbf{V}$ be a model of $\mathsf{ZFC} + \mathsf{CH}$, let $\kappa \geq \omega_2$ be a cardinal, and let G be $\mathbb{C}_\kappa$-generic over $\mathbf{V}$ (by Proposition 18.3 we could equally well work with the finite support product $\mathbb{C}^\kappa$). By Theorem 14.21 we know that $\mathbf{V}[G] \vDash \mathfrak{c} \geq \kappa$. Thus, it remains to show that $\mathbf{V}[G]$ contains a *mad* family of size ω_1. Firstly, we shall construct a family $\mathscr{A}_0 \subseteq [\omega]^\omega$ of size ω_1 in $\mathbf{V}$ such that whenever g is $\mathbb{C}$-generic over $\mathbf{V}$, then $\mathbf{V}[g] \vDash$ "$\mathscr{A}_0$ is *mad*". Then we shall show that $\mathscr{A}_0$ — which is obviously an almost disjoint family in $\mathbf{V}[G]$ — is still maximal in $\mathbf{V}[G]$.

Construction of $\mathscr{A}_0$ in $\mathbf{V}$: Consider Cohen forcing $\mathbb{C} = \big(\operatorname{Fn}(\omega, 2), \subseteq\big)$. Within $\mathbf{V}$, let $\big\{ \langle p_\xi, \underset{\sim}{x}_\xi \rangle : \omega \leq \xi \in \omega_1 \big\}$ be an enumeration of all pairs $\langle p, \underset{\sim}{x} \rangle$ such that $p \in \operatorname{Fn}(\omega, 2)$ and $\underset{\sim}{x}$ is a *nice name* for a subset of ω, *i.e.*, for all $\langle \underset{\cdot}{n}, q_1 \rangle, \langle \underset{\cdot}{n}, q_2 \rangle \in \underset{\sim}{x}$, either $q_1 = q_2$ or $q_1 \perp q_2$ (see the proof of Theorem 16.4). Notice that since $\mathbf{V} \vDash \mathsf{CH}$, there are just ω_1 nice names in $\mathbf{V}$ for subsets of ω. The set $\mathscr{A}_0 = \{ A_\xi \in [\omega]^\omega : \xi \in \omega_1 \}$ is constructed as follows: Let

$\{A_n \in [\omega]^\omega : n \in \omega\}$ be any family of pairwise disjoint infinite subsets of ω. Let $\omega \leq \xi \in \omega_1$ and assume that we have already defined A_η for all $\eta \in \xi$. Then, choose $A_\xi \in [\omega]^\omega$ such that the following conditions are satisfied:

(1) For all $\eta \in \xi$, $A_\eta \cap A_\xi$ is finite.

(2) If
$$p_\xi \Vdash_{\mathbb{C}} |\underset{\sim}{x}_\xi| = \underset{\cdot}{\omega} \ \wedge\ \forall \eta \in \xi \big(p_\xi \Vdash_{\mathbb{C}} \big|\underset{\sim}{x}_\xi \cap \underset{\cdot}{A}_\eta\big| < \underset{\cdot}{\omega}\big)\,, \tag{$\substack{*\\*}$}$$
then the set $\big\{r \geq p_\xi : r \Vdash_{\mathbb{C}} |\underset{\cdot}{A}_\xi \cap \underset{\sim}{x}_\xi| = \underset{\cdot}{\omega}\big\}$ is dense above p_ξ.

To see that A_ξ may be chosen that way, notice that whenever $(\substack{*\\*})$ fails, then we just have to take care of (1) and we simply apply the fact that ξ is countable and therefore the almost disjoint family $\{A_\eta : \eta \in \xi\}$ cannot be maximal. On the other hand, if $(\substack{*\\*})$ holds, then whenever g is $\mathbb{C}$-generic over $\mathbf{V}$ and $p_\xi \in g$ we have
$$\mathbf{V}[g] \vDash \underset{\sim}{x}_\xi[g] \in [\omega]^\omega \wedge \forall \eta \in \xi \big(\big|\underset{\sim}{x}_\xi[g] \cap A_\eta\big| < \omega\big)\,.$$
In other words, $\underset{\sim}{x}_\xi[g]$ witnesses that the almost disjoint family $\{A_\eta : \eta \in \xi\}$ is not maximal in $\mathbf{V}[g]$.

Now, we construct A_ξ, satisfying (1), such that $\mathbf{V}[g] \vDash |\underset{\sim}{x}_\xi[g] \cap A_\xi| = \omega$: For this, let $\{B_i : i \in \omega\}$ be an enumeration of the set $\{A_\eta : \eta \in \xi\}$ and let $\big\{\langle n_i, q_i\rangle : i \in \omega\big\}$ be an enumeration of $\omega \times \big\{q : q \geq p_\xi\big\}$. By $(\substack{*\\*})$, for each $i \in \omega$ we obviously have
$$q_i \Vdash_{\mathbb{C}} \big|\underset{\sim}{x}_\xi \setminus (\underset{\cdot}{B}_0 \cup \ldots \cup \underset{\cdot}{B}_i)\big| = \underset{\cdot}{\omega}\,.$$
Thus, we find a $\mathbb{C}$-condition $r_i \geq q_i$ as well as an integer $m_i \geq n_i$ such that $m_i \notin \big(B_0 \cup \ldots \cup B_i\big)$ and $r_i \Vdash_{\mathbb{C}} \underset{\cdot}{m}_i \in \underset{\sim}{x}_\xi$, and define $A_\xi := \{m_i : i \in \omega\}$. What have we achieved? By $(\substack{*\\*})$, for every $q \geq p_\xi$, every $n \in \omega$, and every finite set $\{\eta_0, \ldots, \eta_k\} \subseteq \xi$, there is a condition $q' \geq q$ and an integer $m \geq n$ such $q' \Vdash_{\mathbb{C}} m \in \underset{\sim}{x}_\xi \wedge \underset{\cdot}{m} \notin \bigcup_{i \in k} \underset{\cdot}{A}_{\eta_i}$. Thus, $\underset{\sim}{x}_\xi[g]$ is not a witness for the statement "$\{A_\eta : \eta \in \xi + 1\}$ is not a *mad* family in $\mathbf{V}[g]$", which implies that $\mathscr{A}_0 = \{A_\xi \in [\omega]^\omega : \xi \in \omega_1\}$ is in fact a *mad* family in $\mathbf{V}[g]$. In other words, $\mathscr{A}_0$ is a *mad* family in $\mathbf{V}$ which remains *mad* after adding a single Cohen real. In the next step we show that the same is true even if we add many Cohen reals.

$\mathscr{A}_0$ is mad in $\mathbf{V}[G]$: Consider now the forcing notion $\mathbb{C}_\kappa$. Let G be $\mathbb{C}_\kappa$-generic over $\mathbf{V}$ and assume towards a contradiction that
$$\mathbf{V}[G] \vDash \exists x \in [\omega]^\omega\, \forall A_\xi \in \mathscr{A}_0 \,\big(|x \cap A_\xi| < \omega\big)\,.$$
Then there would be a $\mathbb{C}_\kappa$-name $\underset{\sim}{x}$ for a subset of ω and a $\mathbb{C}_\kappa$-condition p such that for all $\xi \in \omega_1$,
$$p \Vdash_{\mathbb{C}_\kappa} |\underset{\sim}{x}| = \underset{\cdot}{\omega} \ \wedge\ |\underset{\sim}{x} \cap \underset{\cdot}{A}_\xi| < \underset{\cdot}{\omega}\,.$$
By the facts proved earlier and since $\mathbb{C}_\kappa$ satisfies *ccc* and every $\mathbb{C}_\kappa$-condition is finite, there is a countable set $I_0 \subseteq \kappa$ such that, with respect to $\mathbb{C}_{I_0} =$

$\big(\mathrm{Fn}(\omega \times I_0, 2), \subseteq\big)$, there is a nice $\mathbb{C}_{I_0}$-name $\underset{\sim}{x}_0$ for a subset of ω as well as a $\mathbb{C}_{I_0}$-condition p_0 such that for all $\xi \in \omega_1$,

$$p_0 \Vdash_{\mathbb{C}_{I_0}} |\underset{\sim}{x}_0| = \underset{\cdot}{\omega} \ \wedge\ |\underset{\sim}{x}_0 \cap \underset{\cdot}{A}_\xi| < \underset{\cdot}{\omega}\,.$$

By PROPOSITION 18.3, $\mathbb{C} \approx \mathbb{C}_{I_0}$, and hence we can replace $\mathbb{C}_{I_0}$ by $\mathbb{C}$. Thus, there exists a pair $\langle p_{\xi_0}, \underset{\sim}{x}_{\xi_0}\rangle$, consisting of a $\mathbb{C}$-condition p_{ξ_0} and a nice name $\underset{\sim}{x}_{\xi_0}$ for a subset of ω, such that for all $\xi \in \omega_1$,

$$p_{\xi_0} \Vdash_{\mathbb{C}} |\underset{\sim}{x}_{\xi_0}| = \underset{\cdot}{\omega} \ \wedge\ |\underset{\sim}{x}_{\xi_0} \cap \underset{\cdot}{A}_\xi| < \underset{\cdot}{\omega}\,.$$

In particular, for A_{ξ_0} we would have

$$p_{\xi_0} \Vdash_{\mathbb{C}} |\underset{\sim}{x}_{\xi_0} \cap \underset{\cdot}{A}_{\xi_0}| < \underset{\cdot}{\omega}\,,$$

which contradicts the construction of A_{ξ_0}. $\dashv$

For a proof using iterated forcing (introduced below) see RELATED RESULT 99.

Iterations

Below, we shall develop some methods to add generic filters step by step. The simplest case, which we consider first, is when only two generic filters are added. This so-called two-step iteration is quite easy to understand, but because it involves most of the tools which are used to handle longer iterations, it is worthwhile to consider this case in greater detail. Nevertheless, the situation becomes more difficult when the length of the iteration is infinite — which will be discussed in a slightly less detailed way.

Two-Step Iterations

Let us start with an example: Let $\mathbf{V}$ be a model of ZFC. Assume we want to construct an infinite set $H \subseteq \omega$ in some generic extension of $\mathbf{V}$ which is almost homogeneous for each colouring $\pi : [\omega]^n \to r$ which belongs to $\mathbf{V}$ (where $n \in \omega$ and r is a positive integer). Recall that an infinite set $H \subseteq \omega$ is almost homogeneous for a colouring $\pi : [\omega]^n \to r$, if there is a finite set $K \in \mathrm{fin}(\omega)$ such that $[H \setminus K]^n$ is monochromatic. There are many different ways to obtain such a real H. For example, if there is a Ramsey ultrafilter $\mathscr{U}$ in $\mathbf{V}$, then it would be enough to force the existence of a set $H \in [\omega]^\omega$ which is almost contained in each $x \in \mathscr{U}$. Why? Since $\mathscr{U}$ is a Ramsey ultrafilter, for every colouring $\pi : [\omega]^n \to r$ there is an $x \in \mathscr{U}$ which is homogeneous for π. Now, if H is almost contained in x, then H is almost homogeneous for π. However, if there is no Ramsey ultrafilter in $\mathbf{V}$ (see for example PROPOSITION 25.11), we first have to force the existence of a Ramsey ultrafilter. In order to force a Ramsey ultrafilter we use the forcing notion $\mathbb{U} = \big([\omega]^\omega/\,\mathrm{fin}, \leq\big)$ which was introduced in Chapter 14. Let G_0 be $\mathbb{U}$-generic over $\mathbf{V}$ and let $\mathscr{U} = \bigcup G_0$. Then, by PROPOSITION 14.18, $\mathscr{U}$ is a Ramsey ultrafilter in $\mathbf{V}[G_0]$. Now, we force the existence of a set $H \in [\omega]^\omega$ which is almost contained in each $x \in \mathscr{U}$: In $\mathbf{V}[G_0]$, consider the forcing notion $\mathbb{Q}_{\mathscr{U}} = (Q_{\mathscr{U}}, \leq)$, where $Q_{\mathscr{U}}$ is the set of all ordered pairs $\langle s, E\rangle$ such that $s \in \text{fin}(\omega)$ and $E \in \text{fin}(\mathscr{U})$, and for all $\langle s, E\rangle, \langle t, F\rangle \in Q_{\mathscr{U}}$ we define

$$\langle s, E\rangle \leq \langle t, F\rangle \iff s \subseteq t \wedge E \subseteq F \wedge (t \setminus s) \subseteq \bigcap E\,.$$

If G_1 is $\mathbb{Q}_{\mathscr{U}}$-generic over $\mathbf{V}[G_0]$, then the set

$$H_0 = \bigcup \bigl\{ s \in \text{fin}(\omega) : \exists E \in \text{fin}(\mathscr{U}) \bigl(\langle s, E\rangle \in G_1\bigr)\bigr\}\,,$$

which belongs to the model $\mathbf{V}[G_0][G_1]$, is almost homogeneous for all colourings $\pi : [\omega]^n \to r$ which belong to $\mathbf{V}$.

Notice that the forcing notion $\mathbb{Q}_{\mathscr{U}}$ belongs to $\mathbf{V}[G_0]$, so, there is a $\mathbb{U}$-name $\underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$ in $\mathbf{V}$ for $\mathbb{Q}_{\mathscr{U}}$. Forcing first with $\mathbb{U}$ over $\mathbf{V}$, followed by forcing with $\mathbb{Q}_{\mathscr{U}}$ over $\mathbf{V}[G_0]$, is a two-step "process" which we shall denote by $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$. The goal is now to find a forcing notion $\mathbb{P}$ in $\mathbf{V}$ such that $\mathbb{P}$ is equivalent to $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$, in other words, the goal is to write the two-step "process" $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$ as a single forcing extension over the ground model $\mathbf{V}$.

More generally, we have the following situation: We start in some ground model $\mathbf{V}$ of ZFC, where in $\mathbf{V}$ we have a forcing notion $\mathbb{P} = (P, \leq_{\mathbb{P}}, \mathbf{0}_{\mathbb{P}})$. If G is $\mathbb{P}$-generic over $\mathbf{V}$, then $\mathbf{V}[G]$ is again a model of ZFC. Assume that $\mathbb{Q} = (Q, \leq_{\mathbb{Q}}, \mathbf{0}_{\mathbb{Q}})$ is a forcing notion in $\mathbf{V}[G]$ (which is not necessarily in $\mathbf{V}$) and that H is $\mathbb{Q}$-generic over $\mathbf{V}[G]$. Then $\mathbf{V}[G][H]$ is a model of ZFC, too.

Since $\mathbb{Q}$ belongs to $\mathbf{V}[G]$, there is a $\mathbb{P}$-name $\underset{\sim}{\mathbb{Q}}$ in $\mathbf{V}$ for $\mathbb{Q}$. So, by combining the conditions in P with $\mathbb{P}$-names for $\mathbb{Q}$-conditions, it should be possible to write the so-called *two-step iteration* $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$ as a single forcing notion $\mathbb{R}$ which belongs to the ground model $\mathbf{V}$. Furthermore, it would be interesting to know whether some combinatorial properties of $\mathbb{P}$ and $\mathbb{Q}$ are preserved in the two-step iteration. For example, if $\mathbb{P}$ and $\mathbb{Q}$ both satisfy *ccc*, does this imply that $\mathbb{R}$ also satisfies *ccc*? Before we can answer this question (in the affirmative), we first have to show that $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$ is indeed equivalent to a single forcing notion which belongs to $\mathbf{V}$ — which is consequently denoted by $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$.

Let $\mathbf{V}$ be a model of ZFC and let $\mathbb{P} = (P, \leq_{\mathbb{P}}, \mathbf{0})$ be a forcing notion in $\mathbf{V}$ with smallest element $\mathbf{0}$. Notice that by FACT 14.4 we may always assume that the smallest element of a forcing notion is $\emptyset$, *i.e.*, $\mathbf{0} = \emptyset$. A $\mathbb{P}$-name in $\mathbf{V}$ for a forcing notion $\mathbb{Q} = (Q, \preccurlyeq, \emptyset)$ in the $\mathbb{P}$-generic extension of $\mathbf{V}$ is a triple of $\mathbb{P}$-names $\langle \underset{\sim}{Q}, \underset{\sim}{\preccurlyeq}, \underset{\cdot}{\emptyset}\rangle$ which has the following properties:

(a) $\emptyset \Vdash_{\mathbb{P}}$ "$\underset{\sim}{\preccurlyeq}$ is a partial ordering of $\underset{\sim}{Q}$" (recall that a partial ordering is a binary relation which is transitive, reflexive, and anti-symmetric).

(b) If $p \Vdash_{\mathbb{P}} \underset{\sim}{q} \in \underset{\sim}{Q}$ for some $\mathbb{P}$-name $\underset{\sim}{q}$, then there is a $\mathbb{P}$-condition p' such that $p \leq_{\mathbb{P}} p'$, and there are $\mathbb{P}$-names $\underset{\sim}{r}_1$ and $\underset{\sim}{r}_2$ such that

$$p' \Vdash_{\mathbb{P}} \underset{\sim}{r}_1 \in \underset{\sim}{Q} \wedge \underset{\sim}{r}_2 \in \underset{\sim}{Q} \wedge \underset{\sim}{q} \underset{\sim}{\preccurlyeq} \underset{\sim}{r}_1 \wedge \underset{\sim}{q} \underset{\sim}{\preccurlyeq} \underset{\sim}{r}_2 \wedge \underset{\sim}{r}_1 \underset{\sim}{\perp} \underset{\sim}{r}_2\,.$$

(c) $\emptyset \Vdash_{\mathbb{P}} \underset{\cdot}{\emptyset} \in \underset{\sim}{Q}$.

(d) If $p \Vdash_{\mathbb{P}} \underset{\sim}{q} \in \underset{\sim}{Q}$, then $p \Vdash_{\mathbb{P}} \underset{\cdot}{\emptyset} \underset{\sim}{\precsim} \underset{\sim}{q}$.

Now, we first define a forcing notion $\mathbb{R}$ in $\mathbf{V}$, which depends on $\mathbb{P}$ & $\underset{\sim}{\mathbb{Q}}$, and then we show that forcing with $\mathbb{R}$ yields the same generic extension as the two-step iteration $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$.

Let $\mathbb{R} = (R, \leq_{\mathbb{R}}, \mathbf{0}_{\mathbb{R}})$ where

$$R = \left\{ \langle p, \underset{\sim}{q} \rangle : p \in P \wedge p \Vdash_{\mathbb{P}} \underset{\sim}{q} \in \underset{\sim}{Q} \right\} \quad \text{and} \quad \mathbf{0}_{\mathbb{R}} = \langle \emptyset, \underset{\cdot}{\emptyset} \rangle \,,$$

and for all $\langle p_1, \underset{\sim}{q_1} \rangle, \langle p_2, \underset{\sim}{q_2} \rangle \in R$, let

$$\langle p_1, \underset{\sim}{q_1} \rangle \leq_{\mathbb{R}} \langle p_2, \underset{\sim}{q_2} \rangle \iff p_1 \leq_{\mathbb{P}} p_2 \wedge p_2 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \underset{\sim}{\precsim} \underset{\sim}{q_2} \,.$$

Before we show that forcing with $\mathbb{R}$ is equivalent to $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$, we have to show that $\mathbb{R} = (R, \leq_{\mathbb{R}}, \mathbf{0}_{\mathbb{R}})$ is a forcing notion with smallest element $\mathbf{0}_{\mathbb{R}}$.

For this, we first show that the binary relation $\leq_{\mathbb{R}}$ is a partial ordering, *i.e.*, we show that $\leq_{\mathbb{R}}$ is (1) reflexive, (2) transitive, and (3) has the property that

$$\big(\langle p_1, \underset{\sim}{q_1} \rangle \leq_{\mathbb{R}} \langle p_2, \underset{\sim}{q_2} \rangle \wedge \langle p_2, \underset{\sim}{q_2} \rangle \leq_{\mathbb{R}} \langle p_1, \underset{\sim}{q_1} \rangle \big) \to (p_1 = p_2)$$

and that $p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} = \underset{\sim}{q_2}$: For (1)–(3), let $\langle p, \underset{\sim}{q} \rangle, \langle p_1, \underset{\sim}{q_1} \rangle, \langle p_2, \underset{\sim}{q_2} \rangle$, $\langle p_3, \underset{\sim}{q_3} \rangle$, be arbitrary $\mathbb{R}$-conditions.

(1) $\langle p, \underset{\sim}{q} \rangle \leq_{\mathbb{R}} \langle p, \underset{\sim}{q} \rangle \iff p \leq_{\mathbb{P}} p \wedge p \Vdash_{\mathbb{P}} \underset{\sim}{q} \underset{\sim}{\precsim} \underset{\sim}{q}$.

Since $\leq_{\mathbb{P}}$ is a partial ordering, $p \leq_{\mathbb{P}} p$, and by (a) we have $p \Vdash_{\mathbb{P}} \underset{\sim}{q} \underset{\sim}{\precsim} \underset{\sim}{q}$.

(2) $\langle p_1, \underset{\sim}{q_1} \rangle \leq_{\mathbb{R}} \langle p_2, \underset{\sim}{q_2} \rangle \wedge \langle p_2, \underset{\sim}{q_2} \rangle \leq_{\mathbb{R}} \langle p_3, \underset{\sim}{q_3} \rangle \iff$

$$\underbrace{p_1 \leq_{\mathbb{P}} p_2 \wedge p_2 \leq_{\mathbb{P}} p_3}_{\text{which implies } p_1 \leq_{\mathbb{P}} p_3} \wedge \underbrace{p_2 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \underset{\sim}{\precsim} \underset{\sim}{q_2} \wedge p_3 \Vdash_{\mathbb{P}} \underset{\sim}{q_2} \underset{\sim}{\precsim} \underset{\sim}{q_3}}_{\text{since } p_2 \leq_{\mathbb{P}} p_3 \text{ we get } p_3 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \underset{\sim}{\precsim} \underset{\sim}{q_2} \wedge \underset{\sim}{q_2} \underset{\sim}{\precsim} \underset{\sim}{q_3}}$$

By (a) we get $p_3 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \underset{\sim}{\precsim} \underset{\sim}{q_3}$, and hence, $\langle p_1, \underset{\sim}{q_1} \rangle \leq_{\mathbb{R}} \langle p_3, \underset{\sim}{q_3} \rangle$.

(3) $\langle p_1, \underset{\sim}{q_1} \rangle \leq_{\mathbb{R}} \langle p_2, \underset{\sim}{q_2} \rangle \wedge \langle p_2, \underset{\sim}{q_2} \rangle \leq_{\mathbb{R}} \langle p_1, \underset{\sim}{q_1} \rangle \iff$

$$\underbrace{p_1 \leq_{\mathbb{P}} p_2 \wedge p_2 \leq_{\mathbb{P}} p_1}_{\text{which implies } p_1 = p_2} \wedge \underbrace{p_2 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \underset{\sim}{\precsim} \underset{\sim}{q_2} \wedge p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_2} \underset{\sim}{\precsim} \underset{\sim}{q_1}}_{\text{since } p_1 = p_2 \text{ we get } p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \underset{\sim}{\precsim} \underset{\sim}{q_2} \wedge \underset{\sim}{q_2} \underset{\sim}{\precsim} \underset{\sim}{q_1}}$$

By (a), $\underset{\sim}{\precsim}$ is forced to be anti-symmetric, thus, $p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} = \underset{\sim}{q_2}$.

Now, we show that $\mathbf{0}_{\mathbb{R}}$ (*i.e.*, $\langle \emptyset, \underset{\cdot}{\emptyset} \rangle$) belongs to R and that $\mathbf{0}_{\mathbb{R}}$ is the smallest element (with respect to the partial ordering $\leq_{\mathbb{R}}$):

- $\langle \emptyset, \underset{\cdot}{\emptyset} \rangle \in R \iff \emptyset \Vdash_{\mathbb{P}} \underset{\cdot}{\emptyset} \in \underset{\sim}{Q}$, which is just (c).
- Let $\langle p, \underset{\sim}{q} \rangle$ be an arbitrary $\mathbb{R}$-condition. Since $\langle p, \underset{\sim}{q} \rangle \in R$ we have $p \Vdash_{\mathbb{P}} \underset{\sim}{q} \in \underset{\sim}{Q}$, and further we have $\langle \emptyset, \underset{\cdot}{\emptyset} \rangle \leq_{\mathbb{R}} \langle p, \underset{\sim}{q} \rangle \iff p \Vdash_{\mathbb{P}} \underset{\cdot}{\emptyset} \underset{\sim}{\precsim} \underset{\sim}{q}$, which is in fact just (d).

Finally, we show that $\mathbb{R} = (R, \leq_{\mathbb{R}})$ is indeed a forcing notion: For this we have to show that there are incompatible conditions above each $\langle p, \underset{\sim}{q} \rangle \in R$. Let $p_1, p_2 \in P$ be such that $p \leq_{\mathbb{P}} p_1$, $p \leq_{\mathbb{P}} p_2$, and $p_1 \perp_{\mathbb{P}} p_2$. Then $\langle p, \underset{\sim}{q} \rangle \leq_{\mathbb{R}} \langle p_1, \underset{\sim}{q} \rangle$, $\langle p, \underset{\sim}{q} \rangle \leq_{\mathbb{R}} \langle p_2, \underset{\sim}{q} \rangle$, and $\langle p_1, \underset{\sim}{q} \rangle \perp_{\mathbb{R}} \langle p_2, \underset{\sim}{q} \rangle$, as required.

It remains to show that forcing with $\mathbb{R}$ is equivalent to the two-step iteration $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$. We shall give a detailed proof of one direction and leave the other direction as an exercise to the reader.

Proposition 18.6. *Let* $\mathbf{V}$ *be a model of* ZFC *and let* G *be* $\mathbb{R}$*-generic over* $\mathbf{V}$*. Then there are sets* G_0 *and* G_1 *in* $\mathbf{V}[G]$*, such that* G_0 *is* $\mathbb{P}$*-generic over* $\mathbf{V}$ *and* G_1 *is* $\underset{\sim}{\mathbb{Q}}[G_0]$*-generic over* $\mathbf{V}[G_0]$*.*

Proof. In the model $\mathbf{V}[G]$ we define

$$G_0 = \big\{ p \in P : \exists \underset{\sim}{q} \in \underset{\sim}{Q} (\langle p, \underset{\sim}{q} \rangle \in G) \big\}$$

and

$$G_1 = \big\{ \underset{\sim}{q}[G_0] \in \underset{\sim}{Q}[G_0] : \exists p \in G_0 (\langle p, \underset{\sim}{q} \rangle \in G) \big\}\,.$$

We first show that G_0 and G_1 are filters, *i.e.*, G_0 and G_1 are both downwards closed and directed.

G_0 *is downwards closed and directed*: If $p \in G_0$, then there is a $\underset{\sim}{q} \in \underset{\sim}{Q}$ such that $\langle p, \underset{\sim}{q} \rangle \in G$, and for any $p' \leq p$ we have $\langle p', \underset{\sim}{\emptyset} \rangle \leq \langle p, \underset{\sim}{q} \rangle$. Since G is downwards closed, this implies $\langle p', \underset{\sim}{\emptyset} \rangle \in G$, and therefore $p' \in G_0$. Furthermore, if p_0 and p_1 belong to G_0, then we find $\langle p_0, \underset{\sim}{q_0} \rangle$ and $\langle p_1, \underset{\sim}{q_1} \rangle$ in G, and since G is directed, there is an $\mathbb{R}$-condition $\langle p, \underset{\sim}{q} \rangle \in G$ such that $\langle p_0, \underset{\sim}{q_0} \rangle \leq \langle p, \underset{\sim}{q} \rangle \geq \langle p_1, \underset{\sim}{q_1} \rangle$. Thus, $p \in G_0$ and $p_0 \leq p \geq p_1$.

G_1 *is downwards closed and directed*: If $\underset{\sim}{q_0}[G_0] \in G_1$, then there is a $p_0 \in G_0$ such that $\langle p_0, \underset{\sim}{q_0} \rangle \in G$. Assume that in $\mathbf{V}[G_0]$, $\underset{\sim}{q_1}[G_0] \leq \underset{\sim}{q_0}[G_0]$. We have to show that $\underset{\sim}{q_1}[G_0] \in G_1$. Firstly, there is a $p' \in G_0$ such that $p' \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \leq \underset{\sim}{q_0}$. Secondly, since G is directed, there is a $\langle p_1, \underset{\sim}{q_2} \rangle \in G$ such that $\langle p', \underset{\sim}{\emptyset} \rangle \leq \langle p_1, \underset{\sim}{q_2} \rangle \geq \langle p_0, \underset{\sim}{q_0} \rangle$, in particular we get $p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_0} \leq \underset{\sim}{q_2}$. Now, since $p_1 \geq p'$, we also have $p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \leq \underset{\sim}{q_0}$. Thus, $p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q_1} \leq \underset{\sim}{q_2}$, which implies $\langle p_1, \underset{\sim}{q_2} \rangle \geq \langle p_1, \underset{\sim}{q_1} \rangle$, and since G is downwards closed, $\langle p_1, \underset{\sim}{q_1} \rangle \in G$. Hence, $\underset{\sim}{q_1}[G_0] \in G_1$. Furthermore, if $\underset{\sim}{q_0}[G_0]$ and $\underset{\sim}{q_1}[G_0]$ belong to G_1, then we find $\langle p_0, \underset{\sim}{q_0} \rangle$ and $\langle p_1, \underset{\sim}{q_1} \rangle$ in G, and since G is directed, there is an $\mathbb{R}$-condition $\langle p, \underset{\sim}{q} \rangle \in G$ — and therefore $\underset{\sim}{q}[G_0] \in G_1$ — such that $\langle p_0, \underset{\sim}{q_0} \rangle \leq \langle p, \underset{\sim}{q} \rangle \geq \langle p_1, \underset{\sim}{q_1} \rangle$. Thus, $p \Vdash_{\mathbb{P}} \underset{\sim}{q_0} \leq \underset{\sim}{q} \geq \underset{\sim}{q_1}$, and since $p \in G_0$ we get $\underset{\sim}{q_0}[G_0] \leq \underset{\sim}{q}[G_0] \geq \underset{\sim}{q_1}[G_0]$.

Now we show that G_0 and G_1 are generic, *i.e.*, G_0 and G_1 meet every open dense set in $\mathbf{V}$ and $\mathbf{V}[G_0]$ respectively.

G_0 *is generic*: Let $D_0 \subseteq P$ be an open dense subset of P and let

$$D_0' = \big\{ \langle p, \underset{\sim}{q} \rangle \in R : p \in D_0 \big\}\,.$$

Then D_0' is an open dense subset of R, and since G is $\mathbb{R}$-generic over $\mathbf{V}$, there is an $\mathbb{R}$-condition $\langle p, \underset{\sim}{q} \rangle \in G$ — and therefore $p \in G_0$ — such that p belongs to D_0. Hence, $G_0 \cap D_0 \neq \emptyset$, which shows that G_0 is $\mathbb{P}$-generic over $\mathbf{V}$.

G_1 *is generic*: Let D_1 be an arbitrary open dense subset of $\underset{\sim}{Q}[G_0]$. Then there is a $\mathbb{P}$-name $\underset{\sim}{D}_1$ for D_1 and a $\mathbb{P}$-condition $p_0 \in G_0$ such that

$$p_0 \Vdash_{\mathbb{P}} \text{“}\underset{\sim}{D}_1 \textit{ is open dense in } \underset{\sim}{Q}\text{”}.$$

With respect to $\underset{\sim}{D}_1$ define

$$D_1' = \bigl\{\langle p, \underset{\sim}{q}\rangle \in R : p \Vdash_{\mathbb{P}} \underset{\sim}{q} \in \underset{\sim}{D}_1\bigr\}.$$

Then $D_1' \subseteq R$ is open dense above $\langle p_0, \underset{\cdot}{\emptyset}\rangle$, and since $\langle p_0, \underset{\cdot}{\emptyset}\rangle \in G$ (because $p_0 \in G_0$), we get that $G \cap D_1' \neq \emptyset$, say $\langle p_1, \underset{\sim}{q}_1\rangle \in G \cap D_1'$. Now, $\langle p_1, \underset{\sim}{q}_1\rangle \in G$ implies that $p_1 \in G_0$ and that $\underset{\sim}{q}_1[G_0] \in G_1$. Furthermore, by definition of D_1' we get $p_1 \Vdash_{\mathbb{P}} \underset{\sim}{q}_1 \in \underset{\sim}{D}_1$, and therefore $\underset{\sim}{q}_1[G_0] \in D_1$. Hence, $\underset{\sim}{q}_1[G_0] \in G_1 \cap D_1$, which shows that G_1 is $\underset{\sim}{\mathbb{Q}}[G_0]$-generic over $\mathbf{V}[G_0]$. ⊣

In the next section we shall investigate general iterations, but before let us show that two-step iterations of *ccc* forcing notions satisfy *ccc*.

LEMMA 18.7. *If $\mathbb{P}$ satisfies ccc and*

$$\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} \text{“}\underset{\sim}{\mathbb{Q}} \textit{ satisfies ccc}\text{”}$$

then also $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$ satisfies ccc.

Proof. Let $\mathbb{P} = (P, \leq)$ and let $\underset{\sim}{\mathbb{Q}} = (\underset{\sim}{Q}, \underset{\sim}{\preccurlyeq})$. Assume towards a contradiction that in the ground model $\mathbf{V}$ there are uncountably many pairwise incompatible $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$-conditions $\bigl\{\langle p_\xi, \underset{\sim}{q}_\xi\rangle : \xi \in \omega_1\bigr\}$. Let $\underset{\sim}{x} = \bigl\{\langle \underset{\cdot}{\xi}, p_\xi\rangle : \xi \in \omega_1\bigr\}$; then $\underset{\sim}{x}$ is a $\mathbb{P}$-name for a subset of ω_1, *i.e.*, $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \underset{\cdot}{\omega}_1$. Let G be $\mathbb{P}$-generic over $\mathbf{V}$. Then $\underset{\sim}{x}[G] = \{\xi \in \omega_1 : p_\xi \in G\}$. We shall show that there is an ordinal $\beta \in \omega_1$ such that $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \underset{\cdot}{\beta}$, but first we prove the following

CLAIM 1. *In $\mathbf{V}[G]$, the set $\bigl\{\underset{\sim}{q}_\xi[G] : \xi \in \underset{\sim}{x}[G]\bigr\}$ is an anti-chain in $\underset{\sim}{Q}[G]$.*

Proof of Claim 1. Assume towards a contradiction that there are distinct $\xi, \eta \in \underset{\sim}{x}[G]$, such that $\underset{\sim}{q}_\xi[G]$ and $\underset{\sim}{q}_\eta[G]$ are compatible elements of $\underset{\sim}{Q}[G]$. This would imply that there is a $\mathbb{P}$-condition $p \in G$, as well as a $\mathbb{P}$-name $\underset{\sim}{q}$ for a $\underset{\sim}{\mathbb{Q}}[G]$-condition, such that

$$p \Vdash_{\mathbb{P}} \underset{\sim}{q} \in \underset{\sim}{Q} \wedge \underset{\sim}{q}_\xi \underset{\sim}{\preccurlyeq} \underset{\sim}{q} \wedge \underset{\sim}{q}_\eta \underset{\sim}{\preccurlyeq} \underset{\sim}{q}.$$

In fact, by extending p if necessary, we get a $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$-condition $\langle p, \underset{\sim}{q}\rangle$ which is stronger than both $\langle p_\xi, \underset{\sim}{q}_\xi\rangle$ and $\langle p_\eta, \underset{\sim}{q}_\eta\rangle$, contradicting our assumption that $\bigl\{\langle p_\xi, \underset{\sim}{q}_\xi\rangle : \xi \in \omega_1\bigr\}$ is a set of pairwise incompatible $\mathbb{P} * \underset{\sim}{\mathbb{Q}}$-conditions. $\dashv_{\text{Claim 1}}$

Since $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}}$ “$\underset{\sim}{\mathbb{Q}}$ *satisfies ccc*”, and therefore preserves ω_1 (by LEMMA 14.20), we get that $\mathbf{V}[G] \vDash \bigl|\underset{\sim}{x}[G]\bigr| < \omega_1$ whenever G is $\mathbb{P}$-generic over $\mathbf{V}$, hence, $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} |\underset{\sim}{x}| < \underset{\cdot}{\omega}_1$.

CLAIM 2. *There is an ordinal $\beta \in \omega_1$ such that $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \underset{\cdot}{\beta}$.*

Proof of Claim 2. In $\mathbf{V}$, let

$$E = \left\{\alpha \in \omega_1 : \exists r \in P \,\forall \beta \in \alpha\big(r \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \dot{\alpha} \wedge \underset{\sim}{x} \nsubseteq \dot{\beta}\big)\right\}.$$

Further, for every $\alpha \in E$ choose a $\mathbb{P}$-condition r_α such that for all $\beta \in \alpha$, $r_\alpha \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \dot{\alpha} \wedge \underset{\sim}{x} \nsubseteq \dot{\beta}$. The set $\{r_\alpha : \alpha \in E\}$, which belongs to $\mathbf{V}$, is an antichain in P, and since $\mathbb{P}$ satisfies *ccc*, $|E| < \omega_1$. Thus, there exists a $\beta \in \omega_1$ such that $E \subseteq \beta$, which implies that $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \dot{\beta}$. $\dashv_{\text{Claim 2}}$

By definition of $\underset{\sim}{x}$, for all $\xi \in \omega_1$ we have $p_\xi \Vdash_{\mathbb{P}} \dot{\xi} \in \underset{\sim}{x}$. In particular we get $p_\beta \Vdash_{\mathbb{P}} \dot{\beta} \in \underset{\sim}{x}$, which is a contradiction to $\mathbf{0}_{\mathbb{P}} \Vdash_{\mathbb{P}} \underset{\sim}{x} \subseteq \dot{\beta}$. $\dashv$

As a matter of fact we would like to mention that LEMMA 18.7 does not have an analogue for products; in other words, the product of two *ccc* forcing notions does not necessarily satisfy *ccc* (see RELATED RESULT 98).

General Iterations

In the previous section we have constructed a two-step iteration $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$ in such a way that whenever G is $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$-generic over $\mathbf{V}$, then there is an infinite set $H_0 \in [\omega]^\omega \cap \mathbf{V}[G]$ which is almost homogeneous for all colourings $\pi : [\omega]^n \to r$ which belong to the ground model $\mathbf{V}$. Obviously, such a set H_0 cannot belong to $\mathbf{V}$. Now, we can ask what happens if we iterate the forcing notion $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$? As we have seen, at each stage we obtain a new set $H \in [\omega]^\omega$ which is almost homogeneous for all "old" colourings $\pi : [\omega]^n \to r$. So, for example an ω_1-stage iteration of $\mathbb{U} * \underset{\sim}{\mathbb{Q}}_{\mathscr{U}}$, starting in a model $\mathbf{V}$ of ZFC in which $\mathfrak{c} = \omega_2$, would generate a family $\{H_\alpha : \alpha \in \omega_1\}$ of size $\omega_1^{\mathbf{V}}$, where each H_α is almost homogeneous with respect to all "old" colourings $\pi : [\omega]^n \to r$. Recall that for any integers $n, r \geq 2$ there exists a bijection between the set of colourings $\pi : [\omega]^n \to r$ and the set of real numbers, thus, every "old" colouring can be encoded by an "old" real (and vice versa). Now, if every colouring $\pi : [\omega]^n \to r$ (*i.e.*, real number) appears at some stage $\alpha \in \omega_1$ in the iteration, and if the cardinal numbers $\omega_1^{\mathbf{V}}$, $\omega_2^{\mathbf{V}}$, $\mathfrak{c}^{\mathbf{V}}$ are the same as ω_1, ω_2, $\mathfrak{c}$ in the final generic extension, then we would get a model in which $\omega_1 = \mathfrak{hom} < \omega_2 = \mathfrak{c}$. But do we really get such a model?

To understand the previous example as well as iterations in general, we have to answer questions like:

1. Is every iteration of forcing notions equivalent to a single forcing notion?
2. How is the iteration defined at limit stages?
3. Does the iteration add reals at limit stages of uncountable cofinality?
4. Does the iteration preserve cardinals?

Below, we shall give a complete answer to Questions 1–3 and we shall give an answer to Question 4 with respect to forcing notions satisfying *ccc*; regarding the forcing notion $\mathbb{U} * \underset{\sim}{\mathbb{Q}}$, we refer the reader to Chapter 20 and Chapter 23 | RELATED RESULT 138.

Let us now consider α-stage iterations of forcing notions for arbitrary ordinals α (recall that by FACT 14.4 we may always assume that the smallest element of a forcing notion is $\emptyset$).

For $\alpha = 1$ we get ordinary forcing, and for $\alpha = 2$ we get two-step iterations which we already discussed in the previous section.

For $\alpha = 3$ we start with an arbitrary forcing notion $\mathbb{P}_1 = (P_1, \leq)$ which belongs to some ground model $\mathbf{V}$. Let $\underset{\sim}{\mathbb{Q}}_1$ be a $\mathbb{P}_1$-name for a forcing notion $(Q_1, \leq)$ in the $\mathbb{P}_1$-generic extension of $\mathbf{V}$ and let $\mathbb{P}_2 := \mathbb{P}_1 * \underset{\sim}{\mathbb{Q}}_1$. Further, let $\underset{\sim}{\mathbb{Q}}_2$ be a $\mathbb{P}_2$-name for a forcing notion $(Q_2, \leq)$ in the $\mathbb{P}_2$-generic extension of $\mathbf{V}$ and let $\mathbb{P}_3 := \mathbb{P}_2 * \underset{\sim}{\mathbb{Q}}_2$. Then every $\mathbb{P}_3$-condition is of the form $\big\langle\langle q_0, \underset{\sim}{q}_1\rangle, \underset{\sim}{q}_2\big\rangle$, where $q_0 \in P_1$, $q_0 \Vdash_{\mathbb{P}_1} \underset{\sim}{q}_1 \in \underset{\sim}{Q}_1$, and $\langle q_0, \underset{\sim}{q}_1\rangle \Vdash_{\mathbb{P}_2} \underset{\sim}{q}_2 \in \underset{\sim}{Q}_2$.

To form an α-stage iteration for $3 < \alpha \in \omega$, we just repeat this procedure. Thus, for positive integers n, every $\mathbb{P}_n$-condition is of the form $\langle\langle\cdots\langle\langle q_0, \underset{\sim}{q}_1\rangle, \underset{\sim}{q}_2\rangle \cdots \underset{\sim}{q}_{n-2}\rangle, \underset{\sim}{q}_{n-1}\rangle$, for which we shall write the typographically less cumbersome (and easier to read) n-tuple $\langle q_0, \underset{\sim}{q}_1, \ldots, \underset{\sim}{q}_{n-1}\rangle$. With this convention, for positive integers n, $\mathbb{P}_n$-conditions are sequences of length n.

For $n = 0$ let $\mathbb{P}_0 := \big(\{\emptyset\}, \subseteq\big)$. When we define $\mathbb{P}_0$-names, we find that $G = \{\emptyset\}$ is the unique $\mathbb{P}_0$-generic filter over $\mathbf{V}$. In particular we get that a 0-stage extension of $\mathbf{V}$ is just $\mathbf{V}$.

The sequence of forcing notions $\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_n$, where $\mathbb{P}_k = (P_k, \leq, \emptyset)$, has the property that if $p = \langle q_0, \underset{\sim}{q}_1, \ldots, \underset{\sim}{q}_{n-1}\rangle \in P_n$, then for all $k \in n$, $p|_k \in P_k$ and $p|_k \Vdash_{\mathbb{P}_k} \underset{\sim}{q}_k \in \underset{\sim}{Q}_k$, where $\underset{\sim}{\mathbb{Q}}_k$ is a $\mathbb{P}_k$-name for a forcing notion $(Q_k, \leq)$ in the $\mathbb{P}_k$-generic extension of $\mathbf{V}$. In particular, $\mathbb{P}_1 = \underset{\sim}{\mathbb{Q}}_0$ is a $\mathbb{P}_0$-name for a forcing notion $(Q_0, \leq)$ in the $\mathbb{P}_0$-generic extension of $\mathbf{V}$, which is just $\mathbf{V}$ itself. In other words, $\mathbb{P}_1$ is a $\mathbb{P}_0$-name for forcing notion $(P_1, \leq)$ which belongs to $\mathbf{V}$. Thus, every $\mathbb{P}_n$-condition is of the form $\langle \underset{\sim}{q}_0, \underset{\sim}{q}_1, \ldots, \underset{\sim}{q}_{n-1}\rangle$, where $\underset{\sim}{q}_0$ is a $\mathbb{P}_0$-name for a $\mathbb{Q}_0$-condition. This completes the definition of α-stage iterations for $\alpha \in \omega$.

Similarly, we define $(\alpha+1)$-stage iterations for arbitrary ordinals α: If the α-stage iteration $\mathbb{P}_\alpha = \big\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \big\rangle$ is already defined and $\underset{\sim}{\mathbb{Q}}_\alpha$ is a $\mathbb{P}_\alpha$-name for a forcing notion in the $\mathbb{P}_\alpha$-generic extension, then $\mathbb{P}_{\alpha+1} := \mathbb{P}_\alpha * \underset{\sim}{\mathbb{Q}}_\alpha$.

Let us now consider the case when α is a limit ordinal. At first glance, the set of $\mathbb{P}_\alpha$-conditions consists of all α-sequences $\langle \underset{\sim}{q}_\beta : \beta \in \alpha\rangle$, but having a closer look we see that there is some freedom in defining the set of $\mathbb{P}_\alpha$-conditions. For example we can require that $\underset{\sim}{q}_\beta = \underset{\sim}{\emptyset}$ for all but finitely many $\beta \in \alpha$, which is called **finite support iteration**, or that $\underset{\sim}{q}_\beta = \underset{\sim}{\emptyset}$ for all but countably many $\beta \in \alpha$, which is called **countable support iteration**.

For $\mathbb{P}_\alpha$-conditions $p = \langle \underset{\sim}{q}_\beta : \beta \in \alpha\rangle$ we define

$$\operatorname{supp}(p) = \big\{\beta \in \alpha : \underset{\sim}{q}_\beta \neq \underset{\sim}{\emptyset}\big\},$$

and like for products we call $\operatorname{supp}(p)$ the **support** of p. For example, a countable support iteration $\mathbb{P}_\alpha$ consists of all $\mathbb{P}_\alpha$-conditions p that have countable support, *i.e.*, $|\operatorname{supp}(p)| \leq \omega$.

Because of the following result (which will be stated without proof), finite support iterations are often used in iterations of forcing notions satisfying *ccc*.

PROPOSITION 18.8. *Any finite support iteration of ccc forcing notions satisfies ccc. In other words, if $\mathbb{P}_\alpha$ is a finite support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \rangle$, where for each $\beta \in \alpha$ we have*

$$\mathbf{0}_\beta \Vdash_\beta \text{“}\underset{\sim}{\mathbb{Q}}_\beta \textit{ satisfies ccc”},$$

then also $\mathbb{P}_\alpha$ satisfies ccc.

Before we give an example of a finite support iteration, let us first settle some notation: Let $\mathbb{P}_\alpha = \langle \underset{\sim}{\mathbb{Q}}_\gamma : \gamma \in \alpha \rangle$ be any α-stage iteration and let G be $\mathbb{P}_\alpha$-generic over some model $\mathbf{V}$. Then, for $\beta \in \alpha$, let

$$G(\beta) = \left\{ q_\beta : \exists \langle \underset{\sim}{p}_\gamma : \gamma \in \alpha \rangle \in \underset{\sim}{G} \left(q_\beta = \underset{\sim}{p}_\beta[G] \right) \right\}$$

and

$$G|_\beta = \left\{ \langle q_\gamma : \gamma \in \beta \rangle : \exists \langle \underset{\sim}{p}_\gamma : \gamma \in \alpha \rangle \in \underset{\sim}{G} \ \forall \gamma \in \beta \left(q_\beta = \underset{\sim}{p}_\beta[G] \right) \right\}.$$

In other words, $G|_\beta$ denotes the $\mathbb{P}_\beta$-generic filter generated by G. In abuse of notation, for $\mathbb{P}_\alpha = \langle \underset{\sim}{\mathbb{Q}}_\gamma : \gamma \in \alpha \rangle$ we usually write $\mathbb{P}_\alpha = \langle \mathbb{Q}_\gamma : \gamma \in \alpha \rangle$, where for all $\gamma \in \alpha$, $\mathbb{Q}_\gamma := \underset{\sim}{\mathbb{Q}}_\gamma \left[G|_\gamma \right]$. In other words, we usually consider an α-stage iteration $\mathbb{P}_\alpha$, starting in some model $\mathbf{V}$, as an α-sequence of forcing notions $\mathbb{Q}_\gamma$ (not just $\mathbb{P}_\gamma$-names for forcing notions), where for each $\gamma \in \alpha$, $\mathbb{Q}_\gamma$ belongs to the $\mathbb{P}_\gamma$-generic extension $\mathbf{V}\left[G|_\gamma \right]$. Consequently, for $\beta \in \alpha$ we also write $\mathbf{V}\left[\langle G(\gamma) : \gamma \in \beta \rangle \right]$ instead of $\mathbf{V}\left[G|_\beta \right]$, having in mind that we add one generic filter after the other, rather than adding just the single generic filter $G|_\beta$.

We conclude this section by showing that in finite support or countable support iterations or products of certain forcing notions (*e.g.*, *ccc* forcing notions), no new reals are added at limit stages of uncountable cofinality — a result which will be used quite often in the forthcoming chapters.

LEMMA 18.9. *Let λ be an infinite limit ordinal of uncountable cofinality (i.e., $\operatorname{cf}(\lambda) > \omega$), let $\mathbb{P}_\lambda = \langle \underset{\sim}{\mathbb{Q}}_\alpha : \alpha \in \lambda \rangle$ be any finite support or countable support iteration or product of arbitrary forcing notions $\mathbb{Q}_\alpha$, and let G be $\mathbb{P}_\lambda$-generic over some model $\mathbf{V}$ of* ZFC. *If $\mathbf{V}[G] \vDash \operatorname{cf}(\lambda) > \omega$, then no new reals are added at stage λ; more formally,*

$${}^\omega\omega \cap \mathbf{V}[G] = \bigcup_{\alpha \in \lambda} {}^\omega\omega \cap \mathbf{V}[G|_\alpha].$$

Proof. Let $\underset{\sim}{f}$ be a $\mathbb{P}_\lambda$-name for a function in ${}^\omega\omega \cap \mathbf{V}[G]$. For every $\beta \in \lambda$ define a $\mathbb{P}_\beta$-name $\underset{\sim}{g}_\beta$ for a partial function from ω to ω by stipulating

$$\underset{\sim}{g}_\beta = \left\{ \left\langle \operatorname{op}(\underset{\cdot}{n}, \underset{\cdot}{m}), p \right\rangle \in \underset{\sim}{f} : \operatorname{supp}(p) \subseteq \beta \wedge p \in G \right\},$$

where $\operatorname{op}(\underset{\cdot}{n}, \underset{\cdot}{m})$ is the canonical $\mathbb{P}_\lambda$-name for the ordered pair $\langle \underset{\cdot}{n}, \underset{\cdot}{m} \rangle$ (which was defined in Chapter 14). Now, we show that there exist an $\alpha \in \lambda$ such that $\mathbf{V}[G|_\alpha] \vDash \underset{\sim}{f}[G|_\alpha] = \underset{\sim}{g}_\alpha[G|_\alpha]$, *i.e.*, the function $\underset{\sim}{f}[G]$ appears already in the model $\mathbf{V}[G|_\alpha]$: Let us work in the model $\mathbf{V}[G]$. For every $n \in \omega$ we can choose a $p_n \in G$ which decides the value of $\underset{\sim}{f}(n)$, *i.e.*, $\langle \operatorname{op}(\underset{\cdot}{n}, \underset{\cdot}{m}), p_n \rangle \in \underset{\sim}{f}$ for some $m \in \omega$. Using the fact that $\mathbf{V}[G] \vDash \operatorname{cf}(\tilde{\lambda}) > \omega$ and that the supports of the p_n's are at most countable (*i.e.*, finite or countably infinite), we get that in $\mathbf{V}[G]$, $\bigcup_{n\in\omega} \operatorname{supp}(p_n) \subsetneq \lambda$. Thus, there is an $\alpha \in \lambda$ such that $\bigcup_{n\in\omega} \operatorname{supp}(p_n) \subseteq \alpha$, and by construction we have $\underset{\sim}{g}_\alpha[G|_\alpha] \in {}^\omega\omega \cap \mathbf{V}[G|_\alpha]$ and $\mathbf{V}[G] \vDash \underset{\sim}{f}[G] = \underset{\sim}{g}_\alpha[G]$. $\dashv$

A Model in which $\mathfrak{i} < \mathfrak{c}$

In this section we shall construct — by a finite support iteration of *ccc* forcing notions — a model in which $\mathfrak{i} < \mathfrak{c}$, where $\mathfrak{i}$ is the least cardinality of a maximal independent family; but first, let us recall a few notions: A set $\mathscr{I} \subseteq [\omega]^\omega$ is an independent family, denoted *i.f.*, if for any $A, B \in \operatorname{fin}(\mathscr{I})$ with $A \cap B = \emptyset$ we have $\bigcap A \setminus \bigcup B$ is infinite, where we stipulate $\bigcap \emptyset := \omega$ (see Chapter 8). Furthermore, for independent families $\mathscr{I}$, let $\operatorname{bc}(\mathscr{I})$ be the set of all finite boolean combinations of distinct elements of $\mathscr{I}$, in other words,

$$\operatorname{bc}(\mathscr{I}) = \Big\{ \bigcap A \setminus \bigcup B : \{A, B\} \subseteq \operatorname{fin}(\mathscr{I}) \wedge A \cap B = \emptyset \Big\}.$$

Notice that $\operatorname{bc}(\mathscr{I}) \subseteq [\omega]^\omega$ and that for $\mathscr{I} = \emptyset$ we have $\operatorname{bc}(\mathscr{I}) = \{\omega\}$.

The following lemma — which is in fact a ZFC result — will be crucial in the construction of the forcing notion which will be used in the iteration below.

LEMMA 18.10. *Let $\mathbf{V}$ be an arbitrary model of ZFC and let $\mathscr{I} \subseteq [\omega]^\omega$ be an arbitrary i.f. in $\mathbf{V}$. Then there exists an ideal $I \subseteq \mathscr{P}(\omega)$ in $\mathbf{V}$ such that*

(a) $I \cap \operatorname{bc}(\mathscr{I}) = \emptyset$, and

(b) for every $y \in [\omega]^\omega \cap \mathbf{V}$ there exists an $x \in \operatorname{bc}(\mathscr{I})$ such that $x \cap y$ or $x \setminus y$ belongs to I.

Proof. Let $\{y_\alpha \in [\omega]^\omega : \alpha \in \mathfrak{c}\}$ be an arbitrary enumeration of $[\omega]^\omega$. With respect to this enumeration we construct the ideal I by induction on $\mathfrak{c}$. Firstly, let $I_0 := \operatorname{fin}(\omega)$. Then I_0 is an ideal and $I_0 \cap \operatorname{bc}(\mathscr{I}) = \emptyset$. Assume that we have already defined the ideal I_α for some $\alpha \in \mathfrak{c}$. If there are $x \in \operatorname{bc}(\mathscr{I})$ and $u \in I_\alpha$ such that

$$x \subseteq y_\alpha \cup u\,,$$

then $I_{\alpha+1} := I_\alpha$; otherwise, $I_{\alpha+1}$ is the ideal generated by $I_\alpha \cup \{y_\alpha\}$, *i.e.*, $u \in I_{\alpha+1}$ *iff* there is an $A \in \operatorname{fin}\big(I_\alpha \cup \{y_\alpha\}\big)$ such that $u \subseteq \bigcup A$. Further, for limit ordinals $\lambda \in \mathfrak{c}$ let $I_\lambda := \bigcup_{\alpha\in\lambda} I_\alpha$, and let

$$I = \bigcup_{\alpha\in\mathfrak{c}} I_\alpha\,.$$

It remains to show that the ideal I has the required properties (we leave it as an exercise to the reader to show that I is indeed an ideal):

(a) Assume towards a contradiction that there is an $x \in \mathrm{bc}(\mathscr{I}) \cap I$. Since $I_0 \cap \mathrm{bc}(\mathscr{I}) = \emptyset$, there exists a least ordinal $\alpha \in \mathfrak{c}$ such that $x \in I_{\alpha+1}$. In particular, $x \notin I_\alpha$, which implies that $I_{\alpha+1} \neq I_\alpha$. Hence, $I_{\alpha+1}$ must be the ideal generated by $I_\alpha \cup \{y_\alpha\}$. Thus, by construction, there is no $u \in I_\alpha$ such that $x \subseteq y_\alpha \cup u$. In other words, for each $u \in I_\alpha$ we have $x \nsubseteq y_\alpha \cup u$, which contradicts the fact that $x \in I_{\alpha+1}$.

(b) Take any $y \in [\omega]^\omega$ and let $\alpha \in \mathfrak{c}$ be such that $y = y_\alpha$. If there are $x \in \mathrm{bc}(\mathscr{I})$ and $u \in I_\alpha$ such that $x \subseteq y_\alpha \cup u$, then $x \setminus y_\alpha \subseteq u$, and consequently $x \setminus y \in I$; otherwise, $y_\alpha \in I_{\alpha+1}$, which implies that $x \cap y_\alpha \in I_{\alpha+1}$, and consequently $x \cap y \in I$. ⊣

Now we are ready to construct a model in which $\mathfrak{i} < \mathfrak{c}$.

PROPOSITION 18.11. *$\mathfrak{i} < \mathfrak{c}$ is consistent with* ZFC.

Proof. The proof will be given in two steps: In the first step, with respect to some *i.f.* $\mathscr{I}$ we shall construct a forcing notion $\mathbb{Q}_I$ (where $\mathscr{I}$ and I are as in LEMMA 18.10), and will show that $\mathbb{Q}_I$ adds a generic real $g \in [\omega]^\omega$ (over some model $\mathbf{V}$) which has the following properties:

- $\mathscr{I} \cup \{g\}$ is an *i.f.* in $\mathbf{V}[g]$.
- If $y \in [\omega]^\omega \cap \mathbf{V}$ is such that $\mathscr{I} \cup \{y\}$ is independent and $y \notin \mathscr{I}$, then $\mathscr{I} \cup \{g, y\}$ is not independent.

In the second step, by a finite support iteration of length ω_1 of forcing notions $\mathbb{Q}_I$, we shall construct a generic model in which the set of generic reals, added by the forcing notions $\mathbb{Q}_I$, is a maximal *i.f.* of size ω_1.

1st Step: Let $\mathbf{V}$ be an arbitrary model of ZFC and let $\mathscr{I} \subseteq [\omega]^\omega$ be an arbitrary countable *i.f.* in $\mathbf{V}$. Furthermore, let $I \subseteq \mathscr{P}(\omega)$ be the ideal constructed in LEMMA 18.10 with respect to $\mathscr{I}$, *i.e.*, $I \cap \mathscr{I} = \emptyset$, and for every $y \in [\omega]^\omega \cap \mathbf{V}$ there exists an $x \in \mathrm{bc}(\mathscr{I})$ such that $x \cap y$ or $x \setminus y$ belongs to I. With respect to the ideal I we define the forcing notion $\mathbb{Q}_I = (Q_I, \leq)$ as follows: A $\mathbb{Q}_I$-condition is an ordered pair $\langle s, E\rangle$ where $s \in \mathrm{fin}(\omega)$ and $E \in \mathrm{fin}(I)$, and for $\mathbb{Q}_I$-conditions $\langle s, E\rangle$ and $\langle t, F\rangle$ we define

$$\langle s, E\rangle \leq \langle t, F\rangle \iff s \subseteq t \,\wedge\, E \subseteq F \,\wedge\, (t \setminus s) \cap \bigcup_{u \in E} u = \emptyset\,.$$

Notice that for any $E, F \in \mathrm{fin}(I)$ and any $s \in \mathrm{fin}(\omega)$, $\langle s, E\rangle$ and $\langle s, F\rangle$ are compatible, and since the set $\mathrm{fin}(\omega)$ is countable, $\mathbb{Q}_I$ satisfies *ccc*.

Let G be $\mathbb{Q}_I$-generic over $\mathbf{V}$ and let

$$g = \bigcup \Big\{ s \in \mathrm{fin}(\omega) : \exists E \in \mathrm{fin}(I) \big(\langle s, E\rangle \in G\big) \Big\}\,.$$

We leave it as an exercise to the reader to show that $g \in [\omega]^\omega$ and that $\mathbf{V}[g] = \mathbf{V}[G]$. Thus, we can equally well work with g instead of G, in other words, g is a $\mathbb{Q}_I$-generic real over $\mathbf{V}$.

Now, we show that $\mathscr{I} \cup \{g\}$ is an *i.f.* in $\mathbf{V}[g]$ which is even maximal with respect to the reals y which belong to $\mathbf{V}$ — notice that this property of g does not depend on the particular ideal I which is involved in the construction of the forcing notion $\mathbb{Q}_I$.

Claim. *If g is $\mathbb{Q}_I$-generic over $\mathbf{V}$, then $\mathscr{I} \cup \{g\}$ is an independent family in $\mathbf{V}[g]$, but for all $y \in [\omega]^\omega \cap \mathbf{V}$ with $y \notin \mathscr{I}$, $\mathscr{I} \cup \{g, y\}$ is not independent.*

Proof of Claim. Firstly we show that $\mathscr{I} \cup \{g\}$ is an *i.f.* in $\mathbf{V}[g]$, *i.e.*, we have to show that for every $x \in \mathrm{bc}(\mathscr{I})$, both sets $g \cap x$ and $(\omega \setminus g) \cap x$ are infinite: For every $x \in \mathrm{bc}(\mathscr{I})$ and every $n \in \omega$ define

$$A_{n,x} = \big\{\langle s, E\rangle \in Q_I : |s \cap x| > n\big\},$$

$$B_{n,x} = \big\{\langle s, E\rangle \in Q_I : \big|\bigcup E \cap x\big| > n\big\}.$$

We leave it as an exercise to the reader to show that for all $x \in \mathrm{bc}(\mathscr{I})$ and $n \in \omega$, $A_{n,x}$ and $B_{n,x}$ are open dense subsets of Q_I, which implies that $\mathscr{I} \cup \{g\}$ is an *i.f.* in $\mathbf{V}[g]$.

Now, we show that for all $y \in [\omega]^\omega \cap \mathbf{V}$ with $y \notin \mathscr{I}$, $\mathscr{I} \cup \{g, y\}$ is not independent: Let $y \in [\omega]^\omega \cap \mathbf{V}$ be an arbitrary real. If for all $u \in I$ and $x \in \mathrm{bc}(\mathscr{I})$ we have $x \nsubseteq y \cup u$, then let

$$C_y = \big\{\langle s, E\rangle \in Q_I : y \in E\big\},$$

otherwise, there is a $u_0 \in I$ and an $x \in \mathrm{bc}(\mathscr{I})$ such that $x \subseteq y \cup u_0$ and we define

$$C_y = \big\{\langle s, E\rangle \in Q_I : u_0 \in E\big\}.$$

By the properties of the ideal I we get that C_y is an open dense subset of Q_I for all $y \in [\omega]^\omega$. This implies that for each $y \in [\omega]^\omega$ we find an $x \in \mathrm{bc}(\mathscr{I})$ such that $g \cap y$ is finite (in the case when $y \in I$), or $g \cap (x \setminus y)$ is finite (in the case when $x \subseteq y \cup u$ for some $u \in I$). However, in both cases we get that $\mathscr{I} \cup \{g, y\}$ is not independent whenever $y \in [\omega]^\omega \setminus \mathscr{I}$. $\dashv_{\text{Claim}}$

2nd Step: Now, we are ready to define the finite support iteration which will yield a generic model in which there exists a maximal independent family $\mathscr{I}$ of cardinality ω_1: Let $\mathbf{V}$ be an arbitrary model of ZFC in which $\mathfrak{c} > \omega_1$. We construct the *i.f.* $\mathscr{I}$ by induction on $\alpha \in \omega_1$. Let $\mathscr{I}_0 = \emptyset$ and assume that we have already constructed the *i.f.* $\mathscr{I}_\alpha$ for some $\alpha \in \omega_1$. Furthermore, let $I_\alpha \subseteq \mathscr{P}(\omega)$ be the ideal constructed in the proof of Lemma 18.10 with respect to the *i.f.* $\mathscr{I}_\alpha$, and let g_α be a $\mathbb{Q}_{I_\alpha}$-generic real over $\mathbf{V}\big[\langle g_\gamma : \gamma \in \alpha\rangle\big]$. Now, let $\mathscr{I}_{\alpha+1} := \mathscr{I}_\alpha \cup \{g_\alpha\}$; and for limit ordinals $\lambda \in \omega_1$ let $\mathscr{I}_\lambda := \bigcup_{\beta\in\lambda} \mathscr{I}_\beta$. Notice that for each $\alpha \in \omega_1$, $\mathscr{I}_\alpha = \{g_\gamma : \gamma \in \alpha\}$ is a countable *i.f.* in $\mathbf{V}\big[\langle g_\gamma : \gamma \in \alpha\rangle\big]$.

Let $\mathbb{P}_{\omega_1} = \big\langle \mathbb{Q}_{I_\alpha} : \alpha \in \omega_1\big\rangle$ be the finite support iteration of the forcing notions $\mathbb{Q}_{I_\alpha}$, let $G = \langle g_\alpha : \alpha \in \omega_1\rangle$, and let $\mathscr{I} = \{g_\alpha : \alpha \in \omega_1\}$. Then G is $\mathbb{P}_{\omega_1}$-generic over $\mathbf{V}$ and $\mathscr{I}$ is an *i.f.* in $\mathbf{V}[G]$ of cardinality ω_1. It remains to show that $\mathscr{I}$ is maximal and that $\mathbf{V}[G] \vDash \mathfrak{c} > \omega_1$: Since $\mathbb{P}_{\omega_1}$ is a finite support iteration of *ccc* forcing notions (recall that $\mathbb{Q}_I$ satisfies *ccc*), by PROPOSITION 18.8 we get that also $\mathbb{P}_{\omega_1}$ satisfies *ccc*, and therefore, by LEMMA 14.20, all cardinals are preserved. In particular, since $\mathbf{V} \vDash \mathfrak{c} > \omega_1$, we get that $\mathbf{V}[G] \vDash \mathfrak{c} > \omega_1$. Furthermore, by LEMMA 18.9 we know that the iteration does not add new reals at stage ω_1. Thus, for every real $y \in [\omega]^\omega \cap \mathbf{V}[G]$ there exists an $\alpha \in \omega_1$ such that $y \in \mathbf{V}\big[\langle g_\gamma : \gamma \in \alpha\rangle\big]$. Now, by the CLAIM we know that for each $y \in [\omega]^\omega \cap \mathbf{V}\big[\langle g_\gamma : \gamma \in \alpha\rangle\big]$ which does not belong to $\mathscr{I}_\alpha$, $\mathscr{I}_\alpha \cup \{g_\alpha, y\}$ is not independent. Consequently, for each $y \in [\omega]^\omega \cap \mathbf{V}[G]$ we get that $\mathscr{I} \cup \{y\}$ is not independent whenever $y \notin \mathscr{I}$. This shows that $\mathscr{I}$ is a maximal independent family in $\mathbf{V}[G]$, and since $|\mathscr{I}| = \omega_1$ and $\omega_1 < \mathfrak{c}$, we get that $\omega_1 = \mathfrak{i} < \mathfrak{c}$ is consistent with ZFC. ⊣

Considering the diagram at the end of Chapter 8, we see that the independence number $\mathfrak{i}$ appears on the top of the diagram. However, as we have seen above, $\mathfrak{i}$ can be quite small compared to $\mathfrak{c}$. In the next chapter we consider a cardinal characteristic on the bottom of the diagram, namely $\mathfrak{p}$, and show that $\mathfrak{p}$ can be equal to $\mathfrak{c}$, even in the case when $\mathfrak{c} > \omega_1$.

NOTES

Products and iterations. For a more detailed introduction to products and iterations of forcing notions we refer the reader to Kunen [5, Chapter VIII], Baumgartner [1], and Goldstern [3] — where one can also find many more applications of these forcing tools. In particular, PROPOSITION 18.5 is taken from Kunen [5, p. 256, Theorem 2.3] and the idea for the proof of PROPOSITION 18.11 is taken from Kunen [5, p. 289, A12] (where the actual construction is due to Jörg Brendle).

RELATED RESULTS

96. *Iterating Cohen forcing.* A special feature of Cohen forcing $\mathbb{C} = \big(\mathrm{Fn}(\omega, 2), \subseteq\big)$ is that the set $\mathrm{Fn}(\omega, 2)$ is the same in every transitive model of ZFC. In particular, for any cardinal κ we get that (finite/countable support) iterations of length κ of Cohen forcing $\mathbb{C}$ are equivalent to (finite/countable support) products of κ copies of $\mathbb{C}$ (*cf.* LEMMA 21.9).

97. *Products as two-step iterations.* Let $\mathbb{P}_0$ and $\mathbb{P}_1$ be some forcing notions in some model $\mathbf{V}$ of ZFC, let G be $\mathbb{P}_0 \times \mathbb{P}_1$-generic over $\mathbf{V}$, and let $G(0)$ and $G(1)$ be as above. Then $G(0)$ is $\mathbb{P}_0$-generic over $\mathbf{V}[G(1)]$ and $G(1)$ is $\mathbb{P}_1$-generic over $\mathbf{V}[G(0)]$ (see for example Kunen [5, Chapter VIII, Theorem 1.4] and compare with LEMMA 18.1).

98. *Products and the countable chain condition.* It is consistent with ZFC that there are forcing notions $\mathbb{P}$ and $\mathbb{Q}$, both satisfying *ccc*, such that product $\mathbb{P} \times \mathbb{Q}$ does not satisfy *ccc* (compare with LEMMA 18.7). Examples of such forcing notions can be found in Kunen [5, Chapter VIII, p. 291 f.].

99. *The consistency of* $\mathfrak{c} > \mathfrak{a}$ *revisited.* Let $\mathbf{V}$ be a model in which $\mathfrak{c} > \omega_1$ and let $\mathscr{A} \subseteq [\omega]^\omega$ be a countable almost disjoint family. With respect to $\mathscr{A}$ we define the following forcing notion $\mathbb{Q}_{\mathscr{A}}$: The conditions of $\mathbb{Q}_{\mathscr{A}}$ are of the form $\langle s, X\rangle$, where s is a finite sequence of ω and $X \in [\mathscr{A}]^{<\omega}$ and we define $\langle s, X\rangle \leq \langle s', X'\rangle$ if $s \subseteq s'$, $X \subseteq X'$, and $(s' \setminus s) \cap \bigcup X = \emptyset$. For $\mathscr{B} = \{B \in [\omega]^\omega : \forall A \in \mathscr{A}(|B \cap A| < \omega)\}$ we get that the generic real $A \in [\omega]^\omega$, generated by the finite sets s, is almost disjoint from every member of $\mathscr{A}$ and has infinite intersection with each member of $\mathscr{B}$ (*cf.* Kunen [5, Chapter II, Lemma 2.17]). Thus, $\mathscr{A} \cup \{A\}$ is a *mad* family for the old reals (*i.e.*, every real $x \in [\omega]^\omega$ in the ground model $\mathbf{V}$ has infinite intersection with either A or an element of $\mathscr{A}$). Furthermore, it is not hard to show that the forcing notion $\mathbb{Q}_{\mathscr{A}}$ satisfies *ccc* (*cf.* Kunen [5, Chapter II, Lemma 2.14]). Now, let $\mathscr{A}_0$ be an arbitrary countable almost disjoint family in $\mathbf{V}$ and for non-zero ordinals $\alpha \in \omega_1$ define $\mathscr{A}_\alpha$ by transfinite induction as follows: If α is a limit ordinal, then $\mathscr{A}_\alpha := \bigcup_{\beta\in\alpha} \mathscr{A}_\beta$, and if $\alpha = \beta + 1$, then let $\mathscr{A}_\alpha := \mathscr{A}_\beta \cup \{A_\beta\}$, where $A_\beta \in [\omega]^\omega$ is $\mathbb{Q}_{\mathscr{A}_\beta}$-generic over $\mathbf{V}\big[\langle A_\gamma : \gamma \in \beta\rangle\big]$. Finally, by the facts mentioned above we get that the finite support iteration $\big\langle \mathbb{Q}_{\mathscr{A}_\alpha} : \alpha \in \omega_1\big\rangle$, starting in $\mathbf{V}$, yields a model in which we have still $\mathfrak{c} > \omega_1$ and in which there exists a *mad* family of size ω_1, namely $\mathscr{A}_0 \cup \{A_\alpha : \alpha \in \omega_1\}$.

100. *Easton forcing.* With so-called *Easton forcing*, which is a product forcing notion, one can modify the powers of infinitely many regular cardinals at once. In fact, one can show that cardinal exponentiation on the regular cardinals can be anything not "obviously false". For example one can force that $\forall n \in \omega\, (2^{\omega_n} = \omega_{\omega_1+n})$, but one cannot force that $2^\omega = \omega_{\omega+\omega}$ (since $\operatorname{cf}(2^\omega) > \omega$). For Easton forcing see Easton [2] or Kunen [5, Chapter VIII, §4].

101. *Preservation of* κ*-chain condition.* In Chapter 16 | RELATED RESULT 87 we generalised the notion of *ccc* by saying that a forcing notion $\mathbb{P} = (P, \leq)$ satisfies the *κ-chain condition* if every anti-chain in P has cardinality $<\kappa$. Now, if κ is a regular uncountable cardinal and $\mathbb{P}_\alpha = \big\langle \mathbb{Q}_\beta : \beta \in \alpha\big\rangle$ is a finite support iteration, where for each $\beta \in \alpha$ we have $\mathbf{0}_\beta \Vdash_\beta$ "$\underset{\sim}{\mathbb{Q}}_\beta$ *satisfies the κ-chain condition*", then $\mathbb{P}_\alpha$ satisfies the κ-chain condition too (see for example Kunen [5, Chapter VIII, Lemma 5.12] or Jech [4, Part II, Theorem 2.7]).

REFERENCES

1. JAMES E. BAUMGARTNER, *Iterated forcing*, in ***Surveys in Set Theory*** (A.R.D. Mathias, ed.), [London Mathematical Society Lecture Note Series 87], Cambridge University Press, Cambridge, 1983, pp. 1–59.
2. WILLIAM B. EASTON, *Powers of regular cardinals*, ***Annals of Pure and Applied Logic***, vol. 1 (1970), 139–178.
3. MARTIN GOLDSTERN, *Tools for your forcing construction*, in ***Set Theory of the Reals*** (H. Judah, ed.), [Israel Mathematical Conference Proceedings], Bar-Ilan University, Israel, 1993, pp. 305–360.
4. THOMAS JECH, ***Multiple Forcing***, [Cambridge Tracts in Mathematics], Cambridge University Press, Cambridge, 1986.
5. KENNETH KUNEN, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.

19

Models in which $\mathfrak{p} = \mathfrak{c}$

In this chapter we shall consider models of ZFC in which $\mathfrak{p} = \mathfrak{c}$. Since $\omega_1 \leq \mathfrak{p}$ (by THEOREM 8.1) and $\mathfrak{p} \leq \mathfrak{c}$, we have $\mathfrak{p} = \mathfrak{c}$ in all models in which $\mathfrak{c} = \omega_1$, but of course, these are not the models we are interested in.

By THEOREM 13.6 we know that $\mathsf{MA}(\sigma\text{-centred})$ implies $\mathfrak{p} = \mathfrak{c}$, moreover, by Chapter 13 | RELATED RESULT 79 we even have $\mathsf{MA}(\sigma\text{-centred}) \iff \mathfrak{p} = \mathfrak{c}$. On the other hand, in a model in which $\omega_1 < \mathfrak{p} = \mathfrak{c}$ we do not necessarily have MA (because $\mathsf{MA}(\sigma\text{-centred})$ is weaker than MA) and in fact it is slightly easier to force just $\omega_1 < \mathfrak{p} = \mathfrak{c}$ than to force $\mathsf{MA} + \neg\mathsf{CH}$. Thus, we shall first construct a model of $\omega_1 < \mathfrak{p} = \mathfrak{c}$, which — by Chapter 13 | RELATED RESULT 79 — proves the consistency of $\mathsf{MA}(\sigma\text{-centred}) + \neg\mathsf{CH}$ with ZFC, and then we shall sketch the construction of a generic model in which we have $\mathsf{MA} + \neg\mathsf{CH}$. Finally, we shall consider the case when a single Cohen real c is added to a model $\mathbf{V} \vDash \mathsf{ZFC}$ in which $\mathsf{MA} + \neg\mathsf{CH}$ holds. Even though full MA fails in $\mathbf{V}[c]$ (see RELATED RESULT 104), we shall see that $\mathfrak{p} = \mathfrak{c}$ still holds in $\mathbf{V}[c]$ — a result which will be used in Chapter 27.

A Model in which $\mathfrak{p} = \mathfrak{c} = \omega_2$

In this section, we shall construct a generic model in which $\mathfrak{p} = \mathfrak{c} = \omega_2$ — for the general case see RELATED RESULT 102.

PROPOSITION 19.1. *$\mathfrak{p} = \mathfrak{c} = \omega_2$ is consistent with* ZFC.

Proof. We start with a model $\mathbf{V} \vDash \mathsf{ZFC} + \mathsf{CH}$ in which we have $\mathbf{V} \vDash 2^{\omega_1} = \omega_2$. In order to obtain such a model, use the techniques developed in Chapter 14 or see Chapter 18 | RELATED RESULT 100.

In $\mathbf{V}$ we shall define a finite support iteration $\mathbb{P}_{\omega_2} = \langle \mathbb{Q}_\xi : \xi \in \omega_2 \rangle$ of *ccc* forcing notions $\mathbb{Q}_\xi$, such that in the $\mathbb{P}_{\omega_2}$-generic model $\mathbf{V}[G]$ we have $\mathbf{V} \vDash \mathfrak{p} = \mathfrak{c}$. Since for each $\xi \in \omega_2$ the forcing notion $\mathbb{Q}_\xi$ will satisfy *ccc*, by PROPOSITION 18.8 we get that also each $\mathbb{P}_\xi$ will satisfy *ccc*, and therefore, by

LEMMA 18.9 and the proof of THEOREM 16.4, for any $\xi \in \omega_2$ we shall have $\mathbf{V}[G|_\xi] \vDash \mathfrak{c} = \omega_1 \wedge 2^{\omega_1} = \omega_2$. Furthermore, since for each $\xi \in \omega_2$ the forcing notion $\mathbb{Q}_\xi$ will be of cardinality at most ω_1, also $\mathbb{P}_\xi$ will be of cardinality at most ω_1.

Like in the proof of THEOREM 16.4, one can show that for any $\nu \in \omega_2$, there are ω_1 nice $\mathbb{P}_\nu$-names for subsets of ω, and because $\mathbf{V}[G|_\nu] \vDash 2^{\omega_1} = \omega_2$, for each $\nu \in \omega_2$ there exists a bijection $A_\nu : \omega_2 \to \mathscr{P}\big([\omega]^\omega\big)$ in $\mathbf{V}[G|_\nu]$. In particular, for all $\nu, \eta \in \omega_2$ we have $A_\nu(\eta) \subseteq [\omega]^\omega$, and since $\mathfrak{c} = \omega_1$ we get $|A_\nu(\eta)| \leq \omega_1$. Strictly speaking, we should work with some $\mathbb{P}_\nu$-name for A_ν, not with the actual function, but for the sake of simplicity we shall omit this technical difficulty and leave it as an exercise to the reader.

Now we are ready to construct the *ccc* forcing notions $\mathbb{Q}_\xi$: To start with, fix a bijection $g : \omega_2 \to \omega_2 \times \omega_2$ in $\mathbf{V}$ (which will serve as a bookkeeping function) such that for every $\xi \in \omega_2$ we have

$$\big(g(\xi) = \langle \nu, \eta \rangle\big) \to \nu \leq \xi\,.$$

Let $\xi \in \omega_2$ be an arbitrary but fixed ordinal number and let $\langle \nu, \eta \rangle := g(\xi)$. Since $\nu \leq \xi$, $\mathbf{V}[G|_\nu] \subseteq \mathbf{V}[G|_\xi]$, and the set $A_\nu(\eta) \subseteq [\omega]^\omega$, originally defined in $\mathbf{V}[G|_\nu]$, also belongs to $\mathbf{V}[G|_\xi]$.

In order to define $\mathbb{Q}_\xi = (Q_\xi, \leq)$ we work in $\mathbf{V}[G|_\nu]$ and consider the following two cases: If the family $A_\nu(\eta) \subseteq [\omega]^\omega$ has the strong finite intersection property *sfip* (*i.e.*, intersections of finitely many members of $A_\nu(\eta)$ are infinite), then we define

$$Q_\xi = \big\{\langle s, E\rangle : s \in \operatorname{fin}(\omega) \wedge E \in \operatorname{fin}\big(A_\nu(\eta)\big)\big\}\,,$$

and for $\langle s, E\rangle, \langle t, F\rangle \in Q_\xi$ we stipulate

$$\langle s, E\rangle \leq \langle t, F\rangle \iff s \subseteq t \,\wedge\, E \subseteq F \,\wedge\, (t \setminus s) \subseteq \bigcap E\,.$$

In the case when $A_\nu(\eta)$ does not have the *sfip*, let $\mathbb{Q}_\xi$ be the trivial forcing notion $\big(\{\emptyset\}, \subseteq\big)$.

The forcing notion $\mathbb{Q}_\xi$ (in the case when $\mathbb{Q}_\xi$ is non-trivial) was already introduced in the proof of THEOREM 13.6, where it was shown that $\mathbb{Q}_\xi$ satisfies *ccc* and that the generic filter induces a pseudo-intersection of $A_\nu(\eta)$. Hence, we either have $\mathbf{V}[G|_{\xi+1}] = \mathbf{V}[G|_\xi]$ (in the case when $\mathbb{Q}_\xi$ is trivial), or the family $A_\nu(\eta)$ has a pseudo-intersection in $\mathbf{V}[G|_{\xi+1}]$. In particular, the family $A_\nu(\eta)$, which is a family of cardinality at most ω_1, is not a witness for $\mathfrak{p} = \omega_1$.

Let G be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$ and let $\mathscr{F} \subseteq [\omega]^\omega$ be an arbitrary family in $\mathbf{V}[G]$ of cardinality ω_1 which has the *sfip*. Since for each $\xi \in \omega_2$, $\mathbb{Q}_\xi$ satisfies *ccc*, by PROPOSITION 18.8, also $\mathbb{P}_{\omega_2}$ satisfies *ccc*, and therefore, by LEMMA 18.9, $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$.

Since $|\mathscr{F}| = \omega_1$, similar to CLAIM 2 in the proof of PROPOSITION 24.12, there exists a $\nu \in \omega_2$ such that the family $\mathscr{F}$ belongs to $\mathbf{V}[G|_\nu]$. In particular, there is an $\eta \in \omega_2$ such that $\mathbf{V}[G|_\nu] \vDash \mathscr{F} = A_\nu(\eta)$. Hence, for $\xi = g^{-1}(\langle \nu, \eta\rangle)$, there is a pseudo-intersection for $\mathscr{F}$ in $\mathbf{V}[G|_{\xi+1}]$, and since $\mathscr{F}$ was arbitrary, we get $\mathbf{V}[G] \vDash \mathfrak{p} \geq \omega_2$. Now, since $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$, we finally get $\mathbf{V}[G] \vDash \mathfrak{p} = \mathfrak{c} = \omega_2$. ⊣

On the Consistency of $\mathsf{MA} + \neg\mathsf{CH}$

In this section we shall sketch the proof that $\mathsf{MA} + \mathfrak{c} = \omega_2$ is consistent with ZFC (for the general case see RELATED RESULT 103). The crucial point in the proof is the fact that every *ccc* forcing notion is equivalent to a forcing notion of cardinality strictly less than $\mathfrak{c}$; but let us recall first Martin's Axiom:

> Martin's Axiom (MA): If $\mathbb{P} = (P, \leq)$ is a partially ordered set which satisfies *ccc*, and $\mathscr{D}$ is a set of less than $\mathfrak{c}$ open dense subsets of P, then there exists a $\mathscr{D}$-generic filter on P.

At first glance, we can build a model in which we have $\mathsf{MA}+\neg\mathsf{CH}$ by starting in some model of $\mathsf{ZFC}+\neg\mathsf{CH}$, and then add a $\mathscr{D}$-generic filters for every partially ordered set $\mathbb{P} = (P, \leq)$ satisfying *ccc*. However, the collection of all partially ordered sets satisfying *ccc* is a proper *class*. So, we first have to show that it is enough to consider just the *set* of *ccc* partially ordered sets $\mathbb{P} = (P, \leq)$ satisfying $|P| < \mathfrak{c}$:

LEMMA 19.2. *The following statements are equivalent:*

(a) MA.

(b) If $\mathbb{P} = (P, \leq)$ is a partially ordered set that satisfies ccc and $|P| < \mathfrak{c}$, and if $\mathscr{D}$ is a set of less than $\mathfrak{c}$ open dense subsets of P, then there exists a $\mathscr{D}$-generic filter on P.

Proof. Obviously it is enough to prove that (b) implies (a): Let P be a *ccc* partially ordered set, and let $\mathscr{D}$ be a family of fewer than $\mathfrak{c}$ open dense subsets of P, *i.e.*, $|\mathscr{D}| = \kappa$ for some $\kappa < \mathfrak{c}$. For each $D \in \mathscr{D}$, let $A_D \subseteq D$ be a maximal incompatible subset of D. Then, since $\mathbb{P}$ satisfies *ccc*, each A_D is countable. Now, we can construct a set $Q \subseteq P$ of cardinality at most κ such that Q contains each A_D, and whenever $p, q \in Q$ are compatible in P, then they are also compatible in Q (*i.e.*, there is an $r \in Q$ such that $p \leq r \geq q$) — for the latter notice that $\big|[\kappa]^2\big| = \kappa$. By construction of Q we get that for each $D \in \mathscr{D}$, A_D is a maximal anti-chain in Q. Finally, for each $D \in \mathscr{D}$ let $E_D = \big\{q \in Q : \exists p \in A_D\,(q \geq p)\big\}$. Then each E_D is open dense in Q.

Now, $(Q, \leq)$ is a partially ordered set which satisfies *ccc* and $|Q| \leq \kappa < \mathfrak{c}$. Thus, by (b), there is a filter G on Q that meets every open dense set E_D, and consequently, $\bar{G} = \big\{p \in P : \exists q \in G\,(p \leq q)\big\}$ is a $\mathscr{D}$-generic filter on P. ⊣

PROPOSITION 19.3. $\mathsf{MA} + \mathfrak{c} = \omega_2$ *is consistent with* ZFC.

Proof (Sketch). The proof is essentially the same as the proof of PROPOSITION 19.1. We start again in a model $\mathbf{V}$ of ZFC in which $\mathfrak{c} = \omega_1$ and $2^{\omega_1} = \omega_2$, and extend $\mathbf{V}$ by a finite support iteration $\mathbb{P}_{\omega_2} = \langle \mathbb{Q}_\xi : \xi \in \omega_2 \rangle$, where for each $\xi \in \omega_2$, $\mathbb{Q}_\xi = (Q_\xi, \leq)$ satisfies *ccc* and $Q_\xi \subseteq \omega_1$. Since in the final model $\mathbf{V}[G]$ we have $\mathfrak{c} = \omega_2$, by LEMMA 19.2 we can arrange the iteration so that every *ccc* forcing notion in $\mathbf{V}[G]$ of size $< \omega_2$ is isomorphic to some forcing notion $\mathbb{Q}_\xi$ (for some $\xi \in \omega_2$). A minor problem is that by adding new generic sets, we also might add new dense subsets to old partially ordered sets. This problem is solved by making sure that every *ccc* forcing notion $\mathbb{Q}_\xi$ appears arbitrarily late in the iteration, which is done by a bookkeeping function similar to that used in the proof of PROPOSITION 19.1. $\dashv$

$\mathfrak{p} = \mathfrak{c}$ is Preserved under Adding a Cohen Real

The following result, which will be used in the proof of PROPOSITION 27.9, shows that $\mathfrak{p} = \mathfrak{c}$ is preserved under adding a Cohen real (*cf.* RELATED RESULT 104).

THEOREM 19.4. *If* $\mathbf{V} \vDash \mathfrak{p} = \mathfrak{c}$ *and* c *is a Cohen real over* $\mathbf{V}$, *then* $\mathbf{V}[c] \vDash \mathfrak{p} = \mathfrak{c}$.

Proof. Throughout this proof, we shall consider the Cohen forcing notion $\mathbb{C} = \big(\bigcup_{n\in\omega} {}^n 2, \subseteq\big)$. Let $\mathbf{V}$ be a model of ZFC and let $c \in {}^\omega 2$ be a Cohen real over $\mathbf{V}$.

If $\mathbf{V} \vDash \mathsf{CH}$, then also $\mathbf{V}[c] \vDash \mathsf{CH}$ which implies $\mathbf{V}[c] \vDash \mathfrak{p} = \mathfrak{c}$. So, let us assume that $\mathbf{V} \vDash \mathfrak{c} > \omega_1$ and therefore, since Cohen forcing preserves cardinals, $\mathbf{V}[c] \vDash \mathfrak{c} > \omega_1$.

We have to show that every family $\{X_\alpha \in [\omega]^\omega : \alpha \in \kappa < \mathfrak{c}\}$ in $\mathbf{V}[c]$ which has the *sfip* has also a pseudo-intersection. To start with, fix a cardinal κ with $\omega_1 \leq \kappa < \mathfrak{c}$, and let $\{X_\alpha : \alpha \in \kappa\} \subseteq [\omega]^\omega$ be an arbitrary but fixed family in $\mathbf{V}[c]$ which has the *sfip*. Furthermore, let

$$\{\underset{\sim}{X}_\alpha : \alpha \in \kappa\}$$

be a set of $\mathbb{C}$-names such that $\{\underset{\sim}{X}_\alpha[c] : \alpha \in \kappa\} = \{X_\alpha : \alpha \in \kappa\}$. Now, since $\{X_\alpha : \alpha \in \kappa\}$ has the *sfip* in $\mathbf{V}[c]$, there exists a $\mathbb{C}$-condition q such that for all $E \in \operatorname{fin}(\kappa)$ we have

$$q \Vdash_{\mathbb{C}} \big|\bigcap \{\underset{\sim}{X}_\alpha : \alpha \in E\}\big| = \omega\,,$$

where we define $\bigcap \emptyset := \omega$. For the sake of simplicity, let us assume that $q = \mathbf{0}$. The goal is now to construct a set $Y \in \mathbf{V}[c]$ which is a pseudo-intersection of $\{\underset{\sim}{X}_\alpha[c] : \alpha \in \kappa\}$. For this, we define (in $\mathbf{V}$) the following σ-centred forcing notion $\mathbb{P} = (P, \leq)$:

The set of $\mathbb{P}$-conditions P consists of pairs $\langle h, A\rangle$, where $A \in \text{fin}(\kappa)$ and

$$h : \bigcup \{{}^k2 : k \in m\} \to \text{fin}(\omega) \qquad \text{for some } m \in \omega\,.$$

For $\langle h, A\rangle, \langle l, B\rangle \in P$, let $\langle h, A\rangle \leq \langle l, B\rangle$ if and only if

- $h \subseteq l$, $A \subseteq B$, and
- for each $p \in \text{dom}(l) \setminus \text{dom}(h)$ we have $p \Vdash_{\mathbb{C}} l(p) \subseteq \bigcap \{\underset{\sim}{X}_\alpha : \alpha \in A\}$.

We leave it as an exercise to the reader to show that $|P| = \kappa$ and that $\mathbb{P}$ is σ-centred — for the latter, notice that for any $\langle h, A\rangle, \langle h, B\rangle \in P$ we have $\langle h, A\rangle \leq \langle h, A \cup B\rangle \geq \langle h, B\rangle$. Now, for every $\alpha \in \kappa$ and $n \in \omega$ we define the set $D_{\alpha,n} \subseteq P$ by stipulating $\langle h, A\rangle \in D_{\alpha,n}$ if and only if

- $\alpha \in A$,
- $\text{dom}(h) = \{{}^k2 : k \in m\}$ for some $m \geq n$,
- for each $p \in {}^m2$, $\left|\bigcup_{i\in m} h(p|_i)\right| \geq n$.

We leave it as an exercise to the reader to show that every set $D_{\alpha,n}$ is an open dense subset of P and that $\left|\{D_{\alpha,n} : \alpha \in \kappa \wedge n \in \omega\}\right| = \kappa$. The open dense sets $D_{\alpha,n}$ make sure that the set Y, constructed below, will be a pseudo-intersection of $\{\underset{\sim}{X}_\alpha[c] : \alpha \in \kappa\}$, in particular, Y will be infinite. At the moment, just notice the following fact: If $\langle h, A\rangle \in D_{\alpha,n}$ and $\langle h, A\rangle \leq \langle l, B\rangle$, where $\text{dom}(l) = \{{}^k2 : k \in m\}$, then for each $p \in {}^m2$ we have $\left|\bigcup_{i\in m} l(p|_i)\right| \geq n$, and for each $p \in \text{dom}(l) \setminus \text{dom}(h)$ we have $p \Vdash_{\mathbb{C}} l(p) \subseteq \underset{\sim}{X}_\alpha$.

The crucial point is now to show that there exists a filter $G \subseteq P$ in $\mathbf{V}$ which meets every set $D_{\alpha,n}$.

Claim. *Let $\mathscr{D} = \{D_{\alpha,n} : n \in \omega \wedge \alpha \in \kappa\}$. Then there exists in $\mathbf{V}$ a $\mathscr{D}$-generic filter G on P, i.e., there exists a directed and downwards closed set $G \subseteq P$ which meets every open dense subset of P which belongs to $\mathscr{D}$.*

Proof of Claim. The following proof is essentially the proof of the fact that $\mathfrak{p} = \mathfrak{c}$ is equivalent to $\mathsf{MA}(\sigma\text{-centred})$ (see Chapter 13 | Related Result 79).

Firstly notice that for each $m \in \omega$ there are just countably many functions $h : \bigcup \{{}^k2 : k \in m\} \to \text{fin}(\omega)$. For each $m \in \omega$ fix an enumeration $\{h_{m,i} : i \in \omega\}$ of all these countably many functions and let $\eta : \omega \times \omega \to \omega$ be a bijection. For each $n \in \omega$ we define the set $P_n \subseteq P$ by stipulating

$$P_n = \{\langle h_{m,i}, A\rangle \in P : \eta(\langle m, i\rangle) = n\}\,.$$

Notice that $\bigcup_{n\in\omega} P_n = P$ and that each P_n consists of pairwise compatible $\mathbb{P}$-conditions.

Secondly, for each $\mathbb{P}$-condition $p = \langle h, A\rangle \in P$ and for every open dense set $D \in \mathscr{D}$ let

$$[p, D] = \{n \in \omega : \exists q \in P_n (q \in D \wedge q \geq p)\}\,.$$

Notice that $[p, D] \in [\omega]^\omega$. Furthermore, for all $k, r \in \omega$, any $\mathbb{P}$-conditions $\langle h, A_0\rangle, \dots, \langle h, A_k\rangle \in P_r$, and any open dense sets $D_0, \dots, D_k \in \mathscr{D}$, we get that $\bigcap_{i \leq k} \bigl[\langle h, A_i\rangle, D_i\bigr]$ is infinite. This implies that for each $r \in \omega$, the family $\mathscr{F}_r = \bigl\{[p, D] : p \in P_r \wedge D \in \mathscr{D}\bigr\}$ has the *sfip*. Now, since $\mathbf{V} \vDash \mathfrak{p} = \mathfrak{c}$ and $|\mathscr{F}_r| = |P_r \times \mathscr{D}| \leq \kappa \times \kappa = \kappa < \mathfrak{c}$, we have $\mathbf{V} \vDash |\mathscr{F}_r| < \mathfrak{p}$. Hence, in $\mathbf{V}$ there exists a pseudo-intersection I_r of $\mathscr{F}_r$. In other words, for every $r \in \omega$ there is an $I_r \in [\omega]^\omega$ such that for all $p \in P_r$ and $D \in \mathscr{D}$, $I_r \setminus [p, D]$ is finite.

In the following step we encode the elements of the sets I_r by finite sequences: Let $\mathrm{seq}(\omega)$ be the set of all finite sequences which can be formed with elements of ω. For $s \in \mathrm{seq}(\omega)$ and $i \in \omega$, $s^\frown i$ denotes the concatenation of the sequences s and $\langle i\rangle$.

Now, define the function $\nu : \mathrm{seq}(\omega) \to \omega$ by stipulating

- $\nu(\emptyset) = 0$, and
- for all $s \in \mathrm{seq}(\omega)$: $\bigl\{\nu(s^\frown i) : i \in \omega\bigr\}$ enumerates $I_{\nu(s)}$ in ascending order.

In particular, $\bigl\{\nu(\langle i\rangle) : i \in \omega\bigr\} = I_0$, where for all $i, i' \in \omega$, $i < i'$ implies $\nu(\langle i\rangle) < \nu(\langle i'\rangle)$.

Furthermore, for every $D \in \mathscr{D}$ and every $s \in \mathrm{seq}(\omega)$ we choose a $\mathbb{P}$-condition $p^s_D \in P_{\nu(s)}$ such that for all $i \in \omega$,

$$\nu(s^\frown i) \in \bigl[p^s_D, D\bigr] \;\to\; \bigl(p^s_D \leq p^{s^\frown i}_D\bigr) \wedge \bigl(p^{s^\frown i}_D \in D\bigr). \tag{$*$}$$

Notice that for any $D \in \mathscr{D}$ and $s \in \mathrm{seq}(\omega)$, $I_{\nu(s)} \setminus \bigl[p^s_D, D\bigr]$ is finite. Thus, for each $D \in \mathscr{D}$ and each $s \in \mathrm{seq}(\omega)$ there is a least integer $g_D(s) \in \omega$ such that for every $i \geq g_D(s)$ we have $\nu(s^\frown i) \in \bigl[p^s_D, D\bigr]$. So, for every $D \in \mathscr{D}$, we obtain a function $g_D : \mathrm{seq}(\omega) \to \omega$. Then, the family $\mathscr{E} = \{g_D : D \in \mathscr{D}\}$ is a family of size κ of functions from the countable set $\mathrm{seq}(\omega)$ to ω.

Now we show that $\mathscr{E}$ is bounded: For this, recall first that for the bounding number $\mathfrak{b}$ we have $\mathfrak{p} \leq \mathfrak{b} \leq \mathfrak{c}$ (see Chapter 8). Since in $\mathbf{V}$ we have $\mathfrak{p} = \mathfrak{c}$, in particular $\mathbf{V} \vDash \mathfrak{b} = \mathfrak{c}$, and since $|\mathscr{E}| = \kappa < \mathfrak{c}$, $\mathbf{V} \vDash |\mathscr{E}| < \mathfrak{b}$. Thus, $\mathscr{E}$ is bounded in $\mathbf{V}$, *i.e.*, in $\mathbf{V}$ there exists a function $g : \mathrm{seq}(\omega) \to \omega$ such that for each $D \in \mathscr{D}$,

$$g_D(s) < g(s) \qquad \text{for all but finitely many } s \in \mathrm{seq}(\omega).$$

By induction on $n \in \omega$, define the function $f \in {}^\omega\omega$ such that for all $n \in \omega$, $f(n) := g(f|_n)$. Then, by definition of f and the property of g, for each $D \in \mathscr{D}$,

$$g_D(f|_n) < f(n) \qquad \text{for all but finitely many } n \in \omega.$$

In other words, for every $D \in \mathscr{D}$ there exists an integer $m_D \in \omega$ such that for all $n \geq m_D$, $f(n) > g_D(f|_n)$.

We are now ready to define the $\mathscr{D}$-generic set $G \subseteq P$, but before we do so, let us summarise a few facts which we have achieved so far: Let $D \in \mathscr{D}$ and $n \geq m_D$ be arbitrary, and let $s := f|_n$ and $i := f(n)$.

(0) $f(n) = g(f|_n) = g(s)$, *i.e.*, $i = g(s)$, and $f(n+1) = g(f|_{n+1}) = g(s^\frown i)$.

(1) Since $n \geq m_D$, we get $g(f|_n) > g_D(f|_n)$, *i.e.*, $g(s) > g_D(s)$, and therefore $i > g_D(s)$.

(2) Since $i > g_D(s)$, we get $\nu(s^\frown i) \in \big[p^s_D, D\big]$, *i.e.*,

$$\nu(f|_{n+1}) \in \big[p^{f|_n}_D, D\big] .$$

(3) Thus, by $(*)$ and (2) we get $p^s_D \leq p^{s^\frown i}_D$ and $p^{s^\frown i}_D \in D$, *i.e.*,

$$p^{f|_n}_D \leq p^{f|_{n+1}}_D \quad \text{and} \quad p^{f|_{n+1}}_D \in D .$$

Now, let $G \subseteq P$ be defined by

$$G = \big\{q \in P : \exists D \in \mathscr{D}\, \exists n \in \omega \,\big(n \geq m_D \wedge q \leq p^{f|_n}_D\big)\big\} .$$

It remains to check that G has the required properties, *i.e.*, G is a filter which meets every $D \in \mathscr{D}$.

G is a filter: By definition, G is downwards closed. To see that G is directed, take any $q, q' \in G$ and, for some $D, D' \in \mathscr{D}$ and $n, n' \in \omega$, let $p^{f|_n}_D, p^{f|_{n'}}_{D'} \in G$ be such that $q \leq p^{f|_n}_D$ and $q' \leq p^{f|_{n'}}_{D'}$. Without loss of generality we may assume that $n \geq n'$. Then $p^{f|_n}_{D'} \geq p^{f|_{n'}}_{D'}$. Now, $p^{f|_n}_D$ and $p^{f|_n}_{D'}$ both belong to $P_{\nu(f|_n)}$ and are therefore compatible. Thus, there exists an $r \in P_{\nu(f|_n)}$ such that $p^{f|_n}_D \leq r \geq p^{f|_n}_{D'}$, and consequently we have $q \leq r \geq q'$ where $r \in G$.

G is $\mathscr{D}$-generic: By (3), for each $D \in \mathscr{D}$ and every $n \geq m_D$ we have $p^{f|_{n+1}}_D \in D \cap G$, and hence, $G \cap D \neq \emptyset$. $\dashv_{\text{Claim}}$

With the $\mathscr{D}$-generic filter $G \subseteq P$ constructed above we define the function

$$H = \bigcup \big\{h : \exists\big[\langle h, A\rangle \in G\big]\big\} .$$

By construction, the function $H : \bigcup_{n\in\omega} {}^n2 \to \omega$ has the following property: If $\alpha \in \kappa$ and $\langle h, A\rangle \in G$ with $\alpha \in A$, then for every $p \in \bigcup_{n\in\omega} {}^n2 \setminus \operatorname{dom}(h)$ we have

$$p \Vdash_{\mathbb{C}} H(p) \subseteq \underset{\sim}{X}_\alpha .$$

In particular, if c is a Cohen real over $\mathbf{V}$, then for $Y := \bigcup_{n\in\omega} H(c|_n)$, which is a set in $\mathbf{V}[c]$, we have

$$\mathbf{V}[c] \vDash \forall\alpha \in \kappa\big(Y \subseteq^* \underset{\sim}{X}_\alpha[c]\big) .$$

We leave it as an exercise to the reader to show that $\mathbf{V}[c] \vDash |Y| = \omega$ (for this, recall the definition of the open dense sets $D_{\alpha,n}$). Thus, in $\mathbf{V}[c]$, the arbitrarily chosen family $\big\{\underset{\sim}{X}_\alpha[c] : \alpha \in \kappa < \mathfrak{c}\big\}$ has a pseudo-intersection, which shows that $\mathbf{V}[c] \vDash \mathfrak{p} = \mathfrak{c}$. $\dashv$

Notes

The consistency of $\mathsf{MA}+\neg\mathsf{CH}$. A complete proof for the consistency of $\mathsf{MA}+\neg\mathsf{CH}$ with ZFC can be found for example in Kunen [5, Chapter VIII, §6] (see also Martin and Solovay [6]).

On $\mathfrak{p} = \mathfrak{c}$ ***after adding one Cohen real.*** THEOREM 19.4 is due to Roitman [7], but the proof given here follows the proof of Bartoszyński and Judah [1, Theorem 3.3.8], where the proof of the CLAIM, originally proved by Bell [2], is taken from Fremlin [3, 14C].

Related Results

102. *On the consistency of* $\mathfrak{p} = \kappa$. Let $\mathbf{V}$ be a model of $\mathsf{ZFC}+\mathsf{GCH}$ and assume that in $\mathbf{V}$, κ is an uncountable regular cardinal such that $\big|[\kappa]^{<\kappa}\big| = \kappa$. Then, by a slight modification of the proof of PROPOSITION 19.1, we get a generic extension of $\mathbf{V}$ in which $\mathfrak{p} = \kappa$.

103. *On the consistency of* $\mathsf{MA} + \mathfrak{c} = \kappa$. As in RELATED RESULT 103, let $\mathbf{V}$ be again a model of $\mathsf{ZFC}+\mathsf{GCH}$ and assume that in $\mathbf{V}$, κ is an uncountable regular cardinal such that $\big|[\kappa]^{<\kappa}\big| = \kappa$. Then there exists a *ccc* forcing notion $\mathbb{P}$ in $\mathbf{V}$, such that in the $\mathbb{P}$-generic extension $\mathbf{V}[G]$ we have $\mathsf{MA} + \mathfrak{c} = \kappa$ (for a proof see Kunen [5, Chapter VIII, Theorem 6.3]).

104. *Martin's Axiom and Cohen reals.* By Chapter 13 | RELATED RESULT 79, which asserts $\mathfrak{p} = \mathfrak{c} \iff \mathsf{MA}(\sigma\text{-centred})$, we get that $\mathbf{V} \vDash \mathsf{MA}(\sigma\text{-centred})$ if and only if $\mathbf{V} \vDash \mathfrak{p} = \mathfrak{c}$. Hence, THEOREM 19.4 implies that $\mathsf{MA}(\sigma\text{-centred})$ is preserved under Cohen forcing, *i.e.*, if $\mathbf{V} \vDash \mathsf{MA}(\sigma\text{-centred})$ and c is a Cohen real over $\mathbf{V}$, then $\mathbf{V}[c] \vDash \mathsf{MA}(\sigma\text{-centred})$. However, this is not the case for full MA. In fact one can show that if $\mathbf{V} \vDash \neg\mathsf{CH}$ and c is a Cohen real over $\mathbf{V}$, then $\mathbf{V}[c] \vDash \neg\mathsf{MA}$. The proof uses the fact that if $\mathbf{V} \vDash \mathsf{MA}(\omega_1)$, then there is no *Suslin tree* in $\mathbf{V}$ (see for example Jech [4, Theorem 16.16]). On the other hand, one can show that whenever c is a Cohen real over $\mathbf{V}$, then $\mathbf{V}[c]$ contains a Suslin tree (see Shelah [8, §1], Todorčević [9], or Bartoszyński and Judah [1, Section 3.3.A]).

References

1. TOMEK BARTOSZYŃSKI AND HAIM JUDAH, ***Set Theory: on the structure of the real line***, A. K. Peters, Wellesley, 1995.
2. MURRAY G. BELL, *On the combinatorial principle* $P(\mathfrak{c})$, ***Fundamenta Mathematicae***, vol. 114 (1981), 149–157.
3. DAVID H. FREMLIN, ***Consequences of Martin's axiom***, Cambridge Tracts in Mathematics 84, Cambridge University Press, Cambridge, 1984.
4. THOMAS JECH, ***Set Theory,*** *The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
5. KENNETH KUNEN, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.
6. DONALD A. MARTIN AND ROBERT M. SOLOVAY, *Internal Cohen extensions*, ***Annals of Mathematical Logic***, vol. 2 (1970), 143–178.

7. JUDY ROITMAN, *Adding a random or a Cohen real: topological consequences and the effect on Martin's axiom*, ***Fundamenta Mathematicae***, vol. 103 (1979), 47–60.
8. SAHARON SHELAH, *Can you take Solovay's inaccessible away?*, ***Israel Journal of Mathematics***, vol. 48 (1984), 1–47.
9. STEVO TODORČEVIĆ, *Partitioning pairs of countable sets*, ***Proceedings of the American Mathematical Society***, vol. 111 (1991), 841–844.

Part III

Combinatorics of Forcing Extensions

...the parts sing one after another in so-called fugue (fuga) or consequence (consequenza), which some also call reditta. All mean the same thing: a certain repetition of some notes or of an entire melody contained in one part by another part, after an interval of time. The second part sings the same note values or different ones, and the same intervals of whole tones, semitones, or similar ones.
There are two type of fugues or consequences namely strict and free.
In free writing, the imitating voice duplicates the other in fugue or consequence only up to a point; beyoind that point it is free to proceed independently.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

Properties of Forcing Extensions

In this chapter we shall introduce some combinatorial properties of forcing notions which will accompany us throughout the remainder of this book. Furthermore, these properties will be the main tool in order to investigate various combinatorial properties of generic models of ZFC.

However, before we start with some definitions, let us modify our notation concerning names in the forcing language: Let $\mathbb{P}$ be a forcing notion and let G be $\mathbb{P}$-generic over some ground model $\mathbf{V}$.

- Instead of canonical $\mathbb{P}$-names for sets in $\mathbf{V}$ like $\underset{\cdot}{\emptyset}$, $\underset{\cdot}{27}$, $\underset{\cdot}{\omega}$, *et cetera*, we just write $\emptyset$, 27, ω, *et cetera*.
- If $\underset{\sim}{f}$ is a $\mathbb{P}$-name for a function in $\mathbf{V}[G]$ with domain $A \in \mathbf{V}$ and $a \in A$, then we write
$$\underset{\sim}{f}(a) \text{ instead of } f\underset{\sim}{(a)}\,.$$

For example, if $\mathbb{P} = \mathbb{C}$ and $\underset{\cdot}{c}$ is the canonical name for a Cohen real $c \in {}^{\omega}\omega$, then, for $k \in \omega$, $\underset{\cdot}{c}(k) = \big\{\langle \underset{\cdot}{m}, p\rangle : p \in \bigcup_{n\in\omega} {}^{n}\omega \wedge k \in \operatorname{dom}(p) \wedge p(k) = m\big\}$ denotes the canonical $\mathbb{C}$-name for the integer $c(k)$ — properly denoted by $c(\underset{\cdot}{k})$.

Dominating, Splitting, Bounded, and Unbounded Reals

First we recall some notions defined in Chapter 8: For two functions $f, g \in {}^{\omega}\omega$ we say that g is **dominated** by f, denoted $g <^* f$, if there is an $n \in \omega$ such that for all $k \geq n$ we have $g(k) < f(k)$. For two sets $x, y \in [\omega]^{\omega}$ we say that x **splits** y if $y \cap x$ as well as $y \setminus x$ is infinite.

Now let $\mathbf{V}$ be any model of ZFC and let $\mathbf{V}[G]$ be a generic extension (*i.e.*, G is $\mathbb{P}$-generic over $\mathbf{V}$ with respect to some forcing notion $\mathbb{P}$). Let $f \in {}^{\omega}\omega$ be a function in the model $\mathbf{V}[G]$. Then f is called a **dominating real** (over $\mathbf{V}$) if each function $g \in {}^{\omega}\omega \cap \mathbf{V}$ is dominated by f, and f is called an **unbounded real** (over $\mathbf{V}$) if it is not dominated by any function $g \in {}^{\omega}\omega \cap \mathbf{V}$. Furthermore, a set $x \in [\omega]^{\omega}$ in $\mathbf{V}[G]$ is called a **splitting real** (over $\mathbf{V}$) if it splits each set

$y \in [\omega]^\omega$ in the ground model $\mathbf{V}$. Notice that we identify functions $f \in {}^\omega\omega$ with real numbers.

FACT 20.1. *If $\mathbf{V}[G]$ contains a dominating real, then it also contains a splitting real.*

Proof. We can just follow the proof of THEOREM 8.4: Whenever a function $f \in {}^\omega\omega$ belongs $\mathbf{V}[G]$, then also the set

$$\sigma_f = \bigcup \Big\{ \big[f^{2n}(0), f^{2n+1}(0)\big) : n \in \omega \Big\}$$

belongs to $\mathbf{V}[G]$, where $[a,b) = \{k \in \omega : a \le k < b\}$ and $f^{n+1}(0) = f\big(f^n(0)\big)$ with $f^0(0) := 0$. Now let $f \in {}^\omega\omega$ be a dominating real. Without loss of generality we may assume that f is strictly increasing and that $f(0) > 0$. Fix any $x \in [\omega]^\omega \cap \mathbf{V}$ and let $g_x : \omega \to x$ be the (unique) strictly increasing bijection between ω and x. Since f is dominating we have $g_x <^* f$, which implies that there is an $n_0 \in \omega$ such that for all $k \ge n_0$ we have $g_x(k) < f(k)$. For each $k \in \omega$ we have $k \le f^k(0)$ as well as $k \le g_x(k)$. Moreover, for $k \ge n_0$ we have

$$f^k(0) \le g_x\big(f^k(0)\big) < f\big(f^k(0)\big) = f^{k+1}(0)$$

and therefore $g_x\big(f^k(0)\big) \in \big[f^k(0), f^{k+1}(0)\big)$. Thus, for all $k \ge n_0$ we have $g_x\big(f^k(0)\big) \in \sigma_f$ *iff* k is even, which shows that both $x \cap \sigma_f \cap x$ and $x \setminus \sigma_f$ are infinite. Hence, since $x \in [\omega]^\omega$ was arbitrary, σ_f is a splitting real. $\dashv$

It is worth mentioning that the converse of FACT 20.1 does not hold, *i.e.*, we cannot construct a dominating real from a splitting real (*cf.* LEMMA 21.2 and LEMMA 21.3).

A forcing notion $\mathbb{P}$ is said to *add dominating (unbounded, splitting) reals* if every $\mathbb{P}$-generic extension of $\mathbf{V}$ contains a dominating (unbounded, splitting) real. More formally, let $\mathbf{V} \vDash \mathsf{ZFC}$ and let $\mathbb{P} \in \mathbf{V}$ be a forcing notion. Then we say that

$\mathbb{P}$ adds dominating reals *iff* $\mathbf{0} \Vdash_{\mathbb{P}} \exists \underset{\sim}{f} \in {}^\omega\underset{\sim}{\omega}\, \forall g \in {}^\omega\omega (g <^* \underset{\sim}{f})$,

$\mathbb{P}$ adds unbounded reals *iff* $\mathbf{0} \Vdash_{\mathbb{P}} \exists \underset{\sim}{f} \in {}^\omega\underset{\sim}{\omega}\, \forall g \in {}^\omega\omega (\underset{\sim}{f} \not<^* g)$,

and

$\mathbb{P}$ adds splitting reals *iff* $\mathbf{0} \Vdash_{\mathbb{P}} \exists \underset{\sim}{x} \subseteq \omega\, \forall y \in [\omega]^\omega \big(|y \cap \underset{\sim}{x}| = |y \setminus \underset{\sim}{x}| = \omega\big)$.

Notice that in this context, *i.e.*, in statements being forced, ${}^\omega\omega$ and $[\omega]^\omega$ stand for the canonical names for sets in the ground model, whereas for example ${}^\omega\underset{\sim}{\omega}$ is a $\mathbb{P}$-name for the set ${}^\omega\omega$ in the $\mathbb{P}$-generic extension.

A forcing notion $\mathbb{P}$ is called $\boldsymbol{{}^\omega\omega}$**-bounding** if there are no unbounded reals in $\mathbb{P}$-generic extensions. In other words, if $\mathbb{P}$ is ${}^\omega\omega$-bounding and G is $\mathbb{P}$-generic over $\mathbf{V}$, then every function $f \in {}^\omega\omega$ in $\mathbf{V}[G]$ is dominated by some function from the ground model $\mathbf{V}$. Obviously, a forcing notion which adds a dominating real also adds unbounded reals and therefore cannot be ${}^{\omega}\omega$-bounding, and by FACT 20.1, such a forcing notion also adds splitting reals. On the other hand, none of these implications is reversible. An example of a forcing notion which is ${}^{\omega}\omega$-bounding but adds splitting reals is Silver forcing (investigated in Chapter 22), and Cohen forcing, discussed in the next chapter, is an example of a forcing notion which adds unbounded and splitting reals but does not add dominating reals. Furthermore, Miller forcing (discussed in Chapter 23) adds unbounded reals but does not add splitting reals, and Mathias forcing (discussed in Chapter 24) adds dominating reals but does not add Cohen reals.

The Laver Property and Not Adding Cohen Reals

In the following chapters we shall investigate different forcing notions like Cohen forcing, Silver forcing, Mathias forcing, *et cetera*. In fact, we shall investigate what kind of new reals (*e.g.*, dominating reals or Cohen reals) are added by (an iteration of) a given forcing notion. In particular, we have to decide whether an iteration of a given forcing notion adds Cohen reals. Our main tool to solve this problem will be the following combinatorial property.

> LAVER PROPERTY: Let $\mathcal{F}$ be the set of all functions $S : \omega \to \operatorname{fin}(\omega)$ such that for every $n \in \omega$, $|S(n)| \leq 2^n$. A forcing notion $\mathbb{P}$ has the **Laver property** if and only if for every function $f \in {}^{\omega}\omega \cap \mathbf{V}$ in the ground model and every $\mathbb{P}$-name $\underset{\sim}{g}$ for a function in ${}^{\omega}\omega$ such that $\mathbf{0} \Vdash_{\mathbb{P}} \forall n \in \omega\big(\underset{\sim}{g}(n) \leq f(n)\big)$, we have $\mathbf{0} \Vdash_{\mathbb{P}} \exists S \in \mathcal{F} \cap \mathbf{V}\ \forall n \in \omega\big(\underset{\sim}{g}(n) \in S(n)\big)$.

Roughly speaking, if a forcing notion has the Laver property, then for every function $g \in {}^{\omega}\omega$ in the generic extension which is bounded by a function from the ground model, and for every $n \in \omega$, the value $g(n)$ belongs to some finite set of size 2^n and the sequence of these finite sets is in the ground model.

Now we show that a forcing notion which has the Laver property does not add Cohen reals.

PROPOSITION 20.2. *If the forcing notion $\mathbb{P}$ has the Laver property, then $\mathbb{P}$ does not add Cohen reals.*

Proof. Suppose that $\mathbb{P}$ has the Laver property. Let $\{I_n : n \in \omega\}$ be a partition of ω (in the ground model $\mathbf{V}$) such that for all $n \in \omega$, $|I_n| = 2n$ and $\max(I_n) < \min(I_{n+1})$. Let $\underset{\sim}{h}$ be a $\mathbb{P}$-name for an arbitrary element of ${}^{\omega}2$, *i.e.*, $\mathbf{0} \Vdash_{\mathbb{P}} \underset{\sim}{h} \in \underset{\sim}{{}^{\omega}2}$. We show that $\underset{\sim}{h}$ is not the name for a Cohen real, *i.e.*, $\underset{\sim}{h}$ is not the name for a real which corresponds to a $\mathbb{C}$-generic filter over $\mathbf{V}$, where $\mathbb{C} = \big(\bigcup_{n\in\omega} {}^{n}2, \subseteq\big)$.

For every $n \in \omega$, let $\underset{\sim}{H}(n) := \underset{\sim}{h}|_{I_n}$. Then $\underset{\sim}{H}(n) : I_n \to 2$, and since $|I_n| = 2n$, $\underset{\sim}{H}(n)$ amounts to an element of ${}^{2n}2$. Thus, we can encode $\underset{\sim}{H}(n)$

by a $\mathbb{P}$-name for an integer in 2^{2n}; let $\eta\big(\underset{\sim}{H}(n)\big)$ be that code and let $\underset{\sim}{g}(n) := \eta\big(\underset{\sim}{H}(n)\big)$. Thus, $\mathbf{0} \Vdash_{\mathbb{P}} \forall n \in \omega\big(\underset{\sim}{g}(n) \leq 2^{2n}\big)$, and since $\mathbb{P}$ has the Laver property, $\mathbf{0} \Vdash_{\mathbb{P}} \exists S \in \mathcal{F} \cap \mathbf{V}\ \forall n \in \omega\big(\underset{\sim}{g}(n) \in S(n)\big)$. In the ground model $\mathbf{V}$, let p_0 be a $\mathbb{P}$-condition such that for some $S \in \mathcal{F} \cap \mathbf{V}$ we have $p_0 \Vdash_{\mathbb{P}} \forall n \in \omega\big(\underset{\sim}{g}(n) \in S(n)\big)$. Further, let

$$D = \Big\{ s \in \bigcup_{n \in \omega} {}^{n}2 : \exists k \left(I_k \subseteq \operatorname{dom}(s) \wedge \eta(s|_{I_k}) \notin S(k) \right) \Big\}.$$

Then D is an open dense subset of $\bigcup_{n\in\omega} {}^{n}2$. Indeed, for any $m \in \omega$ and any $t \in {}^{m}2$ there exists $k > m$ such that $I_k \cap \operatorname{dom}(t) = \emptyset$, and we find an $s \in \bigcup_{n\in\omega} {}^{n}2$ such that $t \subseteq s$, $I_k \subseteq \operatorname{dom}(s)$, and $\eta(s|_{I_k}) \notin S(k)$ — here we use that for any positive integer k, $|S(k)| \leq 2^k < 2^{2k} = \big|{}^{I_k}2\big|$.

Now, for every $n \in \omega$ define $A_n = \big\{x \in {}^{\omega}2 : \eta(x|_{I_n}) \in S(n)\big\} \subseteq {}^{\omega}2$ and let $A = \bigcap_{n\in\omega} A_n$. Since $p_0 \Vdash_{\mathbb{P}} \forall n \in \omega\big(\underset{\sim}{g}(n) \in S(n)\big)$, we have $p_0 \Vdash_{\mathbb{P}} \underset{\sim}{h} \in A$, and consequently we get that $p_0 \Vdash_{\mathbb{P}} \forall k \in \omega\big(\underset{\sim}{h}|_k \notin D\big)$. Hence, $\underset{\sim}{h}$ is not a $\mathbb{P}$-name for a Cohen real over $\mathbf{V}$, which completes the proof. ⊣

So, we know that if a forcing $\mathbb{P}$ has the Laver property, then forcing with $\mathbb{P}$ does not add Cohen reals; but what can we say about products or iterations of $\mathbb{P}$? On the one hand, it is possible that $\mathbb{P} \times \mathbb{P}$ adds Cohen reals, even though $\mathbb{P}$ has the Laver property (see for example Chapter 24). On the other hand, in the next section we shall see that the Laver property is preserved under countable support iteration of proper forcing notions. More precisely, if $\mathbb{P}$ is a forcing notion which is *proper* (see below) and has the Laver property, then any countable support iteration of $\mathbb{P}$ has the Laver property, and therefore does not add Cohen reals.

Proper Forcing Notions and Preservation Theorems

The Notion of Properness

By PROPOSITION 18.8 we know that finite support iterations of *ccc* forcing notions satisfy *ccc*. In other words, *ccc* is preserved under finite support iteration of *ccc* forcing notions. Below, we shall present a generalisation of that result, but before we have to introduce some preliminary definitions: For every infinite regular cardinal χ let

$$\mathrm{H}_\chi = \big\{ x \in \mathrm{V}_\chi : |\operatorname{TC}(x)| < \chi \big\}.$$

For example the sets in H_ω are the *hereditarily finite* sets and the sets in $\mathrm{H}(\omega_1)$ are the *hereditarily countable* sets. Notice that each H_χ is transitive and that $x \in \mathrm{H}_\chi$ *iff* $|\operatorname{TC}(x)| < \chi$, *i.e.*, H_χ contains *all* sets which are hereditarily of cardinality $<\chi$. It is worth mentioning that for every regular uncountable cardinal χ, H_χ is a model of ZFC minus the Axiom of Power Set (*cf.* Chapter 15 | RELATED RESULT 84).

For the following discussion, let χ be a "large enough"regular cardinal, where "large enough"means that for all forcing notions $\mathbb{P} = (P, \leq)$ we shall consider in the forthcoming chapters we have $\mathscr{P}(P) \in \mathrm{H}_\chi$, *i.e.*, the power set of P is hereditarily of size $<\chi$. If we assume that GCH holds in the ground model, then $\chi = \omega_3$ would be sufficient, but to be on the safe side we let

$$\chi = \beth_\omega^+ ,$$

where the so-called *beth function* $\beth_\alpha$ is defined by induction on $\alpha \in \Omega$, stipulating $\beth_0 := \omega$, $\beth_{\alpha+1} := 2^{\beth_\alpha}$, and for limit ordinals α, $\beth_\alpha := \bigcup \{\beth_\beta : \beta \in \alpha\}$.

Let $\mathbf{N} = (N, \in)$ be an elementary submodel of $(\mathrm{H}_\chi, \in)$, *i.e.*, $(N, \in) \prec (\mathrm{H}_\chi, \in)$. Furthermore, let $\mathbb{P} = (P, \leq)$ be a forcing notion such that $(P, \leq) \in \mathbf{N}$. Since $\mathbf{N}$ is an elementary submodel of $(\mathrm{H}_\chi, \in)$, for all $p, q \in P \cap N$ we have $\mathbf{N} \vDash p \perp q$ implies $\mathbf{V} \vDash p \perp q$, *i.e.*, if p and q are incompatible in $\mathbf{N}$, then they are also incompatible in the ground model $\mathbf{V}$. We say that $G \subseteq P$ is **N-generic for** $\mathbb{P}$ if G has the following property.

> Whenever $D \in N$ and $\mathbf{N} \vDash$ "*$D \subseteq P$ is an open dense subset of P*", then $G \cap N \cap D \neq \emptyset$.

Notice that G is $\mathbf{N}$-generic *iff* $G \cap N$ is $\mathbf{N}$-generic. By FACT 14.6, we can replace "open dense" for example by "maximal anti-chain". Furthermore, we say that a condition $q \in P$, which is not necessarily in N, is **N-generic** if

$$\mathbf{V} \vDash q \Vdash_{\mathbb{P}} \text{“}\underset{\cdot}{G} \textit{ is } \mathbf{N}\textit{-generic”},$$

where $\underset{\cdot}{G}$ is the canonical $\mathbb{P}$-name for the $\mathbb{P}$-generic filter over the ground model $\mathbf{V}$. Notice that if q is $\mathbf{N}$-generic and $q' \geq q$, then q' is $\mathbf{N}$-generic too.

Now, a forcing notion $\mathbb{P} = (P, \leq)$ is called **proper**, if for all countable elementary submodels $\mathbf{N} = (N, \in) \prec (\mathrm{H}_\chi, \in)$ which contain $\mathbb{P}$, and for all conditions $p \in P \cap N$, there exists a condition $q \geq p$ (in $\mathbf{V}$) which is $\mathbf{N}$-generic.

As a first example let us show that any forcing notion $\mathbb{P} = (P, \leq)$ which satisfies *ccc* is proper: Firstly, for any countable set $A \in N$ we have $A \subseteq N$. For this, notice that since $(N, \in) \prec (\mathrm{H}_\chi, \in)$, A must be the range of a function $f : \omega \to \bigcup N$ which belongs to $\mathbf{N}$, and since for all $n \in \omega$, $n \in N$, we also have $f(n) \in N$ for all $n \in \omega$, which shows that $A \subseteq N$. Now, let $A \in N$ be a maximal anti-chain in P. Then, since $\mathbb{P}$ satisfies *ccc*, A is countable and we have $A \subseteq N$. Further, $\mathbf{0} \Vdash_{\mathbb{P}} A \cap \underset{\cdot}{G} \neq \emptyset$, and therefore, $\mathbf{0} \Vdash_{\mathbb{P}} A \cap N \cap \underset{\cdot}{G} = A \cap \underset{\cdot}{G} \neq \emptyset$.

As a second example let us show that any forcing notion $\mathbb{P}(P, \leq)$ which is σ-closed is proper: Since the model $\mathbf{N}$ is countable, there are just countably many open dense subsets of P which belong to $\mathbf{N}$, say $\{D_n : n \in \omega\}$. Let $p \in P \cap N$ and let $\langle q_n : n \in \omega \rangle$ be such that $q_0 \geq p$ and for each $n \in \omega$, $q_{n+1} \geq q_n$ and $q_n \in D_n$. Now, since $\mathbb{P}$ is σ-closed, we find a condition q such that for all $n \in \omega$, $q \geq q_n$. Obviously, $q \geq p$ and q is $\mathbf{N}$-generic.

Let us finish this section by introducing a property of forcing notions which is slightly stronger than properness, but which is often easier to verify than properness (*e.g.*, for the forcing notions introduced in the forthcoming chapters).

> Axiom A: A forcing notion $\mathbb{P} = (P, \leq)$ is said to satisfy Axiom A if there exists a sequence $\{\leq_n : n \in \omega\}$ of orderings on P (not necessarily transitive) which has the following properties:
>
> (1) For all $p, q \in P$, if $q \leq_{n+1} p$ then $q \leq_n p$ and $q \leq p$.
>
> (2) If $\langle p_n \in P : n \in \omega \rangle$ is a sequence of conditions such that $p_n \leq_n p_{n+1}$, then there exists a $q \in P$ such that for all $n \in \omega$, $p_n \leq_n q$.
>
> (3) If $A \subseteq P$ is an anti-chain, then for each $p \in P$ and every $n \in \omega$ there is a $q \in P$ such that $p \leq_n q$ and $\{r \in A : r \textit{ and } q \textit{ are compatible}\}$ is countable.

Examples of forcing notions satisfying Axiom A are forcing notions which are σ-closed or satisfy *ccc*. Furthermore, one can show that every forcing notion which satisfies Axiom A is proper, but not vice versa (for a proof and a counterexample see Baumgartner [4], Theorem 2.4 and Section 3 respectively).

Preservation Theorems for Proper Forcing Notions

Below, we state *without proofs* some preservation theorems for countable support iteration of proper forcing notions. These preservation theorems will be crucial in the following chapters, where we consider countable support iterations of length ω_2 of various proper forcing notions — usually starting with a model in which CH holds.

The first of these preservation theorems states that proper forcing notions do not collapse ω_1 and that properness is preserved under countable support iteration of proper forcing notions (for proofs see Goldstern [6, Corollary 3.14] and Shelah [9, III. §3]).

THEOREM 20.3. *(a) If $\mathbb{P}$ is proper and* $\mathrm{cf}(\delta) > \omega$, *then* $\mathbf{0} \Vdash_{\mathbb{P}} \mathrm{cf}(\delta) > \omega$. *In particular, ω_1 is not collapsed.*

(b) If $\mathbb{P}_\alpha$ is a countable support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \rangle$, where for each $\beta \in \alpha$ we have $\mathbf{0}_\beta \Vdash_\beta$ "$\underset{\sim}{\mathbb{Q}}_\beta$ is proper", then $\mathbb{P}_\alpha$ is proper.

The following lemma is in fact just a consequence of THEOREM 20.3.

LEMMA 20.4. *Let $\mathbb{P}_\alpha$ be a countable support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \rangle$, where for each $\beta \in \alpha$ we have $\mathbf{0}_\beta \Vdash_\beta$ "$\underset{\sim}{\mathbb{Q}}_\beta$ is a proper forcing notion of size $\leq \mathfrak{c}$". If* CH *holds in the ground model and $\alpha \leq \omega_2$, then for all $\beta \in \alpha$, $\mathbf{0}_\beta \Vdash_\beta$* CH.

Since, by LEMMA 18.9, no new reals appear at the limit stage ω_2 one can prove the following theorem — a result which we shall use quite often in the forthcoming chapters.

THEOREM 20.5. *Let $\mathbb{P}_{\omega_2}$ be a countable support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \omega_2 \rangle$, where for each $\beta \in \omega_2$ we have*

$$\mathbf{0}_\beta \Vdash_\beta \text{“}\underset{\sim}{\mathbb{Q}}_\beta \text{ is a proper forcing notion of size } \leq \mathfrak{c} \text{ which adds new reals”}.$$

Further, let $\mathbf{V}$ be a model of $\mathsf{ZFC} + \mathsf{CH}$ and let G be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$. Then we have

(a) $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$, and

(b) for every set of reals $\mathscr{F} \subseteq [\omega]^\omega \cap \mathbf{V}[G]$ of size $\leq \omega_1$ there is a $\beta \in \omega_2$ such that $\mathscr{F} \subseteq \mathbf{V}[G|_\beta]$.

Now, let us say a few words concerning preservation of the Laver property and of ${}^\omega\omega$-boundedness: It can be shown that a countable support iteration of proper ${}^\omega\omega$-bounding forcing notions is ${}^\omega\omega$-bounding (for a proof see Section 5 and Application 1 of Goldstern [6]).

THEOREM 20.6. *If $\mathbb{P}_\alpha$ is a countable support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \rangle$, where for each $\beta \in \alpha$ we have $\mathbf{0}_\beta \Vdash_\beta$ “$\underset{\sim}{\mathbb{Q}}_\beta$ is proper and ${}^\omega\omega$-bounding”, then $\mathbb{P}_\alpha$ is ${}^\omega\omega$-bounding.*

Further, one can show that the Laver property is preserved under countable support iteration of proper forcing notions which have the Laver property (for a proof see Section 5 and Application 4 of Goldstern [6]).

THEOREM 20.7. *If $\mathbb{P}_\alpha$ is a countable support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \rangle$, where for each $\beta \in \alpha$ we have $\mathbf{0}_\beta \Vdash_\beta$ “$\underset{\sim}{\mathbb{Q}}_\beta$ is proper and has the Laver property”, then $\mathbb{P}_\alpha$ has the Laver property.*

Another property which is preserved under countable support iteration of proper forcing notions is preservation of P-points: A forcing notion $\mathbb{P}$ is said to **preserve *P*-points** if for every P-point $\mathscr{U} \subseteq [\omega]^\omega$,

$$\mathbf{0} \Vdash_{\mathbb{P}} \text{“}\mathscr{U} \text{ generates an ultrafilter over } \omega\text{”},$$

i.e., for every set $x \in [\omega]^\omega$ in the $\mathbb{P}$-generic extension there exists a $y \in \mathscr{U}$ such that either $y \subseteq x$ or $y \subseteq \omega \setminus x$. In particular, if the forcing notion $\mathbb{P}$ is proper and CH holds in the ground model, then the ultrafilter in the $\mathbb{P}$-generic extension which is generated by the P-point $\mathscr{U}$ is again a P-point.

One can show that preservation of P-points is preserved under countable support iteration of proper forcing notions (for a proof see Blass and Shelah [5] or Bartoszyński and Judah [2, Theorem 6.2.6]).

THEOREM 20.8. *If $\mathbb{P}_\alpha$ is a countable support iteration of $\langle \underset{\sim}{\mathbb{Q}}_\beta : \beta \in \alpha \rangle$, where for each $\beta \in \alpha$ we have $\mathbf{0}_\beta \Vdash_\beta$ “$\underset{\sim}{\mathbb{Q}}_\beta$ is proper and preserves P-points”, then $\mathbb{P}_\alpha$ preserves P-points.*

There are many more preservation theorems for countable support iteration of proper forcing notions. However, what we presented here is all that we shall use in the forthcoming chapters.

Notes

The notion of properness, which is slightly more general than Axiom A (introduced by Baumgartner [3]), was discovered and investigated by Shelah [8, 9], who realised that properness is a property that is preserved under countable support iteration and that allows to prove several preservation theorems (see for example Shelah [9, VI. §§1–2], where one can find also proofs of the preservation theorems given above). For a brief introduction to proper forcing we refer the reader to Goldstern [6] and for applications of the Proper Forcing Axiom, which is a generalisation of Martin's Axiom, see Baumgartner [4].

Related Results

105. *Reals of minimal degree of constructibility.* Let $\mathbb{P} = (P, \leq)$ be a forcing notion and let g be a real in some $\mathbb{P}$-generic extension of $\mathbf{V}$. Then g is said to be of *minimal degree of constructability*, or just *minimal*, if g does not belong to $\mathbf{V}$ and for every real f in $\mathbf{V}[g]$ we have either $f \in \mathbf{V}$ or $g \in \mathbf{V}[f]$, where $\mathbf{V}[f]$ is the smallest model of ZFC containing f and $\mathbf{V}$. In the latter case we say that f *reconstructs* g. For example no Cohen real is minimal. Indeed, if $c \in {}^{\omega}\omega$ is a Cohen real over $\mathbf{V}$, then the real $c' \in {}^{\omega}\omega \cap \mathbf{V}[c]$ defined by stipulating $c'(n) := c(2n)$ (for all $n \in \omega$) is also a Cohen real over $\mathbf{V}$. Moreover, c is even $\mathbb{C}$-generic over $\mathbf{V}[c']$, which implies that c does not belong to $\mathbf{V}[c']$.

106. *Alternative definitions of properness.* The notion of properness can also be defined in terms of games or with stationary sets (see for example Jech [7, Part III] or Baumgartner [4, Section 2]).

107. *Preservation of ultrafilters.* In general, a forcing notion which adds reals does not preserve all ultrafilters. More precisely, for any forcing notion which adds a new real, say r, to the ground model $\mathbf{V}$, there exists an ultrafilter $\mathscr{U}$ in $\mathbf{V}$ which does not generate an ultrafilter in $\mathbf{V}[r]$. (see Bartoszyński, Goldstern, Judah, and Shelah [1] or Bartoszyński and Judah [2, Theorem 6.2.2]).
Further, one can show that any forcing notion which adds Cohen, dominating, or random reals, does not preserve P-points (see Bartoszyński and Judah [2, Theorem 7.2.22]).

References

1. Tomek Bartoszyński, Martin Goldstern, Haim Judah, and Saharon Shelah, *All meager filters may be null*, ***Proceedings of the American Mathematical Society***, vol. 117 (1993), 515–521.
2. Tomek Bartoszyński and Haim Judah, ***Set Theory: on the structure of the real line***, A. K. Peters, Wellesley, 1995.

3. James E. Baumgartner, *Iterated forcing*, in ***Surveys in Set Theory*** (A.R.D. Mathias, ed.), [London Mathematical Society Lecture Note Series 87], Cambridge University Press, Cambridge, 1983, pp. 1–59.
4. ———, *Applications of the proper forcing axiom*, in ***Handbook of Set-Theoretic Topology*** (K. Kunen and J.E. Vaughan, eds.), North-Holland, Amsterdam, 1990, pp. 913–959.
5. Andreas Blass and Saharon Shelah, *There may be simple $P_{\aleph_1}$- and $P_{\aleph_2}$-points and the Rudin-Keisler ordering may be downward directed*, ***Annals of Pure and Applied Logic***, vol. 33 (1987), 213–243.
6. Martin Goldstern, *Tools for your forcing construction*, in ***Set Theory of the Reals*** (H. Judah, ed.), [Israel Mathematical Conference Proceedings], Bar-Ilan University, Israel, 1993, pp. 305–360.
7. Thomas Jech, ***Multiple Forcing***, [Cambridge Tracts in Mathematics], Cambridge University Press, Cambridge, 1986.
8. Saharon Shelah, ***Proper Forcing***, [Lecture Notes in Mathematics 940], Springer-Verlag, Berlin, 1982.
9. ———, ***Proper and Improper Forcing***, [Perspectives in Mathematical Logic], Springer-Verlag, Berlin, 1998.

21

Cohen Forcing revisited

Properties of Cohen Forcing

Since Cohen forcing is countable, it satisfies *ccc*, hence, Cohen forcing is proper. Furthermore, since forcing notions with the Laver property do not add Cohen reals, Cohen forcing obviously does not have the Laver property.

Not so obvious are the facts that Cohen forcing adds unbounded and splitting, but no dominating reals.

Cohen Forcing adds Unbounded but no Dominating Reals

LEMMA 21.1. *Cohen forcing adds unbounded reals.*

Proof. Consider Cohen forcing $\mathbb{C} = \big(\bigcup_{i\in\omega} {}^{i}\omega, \subseteq\big)$, which is — as we have seen in Chapter 18 — equivalent to the forcing notion $\big(\bigcup_{i\in\omega} {}^{i}2, \subseteq\big)$. Let $c \in {}^{\omega}\omega$ be $\mathbb{C}$-generic over some ground model $\mathbf{V}$ and let $\underset{\sim}{c}$ be the canonical $\mathbb{C}$-name for c. We show that the function c is not dominated by any function $g \in {}^{\omega}\omega \cap \mathbf{V}$. Firstly notice that for every $\mathbb{C}$-condition p we have

$$p \Vdash_{\mathbb{C}} \underset{\sim}{c}|_{\mathrm{dom}(p)} = \underset{\sim}{p}\,.$$

Let $g \in {}^{\omega}\omega$ be any function in the ground model $\mathbf{V}$ (*i.e.*, $g \in {}^{\omega}\omega \cap \mathbf{V}$) and let $n \in \omega$. Then there exist $k \geq n$ and a $\mathbb{C}$-condition $q \geq p$ such that $k \in \mathrm{dom}(q)$ and $q(k) > g(k)$. This implies that for every $n \in \omega$, the set of $\mathbb{C}$-conditions q such that

$$q \Vdash_{\mathbb{C}} \exists k \geq n \, \big(g(k) < \underset{\sim}{c}(k)\big)$$

is open dense in $\bigcup_{i\in\omega} {}^{i}\omega$. Hence, there is no $\mathbb{C}$-condition which forces that c is dominated by some function $g \in {}^{\omega}2 \cap \mathbf{V}$. Consequently, c is not dominated by any function from the ground model, or in other words, the function $c \in {}^{\omega}\omega$ is unbounded. $\dashv$

LEMMA 21.2. *Cohen forcing does not add dominating reals.*

Proof. Consider Cohen forcing $\mathbb{C} = \big(\mathrm{Fn}(\omega,2), \subseteq\big)$. Let $c \in {}^\omega 2$ be $\mathbb{C}$-generic over some ground model $\mathbf{V}$. Further, let $f \in {}^\omega\omega$ be an arbitrary but fixed function in $\mathbf{V}[c]$ and let $\underset{\sim}{f}$ be a $\mathbb{C}$-name for f. In order to show that f is not dominating we have to find a function $g \in {}^\omega\omega \cap \mathbf{V}$ such that for every $n \in \omega$ there is a $k \geq n$ such that $g(k) \geq f(k)$. Let $\{p_k : k \in \omega\}$ be an enumeration of $\mathrm{Fn}(\omega,2)$, *i.e.*, $\{p_k : k \in \omega\} = \mathrm{Fn}(\omega,2)$. For every $k \in \omega$ define

$$g(k) = \min\big\{n : \exists q \geq p_k \left(q \Vdash_{\mathbb{C}} \underset{\sim}{f}(k) = n\right)\big\}.$$

For every $\mathbb{C}$-condition p and every $n \in \omega$ there is a $k \geq n$ such that $p_k \geq p$, and we find a $q \geq p_k$ such that $q \Vdash_{\mathbb{C}} \underset{\sim}{f}(k) = g(k)$. Consequently, for every $n \in \omega$, the set of $\mathbb{C}$-conditions q such that

$$q \Vdash_{\mathbb{C}} \exists k \geq n\big(\underset{\sim}{f}(k) = g(k)\big)$$

is open dense in $\mathrm{Fn}(\omega,2)$. Hence, $g \in {}^\omega\omega \cap \mathbf{V}$ is not dominated by $f \in \mathbf{V}[c]$, and since f was arbitrary, this shows that there are no dominating functions in $\mathbf{V}[c]$, or in other words, Cohen forcing does not add dominating reals. ⊣

Cohen Forcing adds Splitting Reals

LEMMA 21.3. *Cohen forcing adds splitting reals.*

Proof. Consider Cohen forcing $\mathbb{C} = \big(\bigcup_{n\in\omega} {}^i 2, \subseteq\big)$. We show that any real c which is $\mathbb{C}$-generic over some ground model $\mathbf{V}$ generates a splitting real: Let $\sigma_c := \big\{k \in \omega : c(k) = 1\big\}$ and let $\underset{\cdot}{\sigma_c}$ be its canonical $\mathbb{C}$-name. Then for any infinite set $x \in [\omega]^\omega \cap \mathbf{V}$ and any $n \in \omega$, the set of $\mathbb{C}$-conditions p such that

$$p \Vdash_{\mathbb{C}} |x \cap \underset{\cdot}{\sigma_c}| > n \ \wedge |x \setminus \underset{\cdot}{\sigma_c}| > n$$

is open dense, and therefore, σ_c splits every real in the ground model $\mathbf{V}$, or in other words, σ_c is a splitting real. ⊣

Cohen Reals and the Covering Number of Meagre Sets

Below, we shall give a topological characterisation of Cohen reals, but before we introduce a topology on ${}^\omega\omega$ and show how to encode "basic" meagre sets by reals.

For each finite sequence $s = \langle n_0, \dots, n_{k-1}\rangle$ of natural numbers, *i.e.*, $s \in \mathrm{seq}(\omega)$, define the *basic open* set

$$O_s = \{f \in {}^\omega\omega : f|_k = s\}.$$

A set $A \subseteq {}^\omega\omega$ is said to be **open** (in ${}^\omega\omega$) if there is a family $\mathscr{S} \subseteq \mathrm{seq}(\omega)$ of finite sequences in ω such that $A = \bigcup\{O_s : s \in \mathscr{S}\}$. In particular, $\emptyset$ as well as ${}^{\omega}\omega$ are open. Notice that a set $A \subseteq {}^{\omega}\omega$ is open *iff* for all $x \in A$ there exists an $s \in \operatorname{seq}(\omega)$ such that $x \in O_s \subseteq A$. Furthermore, a set $A \subseteq {}^{\omega}\omega$ is called **closed** (in ${}^{\omega}\omega$) if ${}^{\omega}\omega \setminus A$ is open. Evidently, arbitrary unions and finite intersections of open sets are open; or equivalently, arbitrary intersections and finite unions of closed sets are closed. On the other hand, an intersection of countably many open sets is not necessarily open, and a union of countably many closed sets is not necessarily closed (see below). Now, intersections of countably many open sets are called $\boldsymbol{G_\delta}$ **sets**, and unions of countably many closed sets are called $\boldsymbol{F_\sigma}$ **sets**. Notice that every open (closed) set is a G_δ set (F_σ set), and that by De Morgan laws, each F_σ set is the complement of a G_δ set and vice versa. For example the set $C_0 \subseteq {}^{\omega}\omega$ of eventually constant functions (*i.e.*, $f \in C_0$ *iff* there is an $n \in \omega$ such that $f|_{\omega \setminus n}$ is constant) is an F_σ set which is neither closed nor open.

A subset of ${}^{\omega}\omega$ is **dense** (in ${}^{\omega}\omega$) if it meets every non-empty open subset of ${}^{\omega}\omega$. For example C_0 is dense in ${}^{\omega}\omega$. Notice that every dense subset of ${}^{\omega}\omega$ must be infinite. On the other hand, $A \subseteq {}^{\omega}\omega$ is called **nowhere dense** if ${}^{\omega}\omega \setminus A$ contains an open dense set. Notice that every nowhere dense set is contained in a closed nowhere dense set (*i.e.*, the closure of a nowhere dense set is nowhere dense).

Now, a subset of ${}^{\omega}\omega$ is called **meagre** if it is contained in the union of countably many nowhere dense sets. For example C_0 is meagre. Since the closure of a nowhere dense set is nowhere dense, we get that every meagre set is contained in some meagre F_σ set, and that the complement of a meagre set contains a co-meagre G_δ set. Moreover, we have the following result.

THEOREM 21.4 (BAIRE CATEGORY THEOREM). *The intersection of countably many open dense sets is dense. In particular, the complement of meagre set is always dense.*

Proof. Let $\langle D_n : n \in \omega$ be a sequence of open dense subsets of ${}^{\omega}\omega$. We have to show that $D = \bigcap_{n\in\omega} D_n$ is dense, *i.e.*, we have to show that for each basic open set O_s, $D \cap O_s \neq \emptyset$. Let O_{s_0} be an arbitrary but fixed basic open set. By induction on $n \in \omega$ we construct a sequence $t_0 \subseteq t_1 \subseteq \dots$ of elements of $\operatorname{seq}(\omega)$ such that $\bigcap_{n\in\omega} O_{t_n} \subseteq D \cap O_{s_0}$. In fact, we just have to make sure that $\bigcup_{n\in\omega} t_n \in {}^{\omega}\omega$ and that for all $n \in \omega$, $O_{t_n} \subseteq D_n$. Since D_0 is open dense, there exists a $t_0 \in \operatorname{seq}(\omega)$ such that $s_0 \subseteq t_0$ and $O_{t_0} \subseteq (D_0 \cap O_{s_0})$. Assume that $t_n \in \operatorname{seq}(\omega)$ is already constructed for some $n \in \omega$. Then, since D_{n+1} is open dense, there is a $t_{n+1} \in \operatorname{seq}(\omega)$ such that $O_{t_{n+1}} \subseteq (D_{n+1} \cap O_{t_n})$ and $|t_{n+1}| \geq n+1$. Now, by construction, the sequence $t_0 \subseteq t_1 \subseteq \dots$ has the required properties. ⊣

By definition, subsets of meagre sets as well as countable unions of meagre sets are meagre. Thus, the collection of meagre subsets of ${}^{\omega}\omega$, denoted by $\mathscr{M}$, is an ideal on $\mathscr{P}({}^{\omega}\omega)$. By the BAIRE CATEGORY THEOREM 21.4, ${}^{\omega}\omega \notin \mathscr{M}$ but for every $f \in {}^{\omega}\omega$ we have $\{f\} \in {}^{\omega}\omega$, and therefore the set ${}^{\omega}\omega$ can be covered by $\mathfrak{c}$ meagre sets. This observation leads to the following cardinal number.

DEFINITION. The **covering number** of $\mathscr{M}$, denoted $\boldsymbol{cov(\mathscr{M})}$, is the smallest number of sets in $\mathscr{M}$ with union ${}^\omega\omega$; more formally

$$cov(\mathscr{M}) = \min\left\{|\mathscr{C}| : \mathscr{C} \subseteq \mathscr{M} \wedge \bigcup \mathscr{C} = {}^\omega\omega\right\}.$$

Since countable unions of meagre sets are meagre, and since we can cover ${}^\omega\omega$ by $\mathfrak{c}$ meagre sets, we obviously have $\omega_1 \leq cov(\mathscr{M}) \leq \mathfrak{c}$. Moreover, we can show slightly more:

THEOREM 21.5. $\mathfrak{p} \leq cov(\mathscr{M})$.

Proof. Let $\{A_\alpha \subseteq {}^\omega\omega : \alpha \in \kappa < \mathfrak{p}\}$ be any infinite family of cardinality $\kappa < \mathfrak{p}$ of meagre subsets of ${}^\omega\omega$. We have to show that $\bigcup_{\alpha\in\kappa} A_\alpha \neq {}^\omega\omega$, or equivalently, we have to show that for any family $D = \{D_\alpha : \alpha \in \kappa < \mathfrak{p}\}$ of open dense subsets of ${}^\omega\omega$ we have $\bigcap D \neq \emptyset$. Notice the similarity with the proof of the BAIRE CATEGORY THEOREM 21.4. Let $\nu : \mathrm{seq}(\omega) \to \omega$ be a bijection. For every $s \in \mathrm{seq}(\omega)$ and every $\alpha \in \kappa$, let

$$I_{s,\alpha} = \left\{t \in \mathrm{seq}(\omega) : s \subseteq t \wedge O_t \subseteq D_\alpha\right\}.$$

Since D_α is open dense, the set $y_{s,\alpha} := \left\{\nu(t) : t \in I_{s,\alpha}\right\}$ is an infinite subset of ω.

For the moment, let s be an arbitrary but fixed element of $\mathrm{seq}(\omega)$. Then for any finitely many ordinals $\alpha_0, \dots, \alpha_{k-1}$ in κ we get that $\bigcap_{i\in k} y_{s,\alpha_i} \in [\omega]^\omega$. Consider the family $\mathscr{F}_s = \{y_{s,\alpha} : \alpha \in \kappa\} \subseteq [\omega]^\omega$. Obviously, $\mathscr{F}_s$ has the strong finite intersection property, and since $\kappa < \mathfrak{p}$, $\mathscr{F}_s$ has a pseudo-intersection, say x_s. Thus, for every $\alpha \in \kappa$ there exist a $k \in \omega$ such that $x_s \setminus k \subseteq y_{s,\alpha}$.

Now, for each $\alpha \in \kappa$ define $h_\alpha : \mathrm{seq}(\omega) \to \omega$ by stipulating $h_\alpha(s) := \min\{k \in \omega : x_s \setminus k \subseteq y_{s,\alpha}\}$, and let $g_\alpha \in {}^\omega\omega$ be such that for all $n \in \omega$, $g_\alpha(n) := h_\alpha\big(\nu^{-1}(n)\big)$. Since $\kappa < \mathfrak{p}$ and $\mathfrak{p} \leq \mathfrak{b}$, there is a function $f \in {}^\omega\omega$ which dominates each g_α. By construction,

$$U = \bigcup_{s\in\mathrm{seq}(\omega)} \left\{O_t \subseteq {}^\omega\omega : \nu(t) \in x_s \setminus f\big(\nu(s)\big)\right\}$$

is an open dense subset of ${}^\omega\omega$ which has the property that for each $\alpha \in \kappa$ there is a finite set $E_\alpha \in \left[\mathrm{seq}(\omega)\right]^{<\omega}$ such that $U_{E_\alpha} \subseteq D_\alpha$, where for $E \subseteq \mathrm{seq}(\omega)$,

$$U_E = \bigcup_{s\in\mathrm{seq}(\omega)} \left\{O_t \subseteq {}^\omega\omega : \nu(t) \in x_s \setminus f\big(\nu(s)\big) \wedge t \notin E\right\}.$$

Notice that for each $E \in \left[\mathrm{seq}(\omega)\right]^{<\omega}$, U_E is open dense, and since there are only finitely many finite subsets of $\mathrm{seq}(\omega)$, by the BAIRE CATEGORY THEOREM 21.4 we get that

$$T = \bigcap \left\{U_E : E \in [\mathrm{seq}(\omega)]^{<\omega}\right\}$$

is dense, and since T is contained in each D_α we have $T \subseteq \bigcap_{\alpha\in\kappa} D_\alpha$. $\dashv$

With a product of Cohen forcing we shall construct a model in which $\mathfrak{p} < cov(\mathscr{M})$ (see COROLLARY 21.11). The crucial point in the construction will be the fact that Cohen reals over $\mathbf{V}$ are not contained in any meagre F_σ set which can be *encoded* (explained later) by a real $r \in {}^\omega\omega$ which belongs to the ground model $\mathbf{V}$. For this, we have to show the relationship between Cohen reals and meagre sets and have to explain how to encode meagre F_σ sets by real numbers; but first we give the relationship between Cohen reals and open dense subsets of ${}^\omega\omega$.

Consider Cohen forcing $\mathbb{C} = \big(\bigcup_{n\in\omega} {}^n\omega, \subseteq\big)$. To every $\mathbb{C}$-condition s we associate the open set $O_s \subseteq {}^\omega\omega$. Similarly, to every *dense* set $D \subseteq \bigcup_{n\in\omega} {}^n\omega$ we associate the set

$$\mathscr{O}(D) = \bigcup \big\{O_s \subseteq {}^\omega\omega : s \in D\big\},$$

which is an open dense subset of ${}^\omega\omega$. On the other hand, if $\mathcal{O} \subseteq {}^\omega\omega$ is an *open dense* subset of ${}^\omega\omega$, then the set

$$\mathscr{D}(\mathcal{O}) = \big\{s \in \bigcup_{n\in\omega} {}^n\omega : O_s \subseteq \mathcal{O}\big\}$$

is an open dense subset of $\bigcup_{n\in\omega} {}^n\omega$. Notice that for every open dense set $\mathcal{O} \subseteq {}^\omega\omega$ there is a dense set $D \subseteq \bigcup_{n\in\omega} {}^n\omega$ such that $\mathcal{O} = \mathscr{O}(D)$. Hence, if $c \in {}^\omega\omega$ is a Cohen real over $\mathbf{V}$, then in $\mathbf{V}[c]$ we have

$$\mathbf{V}[c] \vDash c \in \bigcap \Big\{\mathscr{O}(D) : D \text{ is dense in } \bigcup_{n\in\omega} {}^n\omega \wedge D \in \mathbf{V}\Big\}.$$

Considering the dense set $D \subseteq \bigcup_{n\in\omega} {}^n\omega$ as the *code* for the open dense set $\mathscr{O}(D) \subseteq {}^\omega\omega$, we get the following

FACT 21.6. *A real $c \in {}^\omega\omega$ is a Cohen real over $\mathbf{V}$ if and only if c is contained in every open dense subset of ${}^\omega\omega$ whose code belongs to $\mathbf{V}$.*

In order to make the notion of *codes* more precise, we show how one can encode meagre F_σ sets by real numbers $r \in {}^\omega\omega$. For this, take two bijections $h_1 : \omega \to \text{seq}(\omega)$ and $h_2 : \omega \times \omega \to \omega$, and for $r \in {}^\omega\omega$ let

$$\begin{aligned} \eta_r : \omega \times \omega \ &\longrightarrow \qquad \text{seq}(\omega) \\ \langle n, m\rangle \ &\longmapsto h_1\big(r\big(h_2(n,m)\big)\big). \end{aligned}$$

For every F_σ set $A = \bigcup_{m\in\omega} \bigcap_{n\in\omega} {}^\omega\omega \setminus O_{s_{n,m}}$, there is a real $r \in {}^\omega\omega$, called *code* of A, such that for all $n, m \in \omega$ we have $\eta_r(n,m) = s_{n,m}$. On the other hand, for every real $r \in {}^\omega\omega$ let $A_r \subseteq {}^\omega\omega$ be defined by

$$A_r = \big\{f \in {}^\omega\omega : \exists m \in \omega\, \forall n \in \omega\, \big(\eta_r(n,m) \nsubseteq f\big)\big\}.$$

As a countable union of closed sets, A_r is an F_σ set. Thus, every real $r \in {}^\omega\omega$ encodes an F_σ set, and vice versa, every F_σ set can be encoded by a real

$r \in {}^\omega\omega$. Now, an F_σ set $A = \bigcup_{m\in\omega}\bigcap_{n\in\omega} {}^\omega\omega \setminus O_{s_{n,m}}$ is meagre *iff* $\bigcup_{n\in\omega} O_{s_{n,m}}$ is dense for each $m \in \omega$. So, for $r \in {}^\omega\omega$ we have

$$A_r \text{ is meagre } \textit{ iff } \quad \forall s \in \mathrm{seq}(\omega)\, \forall m \in \omega\, \exists n \in \omega\, \big(s \subseteq \eta_r(n,m) \vee \eta_r(n,m) \subseteq s\big)\,.$$

The way we have defined A_r, it does not only depend on the real r, but also on the model in which we construct A_r from r (notice that this fact also applies to the sets O_s). So, in order to distinguish the sets A_r constructed in different models, for models $\mathbf{V}$ of ZFC and $r \in {}^\omega\omega \cap \mathbf{V}$ we write

$$A_r^{\mathbf{V}} = \big\{f \in {}^\omega\omega \cap \mathbf{V} : \exists m \in \omega\, \forall n \in \omega\, \big(\eta_r(n,m) \nsubseteq f\big)\big\}\,.$$

By FACT 21.6 we get that if $c \in {}^\omega\omega$ is a Cohen real over $\mathbf{V}$, then c is not contained in any meagre F_σ set $A_r^{\mathbf{V}}$ with $r \in {}^\omega\omega \cap \mathbf{V}$. Now, let $\mathbf{V}$ and $\mathbf{V}'$ be two transitive models of ZFC. Then, for every real $r \in {}^\omega\omega$ which belongs to both models $\mathbf{V}$ and $\mathbf{V}'$ we have

$$\mathbf{V} \vDash A_r^{\mathbf{V}} \text{ is meagre } \textit{ iff } \ \mathbf{V}' \vDash A_r^{\mathbf{V}'} \text{ is meagre}\,.$$

As a consequence we get the following characterisation of Cohen reals:

PROPOSITION 21.7. *Let $\mathbf{V}$ be a model of ZFC, let $\mathbb{P}$ be a forcing notion in $\mathbf{V}$, and let G be $\mathbb{P}$-generic over $\mathbf{V}$. Then the real $c \in {}^\omega\omega \cap \mathbf{V}[G]$ is a Cohen real over $\mathbf{V}$ if and only if c does not belong to any meagre F_σ set $A_r^{\mathbf{V}[G]}$ with code r in $\mathbf{V}$.*

Proof. ($\Rightarrow$) If $c \in {}^\omega\omega \cap \mathbf{V}[G]$ belongs to some meagre F_σ set $A_r^{\mathbf{V}[G]}$ with code r in $\mathbf{V}$, then $c \in \bigcup_{m\in\omega}\bigcap_{n\in\omega} {}^\omega\omega \setminus O_{\eta_r(n,m)}$. Thus, there is an $m_0 \in \omega$ such that c does not belong to the open dense set $\bigcup_{n\in\omega} O_{\eta_r(n,m_0)}$. Now, consider Cohen forcing $\mathbb{C} = \big(\bigcup_{i\in\omega} {}^i\omega, \subseteq\big)$ and let $D := \{\eta_r(n,m_0) : n \in \omega\}$. Then D is an open dense subset of $\bigcup_{i\in\omega} {}^i\omega$ which belongs to the model $\mathbf{V}$. On the other hand we have $\{c|_n : n \in \omega\} \cap D = \emptyset$ which shows that c is not a Cohen real over $\mathbf{V}$.

($\Leftarrow$) Firstly, recall that every meagre set is contained in some meagre F_σ set and that $A_r^{\mathbf{V}}$ is meagre *iff* $A_r^{\mathbf{V}[G]}$ is meagre, and secondly, notice that $A_r^{\mathbf{V}} \subseteq A_r^{\mathbf{V}[G]}$. Hence, a real $c \in {}^\omega\omega \cap \mathbf{V}[G]$ which does not belong to any meagre F_σ set $A_r^{\mathbf{V}[G]}$ with code r in $\mathbf{V}$ does belong to every open dense subset of ${}^\omega\omega$ whose code belongs to $\mathbf{V}$, and therefore, by FACT 21.6, c is a Cohen real over $\mathbf{V}$. ⊣

COROLLARY 21.8. *Let $\mathbb{P}$ be a forcing notion which does not add Cohen reals and let G be $\mathbb{P}$-generic over $\mathbf{V}$, where $\mathbf{V}$ is a model of $\mathsf{ZFC} + \mathsf{CH}$. Then $\mathbf{V}[G] \vDash \mathit{cov}(\mathscr{M}) = \omega_1$, in particular, $\mathbf{V}[G] \vDash \mathfrak{p} = \omega_1$.*

Proof. In $\mathbf{V}$, let $C = \{r \in {}^\omega\omega : A_r \textit{ is meagre}\}$. Then $|C| = \omega_1$ and we obviously have $\bigcup_{r\in C} A_r = {}^\omega\omega$. In other words, the set of meagre sets $\{A_r :$

$r \in C\}$ is of cardinality ω_1 which covers ${}^\omega\omega$. Now, since $\mathbb{P}$ does not add Cohen reals, in $\mathbf{V}[G]$ we have ${}^\omega\omega \setminus \bigcup_{r\in C} A_r^{\mathbf{V}[G]} = \emptyset$. Hence, $\mathbf{V}[G] \vDash \bigcup_{r\in C} A_r^{\mathbf{V}[G]} = {}^\omega\omega$, and since $cov(\mathscr{M})$ is uncountable we get $\mathbf{V}[G] \vDash cov(\mathscr{M}) = \omega_1$. In particular, by THEOREM 21.5, $\mathbf{V}[G] \vDash \mathfrak{p} = \omega_1$. ⊣

We have seen that $cov(\mathscr{M}) \leq \mathfrak{c}$ and by THEOREM 21.5 we know that $\mathfrak{p} \leq cov(\mathscr{M})$. So, $cov(\mathscr{M})$ is an uncountable cardinal number which is less than or equal to $\mathfrak{c}$. Below, we shall compare the covering number $cov(\mathscr{M})$ with other cardinal characteristics of the continuum and give a model of ZFC in which $\mathfrak{p} < cov(\mathscr{M})$.

A Model in which $\mathfrak{a} < \mathfrak{d} = \mathfrak{r} = cov(\mathscr{M})$

The following lemma will be crucial in our proof that $\omega_1 < \mathfrak{r} = cov(\mathscr{M}) = \mathfrak{c}$ is consistent with ZFC (*cf.* LEMMA 18.1 and Chapter 18 | RELATED RESULT 97).

LEMMA 21.9. *Let α be an ordinal number, let $\mathbb{C}^{\alpha+1}$ be the finite support product of $\alpha + 1$ copies of Cohen forcing $\mathbb{C} = \big(\mathrm{Fn}(\omega, 2), \subseteq\big)$, and let G be $\mathbb{C}^{\alpha+1}$-generic over some model $\mathbf{V}$ of ZFC. Then $G(\alpha)$ is $\mathbb{C}$-generic over $\mathbf{V}[G|_\alpha]$, in particular, $\bigcup G(\alpha)$ is a Cohen real over $\mathbf{V}[G|_\alpha]$.*

Proof. Firstly notice that since $\mathrm{Fn}(\omega, 2)$ contains only finite sets, for all transitive models $\mathbf{V}', \mathbf{V}''$ of ZFC we have $\mathrm{Fn}(\omega, 2)^{\mathbf{V}'} = \mathrm{Fn}(\omega, 2)^{\mathbf{V}''}$, *i.e.*, $\mathrm{Fn}(\omega, 2)$ is the same in all transitive models of ZFC, and consequently we get $\mathbb{C}^{\mathbf{V}'} = \mathbb{C}^{\mathbf{V}''}$. In particular, $\mathbb{C}^{\mathbf{V}[G|_\alpha]} = \mathbb{C}^{\mathbf{V}}$.

To simplify the notation, let us work with the forcing notion $\mathbb{C}_\alpha = \big(\mathrm{Fn}(\omega \times \alpha, 2), \subseteq\big)$ instead of $\mathbb{C}^\alpha$ (recall that by PROPOSITION 18.3, $\mathbb{C}_\alpha \approx \mathbb{C}^\alpha$). Now, in the model $\mathbf{V}[G]$, fix an arbitrary dense set $D \subseteq \mathrm{Fn}(\omega, 2)$ and let $\underset{\sim}{D}$ be a $\mathbb{C}^\alpha$-name for D. Further, let $p_0 \in G|_\alpha$ be such that

$$p_0 \Vdash_{\mathbb{C}} \text{“}\underset{\sim}{D} \textit{ is dense in } \mathrm{Fn}(\omega, 2)\text{”},$$

and let

$$E = \big\{\langle q_0, q_1\rangle \in \mathrm{Fn}(\omega \times \alpha, 2) \times \mathrm{Fn}(\omega, 2) : q_0 \geq p_0 \wedge q_0 \Vdash_{\mathbb{C}} \underset{\cdot}{q_1} \in \underset{\sim}{D}\big\}.$$

We leave it as an exercise to the reader to show that E, which is a subset of $\mathrm{Fn}(\omega \times \alpha, 2) \times \mathrm{Fn}(\omega, 2)$, is dense above $\langle p_0, \emptyset\rangle$. Thus, since $\langle p_0, \emptyset\rangle \in \big(G|_\alpha \times G(\alpha)\big)$, there is some $\langle q_0, q_1\rangle \in \big(G|_\alpha \times G(\alpha)\big) \cap E$. So, $q_0 \Vdash_{\mathbb{C}} \underset{\cdot}{q_1} \in \underset{\sim}{D}$ where $q_0 \in G|_\alpha$, and since $q_1 \in G(\alpha)$ we get that $q_1 \in D$ which shows that $G(\alpha) \cap D \neq \emptyset$. Since $D \subseteq \mathrm{Fn}(\omega, 2)$ was chosen arbitrarily, we finally get that $G(\alpha)$ is $\mathbb{C}$-generic over $\mathbf{V}[G|_\alpha]$, or in other words, $\bigcup G(\alpha)$ is a Cohen real over $\mathbf{V}[G|_\alpha]$. ⊣

PROPOSITION 21.10. *$\omega_1 < \mathfrak{d} = \mathfrak{r} = cov(\mathscr{M}) = \mathfrak{c}$ is consistent with ZFC.*

Proof. Let $\mathbf{V}$ be a model of $\mathsf{ZFC} + \mathsf{CH}$, let $\kappa \geq \omega_2$ be a regular cardinal, and let G be $\mathbb{C}^\kappa$-generic over $\mathbf{V}$. Since κ is regular and by PROPOSITION 18.3 $CC^\kappa \approx \mathbb{C}_\kappa$, by THEOREM 14.21 we have $\mathbf{V}[G] \vDash \mathfrak{c} = \kappa$. Thus, it remains to show that $\mathbf{V}[G]$ is a model in which $\mathfrak{d} = \mathfrak{r} = cov(\mathscr{M}) = \mathfrak{c}$.

By LEMMA 18.9, for every real x in $\mathbf{V}[G]$ there is an $\alpha_x \in \kappa$ such that $x \in \mathbf{V}[G|_{\alpha_x}]$. Moreover, since κ is regular, for every set of reals $X \in \mathbf{V}[G]$ with $|X| < \kappa$ we get that $\bigcup\{\alpha_x : x \in X\} \in \kappa$.

Let $\mathscr{E}, \mathscr{C} \subseteq {}^\omega\omega \cap \mathbf{V}[G]$ and $\mathscr{F} \subseteq [\omega]^\omega \cap \mathbf{V}[G]$ be three families in $\mathbf{V}[G]$, each of cardinality strictly less than κ. Then there is an ordinal $\gamma \in \kappa$ such that all three families $\mathscr{E}$, $\mathscr{C}$, and $\mathscr{F}$, belong to $\mathbf{V}[G|_\gamma]$.

Since Cohen forcing adds splitting reals (by LEMMA 21.3) and since $G(\gamma)$ is $\mathbb{C}$-generic over $\mathbf{V}[G|_\gamma]$ (by LEMMA 21.9), in $\mathbf{V}[G|_{\gamma+1}]$ there is a real $s \in [\omega]^\omega$ which is a splitting real over $\mathbf{V}[G|_\gamma]$. Hence, the family $\mathscr{F}$, which belongs to $\mathbf{V}[G|_\gamma]$, is not a reaping family, and since $\mathscr{F}$ was arbitrary, we must have $\mathbf{V}[G] \vDash \mathfrak{r} = \mathfrak{c}$. Similarly, since Cohen forcing adds unbounded reals (by LEMMA 21.1), in $\mathbf{V}[G|_{\gamma+1}]$ there is a function $f \in {}^\omega\omega$ which is unbounded over $\mathbf{V}[G|_\gamma]$. Hence, the family $\mathscr{E}$, which belongs to $\mathbf{V}[G|_\gamma]$, is not a dominating family, and since $\mathscr{E}$ was arbitrary, we must have $\mathbf{V}[G] \vDash \mathfrak{d} = \mathfrak{c}$.

Assume now that $\mathscr{C}$ is a set of codes of meagre F_σ sets, *i.e.*, for every $r \in \mathscr{C}$, $A_r^{\mathbf{V}[G]} \subseteq {}^\omega\omega$ is a meagre F_σ set. Again, since $G(\gamma)$ is $\mathbb{C}$-generic over $\mathbf{V}[G|_\gamma]$, $\bigcup G(\gamma) \in \bigcap_{r\in\mathscr{C}} \big(\omega \setminus A^{\mathbf{V}[G|_\gamma]}\big)$. Hence, in $\mathbf{V}[G]$ we get $\bigcup_{r\in\mathscr{C}} A^{\mathbf{V}[G]} \neq {}^\omega\omega$, and since $\mathscr{C}$ was arbitrary, we must have $\mathbf{V}[G] \vDash cov(\mathscr{M}) = \mathfrak{c}$. $\dashv$

As an immediate consequence of PROPOSITION 18.5 and PROPOSITION 21.10 (using the fact that $\mathbb{C}_\kappa \approx \mathbb{C}^\kappa$), we get the following consistency result.

COROLLARY 21.11. *$\omega_1 = \mathfrak{a} < \mathfrak{d} = \mathfrak{r} = cov(\mathscr{M}) = \mathfrak{c}$ is consistent with* ZFC. *In particular, since $\mathfrak{p} \leq \mathfrak{a}$, we get that $\mathfrak{p} < cov(\mathscr{M})$ is consistent with* ZFC.

A Model in which $\mathfrak{s} = \mathfrak{b} < \mathfrak{d}$

The idea is to start with a model $\mathbf{V}$ in which we have $\omega_1 < \mathfrak{p} = \mathfrak{c}$ (in particular, $\mathbf{V} \vDash \mathfrak{s} = \mathfrak{b} = \mathfrak{d} = \mathfrak{c}$), and then add ω_1 Cohen reals to $\mathbf{V}$. It is not hard to verify that in the resulting model we have $\omega_1 = \mathfrak{s} = \mathfrak{b}$. Slightly more difficult to prove is the fact that we still have $\mathfrak{d} = \mathfrak{c}$, which is a consequence of the following result.

LEMMA 21.12. *Let $\mathbb{P} = (P, \leq)$ be a forcing notion and let G be $\mathbb{P}$-generic over some model $\mathbf{V}$ of* ZFC. *If $\mathbf{V} \vDash |P| < \mathfrak{b}$, then for every function $f \in {}^\omega\omega \cap \mathbf{V}[G]$ we can construct a function $g_f \in {}^\omega\omega \cap \mathbf{V}$ such that for all $h \in {}^\omega\omega \cap \mathbf{V}$ we have*

$$h <^* f \;\rightarrow\; h <^* g_f\,,$$

i.e., whenever the function h is dominated by f (in the model $\mathbf{V}[G]$), it is also dominated by the function g_f from the ground model $\mathbf{V}$. In particular, if $\mathbf{V} \vDash \mathfrak{b} > \omega_1$ and G is $\mathbb{C}^{\omega_1}$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \vDash \mathfrak{d} \geq \mathfrak{d}^{\mathbf{V}}$.

Proof. Let $f \in {}^\omega\omega \cap \mathbf{V}[G]$ and let $\underset{\sim}{f}$ be a $\mathbb{P}$-name for f (in the ground model $\mathbf{V}$) such that $\mathbf{0} \Vdash_{\mathbb{P}} \underset{\sim}{f} \in \underset{\sim}{{}^\omega\omega}$. For every $\mathbb{P}$-condition $p \in P$ define the function $f_p \in {}^\omega\omega \cap \mathbf{V}$ by stipulating

$$f_p(n) = \min\left\{k \in \omega : \exists q \geq p \left(q \Vdash_{\mathbb{P}} \underset{\sim}{f}(n) = k\right)\right\}.$$

Consider the family $\mathscr{F} = \{f_p : p \in P\} \subseteq {}^\omega\omega$. Since $|P| < \mathfrak{b}$, there exists a function $g_f \in {}^\omega\omega$ (in the ground model $\mathbf{V}$) which dominates each member of $\mathscr{F}$. Thus, whenever $p \Vdash_{\mathbb{P}} h <^* \underset{\sim}{f}$ we have $h <^* f_p <^* g_f$, which shows that g_f dominates h.

In order to see that $\mathbf{V}[G] \vDash \mathfrak{d} \geq \mathfrak{d}^{\mathbf{V}}$ whenever $\mathbf{V} \vDash \mathfrak{b} > \omega_1$ and G is $\mathbb{C}^{\omega_1}$-generic over $\mathbf{V}$, recall that $\mathbb{C}^{\omega_1} \approx \mathbb{C}_{\omega_1}$ and notice that $\left|\operatorname{Fn}(\omega \times \omega_1, \omega)\right| \leq \left|\operatorname{fin}(\omega \times \omega_1 \times \omega)\right| = \omega_1$. ⊣

The proof of the following result will be crucial in the proof of PROPOSITION 27.9.

PROPOSITION 21.13. $\omega_1 = \mathfrak{s} = \mathfrak{b} < \mathfrak{d} = \mathfrak{c}$ *is consistent with* ZFC.

Proof. Let $\mathbf{V}$ be a model of $\mathsf{ZFC} + \mathfrak{c} = \mathfrak{p} > \omega_1$ and let $G = \langle c_\alpha : \alpha \in \omega_1\rangle$ be $\mathbb{C}^{\omega_1}$-generic over $\mathbf{V}$, where we work with $\mathbb{C} = \left(\bigcup_{n\in\omega} {}^n\omega, \subseteq\right)$. We shall show that $\mathbf{V}[G] \vDash \omega_1 = \mathfrak{s} = \mathfrak{b} < \mathfrak{d} = \mathfrak{c} = \mathfrak{c}^{\mathbf{V}}$.

Since $\mathbb{C}^{\omega_1}$ satisfies *ccc*, all cardinals are preserved and we obviously have $\mathbf{V}[G] \vDash \mathfrak{c} = \mathfrak{c}^{\mathbf{V}} > \omega_1$. Furthermore, by LEMMA 18.9, for all $f \in {}^\omega\omega$ and $x \in [\omega]^\omega$ which belong to $\mathbf{V}[G]$ there is a $\gamma_0 \in \omega_1$ such that f and x belong to $\mathbf{V}[\langle c_\alpha : \alpha \in \gamma_0\rangle]$.

Since Cohen forcing adds unbounded reals (by LEMMA 21.1) and since c_{γ_0} is $\mathbb{C}$-generic over $\mathbf{V}[G|_{\gamma_0}]$ (by LEMMA 21.9), $c_{\gamma_0} \in {}^\omega\omega$ is not dominated by any function in $\mathbf{V}[\langle c_\alpha : \alpha \in \gamma_0\rangle]$, in particular, c_{γ_0} is not bounded by f. Thus, in $\mathbf{V}[G]$, the family $\{c_\alpha : \alpha \in \omega_1\}$ is an unbounded family of cardinality ω_1, which shows that $\mathbf{V}[G] \vDash \omega_1 = \mathfrak{b}$.

Similarly, let σ_{γ_0} be the splitting real over $\mathbf{V}[\langle c_\alpha : \alpha \in \gamma_0\rangle]$ we get from the Cohen real c_{γ_0} using the construction in the proof of LEMMA 21.3. Then σ_{γ_0} every infinite subset of ω, in particular, σ_{γ_0} splits x. Thus, in $\mathbf{V}[G]$, the family $\{\sigma_\alpha : \alpha \in \omega_1\}$ is a splitting family of cardinality ω_1, which shows that $\mathbf{V}[G] \vDash \omega_1 = \mathfrak{s}$.

Finally, by LEMMA 21.12 we have $\mathbf{V}[G] \vDash \mathfrak{d} = \mathfrak{d}^{\mathbf{V}} > \omega_1$ which shows that

$$\mathbf{V}[G] \vDash \omega_1 = \mathfrak{s} = \mathfrak{b} < \mathfrak{d} = \mathfrak{c}\,.$$

⊣

NOTES

The results presented in this chapter are all classical and most of them can be found in textbooks like Kunen [8] or Bartoszyński and Judah [3] (for example the model in which $\mathfrak{c} > \mathfrak{a} = \omega_1$ as well as the corresponding proofs are taken from Kunen [8, Chapter VIII, §2] and LEMMA 21.12 is just Lemma 3.3.19 of Bartoszyński and Judah [3]).

Related Results

108. *A combinatorial characterisation of* $cov(\mathscr{M})$. Bartoszyński [2] (see also Bartoszyński and Judah [3, Theorem 2.4.1]) showed that $cov(\mathscr{M})$ is the cardinality of the smallest family $\mathscr{F} \subseteq {}^{\omega}\omega$ with the following property: For each $g \in {}^{\omega}\omega$ there is an $f \in \mathscr{F}$, such that for all but finitely many $n \in \omega$ we have $f(n) \neq g(n)$. For another characterisation of $cov(\mathscr{M})$ see Chapter 13 | Related Result 80.

109. $\mathfrak{p} \leq add(\mathscr{M})$. The *additivity* of $\mathscr{M}$, denoted $add(\mathscr{M})$, is the smallest number of meagre sets such that the union is not meagre. Notice that we obviously have $add(\mathscr{M}) \leq cov(\mathscr{M})$. Piotrowski and Szymański showed in [12] that $\mathfrak{p} \leq add(\mathscr{M})$ which follows from the fact that $add(\mathscr{M}) = \min\{cov(\mathscr{M}), \mathfrak{b}\}$ (see Miller [10] and Truss [16], or Bartoszyński and Judah [3, Corollary 2.2.9]). For possible (*i.e.*, consistent with ZFC) relations between $add(\mathscr{M})$ and $cov(\mathscr{M})$ and other cardinal characteristics of the continuum we refer the reader to Bartoszyński and Judah [3, Chapter 7].

110. *Cohen-stable families of subsets of integers.* Kurilic showed in [9] that adding a Cohen real destroys a splitting family $\mathscr{S}$ if and only if $\mathscr{S}$ is isomorphic to a splitting family on the set of rational numbers whose elements have nowhere dense boundaries. Consequently, $|\mathscr{S}| < cov(\mathscr{M})$ implies the Cohen-indestructibility of $\mathscr{S}$. Further, he showed that for a *mad* family in order to remain maximal in any Cohen extension, it is necessary and sufficient that every bijection from ω to the set of rational numbers must have a somewhere dense image on some member of the family.

A forcing notion, introduced by Solovay [13, 14], which is closely related to Cohen forcing $\mathbb{C}$ is the so-called **random forcing**, denoted $\mathbb{B}$, which is defined as follows: $\mathbb{B}$-conditions are closed sets $A \subseteq \mathbb{R}$ of positive Lebesgue measure, and for two $\mathbb{B}$-conditions A and B let $A \leq B \iff A \subseteq B$. Further, if G is $\mathbb{B}$-generic (over some model $\mathbf{V}$), then $r = \bigcap G$ is called a **random real**.

111. *Properties of random forcing.* Obviously, random forcing satisfies *ccc*, and therefore, random forcing is proper. Furthermore, random forcing is ${}^{\omega}\omega$-bounding (see Jech [5, Part I, Lemma 3.3.(a)]), hence, random forcing does not add Cohen reals. For more properties of random forcing see Bartoszyński and Judah [3, Section 3.2] or Blass [4, Section 11.4].

112. *Random reals versus Cohen reals.* Let c be a Cohen real over $\mathbf{V}$ and let r be a random real over $\mathbf{V}[c]$. Then, in $\mathbf{V}[c][r]$, there is a Cohen real (but no random real) over $\mathbf{V}[r]$ (see Pawlikowski [11, Corollary 3.2]).

113. *On partitions of* ${}^{\omega}\omega$ *into* ω_1 *disjoint closed sets.* If CH holds, then the set of singletons $\{\{x\} : x \in {}^{\omega}\omega\}$ is obviously a partition of ${}^{\omega}\omega$ into ω_1 disjoint closed sets. However, if CH fails, then the existence of a partition of ${}^{\omega}\omega$ into ω_1 disjoint closed sets is independent of ZFC:
Now, Stern [15, §1] showed that if G is $\mathbb{C}_{\omega_2}$-generic over $\mathbf{V}$, where $\mathbf{V} \vDash$ GCH, then, in $\mathbf{V}[G]$, there is no partition of ${}^{\omega}\omega$ into ω_1 disjoint closed sets. On the other hand, Stern [15, §2] also showed that adding ω_2 random reals to a model in which GCH holds, yields a model in which CH fails, but in which such a partition of ${}^{\omega}\omega$ still exists.

114. *On the existence of Ramsey ultrafilters.* It can be shown that $cov(\mathscr{M}) = \mathfrak{c}$ *iff* every filter generated by $< \mathfrak{c}$ elements can be extended to a Ramsey ultrafilter (see Bartoszyński and Judah [3, Theorem 4.5.6]). In particular, adding ω_2 Cohen reals to a model in which GCH holds, yields a model in which Ramsey ultrafilters exist. On the other hand, Kunen showed in [7] that adding ω_2 random reals to a model in which GCH holds, yields a model in which there are no Ramsey ultrafilters (see also Jech [6, Theorem 91]).

115. *Random forcing and the ideal of Lebesgue measure zero sets.* Like the set of meagre sets $\mathscr{M}$, also the set $\mathscr{N}$ of Lebesgue measure zero sets forms an ideal. So, we can investigate $add(\mathscr{N})$ and $cov(\mathscr{N})$, and compare these cardinal characteristics with $add(\mathscr{M})$ and $cov(\mathscr{M})$.
For example, Bartoszyński showed in [1] that $add(\mathscr{N}) \leq add(\mathscr{M})$. Furthermore, by Theorem 20.6 (using the fact that random forcing is proper and ${}^{\omega}\omega$-bounding) it follows that a countable support iteration of length ω_2, starting in a model for CH, yields a model in which $cov(\mathscr{N}) > cov(\mathscr{M})$ (*cf.* Bartoszyński and Judah [3, Model 7.6.8]). For more results concerning random reals and the ideal $\mathscr{N}$ see Bartoszyński and Judah [3, Section 3.2].

References

1. Tomek Bartoszyński, *Additivity of measure implies additivity of category*, ***Transactions of the American Mathematical Society***, vol. 281 (1984), 209–213.
2. ———, *Combinatorial aspects of measure and category*, ***Fundamenta Mathematicae***, vol. 127 (1987), 225–239.
3. Tomek Bartoszyński and Haim Judah, ***Set Theory: on the structure of the real line***, A. K. Peters, Wellesley, 1995.
4. Andreas Blass, *Combinatorial Cardinal Characteristics of the Continuum*, in ***Handbook of Set Theory,*** *Volume 1* (Matthew Foreman and Akihiro Kanamori, eds.), Springer-Verlag, Berlin, 2010, pp. 395–490.
5. Thomas Jech, ***Multiple Forcing***, [Cambridge Tracts in Mathematics], Cambridge University Press, Cambridge, 1986.
6. ———, ***Set Theory,*** *The Third Millennium Edition, Revised and Expanded*, [Springer Monographs in Mathematics], Springer-Verlag, Berlin, 2003.
7. Kenneth Kunen, *Some points in βN*, ***Mathematical Proceedings of the Cambridge Philosophical Society***, vol. 80 (1976), 385–398.
8. ———, ***Set Theory, an Introduction to Independence Proofs***, [Studies in Logic and the Foundations of Mathematics 102], North-Holland, Amsterdam, 1983.
9. Miloš S. Kurilić, *Cohen-stable families of subsets of integers*, ***The Journal of Symbolic Logic***, vol. 66 (2001), 257–270.
10. Arnold W. Miller, *Some properties of measure and category*, ***Transactions of the American Mathematical Society***, vol. 266 (1981), 93–114.
11. Janusz Pawlikowski, *Why Solovay real produces Cohen real*, ***The Journal of Symbolic Logic***, vol. 51 (1986), 957–968.
12. Zbigniew Piotrowski and Andrzej Szymański, *Some remarks on category in topological spaces*, ***Proceedings of the American Mathematical Society***, vol. 101 (1987), 156–160.

13. ROBERT M. SOLOVAY, *A model of set theory in which every set of reals is Lebesgue measurable*, ***Annals of Mathematics (2)***, vol. 92 (1970), 1–56.
14. ———, *Real-valued measurable cardinals*, in ***Axiomatic set theory*** (Dana S. Scott, ed.), [Proceedings of Symposia in Pure Mathematics, Vol. XIII, Part I], American Mathematical Society, Providence, Rhode Island, 1971, pp. 397–428.
15. JACQUES STERN, *Partitions of the real line into $\aleph_1$ closed sets*, in ***Higher set theory,*** *Proceedings, Oberwolfach, Germany, April 13–23, 1977* (Gert H. Müller and Dana S. Scott, eds.), [Lecture Notes in Mathematics 669], Springer-Verlag, Berlin, 1978, pp. 455–460.
16. JOHN K. TRUSS, *Sets having calibre $\aleph_1$*, in ***Logic Colloquium 76: proceedings of a conference held in Oxford in July 1976*** (R. O. Gandy and J. M. E. Hyland, eds.), [Studies in Logic and the Foundations of Mathematics 87], North-Holland, Amsterdam, 1977, pp. 595–612.

22

Silver-Like Forcing Notions

On the one hand, we have seen that every forcing notion which adds dominating reals also adds splitting reals (see FACT 20.1). On the other hand, we have seen in the previous chapter that Cohen forcing is a forcing notion which adds splitting reals, but which does not add dominating reals. However, Cohen forcing adds unbounded reals and as an application we constructed a model in which $\mathfrak{s} = \mathfrak{b} < \mathfrak{d} = \mathfrak{r}$. One might ask whether there exists a forcing notion which is even ${}^\omega\omega$-bounding but still adds splitting reals. In this chapter, we shall present such a forcing notion and as an application we shall construct a model in which $\mathfrak{s} = \mathfrak{b} = \mathfrak{d} < \mathfrak{r}$.

Below, let $\mathscr{E}$ be an arbitrary but fixed P-family (introduced in Chapter 10). For a set $x \subseteq \omega$, let ${}^x 2$ denote the set of all functions form x to $\{0,1\}$. **Silver-like forcing** with respect to $\mathscr{E}$, denoted $\mathbb{S}_{\mathscr{E}} = (S_{\mathscr{E}}, \leq)$, is defined as follows:

$$S_{\mathscr{E}} = \bigcup \{ {}^x 2 : x^{\mathsf{c}} \in \mathscr{E} \}$$

where $x^{\mathsf{c}} := \omega \setminus x$, and for $p, q \in S_{\mathscr{E}}$ we stipulate

$$p \leq q \iff \operatorname{dom}(p) \subseteq \operatorname{dom}(q) \wedge q|_{\operatorname{dom}(p)} = p\,.$$

If $\mathscr{E} = [\omega]^\omega$, then we call $\mathbb{S}_{\mathscr{E}}$ just **Silver forcing**, and if $\mathscr{E}$ is a P-point, then $\mathbb{S}_{\mathscr{E}}$ is usually called **Grigorieff forcing**.

As in the case of Cohen forcing we can identify every $\mathbb{S}_{\mathscr{E}}$-generic filter with a real $g \in {}^\omega 2$, called **Silver real**, which is in fact just the union of the functions which belong to the generic filter. More formally, if G is $\mathbb{S}_{\mathscr{E}}$-generic over some model $\mathbf{V}$, then the corresponding Silver real $g \in {}^\omega 2$ is defined by

$$g = \bigcup \{ f \in S_{\mathscr{E}} : f \in G \}\,.$$

On the other hand, from a Silver real one can always reconstruct the corresponding generic filter, and therefore, $\mathbf{V}[G] = \mathbf{V}[g]$ (we leave the reconstruction as an exercise to the reader). Furthermore, Silver reals can be characterised as follows: A real $g \in {}^\omega 2$ is a Silver real over a model $\mathbf{V}$ of ZFC *iff* for every open dense subset $D \subseteq S_{\mathscr{E}}$ there is a $p \in D$ such that $g|_{\operatorname{dom}(p)} = p$.

Properties of Silver-Like Forcing

Silver-Like Forcing is Proper and ${}^{\omega}\omega$-bounding

Before we show that Silver-like forcing $\mathbb{S}_{\mathscr{E}}$ is proper and ${}^{\omega}\omega$-bounding, let us introduce the following notation: For a condition $p \in S_{\mathscr{E}}$ (*i.e.*, $p : x \to \{0,1\}$ where $x^{\mathsf{c}} \in \mathscr{E}$) and a finite set $t \subseteq \mathrm{dom}(p)$ let

$$\overline{p \,\text{-}\, t} = \left\{ q \in S_{\mathscr{E}} : \mathrm{dom}(q) = \mathrm{dom}(p) \,\wedge\, q|_{\mathrm{dom}(q)\setminus t} = p|_{\mathrm{dom}(p)\setminus t} \right\}.$$

LEMMA 22.1. *Silver-like forcing $\mathbb{S}_{\mathscr{E}}$ is proper.*

Proof. As described in Chapter 20, let χ be a sufficiently large regular cardinal. We have to show that for all countable elementary submodels $\mathbf{N} = (N, \in) \prec (\mathrm{H}_{\chi}, \in)$ which contain $\mathbb{S}_{\mathscr{E}}$, and for all conditions $p \in S_{\mathscr{E}} \cap N$, there exists an $\mathbb{S}_{\mathscr{E}}$-condition $q \geq p$ (in $\mathbf{V}$) which is $\mathbf{N}$-generic (*i.e.*, if $g \in {}^{\omega}2$ is a Silver real over $\mathbf{V}$ and $q \subseteq g$, then g is also a Silver real over $\mathbf{N}$).

So, let $\mathbf{N} = (N, \in)$ be an arbitrary countable elementary submodel of $(\mathrm{H}_{\chi}, \in)$ and let $p \in S_{\mathscr{E}} \cap N$ be an arbitrary $\mathbb{S}_{\mathscr{E}}$-condition which belongs to $\mathbf{N}$. We shall construct in $\mathbf{V}$ an $\mathbb{S}_{\mathscr{E}}$-condition $q \geq p$ which is $\mathbf{N}$-generic by using the fact that $\mathscr{E}$ is a P-family. Firstly, let $\{D_n : n \in \omega\}$ be an enumeration (in $\mathbf{V}$) of all open dense subsets of $S_{\mathscr{E}}$ which belong to $\mathbf{N}$ and choose (in $\mathbf{V}$) some well-ordering "$\prec$" on $S_{\mathscr{E}} \cap N$. We construct the sought $\mathbb{S}_{\mathscr{E}}$-condition $q \geq p$ by running the game $\mathcal{G}^*_{\mathscr{E}}$: The MAIDEN starts the game by playing $x_0 := \mathrm{dom}(q_0)^{\mathsf{c}}$, where $q_0 \in \mathbf{N}$ is the $\prec$-least condition such that $q_0 \geq p$ and $q_0 \in D_0$, and DEATH responds with some finite set $s_0 \subseteq x_0$. Assume that for some $n \in \omega$ we already have x_n, q_n, and s_n. Let $t = \bigcup_{0 \leq i \leq n} s_i$ and $y = x_n \setminus t$. Now, the MAIDEN plays $x_{n+1} \subseteq y$ such that $x_{n+1} = \mathrm{dom}(q_{n+1})^{\mathsf{c}}$, where $q_{n+1} \in \mathbf{N}$ is the $\prec$-least condition such that $q_{n+1} \geq q_n$ and $\overline{q_{n+1} \,\text{-}\, t} \subseteq D_{n+1}$, and DEATH responds with some finite set $s_{n+1} \subseteq x_{n+1}$.

Since $\mathscr{E}$ is a P-family, this strategy of the MAIDEN is not a winning strategy and DEATH can play so that $x' = \bigcup_{n \in \omega} s_n$ belongs to $\mathscr{E}$. For $q' = \bigcup_{n \in \omega} q_n$ we have $x' \subseteq \mathrm{dom}(q')$, and thus, the function $q := q'|_{x'^{\mathsf{c}}}$ is an $\mathbb{S}_{\mathscr{E}}$-condition. In addition, if g is a Silver real over $\mathbf{V}$ such that $q \subseteq g$, then, by construction of q and the properties of the q_n's, for every $n \in \omega$ we have $g|_{\mathrm{dom}(q_n)} \in D_n$, which shows that g is a Silver real over $\mathbf{N}$. ⊣

LEMMA 22.2. *Silver-like forcing $\mathbb{S}_{\mathscr{E}}$ is ${}^{\omega}\omega$-bounding.*

Proof. Let G be $\mathbb{S}_{\mathscr{E}}$-generic over $\mathbf{V}$, let $f \in {}^{\omega}\omega$ be a function in $\mathbf{V}[G]$, and let $\underset{\sim}{f}$ be an $\mathbb{S}_{\mathscr{E}}$-name for f. In order to show that f is bounded by some function in the ground model, it is enough to prove that for every $\mathbb{S}_{\mathscr{E}}$-condition $p \in S_{\mathscr{E}}$ there is a condition $q_0 \geq p$ and a function $g \in {}^{\omega}\omega$ in the ground model $\mathbf{V}$ such that $q_0 \Vdash_{\mathbb{S}_{\mathscr{E}}}$ "g dominates $\underset{\sim}{f}$".

Firstly, choose some well-ordering "$\prec$" on $S_{\mathscr{E}}$. We construct the condition q_0 by running the game $\mathcal{G}^*_{\mathscr{E}}$ where the MAIDEN plays according to the following strategy: Let $m_0 \in \omega$ be the smallest integer for which there exists a condition $r \geq p$ such that $r \Vdash_{\mathbb{S}_{\mathscr{E}}} \underset{\sim}{f}(0) < m_0$ and let p_0 be the least such condition r with respect to the well-ordering "$\prec$". Then the MAIDEN plays $x_0 = \operatorname{dom}(p_0)^{\mathsf{c}}$. For positive integers $i \in \omega$ let $t_i = \bigcup_{k \in i} s_k$, where $s_0, \dots, s_{i-1}$ are the moves of DEATH, and let $p_0 \leq \dots \leq p_{i-1}$ be an increasing sequence of conditions. Further, let $m_i \in \omega$ be the least number for which there exists a condition $r \geq p_{i-1}$ with $\operatorname{dom}(r) \supseteq \operatorname{dom}(p_{i-1}) \cup t_i$ such that for all $q \in \overline{r \text{-} t_i}$ we have $r \Vdash_{\mathbb{S}_{\mathscr{E}}} \underset{\sim}{f}(i) < m_i$, and again, let p_i be the least such condition r (with respect to "$\prec$"). Then the MAIDEN plays $x_i = \operatorname{dom}(p_i)^{\mathsf{c}}$.

Since $\mathscr{E}$ is a P-family, DEATH can play so that $\bigcup_{i \in \omega} s_i \in \mathscr{E}$. Let $h = \bigcup_{i \in \omega} p_i$; then $h \in {}^{x}2$ for some $x \subseteq \omega$ (but h is not necessarily an $\mathbb{S}_{\mathscr{E}}$-condition). Now, let $q_0 \in S_{\mathscr{E}}$ be such that $\operatorname{dom}(q_0) = \operatorname{dom}(h) \setminus \bigcup_{i \in \omega} s_i$ and $q_0 \equiv h|_{\operatorname{dom}(q_0)}$, and define the function $g \in {}^{\omega}\omega$ by stipulating $g(i) := m_i$ (for all $i \in \omega$). Then g belongs to the ground model $\mathbf{V}$ and by construction we have

$$q_0 \Vdash_{\mathbb{S}_{\mathscr{E}}} \forall i \in \omega \left(\underset{\sim}{f}(i) < g(i) \right),$$

which shows that q_0 forces that f is dominated by g. ⊣

Silver-Like Forcing adds Splitting Reals

LEMMA 22.3. *Silver-like forcing $\mathbb{S}_{\mathscr{E}}$ adds splitting reals.*

Proof. Let $g \in {}^{\omega}2$ be a Silver real over $\mathbf{V}$. We can identify g with the function $f \in {}^{\omega}\omega$ by stipulating

$$f(n) = k \iff g(k) = 1 \ \wedge \ \left| \left\{ m < k : g(m) = 1 \right\} \right| = n .$$

Then the set

$$\sigma_f = \bigcup \left\{ \left[f(2n), f(2n+1) \right) : n \in \omega \right\}$$

splits every real in the ground model, where $[a, b) := \{ k \in \omega : a \leq k < b \}$. To see this, recall that $\mathscr{E}$ is a free family, and notice that for each real $x \in [\omega]^{\omega}$ in the ground model $\mathbf{V}$ and for every $n \in \omega$, the set

$$D_{x,n} = \left\{ p \in S_{\mathscr{E}} : p \Vdash_{\mathbb{S}_{\mathscr{E}}} \left(|x \cap \underset{\sim}{\sigma_f}| > n \ \wedge \ |x \setminus \underset{\sim}{\sigma_f}| > n \right) \right\}$$

is open dense in $S_{\mathscr{E}}$. ⊣

A Model in which $\mathfrak{d} < \mathfrak{r}$

PROPOSITION 22.4. $\omega_1 = \mathfrak{d} < \mathfrak{r} = \mathfrak{c}$ *is consistent with* ZFC.

Proof. Let $\mathbf{V}$ be a model of $\mathsf{ZFC} + \mathsf{CH}$, let $\mathbb{P}_{\omega_2}$ be an ω_2-stage, countable support iteration of Silver forcing (*i.e.*, Silver-like forcing $\mathbb{S}_{\mathscr{E}}$ with $\mathscr{E} = [\omega]^{\omega}$), and let G be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$. Since Silver forcing is of size $\mathfrak{c}$, by THEOREM 20.5.(a) we get $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$. Furthermore, since Silver forcing is proper and ${}^\omega\omega$-bounding, by THEOREM 20.6 we get that $\mathbb{P}_{\omega_2}$ is ${}^\omega\omega$-bounding, which implies that in $\mathbf{V}[G]$, ${}^\omega\omega \cap \mathbf{V}$ is a dominating family of size ω_1 (recall that $\mathbf{V} \vDash \mathsf{CH}$), and therefore we have $\mathbf{V}[G] \vDash \mathfrak{d} = \omega_1$. Finally, since Silver forcing adds splitting reals, by THEOREM 20.5.(b) we get that no family $\mathscr{F} \subseteq [\omega]^\omega$ of size ω_1 can be a reaping family, thus, $\mathbf{V}[G] \vDash \mathfrak{r} = \omega_2$. Hence, we get $\mathbf{V}[G] \vDash \omega_1 = \mathfrak{d} < \mathfrak{r} = \omega_2 = \mathfrak{c}$. $\dashv$

NOTES

Most of the results presented here can be found in Grigorieff [10] and Halbeisen [11] (see also Jech [12, p. 21 f.] and Mathias [16]).

RELATED RESULTS

116. *Silver-like forcing $\mathbb{S}_{\mathscr{E}}$ is minimal.* Grigorieff proved in [10] that $\mathbb{S}_{\mathscr{E}}$ is minimal whenever $\mathscr{E}$ is a P-point and in Halbeisen [11] it is shown how Grigorieff's proof can be generalised to arbitrary P-families.

117. *Silver-like forcing has the Laver property.* By similar arguments as in the proof of LEMMA 22.2 one can show that Silver-like forcing has the Laver property.

118. *n-Silver forcing.* For integers $n \geq 2$, the n-Silver forcing notion $\mathbb{S}_n$ consists of functions $f : A \to n$, where $A \subset \omega$ and $\omega \setminus A$ is infinite. $\mathbb{S}_n$ is ordered by inclusion, *i.e.*, $f \leq g$ *iff* g extends f. Notice that $\mathbb{S}_2$ is the same as Silver forcing. If G is $\mathbb{S}_n$-generic, then the function $\bigcup G : \omega \to n$ is called an $\mathbb{S}_n$-generic real. As a corollary of a more general result, it is shown in Rosłanowski and Steprāns [18] that no countable support iteration of $\mathbb{S}_2$ adds an $\mathbb{S}_4$-generic real.

119. *Another model in which $\mathfrak{d} < \mathfrak{r}$.* A model in which $\omega_1 = \mathfrak{a} = \mathfrak{d} < \mathfrak{r} = \omega_2 = \mathfrak{c}$ we get if we add ω_2 random reals to a model $\mathbf{V}$ of $\mathsf{ZFC} + \mathsf{CH}$ (see for example Blass [2, Section 11.4]).

A forcing notion, introduced by Sacks [19], which is somewhat similar to Silver-like forcing, is the so-called **Sacks forcing**, denoted $\mathbb{S}$,. To show the similarity to Silver-like forcing we shall define Sacks forcing in terms of perfect sets — but one can equally well define Sacks forcing in terms of trees. We say that a set $T \subseteq {}^\omega 2$ is **perfect** if for every $f \in T$ and every $n \in \omega$ there is a $g \in T$ and an integer $k \geq n$ such that $g|_n = f|_n$ and $f(k) \neq g(k)$. The set of $\mathbb{S}$-conditions consists of all perfect sets $T \subseteq {}^\omega 2$, and for any $\mathbb{S}$-conditions S and T we stipulate $S \leq T \iff T \subseteq S$. Furthermore, if G is $\mathbb{S}$-generic then the real $\bigcap G \in {}^\omega 2$ is called a **Sacks real**.

120. *Properties of Sacks forcing.* One can show that Sacks forcing has the following properties:
    - Sacks forcing is proper.
    - Sacks forcing is ${}^\omega\omega$-bounding.
    - Sacks forcing has the Laver property.

- Sacks forcing is minimal and every new real is a Sacks real.
- Sacks forcing collapses $\mathfrak{c}$ to $\mathfrak{b}$.

For these and further properties of Sacks forcing, as well as for some applications of Sacks forcing to Ramsey Theory, see Sacks [19], Geschke and Quickert [9], Brendle [3, 4, 5], Simon [20], Blass [2, Section 11.5], Brendle and Löwe [7], and Brendle, Halbeisen, and Löwe [6].

121. *Sacks forcing and splitting reals.* Baumgartner and Laver [1] showed that Sacks forcing does not add splitting reals (see also Miller [17, Prop. 3.2]). Now, by applying the WEAK HALPERN-LÄUCHLI THEOREM 11.6, one can show that also finite products of Sacks forcing do not add splitting reals (see Miller [17, Remark, p. 149] and compare with Chapter 23 | RELATED RESULT 127). Moreover, Laver [15] showed that even arbitrarily large countable support products of Sacks forcing do not add splitting reals.

122. *Splitting families and Sacks forcing.* Using the methods developed by Brendle and Yatabe in [8], Kurilic investigated in [14] the stability of splitting families in several forcing extensions. For example, he proved that a splitting family is preserved by Sacks forcing if and only if it is preserved by some forcing notion which adds new reals (compare with Chapter 21 | RELATED RESULT 110).

123. *Sacks reals out of nowhere.* Kellner and Shelah showed in [13] that there is a countable support iteration of length ω which does not add new reals at finite stages, but which adds a Sacks real at the limit stage ω.

REFERENCES

1. JAMES E. BAUMGARTNER AND RICHARD LAVER, *Iterated perfect-set forcing*, ***Annals of Mathematical Logic***, vol. 17 (1979), 391–397.
2. ANDREAS BLASS, *Combinatorial Cardinal Characteristics of the Continuum*, *in* ***Handbook of Set Theory,*** *Volume 1* (Matthew Foreman and Akihiro Kanamori, eds.), Springer-Verlag, Berlin, 2010, pp. 395–490.
3. JÖRG BRENDLE, *Combinatorial properties of classical forcing notions*, ***Annals of Pure and Applied Logic***, vol. 73 (1995), 143–170.
4. ______, *Strolling through paradise*, ***Fundamenta Mathematicae***, vol. 148 (1995), 1–25.
5. ______, *How small can the set of generics be?*, *in* ***Logic Colloquium '98 (Prague)*** (S.R. Buss, P. Hájek, and P. Pudlák, eds.), [Lecture Notes in Logic, 13], Association for Symbolic Logic, Urbana, IL, 2000, pp. 109–126.
6. JÖRG BRENDLE, LORENZ HALBEISEN, AND BENEDIKT LÖWE, *Silver measurability and its relation to other regularity properties*, ***Mathematical Proceedings of the Cambridge Philosophical Society***, vol. 138 (2005), 135–149.
7. JÖRG BRENDLE AND BENEDIKT LÖWE, *Solovay-type characterizations for forcing-algebras*, ***The Journal of Symbolic Logic***, vol. 64 (1999), 1307–1323.
8. JÖRG BRENDLE AND SHUNSUKE YATABE, *Forcing indestructibility of MAD families*, ***Annals of Pure and Applied Logic***, vol. 132 (2005), 271–312.
9. STEFAN GESCHKE AND SANDRA QUICKERT, *On Sacks Forcing and the Sacks Property*, *in* ***Classical and New Paradigms of Computation and their Complexity Hierarchies*** (Benedikt Löwe, Wolfgang Malzkorn, and Thoralf Räsch, eds.), Papers of the conference *Foundations of the Formal Sciences III*

held in Vienna, September 21–24, 2001 [Trends in Logic 23], Kluwer Academic Publishers, Dordrecht, 2004, pp. 95–139.

10. Serge Grigorieff, *Combinatorics on ideals and forcing*, ***Annals of Mathematical Logic***, vol. 3 (1971), 363–394.
11. Lorenz Halbeisen, *A playful approach to Silver and Mathias forcings*, in ***Foundations of the Formal Sciences V: Infinite Games*** (Stefan Bold, Benedikt Löwe, Thoralf Räsch, and Johan van Benthem, eds.), Papers of a Conference held in Bonn, November 26–29, 2004, [Studies in Logic, vol. 11], College Publications, London, 2007, pp. 123–142.
12. Thomas Jech, ***Multiple Forcing***, [Cambridge Tracts in Mathematics], Cambridge University Press, Cambridge, 1986.
13. Jakob Kellner and Saharon Shelah, *A Sacks real out of nowhere*, ***The Journal of Symbolic Logic***, vol. 75 (2010), 51–75.
14. Miloš S. Kurilić, *Splitting families and forcing*, ***Annals of Pure and Applied Logic***, vol. 145 (2007), 240–251.
15. Richard Laver, *Products of infinitely many perfect trees*, ***Journal of the London Mathematical Society (2)***, vol. 29 (1984), 385–396.
16. Adrian Richard David Mathias, *Surrealist landscape with figures (a survey of recent results in set theory)*, ***Periodica Mathematica Hungarica***, vol. 10 (1979), 109–175.
17. Arnold W. Miller, *Rational perfect set forcing*, in ***Axiomatic Set Theory*** (James E. Baumgartner, Donald A. Martin, and Saharon Shelah, eds.), Contemporary Mathematics, vol. 31, American Mathematical Society, Providence, RI, 1984, pp. 143–159.
18. Andrzej Rosłanowski and Juris Steprāns, *Chasing Silver*, ***Canadian Mathematical Bulletin. Bulletin Canadien de Mathématiques***, vol. 51 (2008), 593–603.
19. Gerald E. Sacks, *Forcing with perfect closed sets*, in ***Axiomatic Set Theory*** (Dana S. Scott, ed.), [Proceedings of Symposia in Pure Mathematics, Vol. XIII, Part I], American Mathematical Society, Providence, Rhode Island, 1971, pp. 331–355.
20. Petr Simon, *Sacks forcing collapses* $\mathfrak{c}$ *to* $\mathfrak{b}$, ***Commentationes Mathematicae Universitatis Carolinae***, vol. 34 (1993), 707–710.

23

Miller Forcing

So far we have seen that Cohen forcing adds unbounded as well as splitting reals, but not dominating reals (see Chapter 21), and that Silver forcing adds splitting reals but not unbounded reals (see Chapter 22). Furthermore, it was mentioned that Sacks forcing adds neither splitting nor unbounded reals (see Chapter 22 | RELATED RESULT 120). In this chapter we shall introduce a forcing notion, called *Miller forcing*, which adds unbounded reals but no splitting reals. As an application of that forcing notion we shall construct a model in which $\mathfrak{r} < \mathfrak{d}$.

Before we introduce Miller forcing, let us first fix some terminology. We shall identify $\operatorname{seq}(\omega)$ (the set of finite sequences of ω) with $\bigcup_{n\in\omega} {}^n\omega$. Consequently, for $s \in \operatorname{seq}(\omega)$ with $|s| = n+1$ we can write $s = \big\langle s(0), \dots, s(n)\big\rangle$. Furthermore, for $s, t \in \operatorname{seq}(\omega)$ with $|s| \leq |t|$ we write $s \preccurlyeq t$ if $t|_{|s|} = s$ (*i.e.*, s is an initial segment of t). A set $T \subseteq \operatorname{seq}(\omega)$ is a **tree**, if it is closed under initial segments, *i.e.*, $t \in T$ and $s \preccurlyeq t$ implies $s \in T$. Elements of a tree are usually called **nodes**. Let $T \subseteq \operatorname{seq}(\omega)$ be a tree and let $s \in T$ be a node of T. Then the tree T_s is defined by

$$T_s = \{t \in T : t \preccurlyeq s \vee s \preccurlyeq t\}.$$

Further, the set of immediate successors of s (with respect to T) is defined by

$$succ_T(s) = \big\{t \in T : \exists n \in \omega \,\big(t = s^\frown n\big)\big\},$$

where $s^\frown n$ denotes the concatenation of the sequences s and $\langle n\rangle$, and finally let

$$next_T(s) = \{n \in \omega : s^\frown n \in T\}.$$

A tree $T \subseteq \operatorname{seq}(\omega)$ is called **superperfect**, if for every $t \in T$ there is an $s \in T$ such that $t \preccurlyeq s$ and $|succ_T(s)| = \omega$, *i.e.*, above every node t there is a node s with infinitely many immediate successors. If $T \subseteq \operatorname{seq}(\omega)$ is a superperfect tree, then let

$$split(T) = \{s \in T : |succ_T(s)| = \omega\}.$$

Thus, a tree $T \subseteq \mathrm{seq}(\omega)$ is superperfect if and only if for each $s \in T$ there exists a $t \in split(T)$ — a so-called *splitting node* — such that $s \preccurlyeq t$. For $k \in \omega$ and $T \subseteq \mathrm{seq}(\omega)$, let

$$split_k(T) = \{s \in split(T) : |\{t \in split(T) : t \preccurlyeq s\}| = k+1\},$$

i.e., a splitting node $s \in split(T)$ belongs to $split_k(T)$ if and only if there are k splitting nodes below s.

Now, **Miller forcing**, denoted by $\mathbb{M} = (M, \leq)$, also known as **rational perfect set forcing**, is defined as follows:

$$M = \{T \subseteq \mathrm{seq}(\omega) : T \textit{ is a superperfect tree}\},$$

and for $T, T' \in M$ we stipulate

$$T \leq T' \iff T' \subseteq T.$$

As in the case of Cohen and Silver forcing we can identify every $\mathbb{M}$-generic filter with a real $g \in {}^{\omega}\omega$, called **Miller real**, which is in fact the union of the intersection of the trees in the generic filter. More formally, if G is $\mathbb{M}$-generic over some model $\mathbf{V}$, then the corresponding Miller real $g \in {}^{\omega}\omega$ has the property that for each $n \in \omega$ we have

$$g|_n \in \bigcap \{T \in M : T \in G\}.$$

Since we can reconstruct the generic filter from the corresponding Miller real, we obviously have $\mathbf{V}[G] = \mathbf{V}[g]$ (we leave the reconstruction as an exercise to the reader).

Properties of Miller Forcing

Miller Forcing is Proper and adds Unbounded Reals

LEMMA 23.1. *Miller forcing is proper.*

Proof. As described in Chapter 20, let χ be a sufficiently large regular cardinal. We have to show that for all countable elementary submodels $\mathbf{N} = (N, \in) \prec (\mathrm{H}_\chi, \in)$ which contain $\mathbb{M}$, and for all conditions $S \in M \cap N$, there exists an $\mathbb{M}$-condition $T \subseteq S$ (in $\mathbf{V}$) which is $\mathbf{N}$-generic.

So, let $\mathbf{N} = (N, \in)$ be an arbitrary countable elementary submodel of $(\mathrm{H}_\chi, \in)$ and let $S \in M \cap N$ be an arbitrary $\mathbb{M}$-condition which belongs to $\mathbf{N}$. We shall construct a superperfect tree $T \subseteq S$ which meets every open dense subset of M which belongs to $\mathbf{N}$: In $\mathbf{V}$, let $\{D_n : n \in \omega\}$ be an enumeration of all open dense subsets of M which belong to $\mathbf{N}$. Firstly, choose a superperfect tree $T^0 \subseteq S$ such that $T^0 \in (D_0 \cap N)$. Assume we have already constructed $T^0 \supseteq \cdots \supseteq T^n$ such that for each $i \leq n$, $T^i \in (D_i \cap N)$. Let $\{s_j : j \in \omega\}$ be an enumeration of $split_{n+1}(T^n)$. For every $j \in \omega$ and for each $t \in succ_{T^n}(s_j)$ choose a superperfect tree $T^{j,t} \subseteq T^n_t$ such that $T^{j,t} \in (D_{n+1} \cap N)$ and let

$$T^{n+1} = \bigcup \left\{ T^{j,t} \in M : j \in \omega \wedge t \in succ_{T^n}(s_j) \right\}.$$

Then T^{n+1} is a superperfect tree and $T^{n+1} \subseteq T^n$. In addition, if G is $\mathbb{M}$-generic over $\mathbf{V}$ and $T^{n+1} \in G$, then there exists a $T^{j,t} \subseteq T^{n+1}$ which belongs to G, and because $T^{j,t} \in D_{n+1}$, we get $G \cap D_{n+1} \neq \emptyset$. Now, let $T = \bigcap_{n\in\omega} T^n$. Then $T \subseteq S$ is a superperfect tree which is $\mathbf{N}$-generic. ⊣

LEMMA 23.2. *Miller forcing adds unbounded reals.*

Proof. In order to prove that Miller forcing adds unbounded reals, it is enough to show that whenever $g \in {}^\omega\omega$ is a Miller real over some model $\mathbf{V}$, then g is unbounded. Let $f \in {}^\omega\omega$ be an arbitrary function in $\mathbf{V}$ and let

$$D_f = \left\{ T \in M : \forall s \in split(T)\, \forall n \in next_T(s) \left(f(|s|) < n \right) \right\}.$$

We leave it as an exercise to the reader to show that D_f is open dense in M, which shows that $g \not\leq^* f$. Thus, g is not dominated by f, and since f was arbitrary, g is unbounded. ⊣

Miller Forcing does not add Splitting Reals

LEMMA 23.3. *Miller forcing does not add splitting reals.*

Proof. Let $\mathbf{V}$ be a model of ZFC, let G be $\mathbb{M}$-generic over $\mathbf{V}$, and let $\underset{\sim}{Y}$ be an $\mathbb{M}$-name for a subset of ω in $\mathbf{V}[G]$, *i.e.*, there is an $\mathbb{M}$-condition $S \in M$ such that $S \Vdash_{\mathbb{M}} \underset{\sim}{Y} \subseteq \omega$. We shall construct an $\mathbb{M}$-condition $S' \subseteq S$ and an $X \in [\omega]^\omega$ (in $\mathbf{V}$) such that $S' \Vdash_{\mathbb{M}} (X \subseteq \underset{\sim}{Y}) \vee (X \cap \underset{\sim}{Y} = \emptyset)$, which shows that $\underset{\sim}{Y}$ is not a splitting real.

The construction of the superperfect tree S' and the infinite set $X \in [\omega]^\omega$ is done in the following three steps.

CLAIM 1. *There is an $\mathbb{M}$-condition $T \subseteq S$ and a sequence $\langle Y_s : s \in split(T) \rangle$ (in $\mathbf{V}$) of subsets of ω, such that for every $s \in split(T)$, each $k \in \omega$, and for all but finitely many $n \in next_T(s)$ we have*

$$T_{s^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = Y_s \cap k,$$

i.e., for every $k \in \omega$ there exists an $n_k \in \omega$ such that for all $n' \in next_T(s)$ with $n' \geq n_k$, $T_{s^\frown n'} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = Y_s \cap k$.

Proof of Claim 1. We construct the condition T by induction. In particular, the superperfect tree T will be the intersection of superperfect trees T^i, where

$$T^0 = S\,,\quad T^{i+1} = \bigcup_{s\in split_i(T^i)} \tilde{T}^i_s\,,\quad \text{and}\quad \tilde{T}^i_s \subseteq T^i_s\,,$$

and where the superperfect trees $\tilde{T}^i_s$ are constructed as follows: Fix an $i \in \omega$ and a splitting node $s \in split_i(T^i)$. For each $n \in next_{T^i}(s)$, choose a superperfect tree $\tilde{T}^i_{s^\frown n} \subseteq T^i_{s^\frown n}$ such that, for some finite set $b_n \in \mathrm{fin}(\omega)$, we have

$$\tilde{T}^i_{s^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap n = b_n\,.$$

For every $k \in \omega$, let $F_k = \{b_n \cap k : n \in next_{T^i}(s)\}$. Notice that all sets F_k are finite, in fact, $F_k \subseteq \mathscr{P}(k)$. Consider now the tree $\mathcal{T}$ with the infinite vertex set $\{\langle b,k\rangle : k \in \omega \wedge b \in F_k\}$, where two vertices $\langle b,k\rangle$ and $\langle b',k'\rangle$ are joined by an edge *iff* $b \subseteq (b' \cap k)$ and $k' = k+1$. Notice that $\mathcal{T}$ is an infinite, finitely branching tree. Hence, by König's Lemma, $\mathcal{T}$ contains an infinite branch, say $(\langle\emptyset,0\rangle, \langle a_1,1\rangle,\dots,\langle a_k,k\rangle,\dots)$. Let $Y_s = \bigcup_{k\in\omega} a_k$ and define the strictly increasing sequence $\langle n_j : j \in \omega\rangle$ of elements of $next_{T^i}(s)$ so that for each $k \in \omega$ and for all $n_j \geq k$ we have

$$\tilde{T}^i_{s^\frown n_j} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = a_k\,.$$

Hence, for each $k \in \omega$ and for all but finitely many $j \in \omega$ we have

$$\tilde{T}^i_{s^\frown n_j} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = Y_s \cap k\,.$$

Now, let $\tilde{T}^i_s = \bigcup_{j\in\omega} \tilde{T}^i_{s^\frown n_j}$. Then, for each $k \in \omega$ and for all but finitely many $n \in next_{\tilde{T}^i_s}(s)$ we have

$$\tilde{T}^i_{s^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap n = Y_s \cap n\,.$$

Finally, let $T^{i+1} = \bigcup\{\tilde{T}^i_s : s \in split_i(T^i)\}$. Notice that for all $j \leq i$, $split_j(T^{i+1}) = split_j(T^i)$; thus, $T = \bigcap_{i\in\omega} T^i$ is a superperfect tree. By construction, for every $s \in split(T)$, for each $k \in \omega$, and for all but finitely many $n \in next_T(s)$ we have

$$T_{s^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = Y_s \cap k\,,$$

where $\langle Y_s : s \in split(T)\rangle$ is an infinite sequence of subsets of ω which belongs to the ground model $\mathbf{V}$. $\dashv_{\text{Claim 1}}$

In the next step we prune the tree T so that the corresponding sets Y_s (or their complements) have the strong finite intersection property *sfip* (*i.e.*, intersections of finitely many sets are infinite).

Claim 2. *There exists a superperfect tree $T' \subseteq T$ such that*

(1) $\{Y_s : s \in split(T')\}$ *has the sfip; or*

(2) $\{\omega \setminus Y_s : s \in split(T')\}$ *has the sfip.*

Proof of Claim 2. Let $\mathscr{U} \subseteq [\omega]^\omega$ be an arbitrary ultrafilter over ω. We partition the set $split(T)$ according to whether the set Y_s belongs to $\mathscr{U}$ or not. More precisely, let $U = \{s \in split(T) : Y_s \in \mathscr{U}\}$ and $V = \{s \in split(T) : (\omega \setminus Y_s) \in \mathscr{U}\}$. Then $U \cap V = \emptyset$ and $U \cup V = split(T)$. We are in at least one of the following two cases:

- There exists an $s \in split(T)$ such that $split(T_s) \subseteq U$.
- For all $s \in split(T)$ there exists a $t \in split(T_s)$ with $t \in V$.

In the former case, let $T' = T_s$, and in the latter case, we can construct a superperfect tree $T' \subseteq T$ such that $split(T') \subseteq V$ — we leave the construction of T' as an exercise to the reader.

If $split(T') \subseteq U$, then $\{Y_s : s \in split(T')\}$ has the *sfip*; and if $split(T') \subseteq V$, then $\{\omega \setminus Y_s : s \in split(T')\}$ has the *sfip*. $\dashv_{\text{Claim 2}}$

In the last step we construct a set $X \in [\omega]^\omega$ which is not split by $\underset{\sim}{Y}$.

CLAIM 3. *Let $T' \subseteq T$ be a superperfect tree such that*

$$\mathscr{Y}_0 = \{Y_s : s \in split(T')\} \qquad or \qquad \mathscr{Y}_1 = \{\omega \setminus Y_s : s \in split(T')\}$$

has the sfip. Then there exists a sequence of superperfect trees $\langle T^i : i \in \omega\rangle$, where $T^0 \subseteq T'$ and $T^{i+1} \subseteq T^i$ (for all $i \in \omega$), as well as a sequence of natural numbers $\langle m_i : i \in \omega\rangle$, where $m_i < m_{i+1}$ (for all $i \in \omega$), such that $\bigcap_{i\in\omega} T^i$ is a superperfect tree and either

$$\forall i \in \omega \left(T^i \Vdash_{\mathbb{M}} m_i \in \underset{\sim}{Y}\right) \qquad or \qquad \forall i \in \omega \left(T^i \Vdash_{\mathbb{M}} m_i \notin \underset{\sim}{Y}\right).$$

Proof of Claim 3. We just consider the case when $\mathscr{Y}_1$ has the *sfip*, in which case we shall later get $X \cap \underset{\sim}{Y} = \emptyset$; the other case, in which would later get $X \subseteq \underset{\sim}{Y}$, is handled analogously and is left as an exercise to the reader.

In order to get $\bigcap_{i\in\omega} T^i \in M$, we shall construct an auxiliary sequence $\langle F_i : i \in \omega\rangle$ of increasing finite subsets of $split(T^i)$, *i.e.*, for every $i \in \omega$, $F_i \subseteq F_{i+1}$ and $F_i \in \text{fin}\left(split(T^i)\right)$. Moreover, we shall construct $\langle F_i : i \in \omega\rangle$ such that $\bigcup_{i\in\omega} F_i$ is infinite and $\bigcup_{i\in\omega} F_i = split\left(\bigcap_{i\in\omega} T^i\right)$.

Let $T^{-1} := T'$, $m_{-1} := 0$, and let $F_{-1} = \{s\}$ for some $s \in split(T')$. Assume that for some $i \in \omega$, we have already constructed a superperfect tree $T^{i-1} \in M$, $m_{i-1} \in \omega$, and $F_{i-1} \in \text{fin}\left(split(T^{i-1})\right)$. Choose a natural number $m_i > m_{i-1}$ such that $m_i \in \bigcap_{s\in F_{i-1}}(\omega \setminus Y_s)$. This can be done since $\mathscr{Y}_1$ has the *sfip*, *i.e.*, $\bigcap_{s\in F_{i-1}}(\omega \setminus Y_s)$ is infinite. Now, with respect to the finite set F_{i-1} define

$$[F_{i-1}] = \{t \in \text{seq}(\omega) : \exists s \in F_{i-1}(t \preccurlyeq s)\}.$$

Then $[F_{i-1}]$ is a *finite* subtree of T^{i-1}. Suppose that $s_0 \in [F_{i-1}]$ is a terminal node of $[F_{i-1}]$, *i.e.*, for all $n \in \omega$, $s_0{}^\frown n \notin [F_{i-1}]$. By construction of Y_{s_0}, for all but finitely many $n \in next_{T^{i-1}}(s_0)$ we have

$$T^{i-1}_{s_0{}^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap (m_i + 1) = Y_{s_0} \cap (m_i + 1).$$

Hence, since $m_i \notin Y_{s_0}$, for all but finitely many $n \in next_{T^{i-1}}(s_0)$ we have

$$T^{i-1}_{s_0^\frown n} \Vdash_{\mathbb{M}} m_i \notin \underset{\sim}{Y} .$$

Now, we prune T^{i-1} by deleting the finitely many subtrees $T^{i-1}_{s_0^\frown n}$ with

$$T^{i-1}_{s_0^\frown n} \not\Vdash_{\mathbb{M}} m_i \notin \underset{\sim}{Y} .$$

Furthermore, we do exactly the same for all other terminal nodes of the finite tree $[F_{i-1}]$. Then, we do the same for all interior nodes of $[F_{i-1}]$, except that we retain all subtrees $T^{i-1}_{s^\frown n}$ with $s^\frown n \in [F_{i-1}]$.
The resulting tree T^i is superperfect and has the property that

$$T^i \Vdash_{\mathbb{M}} m_i \notin \underset{\sim}{Y} .$$

Notice that by construction, if $s \in [F_{i-1}]$ is an interior node of $[F_{i-1}]$ and $s^\frown n \in [F_{i-1}]$ (for some $n \in \omega$), then $s^\frown n \in T^i$. Now, choose a finite set F_i such that $F_{i-1} \subseteq F_i \in \text{fin}\big(split(T^i)\big)$ which has the following property: For each $s \in F_{i-1}$, for which there is an $n_s \in \omega$ such that $s^\frown n_s \in T^i \setminus [F_{i-1}]$, there exists a $t \in F_i \setminus F_{i-1}$ such that $s^\frown n_s \preccurlyeq t$. We leave it as an exercise to the reader to verify that the resulting tree $\bigcap_{i \in \omega} T^i$ is superperfect. $\dashv_{\text{Claim 3}}$

Now, let $X := \{m_i : i \in \omega\}$ and $S' := \bigcap_{i \in \omega} T^i$. Then, in the case when $\mathscr{Y}_1$ has the *sfip*, we have

$$S' \Vdash_{\mathbb{M}} X \cap \underset{\sim}{Y} = \emptyset ,$$

and otherwise we have

$$S' \Vdash_{\mathbb{M}} X \subseteq \underset{\sim}{Y} .$$

In other words, whenever G is $\mathbb{M}$-generic over $\mathbf{V}$, then $\underset{\sim}{Y}[G]$ is not a splitting real over $\mathbf{V}$, and since $\underset{\sim}{Y}$ was an $\mathbb{M}$-name for an arbitrary subset of ω, this shows that Miller forcing does not add splitting reals. $\dashv$

As an immediate consequence we get

FACT 23.4. *Miller forcing does not add dominating reals.*

Proof. By FACT 20.1 we know that every forcing notion which adds dominating reals also adds splitting reals. Thus, since Miller forcing does not add splitting reals, it also does not add dominating reals. $\dashv$

Miller Forcing Preserves *P*-Points

By a similar construction as in the proof of LEMMA 23.3 we can show that every P-point in the ground model generates an ultrafilter in the $\mathbb{M}$-generic extension.

LEMMA 23.5. *Miller forcing preserves P-points.*

Proof. Suppose that $\mathscr{U} \subseteq [\omega]^\omega$ is a P-point in the ground model $\mathbf{V}$ and that G is $\mathbb{M}$-generic over $\mathbf{V}$. We have to show that $\mathscr{U}$ generates an ultrafilter in $\mathbf{V}[G]$, *i.e.*, for every $Y \subseteq \omega$ in $\mathbf{V}[G]$ there exists an $X \in \mathscr{U}$ in $\mathbf{V}$ such that either $X \subseteq Y$ or $X \cap Y = \emptyset$. For this, let $\underset{\sim}{Y}$ be an $\mathbb{M}$-name for an arbitrary but fixed subset of ω in $\mathbf{V}[G]$ (*i.e.*, there is an $\mathbb{M}$-condition $S \in M$ such that $S \Vdash_{\mathbb{M}} \underset{\sim}{Y} \subseteq \omega$). We shall construct an $\mathbb{M}$-condition $S' \subseteq S$ and an $X \in \mathscr{U}$ in $\mathbf{V}$ such that either $S' \Vdash_{\mathbb{M}} X \subseteq \underset{\sim}{Y}$ or $S' \Vdash_{\mathbb{M}} X \cap \underset{\sim}{Y} = \emptyset$. Since $\underset{\sim}{Y}[G]$ is arbitrary, this would imply that the filter in $\mathbf{V}[G]$, generated by $\mathscr{U}$, is an ultrafilter.

As in the proof of LEMMA 23.3, we first construct an $\mathbb{M}$-condition $T \subseteq S$ and a sequence $\big\langle Y_s : s \in \mathit{split}(T)\big\rangle$ of subsets of ω, such that for every $s \in \mathit{split}(T)$, for each $k \in \omega$, and for all but finitely many $n \in \mathit{next}_T(s)$, we have

$$T_{s^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = Y_s \cap k\,.$$

Now, we construct a superperfect tree $T' \subseteq T$ such that either $\big\{Y_s : s \in \mathit{split}(T')\big\} \subseteq \mathscr{U}$ or $\big\{\omega \setminus Y_s : s \in \mathit{split}(T')\big\} \subseteq \mathscr{U}$. Since $\mathscr{U}$ is a P-point, there exists an $X' \in \mathscr{U}$ such that for all $s \in \mathit{split}(T')$, either $X' \subseteq^* Y_s$ or $X' \subseteq^* (\omega \setminus Y_s)$.

Below we just consider the case when $X' \subseteq^* Y_s$ and leave the other case as an exercise to the reader.

In the next step we build a sequence $s_n \in \mathit{split}(T')$, such that both sets, $\{s_{2n} : n \in \omega\}$ and $\{s_{2n+1} : n \in \omega\}$, will be the splitting nodes of some $\mathbb{M}$-condition. At the same time we build a strictly increasing sequence of natural numbers $\langle k_n : n \in \omega\rangle$, such that for all $n \in \omega$, $X' \setminus k_n \subseteq Y_{s_n}$.

The construction is by induction on n: Firstly, let $s_0 \in \mathit{split}_0(T')$, let $s_1 = s_0$, and let $k_0 = 0$. If necessary, modify X' such that $X' \subseteq Y_{s_0} = Y_{s_1}$. Assume that for some $n \in \omega$, we have already constructed s_{2n}, s_{2n+1}, k_{2n}, and k_{2n+1}. Let $i, j \in \omega$ be such that

$$n + 1 = \frac{(i+j)(i+j+1)}{2} + i\,.$$

Notice that i and j are unique and that $n + 1 > i$. Now, we choose a new splitting node $s_{2n+2} \in \mathit{split}(T')$, *i.e.*, $s_{2n+2} \notin \{s_l : l \leq 2n+1\}$, such that $s_{2i}{}^\frown m_0 \preccurlyeq s_{2n+2}$ for some $m_0 \in \mathit{next}_{T'}(s_{2i})$ with $m_0 > k_{2n+1}$, and

$$Y_{s_{2n+2}} \cap k_{2n+1} = Y_{s_{2i}} \cap k_{2n+1}\,.$$

In order to see that such a splitting node s_{2n+2} exists, notice that $2n+2 > 2i$ and that for all but finitely many $m \in \mathit{next}_{T'}(s_{2i})$,

$$T'_{s_{2i}{}^\frown m} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k_{2n+1} = Y_{s_{2i}} \cap k_{2n+1}\,.$$

Hence, there exists an $m_0 \in \mathit{next}_{T'}(s_{2i})$ with $m_0 > k_{2n+1}$, such that for all $s_{2n+2} \succcurlyeq s_{2i}{}^\frown m_0$ we have $Y_{s_{2n+2}} \cap k_{2n+1} = Y_{s_{2i}} \cap k_{2n+1}$. Finally, we choose $k_{2n+2} > k_{2n+1}$ large enough such that

$$X' \setminus k_{2n+2} \subseteq Y_{s_{2n+2}}\,.$$

The splitting node $s_{2n+3} \in split(T')$ (with $s_{2i+1}{}^\frown m_0 \preccurlyeq s_{2n+3}$) and the integer $k_{2n+3} > k_{2n+2}$ are chosen similarly.

Notice that by construction, for each node $s \in \{s_{2n} : n \in \omega\}$ there are infinitely many nodes $t \in \{s_{2n} : n \in \omega\}$ such that $s \preccurlyeq t$, and the same holds for the set $\{s_{2n+1} : n \in \omega\}$. Thus, $\{s_{2n} : n \in \omega\}$ and also $\{s_{2n+1} : n \in \omega\}$ are the splitting nodes of superperfect subtrees of T'. Let $S_0, S_1 \subseteq T'$ be such that $split(S_0) = \{s_{2n} : n \in \omega\}$ and $split(S_1) = \{s_{2n+1} : n \in \omega\}$ respectively. Further, let

$$X_0 = X' \cap \bigcup \{[k_{2n}, k_{2n+1}) : n \in \omega\}$$

and

$$X_1 = X' \cap \bigcup \{[k_{2n+1}, k_{2n+2}) : n \in \omega\}$$

where $[k, k') = \{m \in \omega : k \leq m < k'\}$. Without loss of generality we may assume that $X_0 \in \mathscr{U}$. The goal is to show that $S_0 \Vdash_{\mathbb{M}} X_0 \subseteq \underset{\sim}{Y}$, which is done in the following two claims:

Claim 1. *For every $s \in split(S_0)$, $X_0 \subseteq Y_s$.*

Proof of Claim 1. Firstly, notice that for every $s \in split(S_0)$ there is an $n \in \omega$ such that $s = s_{2n}$. We prove that $X_0 \subseteq Y_{s_{2n}}$ by induction on n: By the choice of X' we have $X' \subseteq Y_{s_0}$; hence, $X_0 \subseteq Y_{s_0}$. If $n > 0$, then by the choice of k_{2n} we have

$$X_0 \setminus k_{2n} \subseteq Y_{s_{2n}} \,,$$

and by the definition of X_0 we have

$$X_0 \cap k_{2n} = X_0 \cap k_{2n-1} \,.$$

Therefore, we find an $i < n$ such that

$$Y_{s_{2n}} \cap k_{2n-1} = Y_{s_{2i}} \cap k_{2n-1} \,.$$

Now, by induction we have $X_0 \subseteq Y_{s_{2i}}$, thus, $(X_0 \cap k_{2n-1}) \subseteq Y_{s_{2i}} \cap k_{2n-1}$. Since $(X_0 \cap k_{2n}) = (X_0 \cap k_{2n-1})$ and $(X_0 \setminus k_{2n}) \subseteq Y_{s_{2n}}$, we finally get

$$X_0 = (X_0 \cap k_{2n}) \cup (X_0 \setminus k_{2n}) \subseteq (Y_{s_{2n}} \cap k_{2n-1}) \cup Y_{s_{2n}} = Y_{s_{2n}} \,.$$

$\dashv_{\text{Claim 1}}$

Claim 2. $S_0 \Vdash_{\mathbb{M}} X_0 \subseteq \underset{\sim}{Y}$.

Proof of Claim 2. Assume towards a contradiction that there is an $\mathbb{M}$-condition $\tilde{S} \subseteq S_0$ and an $m \in X_0$ such that

$$\tilde{S} \Vdash_{\mathbb{M}} m \notin \underset{\sim}{Y} \,.$$

Let $s \in split_0(\tilde{S})$. By construction of T, and since $\tilde{S} \subseteq T$, for each $k \in \omega$ and for all but finitely many $n \in next_{\tilde{S}}(s)$ we have $\tilde{S}_{s^\frown n} \Vdash_{\mathbb{M}} \underset{\sim}{Y} \cap k = Y_s \cap k$. In particular, for $k = m + 1$ and for some $n_0 \in next_{\tilde{S}}(s)$ we have

$$\tilde{S}_{s^\frown n_0} \Vdash_{\mathbb{M}} m \in \underset{\sim}{Y} \leftrightarrow m \in Y_s .$$

Since $X_0 \subseteq Y_s$ and $m \in X_0$, this implies

$$\tilde{S}_{s^\frown n_0} \Vdash_{\mathbb{M}} m \in \underset{\sim}{Y} ,$$

which contradicts our assumption that $\tilde{S} \Vdash_{\mathbb{M}} m \notin \underset{\sim}{Y}$. $\dashv_{\text{Claim 2}}$

Thus, in the case when for all $s \in \mathit{split}(T')$, $X' \subseteq^* Y_s$, there is an $X \in \mathscr{U}$ (where X is either X_0 or X_1) and an $\mathbb{M}$-condition $S' \subseteq T'$ (where S' is either S_0 or S_1) such that $S' \Vdash_{\mathbb{M}} X \subseteq \underset{\sim}{Y}$. In the other case (which was left to the reader), in which for all $s \in \mathit{split}(T')$, $X' \subseteq^* (\omega \setminus Y_s)$, there is an $X \in \mathscr{U}$ and an $S' \subseteq T'$ such that $S' \Vdash_{\mathbb{M}} X \cap \underset{\sim}{Y} = \emptyset$. So, in both cases, $\mathscr{U}$ generates an ultrafilter in the $\mathbb{M}$-generic extension, which is what we had to show. $\dashv$

A Model in which $\mathfrak{r} < \mathfrak{d}$

Below we show that after adding ω_2 Miller reals to a model $\mathbf{V}$ of $\mathsf{ZFC}+\mathsf{CH}$, we get a model $\mathbf{V}[G]$ in which $\mathfrak{r} = \omega_1$ and $\mathfrak{d} = \omega_2$. The reason why $\mathbf{V}[G] \vDash \mathfrak{d} = \omega_2$ is that Miller forcing adds unbounded reals, and the reason why $\mathbf{V}[G] \vDash \mathfrak{r} = \omega_1$ is in fact a consequence of the following

FACT 23.6. *If there exists an ultrafilter $\mathscr{U}$ which is generated by some filter $\mathscr{F} \subseteq [\omega]^\omega$ of cardinality κ, then $\mathfrak{r} \leq \kappa$.*

Proof. Firstly notice that for all $x \in [\omega]^\omega$, either $x \in \mathscr{U}$ or $(\omega \setminus x) \in \mathscr{U}$. Secondly, since $\mathscr{F}$ generates $\mathscr{U}$, for all $x' \in \mathscr{U}$ there is a $y \in \mathscr{F}$ such that $y \subseteq x'$. This shows that $\mathscr{F}$ is a reaping family. $\dashv$

PROPOSITION 23.7. *$\omega_1 = \mathfrak{r} < \mathfrak{d} = \mathfrak{c}$ is consistent with* ZFC.

Proof. Let $\mathbb{P}_{\omega_2}$ be a countable support iteration of Miller forcing, let $\mathbf{V}$ be a model of $\mathsf{ZFC}+\mathsf{CH}$, and let G be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$.

Since Miller forcing is of size $\mathfrak{c}$, by THEOREM 20.5.(a) we get $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$, and since Miller forcing adds unbounded reals, by THEOREM 20.5.(b) we get that no family $\mathscr{F} \subseteq [\omega]^\omega$ of size ω_1 can be a dominating family. Hence, we get $\mathbf{V}[G] \vDash \mathfrak{d} = \omega_2$.

Now we show that $\mathbf{V}[G] \vDash \mathfrak{r} = \omega_1$: Firstly, notice that CH implies that every ultrafilter is of cardinality ω_1, and recall that CH implies the existence of P-points. Thus, since $\mathbf{V} \vDash \mathsf{CH}$, there are P-points in $\mathbf{V}$ of cardinality ω_1. Since Miller forcing is proper and the iteration is a countable support iteration, by THEOREM 20.8 we get that every P-point $\mathscr{F}$ (of cardinality ω_1) in the ground model $\mathbf{V}$ generates an ultrafilter $\mathscr{U} \subseteq [\omega]^\omega$ in $\mathbf{V}[G]$. Thus, by FACT 23.6, we have $\mathbf{V}[G] \vDash \mathfrak{r} = \omega_1$. $\dashv$

Notes

All non-trivial results presented in this chapter are essentially due to Miller and can be found in [14]. In that paper, he introduced what is now called *Miller forcing*, but which he called *rational perfect set forcing*. Miller thought about this forcing notion when he worked on his paper [13], where he used a fusion argument which involved preserving a dynamically chosen countable set of points (see [13, Lemmata 8 & 9]). This led him to perfect sets in which the rationals in them are dense, and shortly after, he realised that this is equivalent to forcing with superperfect trees. Even though superperfect trees appeared first in papers of Kechris [10] and Louveau [12], Miller was the first who investigated the corresponding forcing notion.

Related Results

124. *Characterising Miller reals.* By the proof of LEMMA 23.2 we know that every Miller real g is unbounded. On the other hand, one can show that every function $f \in {}^{\omega}\omega$ in the $\mathbb{M}$-generic extension $\mathbf{V}[g]$ which is unbounded (*i.e.*, not dominated by any function in $\mathbf{V}$) is a Miller real (see Miller [14, Proposition 2]). Furthermore, one can show that Miller forcing is minimal (see Miller [14, p. 147]).

125. *Miller forcing has the Laver property.* One can show that Miller forcing has the Laver property (see Bartoszyński and Judah [1, Theorem 7.3.45]) and therefore does not add Cohen reals. Since the Laver property is preserved under countable support iterations, there are no Cohen reals in the model constructed in the proof of PROPOSITION 23.7.

126. *Miller forcing does not add Cohen, dominating, or random reals.* Since every forcing notion which preserves P-points does not add Cohen, dominating, or random reals (see Chapter 20 | RELATED RESULT 107), Miller forcing adds neither Cohen, nor dominating, nor random reals.

127. $\mathbb{M} \times \mathbb{M}$ *adds splitting reals.* Even though Miller forcing does not add splitting reals, a product of Miller forcing $\mathbb{M}\times\mathbb{M}$ always adds splitting reals (see Miller [14, Remark, p. 151] and compare with Chapter 22 | RELATED RESULT 121).

128. *Miller forcing satisfies* Axiom A. Miller forcing is not just proper, it even satisfies the slightly stronger Axiom A (see Bartoszyński and Judah [1, p. 360]).

129. *Miller forcing preserves* $\mathsf{MA}(\sigma\text{-centred})$. If $\mathbf{V} \vDash \mathsf{MA}(\sigma\text{-centred})$ and g is a Miller real over $\mathbf{V}$, then $\mathbf{V}[g] \vDash \mathsf{MA}(\sigma\text{-centred})$ (see Brendle [5]). Recall that by Chapter 13 | RELATED RESULT 79, $\mathsf{MA}(\sigma\text{-centred}) \iff \mathfrak{p} = \mathfrak{c}$, and compare this result with THEOREM 19.4, which says that Cohen forcing preserves $\mathfrak{p} = \mathfrak{c}$.

130. *Cardinal characteristics in Miller's model.* In Miller's model, which is the model constructed in the proof of PROPOSITION 23.7, we also have $\omega_1 = \mathfrak{a} = \mathfrak{s}$ (see for example Blass [2, Section 11.9]). Furthermore, the proof of PROPOSITION 23.7 shows that in Miller's model we even have $\mathfrak{u} < \mathfrak{d}$ (see also Blass and Shelah [3]).

Another forcing notion with superperfect trees as conditions, which was introduced by Laver in [11], is the so-called **Laver forcing**, denoted $\mathbb{L}$: $\mathbb{L}$-conditions are ordered pairs (s, T), where $T \subseteq \operatorname{seq}(\omega)$ is a superperfect tree, $s \in T$, and for all $t \in T$ we have either $t \preccurlyeq s$ or $s \preccurlyeq t \wedge t \in \mathit{split}(T)$ (*i.e.*, $T_s = T$ and every node $t \succcurlyeq s$ is a splitting node of T). For $\mathbb{L}$-conditions (s, T) and (s', T') let $(s, T) \leq (s', T') \iff s \preccurlyeq s' \wedge T' \subseteq T$. Furthermore, for ultrafilters $\mathscr{U} \subseteq [\omega]^\omega$ we define **restricted Laver forcing**, denoted $\mathbb{L}_{\mathscr{U}}$, as follows: A pair (s, T) is an $\mathbb{L}_{\mathscr{U}}$-condition if it is an $\mathbb{L}$-condition which has the property that for all $t \in \mathit{split}(T)$ we have $\mathit{next}_T(t) \in \mathscr{U}$.

131. *Laver forcing and Borel's conjecture.* A set $X \subseteq \mathbb{R}$ has *strong measure zero* if for every sequence of positive reals $\{\varepsilon_n : n \in \omega\}$ there exists a sequence of intervals $\{I_n : n \in \omega\}$, such that for all $n \in \omega$, $\mu(I_n) \leq \varepsilon_n$, and $X \subseteq \bigcup_{n\in\omega} I_n$. Furthermore, **Borel's conjecture** is the statement that there are no uncountable strong measure zero sets (see Borel [4]). Now, Goldstern, Judah, and Shelah [6] showed that $\mathfrak{b} = \omega_1$ implies that Borel's conjecture fails. On the other hand, using Laver forcing, Laver showed in [11] that Borel's conjecture is consistent with $\mathsf{ZFC} + \mathfrak{c} = \omega_2$ (*cf.* Bartoszyński and Judah [1, Section 8.3]).

132. *Combinatorial properties of Laver forcing.* Laver forcing satisfies Axiom A (see Bartoszyński and Judah [1, Lemma 7.3.27]), and therefore, Laver forcing is proper. Since Laver forcing has the Laver property (see Bartoszyński and Judah [1, Theorem 7.3.29]), it does not add Cohen reals. However, Laver forcing adds dominating reals (see Bartoszyński and Judah [1, Lemma 7.3.28]), and therefore, Laver forcing adds splitting reals. Furthermore, one can show that Laver forcing is minimal (see Gray [8]).

133. $\mathbb{L} \times \mathbb{L}$ *adds Cohen reals.* Even though Laver forcing does not add Cohen reals, by a similar argument as in the proof of FACT 24.9, one can show that a product of Laver forcing $\mathbb{L} \times \mathbb{L}$ always adds Cohen reals.

134. *Two Laver reals added iteratively always force* CH. Brendle [5, Theorem 3.4] showed that Laver forcing collapses $\mathfrak{d}$ to ω_1, and Goldstern, Repický, Shelah, and Spinas [7, Theorem 2.7] showed that Laver forcing (as well as Miller forcing) collapses $\mathfrak{c}$ to a cardinal $\leq \mathfrak{h}$. Thus, two Laver reals added iteratively always force CH (*cf.* Chapter 24 | RELATED RESULT 139).

135. *On the consistency of* $\mathfrak{s} < \mathfrak{b}$. An ω_2-stage iteration with countable support of Laver forcing, starting in a model of $\mathsf{ZFC} + \mathsf{CH}$, yields a model in which $\omega_1 = \mathfrak{s} < \mathfrak{b} = \mathfrak{c}$ (see Blass [2, Section 11.7]).

136. *Combinatorial properties of restricted Laver forcing* $\mathbb{L}_{\mathscr{U}}$. If $\mathscr{U} \subseteq [\omega]^\omega$ is an ultrafilter, then restricted Laver forcing $\mathbb{L}_{\mathscr{U}}$ obviously satisfies *ccc*. It is not hard to show that restricted Laver forcing $\mathbb{L}_{\mathscr{U}}$ adds dominating reals and therefore adds splitting reals. Furthermore, since restricted Laver forcing $\mathbb{L}_{\mathscr{U}}$ has pure decision (see Judah and Shelah [9, Theorem 1.7]), by a similar argument as in the proof of COROLLARY 24.8, one can show that $\mathbb{L}_{\mathscr{U}}$ has the Laver property.

137. *Restricted Laver forcing* $\mathbb{L}_{\mathscr{U}}$ *collapses* $\mathfrak{d}$ *to* ω_1. Brendle [5, Corollary 3.10.(a)] showed that restricted Laver forcing $\mathbb{L}_{\mathscr{U}}$ collapses $\mathfrak{d}$ to ω_1 (*cf.* RELATED RESULT 134).

138. *On the consistency of* $\mathfrak{hom} < \mathfrak{c}$. Judah and Shelah showed in [9, Theorem 1.16] that if a real $r \in [\omega]^\omega$ is $\mathbb{L}_{\mathscr{U}}$-generic over $\mathbf{V}$, then for each colouring $\pi : [\omega]^2 \to 2$ in the ground model there exists an $n \in \omega$ such that $\pi|_{[r\setminus n]^2}$ is constant. Now,

let $\mathbb{P}_{\omega_1} = \langle \mathbb{Q}_\alpha : \alpha \in \omega_1 \rangle$ be an ω_1-stage iteration with finite support, where for each $\alpha \in \omega_1$, $\mathbb{Q}_\alpha$ is restricted Laver forcing $\mathbb{L}_{\mathscr{U}}$ (for some ultrafilter $\mathscr{U} \subseteq [\omega]^\omega$). Further, let $\mathbf{V}$ be a model of ZFC in which $\mathfrak{c} > \omega_1$ and let G be $\mathbb{P}_{\omega_1}$-generic over $\mathbf{V}$. Then $\mathbf{V}[G]$ is a model in which $\omega_1 = \mathfrak{hom} < \mathfrak{c}$.

References

1. Tomek Bartoszyński and Haim Judah, ***Set Theory: on the structure of the real line***, A.K. Peters, Wellesley, 1995.
2. Andreas Blass, *Combinatorial Cardinal Characteristics of the Continuum*, in ***Handbook of Set Theory,*** *Volume 1* (Matthew Foreman and Akihiro Kanamori, eds.), Springer-Verlag, Berlin, 2010, pp. 395–490.
3. Andreas Blass and Saharon Shelah, *Near coherence of filters III: A simplified consistency proof*, ***Notre Dame Journal of Formal Logic***, vol. 30 (1989), 530–538.
4. Émile Borel, *Sur la classification des ensembles de mesure nulle*, ***Bulletin de la Société Mathématique de France***, vol. 47 (1919), 97–125.
5. Jörg Brendle, *Combinatorial properties of classical forcing notions*, ***Annals of Pure and Applied Logic***, vol. 73 (1995), 143–170.
6. Martin Goldstern, Haim Judah, and Saharon Shelah, *Strong measure zero sets without Cohen reals*, ***The Journal of Symbolic Logic***, vol. 58 (1993), 1323–1341.
7. Martin Goldstern, Miroslav Repický, Saharon Shelah, and Otmar Spinas, *On tree ideals*, ***Proceedings of the American Mathematical Society***, vol. 123 (1995), 1573–1581.
8. Charles W. Gray, *Iterated Forcing from the Strategic Point of View*, Ph.D. thesis (1990), University of California, Berkeley (USA).
9. Haim Judah and Saharon Shelah, *Δ^1_2-sets of reals*, ***Annals of Pure and Applied Logic***, vol. 42 (1989), 207–223.
10. Alexander S. Kechris, *On a notion of smallness for subsets of the Baire space*, ***Transactions of the American Mathematical Society***, vol. 229 (1977), 191–207.
11. Richard Laver, *On the consistency of Borel's conjecture*, ***Acta Mathematica***, vol. 137 (1976), 151–169.
12. Alain Louveau, *Une propriété de petitesse des filtres sur ω*, in ***Colloque International de Logique*** *(Clermont-Ferrand, 1975)*, [Colloque International du CNRS 249], CNRS, Paris, 1977, pp. 147–155.
13. Arnold W. Miller, *Covering 2^ω with ω_1 disjoint closed sets*, in ***The Kleene Symposium*** *(Proc. Sympos., Univ. Wisconsin, Madison, Wis., 1978)*, [Studies in Logic and the Foundation of Mathematics 101], North-Holland, Amsterdam, 1980, pp. 415–421.
14. ———, *Rational perfect set forcing*, in ***Axiomatic Set Theory*** (James E. Baumgartner, Donald A. Martin, and Saharon Shelah, eds.), Contemporary Mathematics, vol. 31, American Mathematical Society, Providence, RI, 1984, pp. 143–159.

24

Mathias Forcing

In this chapter we investigate a forcing notion which is closely related to RAMSEY'S THEOREM 2.1 and to Ramsey ultrafilters (defined in Chapter 10). So, it is not surprising that also Ramsey families (also defined in Chapter 10) are involved.

With respect to an arbitrary but fixed Ramsey family $\mathscr{E}$ we define **Mathias forcing** $\mathbb{M}_{\mathscr{E}} = (M_{\mathscr{E}}, \leq)$ as follows:

$$M_{\mathscr{E}} = \big\{(s, x) : s \in \operatorname{fin}(\omega) \wedge x \in \mathscr{E} \wedge \max(s) < \min(x)\big\}$$

$$(s, x) \leq (t, y) \iff s \subseteq t \wedge y \subseteq x \wedge t \setminus s \subseteq x$$

If $\mathscr{E} = [\omega]^\omega$, then we write just $\mathbb{M}$ instead of $\mathbb{M}_{\mathscr{E}}$. The finite set s of a Mathias condition (s, x) is called the **stem** of the condition. Each $\mathbb{M}_{\mathscr{E}}$-generic filter G corresponds to a generic real $m \in [\omega]^\omega$, called **Mathias real**, which is in fact just the union of the stems of the conditions which belong to the generic filter G, *i.e.*, $m = \bigcup \big\{s \in \operatorname{fin}(\omega) : \exists x \in \mathscr{E}\big((s, x) \in G\big)\big\}$.

Properties of Mathias Forcing

Mathias Forcing adds Dominating Reals

LEMMA 24.1. *Mathias forcing* $\mathbb{M}_{\mathscr{E}}$ *adds dominating reals.*

Proof. We show that a Mathias real is always dominating: Let m be $\mathbb{M}_{\mathscr{E}}$-generic over the ground model $\mathbf{V}$, let $p = (s, x)$ be an arbitrary $\mathbb{M}_{\mathscr{E}}$-condition, and let $g \in {}^\omega\omega \cap \mathbf{V}$ be an arbitrary function in $\mathbf{V}$. It is enough to show that there exists an $\mathbb{M}_{\mathscr{E}}$-condition $q \geq p$ such that $q \Vdash_{\mathbb{M}_{\mathscr{E}}}$ "$\underset{\sim}{m}$ *dominates* g". In order to construct the condition q we run the game $\mathcal{G}_{\mathscr{E}}$ where the MAIDEN plays according to the following strategy: The MAIDEN's first move is

$$x_0 = x \setminus \big(g(n_0)^+\big)\,,$$

where $n_0 = |s|$, and for $i \in \omega$ she plays

$$x_{i+1} = x_i \setminus \max\left\{g(n_0+i)^+, a_i^+\right\},$$

where a_i is the i^{th} move of DEATH. Since $\mathscr{E}$ is a Ramsey family, this strategy is not a winning strategy for the MAIDEN and DEATH can play such that $y := \{a_i : i \in \omega\} \in \mathscr{E}$. Now, by construction we get that $(s,y) \geq p$ and

$$(s,y) \Vdash_{\mathbb{M}_{\mathscr{E}}} \forall k \geq n_0 \left(\underset{\sim}{m}(k) > g(k)\right),$$

which shows that m is a dominating real over $\mathbf{V}$. ⊣

Together with Fact 20.1 we get

COROLLARY 24.2. *Mathias forcing $\mathbb{M}_{\mathscr{E}}$ adds splitting reals.*

Mathias Forcing is Proper and has the Laver Property

Properness of Mathias forcing and that it has the Laver property follow quite easily from the fact that for every condition (s,x) and every sentence φ of the forcing language there is a (s,y) which *decides* φ. This property of Mathias forcing is known as *pure decision* and is one of the main features of Mathias forcing.

THEOREM 24.3. *Let (s,x) be an $\mathbb{M}_{\mathscr{E}}$-condition and let φ be a sentence of the forcing language. Then there is an $(s,y) \geq (s,x)$ — with the same stem as (s,x) — such that either $(s,y) \Vdash_{\mathbb{M}_{\mathscr{E}}} \varphi$ or $(s,y) \Vdash_{\mathbb{M}_{\mathscr{E}}} \neg\varphi$ (i.e., (s,y) decides the sentence φ).*

Before we can prove the theorem, we have to introduce some terminology and prove some auxiliary results: For every $\mathbb{M}_{\mathscr{E}}$-condition $(s,x) \in M_{\mathscr{E}}$ let

$$[s,x]^\omega = \left\{z \in [\omega]^\omega : s \subseteq z \subseteq s \cup x\right\}.$$

Notice that the sets $[s,x]^\omega$ agree with the sets of the base for the Ellentuck topology which was introduced in Chapter 9.

For a (fixed) open set $\mathcal{O} \subseteq M_{\mathscr{E}}$ let $\bar{\mathcal{O}} := \bigcup\left\{[s,x]^\omega : (s,x) \in \mathcal{O}\right\}$. An $\mathbb{M}_{\mathscr{E}}$-condition (s,x) is called **good** (with respect to $\mathcal{O}$), if there is a condition $(s,y) \geq (s,x)$ such that $[s,y]^\omega \subseteq \bar{\mathcal{O}}$; otherwise it is called **bad**. Furthermore, the condition (s,x) is called **ugly** if $\left(s \cup \{a\}, x \setminus a^+\right)$ is bad for all $a \in x$. Notice that if (s,x) is ugly, then (s,x) is bad, too. Finally, (s,x) is called **completely ugly** if $\left(s \cup \{a_0,\dots,a_n\}, x \setminus a_n^+\right)$ is bad for all $\{a_0,\dots,a_n\} \subseteq x$ with $a_0 < \dots < a_n$.

LEMMA 24.4. *If an $\mathbb{M}_{\mathscr{E}}$-condition (s,x) is bad, then there is a condition $(s,y) \geq (s,x)$ which is ugly.*

Proof. We run the game $\mathcal{G}_{\mathscr{E}}$ where the MAIDEN plays according to the following strategy: She starts the game by playing $x_0 := x$, and then, for $i \in \omega$, she plays $x_{i+1} \subseteq (x_i \setminus a_i^+)$ such that $[s \cup \{a_i\}, x_{i+1}]^\omega \subseteq \bar{\mathcal{O}}$ if possible, and $x_{i+1} = (x_i \setminus a_i^+)$ otherwise. Strictly speaking we assume that $\mathscr{E}$ is well-ordered and that x_{i+1} is the first element of $\mathscr{E}$ with the required properties. However, since this strategy is not a winning strategy for the MAIDEN, DEATH can play so that $z := \{a_i : i \in \omega\} \in \mathscr{E}$. Now, let $y = \{a_i \in z : [s \cup \{a_i\}, x_{i+1}]^\omega \subseteq \bar{\mathcal{O}}\}$. Because $\mathscr{E}$ is a free family, by LEMMA 10.2 we get that y or $z \setminus y$ belongs to $\mathscr{E}$. If $y \in \mathscr{E}$, then $[s, y]^\omega \subseteq \bar{\mathcal{O}}$ which would imply that (s, x) is good, but this contradicts the premise of the lemma. Hence, $z \setminus y \in \mathscr{E}$, which implies that $(s, z \setminus y)$ is ugly. ⊣

LEMMA 24.5. *If an $\mathbb{M}_{\mathscr{E}}$-condition (s, x) is ugly, then there is a condition $(s, y) \geq (s, x)$ such that (s, y) is completely ugly.*

Proof. This follows by an iterative application of LEMMA 24.4. In fact, for every $i \in \omega$, the MAIDEN can play a set $x_i \in \mathscr{E}$ such that for each $t \subseteq \{a_0, \ldots, a_{i-1}\}$, either the condition $(s \cup t, x_i)$ is ugly or $[s \cup t, x_i]^\omega \subseteq \bar{\mathcal{O}}$. Now DEATH can play such that $y := \{a_i : i \in \omega\} \in \mathscr{E}$. Assume that there exists a finite set $t \subseteq y$ such that $(s \cup t, y \setminus \max(t)^+)$ is good. Notice that since (s, x) was assumed to be ugly, $t \neq \emptyset$. Now let t_0 be a smallest finite subset of y such that $q_0 = (s \cup t_0, y \setminus \max(t_0)^+)$ is good and let $t_0^- = t_0 \setminus \{\max(t_0)\}$. Then by definition of t_0, the condition $q_0^- = \big(s \cup t_0^-, y \setminus \max(t_0)\big)$ is not good, and hence, by the strategy of the MAIDEN, it must be ugly, but if q_0^- is ugly, then q_0 is bad, which is a contradiction to our assumption. Thus, there is no finite set $t \subseteq y$ such that $(s \cup t, y \setminus \max(t)^+)$ is good, which implies that all these conditions are ugly, and therefore (s, y) is completely ugly. ⊣

Now we are ready to prove that Mathias forcing $\mathbb{M}_{\mathscr{E}}$ has pure decision:

Proof of Theorem 24.3. Let (s, x) be an $\mathbb{M}_{\mathscr{E}}$-condition and let φ be a sentence of the forcing language. With respect to φ we define $\mathcal{O}_1 := \{q \in M_{\mathscr{E}} : q \Vdash_{\mathbb{M}_{\mathscr{E}}} \varphi\}$ and $\mathcal{O}_2 := \{q \in M_{\mathscr{E}} : q \Vdash_{\mathbb{M}_{\mathscr{E}}} \neg\varphi\}$. Clearly $\mathcal{O}_1$ and $\mathcal{O}_2$ are both open and $\mathcal{O}_1 \cup \mathcal{O}_2$ is even dense in $M_{\mathscr{E}}$. By LEMMA 24.5 we know that for any (s, x) there exists $(s, y) \geq (s, x)$ such that either $[s, y]^\omega \subseteq \bar{\mathcal{O}}_1$ or $[s, y]^\omega \cap \bar{\mathcal{O}}_1 = \emptyset$. In the former case we have $(s, y) \Vdash_{\mathbb{M}_{\mathscr{E}}} \varphi$ and we are done. In the latter case we find $(s, y') \geq (s, y)$ such that $[s, y']^\omega \subseteq \bar{\mathcal{O}}_2$. (Otherwise we would have $[s, y]^\omega \cap (\bar{\mathcal{O}}_1 \cup \bar{\mathcal{O}}_2) = \emptyset$, which is impossible by the density of $\mathcal{O}_1 \cup \mathcal{O}_2$.) Hence, $(s, y') \Vdash_{\mathbb{M}_{\mathscr{E}}} \neg\varphi$. ⊣

As a consequence of THEOREM 24.3 we can show that *each* infinite subset of a Mathias real is a Mathias real.

COROLLARY 24.6. *If $m \in [\omega]^\omega$ is a Mathias real over $\mathbf{V}$ and m' is an infinite subset of m, then m' is a Mathias real over $\mathbf{V}$ too.*

Proof. Let $D \subseteq M_{\mathscr{E}}$ be an arbitrary open dense subset of $M_{\mathscr{E}}$ which belongs to $\mathbf{V}$ and let D' be the set of all conditions $(s,z) \in M_{\mathscr{E}}$ such that for all $t \subseteq s$, $[t,z]^\omega \subseteq \bar{D}$. Notice that D' belongs to $\mathbf{V}$.

First we show that D' is a dense (and by definition also open) subset of $M_{\mathscr{E}}$: For this take an arbitrary condition $(s,x) \in D$ and let $\{t_i : 0 \leq i \leq h\}$ be an enumeration of all subsets of s. Because D is open dense in $M_{\mathscr{E}}$ we find a condition (t_0, y_0) such that $y_0 \subseteq x$ and $[t_0, y_0]^\omega \in \bar{D}$. Moreover, for each $i < h$ we find a condition (t_{i+1}, y_{i+1}) such that $y_{i+1} \subseteq y_i$ and $[t_{i+1}, y_{i+1}]^\omega \in \bar{D}$. Now, let $y := y_h$. Then $(s,y) \in D'$, which implies that D' is dense in $M_{\mathscr{E}}$.

Let $m \in [\omega]^\omega$ be a Mathias real over $\mathbf{V}$ and let m' be an infinite subset of m. Since D' is an open dense subset of $M_{\mathscr{E}}$ and m is an $\mathbb{M}_{\mathscr{E}}$-generic real, there exists a condition $(s,x) \in D'$ such that $s \subseteq m \subseteq s \cup x$. For $t = m' \cap s$ we get $t \subseteq m' \subseteq t \cup x$, and by definition of D' we have $[t,x]^\omega \subseteq \bar{D}$. Thus, m' meets the open dense set D, and since D was arbitrary, this completes the proof. ⊣

As a consequence we get properness of Mathias forcing:

COROLLARY 24.7. *Mathias forcing $\mathbb{M}_{\mathscr{E}}$ is proper.*

Proof. Let $\mathbf{V}$ be a model of ZFC. Further, let $\mathbf{N} = (N, \in)$ be a countable elementary submodel of $(\mathrm{H}_\chi, \in)$ which contains $\mathbb{M}_{\mathscr{E}}$, and let $(s,x) \in M_{\mathscr{E}} \cap N$. Since N is countable (in $\mathbf{V}$), there exists a Mathias real $m \in [s,x]^\omega \cap \mathbf{V}$ over $\mathbf{N}$. Notice that $(s, m \setminus s) \geq (s,x)$ and that $(s, m \setminus s)$ belongs to $\mathbf{V}$. Now, by COROLLARY 24.6, every $m' \in [s, m \setminus s]^\omega$ is a Mathias real over $\mathbf{N}$, and hence, the $\mathbb{M}_{\mathscr{E}}$-condition $(s, m \setminus s)$ is $\mathbf{N}$-generic. ⊣

In Chapter 21 we have seen that Cohen forcing adds unbounded reals, but not dominating reals. Now we shall show that Mathias forcing $\mathbb{M}_{\mathscr{E}}$, even though it adds dominating reals, it does not add Cohen reals (but see also FACT 24.9):

COROLLARY 24.8. *Mathias forcing $\mathbb{M}_{\mathscr{E}}$ has the Laver property and therefore does not add Cohen reals.*

Proof. Let $f \in {}^\omega\omega \cap \mathbf{V}$ be an arbitrary function which belongs to $\mathbf{V}$ and let $\underset{\sim}{g}$ be an $\mathbb{M}_{\mathscr{E}}$-name for a function in ${}^\omega\omega$ such that $\mathbf{0} \Vdash_{\mathbb{M}_{\mathscr{E}}} \forall n \in \omega\big(\underset{\sim}{g}(n) \leq f(n)\big)$. Further, let $\mathcal{F}$ be the set of all functions $S : \omega \to \mathrm{fin}(\omega)$ such that for every $n \in \omega$, $|S(n)| \leq 2^n$. We have to show that $\mathbf{0} \Vdash_{\mathbb{M}_{\mathscr{E}}} \exists S \in \mathcal{F} \cap \mathbf{V}\ \forall n \in \omega\big(\underset{\sim}{g}(n) \in S(n)\big)$. In other words, we have to show that for every $\mathbb{M}_{\mathscr{E}}$-condition (s,x) there exists an $(s,y) \geq (s,x)$ and an $S \in \mathcal{F} \cap \mathbf{V}$ such that $(s,y) \Vdash_{\mathbb{M}_{\mathscr{E}}} \forall n \in \omega\big(\underset{\sim}{g}(n) \in S(n)\big)$.

By THEOREM 24.3, and since $\underset{\sim}{g}$ is bounded by $f(n)$, for every $\mathbb{M}_{\mathscr{E}}$-condition (t,z) and for every $n \in \omega$ there exists a condition $(t,z') \geq (t,z)$ which decides $\underset{\sim}{g}(n)$, i.e., $(t,z') \Vdash_{\mathbb{M}_{\mathscr{E}}} \underset{\sim}{g}(n) = k$ for some $k \leq f(n)$. Let (s,x) be any $\mathbb{M}_{\mathscr{E}}$-condition. We run the game $\mathcal{G}_{\mathscr{E}}$ where the MAIDEN plays according to the following strategy: She starts the game by playing $x_0 \subseteq x$ such that (s, x_0)

decides $\underset{\sim}{g}(0)$, and we define $S(0) := \big\{k \leq f(0) : (s, x_0) \Vdash_{\mathbb{M}_{\mathscr{E}}} \underset{\sim}{g}(n) = k\big\}$. Notice that $|S(0)| = 1 = 2^0$. In general, for $n \in \omega$, the MAIDEN plays $x_{n+1} \subseteq (x_n \setminus a_n^+)$ such that for every $\bar{a} \subseteq \{a_0, \dots, a_n\}$, $(s \cup \bar{a}, x_{n+1})$ decides $\underset{\sim}{g}(n+1)$, and we define $S(n+1)$ as the set of all $k \leq f(n+1)$ such that, for some $\bar{a} \subseteq \{a_0, \dots, a_n\}$, $(s \cup \bar{a}, x_{n+1}) \Vdash_{\mathbb{M}_{\mathscr{E}}} \underset{\sim}{g}(n+1) = k$. Notice that $|S(n+1)| \leq \big|\mathscr{P}\big(\{a_0, \dots, a_n\}\big)\big| = 2^{n+1}$. Since this strategy is not a winning strategy for the MAIDEN, DEATH can play such that $y := \{a_n : n \in \omega\} \in \mathscr{E}$. Now, by construction, $S \in \mathcal{F} \cap \mathbf{V}$ and for each $n \in \omega$ we have $(s, y) \Vdash_{\mathbb{M}_{\mathscr{E}}} \underset{\sim}{g}(n) \in S(n)$. Thus, the set S and the $\mathbb{M}_{\mathscr{E}}$-condition (s, y) have the required properties, which completes the proof. ⊣

Since Mathias forcing has the Laver property and is proper, a countable support *iteration* of Mathias forcing notions does not add Cohen reals. However, the next result shows that this is not true for a *product* of Mathias forcing (compare with Chapter 23 | RELATED RESULT 127 and with Chapter 22 | RELATED RESULT 121):

FACT 24.9. *The product of any two Mathias forcing notions always adds Cohen reals.*

Proof. Let $G_1 \times G_2$ be $\mathbb{M}_{\mathscr{E}} \times \mathbb{M}_{\mathscr{E}}$-generic over some model $\mathbf{V}$ of ZFC and let m_1 and m_2 be the corresponding Mathias reals (recall that $m_1, m_2 \in [\omega]^\omega$). Further, let $\bar{m}_1, \bar{m}_2 \in {}^\omega\omega$ be the (unique) strictly increasing functions which map ω onto m_1 and m_2 respectively (*i.e.*, for $i \in \{1, 2\}$, $\bar{m}_i$ is strictly increasing and $\bar{m}_i[\omega] = m_i$). We shall show that $c_{m_1,m_2} \in {}^\omega 2$, defined by stipulating

$$c_{m_1,m_2}(k) = \begin{cases} 0 & \text{if } \bar{m}_1(k) \leq \bar{m}_2(k), \\ 1 & \text{otherwise,} \end{cases}$$

is a Cohen real over $\mathbf{V}$.

For $s \in \operatorname{fin}(\omega)$ we define $\bar{s} \in {}^{|s|}\omega$ similarly, *i.e.*, $s = \big\{\bar{s}(k) : k \in |s|\big\}$ and for all $k, l \in |s|$ with $k < l$ we have $\bar{s}(k) < \bar{s}(l)$. Further, for $s, t \in \operatorname{fin}(\omega)$ with $|s| = |t|$ let $\gamma_{s,t} \in {}^{|s|}\omega$ be such that

$$\gamma_{s,t}(k) = \begin{cases} 0 & \text{if } \bar{s}(k) \leq \bar{t}(k), \\ 1 & \text{otherwise.} \end{cases}$$

Now, let

$$E = \big\{\big\langle (s, x), (t, y)\big\rangle \in M_{\mathscr{E}} \times M_{\mathscr{E}} : |s| = |t|\big\}$$

and consider the following function:

$$\begin{array}{rccc} \varGamma : & E & \longrightarrow & \bigcup_{n \in \omega} {}^n 2 \\ & \big\langle (s, x), (t, y)\big\rangle & \longmapsto & \gamma_{s,t} \end{array}$$

Obviously, whenever $D \subseteq \bigcup_{n \in \omega} {}^n 2$ is open dense, then $\varGamma^{-1}[D] = \big\{p \in M_{\mathscr{E}} \times M_{\mathscr{E}} : \varGamma(p) \in E\big\}$ is dense in $M_{\mathscr{E}} \times M_{\mathscr{E}}$, and since $\rangle m_1, m_2\rangle$ is $\mathbb{M}_{\mathscr{E}} \times \mathbb{M}_{\mathscr{E}}$-generic over $\mathbf{V}$, we get that c_{m_1,m_2} is a Cohen real over $\mathbf{V}$. ⊣

A Model in which $\mathfrak{p} < \mathfrak{h}$

Before we construct a model in which $\mathfrak{p} < \mathfrak{h}$, we shall show that $\mathbb{M} \approx \mathbb{U} * \mathbb{M}_{\underset{\cdot}{\mathscr{U}}}$, where $\mathbb{U} = \big([\omega]^\omega/\text{fin}, \leq\big)$ (which was introduced in Chapter 14). To simplify the notation we write $\overset{*}{\omega}$ instead of $[\omega]^\omega/\text{fin}$.

LEMMA 24.10. *$\mathbb{M} \approx \mathbb{U} * \mathbb{M}_{\underset{\cdot}{\mathscr{U}}}$, where $\underset{\cdot}{\mathscr{U}}$ is the canonical $\mathbb{U}$-name for the $\mathbb{U}$-generic ultrafilter.*

Proof. Firstly, recall that every $(\mathbb{U} * \mathbb{M}_{\underset{\cdot}{\mathscr{U}}})$-condition is of the form $\big\langle [z]^{\tilde{}}, \underset{\sim}{(t, y)}\big\rangle$, where

$$[z]^{\tilde{}} \Vdash_{\mathbb{U}} \text{“}\underset{\sim}{(t, y)} \text{ is an } \mathbb{M}_{\underset{\cdot}{\mathscr{U}}}\text{-condition”},$$

in particular, $[z]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{y} \in \underset{\cdot}{\mathscr{U}}$. Furthermore, since $\mathbb{U}$ does not add new reals, for every $\mathbb{U}$-name $\underset{\sim}{(t, y)}$ for an $\mathbb{M}_{\underset{\cdot}{\mathscr{U}}}$-condition, and for every $\mathbb{U}$-condition $[z]^{\tilde{}}$, there is an $\mathbb{M}$-condition (s, x) in the ground model and a $\mathbb{U}$-condition $[z']^{\tilde{}} \geq [z]^{\tilde{}}$ such that

$$[z']^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\cdot}{(s, x)} = \underset{\sim}{(t, y)}\,.$$

With these facts one can show that the function

$$\begin{array}{rccc} h: & M & \longrightarrow & \overset{*}{\omega} \times \underset{\sim}{M_{\mathscr{U}}} \\[1em] & (s, x) & \longmapsto & \big\langle [x]^{\tilde{}}, \underset{\cdot}{(s, x)}\big\rangle \end{array}$$

is a dense embedding — we leave the details as an exercise to the reader. Hence, by FACT 14.3, we get that Mathias forcing $\mathbb{M}$ is equivalent to the two-step iteration $\mathbb{U} * \mathbb{M}_{\underset{\cdot}{\mathscr{U}}}$. ⊣

As a side-result of LEMMA 24.10 we get that whenever $m \in [\omega]^\omega$ is a Mathias real over $\mathbf{V}$, then the set $\mathscr{U} = \{x \subseteq \omega : m \subseteq^* x\}$ is $\mathbb{U}$-generic over $\mathbf{V}$, in particular, $\mathscr{U}$ is a Ramsey ultrafilter in $\mathbf{V}[\mathscr{U}]$. The following fact is just a reformulation of this observation.

FACT 24.11. *If m is a Mathias real over $\mathbf{V}$, then m is almost homogeneous for all colourings $\pi : [\omega]^2 \to 2$ which belong to $\mathbf{V}$.*

PROPOSITION 24.12. *$\mathfrak{p} = cov(\mathcal{M}) < \mathfrak{h}$ is consistent with ZFC.*

Proof. By THEOREM 21.5, and since $\omega_1 \leq \mathfrak{p}$, it is enough to show that $\omega_1 = cov(\mathcal{M}) < \mathfrak{h} = \omega_2$ is consistent with ZFC.

First we show that a ω_2-iteration with countable support of Mathias forcing, starting from a model $\mathbf{V}$ of $\mathsf{ZFC} + \mathsf{CH}$, yields a model in which $\mathfrak{h} = \omega_2$.

Let $\mathbb{P}_{\omega_2} = \langle \underset{\sim}{\mathbb{Q}_\alpha} : \alpha \in \omega_2\rangle$ be a countable support iteration of Mathias forcing, *i.e.*, for all $\alpha \in \omega_2$ we have $\mathbf{0}_\alpha \Vdash_{\mathbb{P}_\alpha}$ “$\underset{\sim}{\mathbb{Q}_\alpha}$ is Mathias forcing”. By LEMMA 24.10 we may assume that for all $\alpha \in \omega_2$ we have

$$\mathbf{0}_\alpha \Vdash_{\mathbb{P}_\alpha} \text{“}\underset{\sim}{\mathbb{Q}_\alpha} \text{ is the two-step iteration } \mathbb{U} * \mathbb{M}_{\underset{\cdot}{\mathscr{U}}}\text{”}\,.$$

Let $\mathbf{V}$ be a model of $\mathsf{ZFC} + \mathsf{CH}$ and let G be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$. Since Mathias forcing is proper, by THEOREM 20.5.(a) we have $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$. In order to show that $\mathbf{V}[G] \vDash \mathfrak{h} = \omega_2$ it is enough to show that in $\mathbf{V}[G]$, the intersection of any family of size ω_1 of open dense subsets of $\overset{*}{\omega}$ is non-empty.

CLAIM 1. *If each family $\{D_\nu : \nu \in \omega_1\}$ of open dense subsets of $\overset{*}{\omega}$ which belongs to $\mathbf{V}[G]$ has non-empty intersection, then $\mathfrak{h} > \omega_1$.*

Proof of Claim 1. The proof is by contraposition. Assume that $\mathscr{H} = \{\mathscr{A}_\nu : \nu \in \omega_1\}$ is a shattering family. For every $\nu \in \omega_1$ let

$$D_\nu = \left\{y \in [\omega]^\omega : \exists z \in \mathscr{A}_\nu\, (y \subseteq^* z)\right\}.$$

Since $\mathscr{H}$ is shattering, for every $x \in [\omega]^\omega$ there is a $\nu_0 \in \omega_1$ such that x has infinite intersection with at least two distinct members of $\mathscr{A}_{\nu_0}$, which implies that $x \notin D_{\nu_0}$ and shows that $\bigcap\{D_\nu : \nu \in \omega_1\} = \emptyset$. $\dashv_{\text{Claim 1}}$

The following claim is a kind of reflection principle (*cf.* THEOREM 15.2).

CLAIM 2. *Let $\{D_\nu : \nu \in \omega_1\}$ be a family of open dense subsets of $\overset{*}{\omega}$ which belongs to $\mathbf{V}[G]$. Then there is an $\alpha \in \omega_2$ such that for every $\nu \in \omega_1$ the set $D_\nu \cap \mathbf{V}[G|_\alpha]$ belongs to $\mathbf{V}[G|_\alpha]$ and is open dense in $\overset{*}{\omega}{}^{\mathbf{V}[G|_\alpha]}$.*

Proof of Claim 2. It is enough to find an ordinal $\alpha \in \omega_2$ such that for every $\nu \in \omega_1$, $D_\nu \cap \mathbf{V}[G|_\alpha]$ belongs to $\mathbf{V}[G|_\alpha]$ and is dense in $\overset{*}{\omega}{}^{\mathbf{V}[G|_\alpha]}$ — that $D_\nu \cap \mathbf{V}[G|_\alpha]$ is open in $\overset{*}{\omega}{}^{\mathbf{V}[G|_\alpha]}$ follows from the fact that $\mathbf{V}[G|_\alpha]$ is transitive.

Since Mathias forcing is proper and $\mathbf{V} \vDash \mathsf{CH}$, by LEMMA 20.4 we get that for each $\gamma \in \omega_2$, $\mathbf{V}[G|_\gamma] \vDash \mathsf{CH}$. For every $\gamma \in \omega_2$ let $\{x^\gamma_\eta : \eta \in \omega_1\}$ be an enumeration of $[\omega]^\omega \cap \mathbf{V}[G|_\gamma]$. Since no new reals are added at limit stages of uncountable cofinality (see LEMMA 18.9), for all $\eta, \nu \in \omega_2$ there is a least ordinal $\gamma^\nu_\eta > \gamma$, $\gamma^\nu_\eta \in \omega_2$, such that there is a set $y^\nu_\eta \in D_\nu \cap \mathbf{V}[G|_{\gamma^\nu_\eta}]$ with $y^\nu_\eta \subseteq^* x^\gamma_\eta$. Let $\beta(\gamma) = \bigcup\left\{\gamma^\nu_\eta : \langle \eta, \nu\rangle \in \omega_1 \times \omega_1\right\}$ and for $\xi \in \omega_1$ let

$$\beta^\xi(0) = \begin{cases} \bigcup_{\xi' \in \xi} \beta^{\xi'}(0) & \text{if } \xi \text{ is a limit ordinal,} \\ \beta\big(\beta^{\xi'}(0)\big) & \text{if } \xi = \xi' + 1. \end{cases}$$

Then $\alpha = \bigcup\left\{\beta^\xi(0) : \xi \in \omega_1\right\}$, which is a limit ordinal below ω_2 of cofinality ω_1, has the required properties. $\dashv_{\text{Claim 2}}$

For every $\nu \in \omega_1$ let $D'_\nu = D_\nu \cap \mathbf{V}[G|_\alpha]$. Further, let $\mathscr{U}_\alpha$ be the $\mathbb{U}$-generic Ramsey filter over $\mathbf{V}[G|_\alpha]$, determined by G. In the model $\mathbf{V}[G|_\alpha][\mathscr{U}_\alpha]$, $\mathscr{U}_\alpha$ meets every D'_ν (*i.e.*, for every $\nu \in \omega_1$, $\mathscr{U}_\alpha \cap D'_\nu \neq \emptyset$). Now, for m_α, the $\mathbb{M}_{\mathscr{U}_\alpha}$-generic Mathias real over $\mathbf{V}[G|_\alpha][\mathscr{U}_\alpha]$ (*i.e.*, the second component of the decomposition of Mathias forcing), we have $m_\alpha \in \bigcap\{D'_\nu : \nu \in \omega_1\}$ which shows that $\bigcap\{D'_\nu : \nu \in \omega_1\}$ is non-empty. Thus, by CLAIM 1 and since $\mathbf{V}[G] \vDash \mathfrak{c} = \omega_2$, $\mathbf{V}[G] \vDash \mathfrak{h} = \omega_2$.

It remains to show that $\mathbf{V}[G] \vDash \omega_1 = \mathit{cov}(\mathcal{M})$. For this, recall that Mathias forcing has the Laver property and therefore, by PROPOSITION 20.2, Mathias forcing does not add Cohen reals. Now, since the Laver property is preserved under countable support iteration of proper forcing notions (see THEOREM 20.7), a countable support iteration of Mathias forcing does not add Cohen reals to the ground model. Hence, by COROLLARY 21.8 (which says that $cov(\mathcal{M})$ is preserved if no Cohen reals are added) we have $\mathbf{V}[G] \vDash \omega_1 = cov(\mathcal{M})$. ⊣

NOTES

Mathias forcing restricted to happy families (which are slightly more general than Ramsey families) was introduced and investigated by Mathias in [11]. However, most of the results presented in this chapter can be found in Halbeisen [5].

RELATED RESULTS

139. *Mathias forcing collapses* $\mathfrak{c}$ *to* $\mathfrak{h}$ *and* $\mathfrak{d}$ *to* ω_1. The fact that Mathias forcing collapses $\mathfrak{c}$ to $\mathfrak{h}$ is just a consequence of LEMMA 24.10 and the fact that ultrafilter forcing $\mathbb{U}$ collapses $\mathfrak{c}$ to $\mathfrak{h}$ (see Chapter 25 | RELATED RESULT 144). Furthermore, Brendle [2, Corollary 3.10.(c)/(d)] showed that Mathias forcing collapses $\mathfrak{d}$ to ω_1, and since $\mathfrak{h} \leq \mathfrak{d}$, one gets that two Mathias reals added iteratively always force CH (*cf.* Chapter 23 | RELATED RESULT 134).

140. *Mathias forcing and Borel's conjecture.* By adding random reals to the model constructed in the proof of PROPOSITION 24.12, Judah, Shelah, and Woodin [10] showed that Borel's conjecture is consistent with $\mathfrak{c}$ being arbitrarily large (*cf.* Chapter 23 | RELATED RESULT 131), and see also Bartoszyński and Judah [1, Theorem 8.3.7]).

141. *Restricted Mathias forcing which does not add dominating reals.* Canjar showed in [3] that under the assumption $\mathfrak{d} = \mathfrak{c}$, there exists an ultrafilter $\mathscr{U}$ over ω such that $\mathbb{M}_{\mathscr{U}}$ does not add dominating reals. Further, he showed that such an ultrafilter is necessarily a P-point.

142. *Between Laver and Mathias forcing.* If $\mathscr{U}$ is an ultrafilter, then restricted Mathias forcing $\mathbb{M}_{\mathscr{U}}$ is equivalent to restricted Laver forcing $\mathbb{L}_{\mathscr{U}}$ if and only if $\mathscr{U}$ is a Ramsey ultrafilter (see Judah and Shelah [8, Theorem 1.20]). On the other hand, if $\mathscr{U}$ is not a Ramsey ultrafilter, then $\mathbb{M}_{\mathscr{U}}$ and $\mathbb{L}_{\mathscr{U}}$ can be quite different (see Judah and Shelah [9]).

143. *The Ramsey property of projective sets*.* The hierarchy of projective subsets of $[\omega]^\omega$ is defined as follows: Let $A \subseteq \big([\omega]^\omega\big)^k$ be a k-dimensional set (for some positive integer k). Then A is a $\mathbf{\Sigma^1_1}$**-set** if A the projection along $[\omega]^\omega$ of a closed set $C \subseteq \big([\omega]^\omega\big)^{k+1}$, and A is a $\mathbf{\Pi^1_1}$**-set** if it is the complement of a $\mathbf{\Sigma^1_1}$-set. In general, for integers $n \geq 1$, A is a $\mathbf{\Sigma^1_{n+1}}$**-set** if A the projection along $[\omega]^\omega$ of a $(k+1)$-dimensional $\mathbf{\Pi^1_n}$-set, and A is a $\mathbf{\Pi^1_{n+1}}$**-set** if it is the complement of a $\mathbf{\Sigma^1_{n+1}}$-set. Furthermore, we say that A is a $\mathbf{\Delta^1_n}$**-set** if A is a $\mathbf{\Sigma^1_n}$-set as well as a $\mathbf{\Pi^1_n}$-set. Below, $\mathbf{\Sigma^1_n}$, $\mathbf{\Pi^1_n}$, and $\mathbf{\Delta^1_n}$, denote the collections of the corresponding subsets of $[\omega]^\omega$. The sets $A \subseteq [\omega]^\omega$ belonging to one of the collections $\mathbf{\Sigma^1_n}$, $\mathbf{\Pi^1_n}$,

or $\mathbf{\Delta}^1_n$, are called *projective* sets. With respect to inclusion, we get the following diagram:

$$\begin{tikzcd}
 & \mathbf{\Sigma}^1_1 \arrow[dr, phantom, sloped, "\subsetneq"] & & \mathbf{\Sigma}^1_2 \arrow[dr, phantom, sloped, "\subsetneq"] & & \mathbf{\Sigma}^1_3 \arrow[dr, phantom, sloped, "\subsetneq"] & \\
\mathbf{\Delta}^1_1 \arrow[ur, phantom, sloped, "\subsetneq"] \arrow[dr, phantom, sloped, "\subsetneq"] & & \mathbf{\Delta}^1_2 \arrow[ur, phantom, sloped, "\subsetneq"] \arrow[dr, phantom, sloped, "\subsetneq"] & & \mathbf{\Delta}^1_3 \arrow[ur, phantom, sloped, "\subsetneq"] \arrow[dr, phantom, sloped, "\subsetneq"] & & \cdots \\
 & \mathbf{\Pi}^1_1 \arrow[ur, phantom, sloped, "\subsetneq"] & & \mathbf{\Pi}^1_2 \arrow[ur, phantom, sloped, "\subsetneq"] & & \mathbf{\Pi}^1_3 \arrow[ur, phantom, sloped, "\subsetneq"] &
\end{tikzcd}$$

If all $\mathbf{\Sigma}^1_n$-sets $A \subseteq [\omega]^\omega$ have the Ramsey property (defined in Chapter 9), then we shall write $\mathbf{\Sigma}^1_n(\mathscr{R})$; the notations $\mathbf{\Pi}^1_n(\mathscr{R})$ and $\mathbf{\Delta}^1_n(\mathscr{R})$ are defined accordingly. It is natural to ask whether all projective sets have the Ramsey property. Even though the answer to this question is not decidable in ZFC, one can show the following facts:

- For all $n \in \omega$: $\mathbf{\Sigma}^1_n(\mathscr{R}) \iff \mathbf{\Pi}^1_n(\mathscr{R})$ (trivial).
- $\mathbf{\Delta}^1_2(\mathscr{R}) \iff \mathbf{\Sigma}^1_2(\mathscr{R})$ (see Judah and Shelah [8, Theorem 2.7]).
- $\mathsf{ZFC} \vdash \mathbf{\Sigma}^1_1(\mathscr{R})$ (see Silver [13] or Ellentuck [4]).
- $\mathbf{L} \nvDash \mathbf{\Delta}^1_2(\mathscr{R})$ (*cf.* Judah and Shelah [8, Lemma 2.2]).
- $\mathrm{Con}(\mathsf{ZFC}) \Rightarrow \mathrm{Con}\big(\mathsf{ZFC} + \mathbf{\Delta}^1_3(\mathscr{R})\big)$ (see Judah [7, Theorem 0.8]).

Furthermore, Mathias showed in [11, Section 5] — using Mathias forcing — that if ZFC + "*there is a strongly inaccessible cardinal*" is consistent (where κ is *strongly inaccessible* if κ is a regular limit cardinal and for all $\lambda < \kappa$, $2^\lambda < \kappa$), then so is ZFC + "*every projective set has the Ramsey property*". However, it is still open whether one can take "Mathias' inaccessible" away, *i.e.*, whether one can construct a model of ZFC in which all projective sets have the Ramsey property without assuming the existence of a strongly inaccessible cardinal (*cf.* Shelah [12]). Moreover, it is not even known whether $\mathbf{\Sigma}^1_3(\mathscr{R})$ implies the existence of a strongly inaccessible cardinal. For partial results see Halbeisen and Judah [6, Theorem 5.3] and Brendle [2, Proposition 4.3].

References

1. Tomek Bartoszyński and Haim Judah, ***Set Theory: on the structure of the real line***, A.K. Peters, Wellesley, 1995.
2. Jörg Brendle, *Combinatorial properties of classical forcing notions*, ***Annals of Pure and Applied Logic***, vol. 73 (1995), 143–170.
3. R. Michael Canjar, *Mathias forcing which does not add dominating reals*, ***Proceedings of the American Mathematical Society***, vol. 104 (1988), 1239–1248.
4. Erik Ellentuck, *A new proof that analytic sets are Ramsey*, ***The Journal of Symbolic Logic***, vol. 39 (1974), 163–165.
5. Lorenz Halbeisen, *A playful approach to Silver and Mathias forcings*, in ***Foundations of the Formal Sciences V: Infinite Games*** (Stefan Bold, Benedikt Löwe, Thoralf Räsch, and Johan van Benthem, eds.), Papers of a Conference held in Bonn, November 26–29, 2004, [Studies in Logic, vol. 11], College Publications, London, 2007, pp. 123–142.
6. Lorenz Halbeisen and Haim Judah, *Mathias absoluteness and the Ramsey property*, ***The Journal of Symbolic Logic***, vol. 61 (1996), 177–193.

7. Haim Judah, *Exact equiconsistency results for Δ^1_3-sets of reals*, ***Archive for Mathematical Logic***, vol. 32 (1992), 101–112.
8. Haim Judah and Saharon Shelah, *Δ^1_2-sets of reals*, ***Annals of Pure and Applied Logic***, vol. 42 (1989), 207–223.
9. ______, *Forcing minimal degree of constructibility*, ***The Journal of Symbolic Logic***, vol. 56 (1991), 769–782.
10. Haim Judah, Saharon Shelah, and W. Hugh Woodin, *The Borel conjecture*, ***Annals of Pure and Applied Logic***, vol. 50 (1990), 255–269.
11. Adrian Richard David Mathias, *Happy families*, ***Annals of Mathematical Logic***, vol. 12 (1977), 59–111.
12. Saharon Shelah, *Can you take Solovay's inaccessible away?*, ***Israel Journal of Mathematics***, vol. 48 (1984), 1–47.
13. Jack Silver, *Every analytic set is Ramsey*, ***The Journal of Symbolic Logic***, vol. 35 (1970), 60–64.

25

On the Existence of Ramsey Ultrafilters

So far we have seen that $\mathfrak{p} = \mathfrak{c}$ implies the existence of Ramsey ultrafilters (see PROPOSITION 10.9). In particular, if we assume CH, then Ramsey ultrafilters exist. Moreover, by PROPOSITION 13.9 we know that MA(countable) implies the existence of $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters. Furthermore, by THEOREM 21.5 we know that $\mathfrak{p} \leq cov(\mathcal{M})$, and Chapter 13 | RELATED RESULT 80 tells us that MA(countable) is equivalent to $cov(\mathcal{M}) = \mathfrak{c}$. Hence, $cov(\mathcal{M}) = \mathfrak{c}$ is a sufficient condition for the existence of Ramsey ultrafilters and it is natural to ask whether $cov(\mathcal{M}) = \mathfrak{c}$ is necessary, too. In the first section of this chapter we shall give a negative answer to this question by constructing a model of $\mathsf{ZFC} + cov(\mathcal{M}) < \mathfrak{c}$ in which there is a Ramsey ultrafilter. Since in that model we have $\mathfrak{h} = \mathfrak{c}$ and $\mathfrak{h}$ is related to the Ramsey property (*cf.* Chapter 9), one might think that perhaps $\mathfrak{h} = \mathfrak{c}$ implies the existence of a Ramsey ultrafilter; but this is not the case, as we shall see in the second section of this chapter.

There may be a Ramsey Ultrafilter and $cov(\mathscr{M}) < \mathfrak{c}$

In the proof of PROPOSITION 24.12 we have constructed a model $\mathbf{V}$ of ZFC, usually called *Mathias' model*, in which $cov(\mathscr{M}) < \mathfrak{c}$. Furthermore, PROPOSITION 14.18 states that if G is $\mathbb{U}$-generic over $\mathbf{V}$, where $\mathbb{U} = \big([\omega]^\omega/\operatorname{fin}, \leq\big)$, then $\bigcup G$ is a Ramsey ultrafilter in $\mathbf{V}[G]$; in particular, ultrafilter forcing $\mathbb{U}$ adds a Ramsey ultrafilter to $\mathbf{V}$. Recall that $[\omega]^\omega/\operatorname{fin} = \big\{[x]^{\tilde{}} : x \in [\omega]^\omega\big\}$ and $[x]^{\tilde{}} \leq [y]^{\tilde{}} \iff y \subseteq^* x$. So, at first glance we just have to force with $\mathbb{U}$ over Mathias' model. However, in order to get a model in which there exists a Ramsey ultrafilter and $cov(\mathscr{M}) < \mathfrak{c}$, it has to be shown that ultrafilter forcing $\mathbb{U}$ does not collapse $\mathfrak{c}$ to $cov(\mathscr{M})$ — for this, we first show that ultrafilter forcing $\mathbb{U}$ does not collapse $\mathfrak{c}$ to any cardinal below $\mathfrak{h}$.

LEMMA 25.1. *If G is $\mathbb{U}$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \vDash \mathfrak{c} \geq \mathfrak{h}^{\mathbf{V}}$, in other words, ultrafilter forcing $\mathbb{U}$ does not collapse $\mathfrak{c}$ to any cardinal $\kappa < \mathfrak{h}^{\mathbf{V}}$.*

Proof. Let G be $\mathbb{U}$-generic over some model $\mathbf{V}$ of ZFC. Since the forcing notion $\mathbb{U}$ is σ-closed (by the proof of THEOREM 8.1), and since σ-closed forcing notions do not add reals (by LEMMA 14.17), ultrafilter forcing $\mathbb{U}$ does not add any new reals to the ground model $\mathbf{V}$. In particular we have $\mathbf{V}[G] \vDash \mathfrak{c} \leq \mathfrak{c}^{\mathbf{V}}$. Thus, in order to show that $\mathbf{V}[G] \vDash \mathfrak{c} \geq \mathfrak{h}^{\mathbf{V}}$, it is enough to prove that in $\mathbf{V}[G]$ there is no surjection from some $\kappa < \mathfrak{h}^{\mathbf{V}}$ onto $\mathfrak{c}$ (which implies $\mathfrak{c} \not< \mathfrak{h}^{\mathbf{V}}$).

Let κ be a cardinal with $\mathbf{V} \vDash \kappa < \mathfrak{h}$ and let $g \in \mathbf{V}[G]$ be a function from κ to $\mathfrak{c}$. In order to prove that g fails to be surjective, it is enough to show that g is in the ground model $\mathbf{V}$ — notice that this would imply $\mathbf{V} \vDash \mathfrak{c} \leq \kappa < \mathfrak{h}$, contradicting the fact that $\mathfrak{h} \leq \mathfrak{c}$. Let $\underset{\sim}{g}$ be a $\mathbb{U}$-name for g and let $x_0 \in [\omega]^\omega$ be such that $[x_0]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{g} : \kappa \to \mathfrak{c}$. For each $\alpha \in \kappa$ let

$$D_\alpha = \left\{ [y]^{\tilde{}} : |y \cap x_0| < \omega \vee \left(y \subseteq^* x_0 \wedge \exists \gamma \in \mathfrak{c} \left([y]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{g}(\alpha) = \gamma \right) \right) \right\}.$$

Each D_α is open dense. Thus, for each $\alpha \in \kappa$ we can choose a *mad* family $\mathscr{A} \subseteq \bigcup D_\alpha$. Now, by LEMMA 8.14 there is a *mad* family $\mathscr{A} \subseteq [\omega]^\omega$ such that

$$\forall \alpha \in \kappa \, \forall y \in \mathscr{A}_\alpha \, \exists x \in \mathscr{A} (x \subseteq^* y).$$

Furthermore, let $D = \left\{ [y]^{\tilde{}} : \exists x \in \mathscr{A} (y \subseteq^* x) \right\}$. Then D is open dense and therefore $G \cap D$ is non-empty. For $[y_0]^{\tilde{}} \in (G \cap D)$ we get $[y_0]^{\tilde{}} \leq [x_0]^{\tilde{}}$, in particular, $[y_0]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{g} : \kappa \to \mathfrak{c}$. Moreover, by construction of D,

$$\forall \alpha \in \kappa \, \exists \gamma \in \mathfrak{c} \big([y_0]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{g}(\alpha) = \gamma \big).$$

Let $g_0 : \kappa \to \mathfrak{c}$ be such that for all $\alpha \in \kappa$, $[y_0]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{g}(\alpha) = g_0(\alpha)$. Then g_0 belongs to the ground model $\mathbf{V}$ and in addition we have $[y_0]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{g} = g_0$. Now, since $[y_0]^{\tilde{}} \in G$, this shows that $g = \underset{\sim}{g}[G]$ belongs to $\mathbf{V}$. ⊣

With this result, we easily can construct a model with a Ramsey ultrafilter in which $cov(\mathscr{M}) < \mathfrak{c}$.

PROPOSITION 25.2. *The existence of a Ramsey ultrafilter is consistent with* $\mathsf{ZFC} + cov(\mathscr{M}) < \mathfrak{c}$.

Proof. Let $\mathbf{V}$ be Mathias' model (*i.e.*, the model constructed in the proof of PROPOSITION 24.12), and let G be $\mathbb{U}$-generic over $\mathbf{V}$. Then we have

$$\mathbf{V} \vDash \omega_1 = cov(\mathscr{M}) < \mathfrak{h} = \mathfrak{c} = \omega_2,$$

and by LEMMA 25.1 we get $\mathbf{V}[G] \vDash \mathfrak{h}^{\mathbf{V}} = \mathfrak{c}$, in particular,

$$\mathbf{V}[G] \vDash cov(\mathscr{M}) < \mathfrak{c}.$$

Finally, by PROPOSITION 14.18 we get that $\bigcup G$ is a Ramsey ultrafilter in $\mathbf{V}[G]$, and therefore, $\mathbf{V}[G]$ is a model with a Ramsey ultrafilter in which $cov(\mathscr{M}) < \mathfrak{c}$. ⊣

There may be no Ramsey Ultrafilter and $\mathfrak{h} = \mathfrak{c}$

The goal of this section is to show that there are no Ramsey ultrafilters in Mathias' model — which is a model of $\mathfrak{h} = \mathfrak{c}$. In fact we prove that not even *rapid filters* exist in that model. For this we first prove a few auxiliary results concerning ω_2-iterations of Mathias forcing. Then we recall the definition of rapid filters (*cf.* Chapter 10 | RELATED RESULT 70) and show that every Ramsey ultrafilter is a rapid filter; and finally we prove that there are no rapid filters in Mathias' model.

Let us start by recalling some terminology of Mathias forcing $\mathbb{M} = (M, \leq)$ and by introducing some notation: Let (s, x) and (t, y) be two $\mathbb{M}$-conditions. Recall that

$$(s, x) \leq (t, y) \iff s \subseteq t \wedge y \subseteq x \wedge t \setminus s \subseteq x .$$

Now, let us define

$$(s, x) \leq^0 (t, y) \iff (s, x) \leq (t, y) \wedge s = t .$$

In order to define "$\leq^n$" for positive integers $n \in \omega$, we write sets $x \in [\omega]^\omega$ in increasing order, *i.e.*, $x = \{a_k : k \in \omega\}$ where $k < k' \to a_k < a_{k'}$. By abuse of notation we shall just write $x = \{a_0 < a_1 < \cdots\}$. Now, for $n \in \omega$ and $x = \{a_0 < a_1 < \cdots\}$ we define

$$(s, x) \leq^n (t, y) \iff (s, x) \leq^0 (t, y) \wedge \forall k \in n \, (a_k \in y) .$$

In this notation, the fact that Mathias forcing has pure decision (see THEOREM 24.3) can be expressed as follows: Let $p \in M$ be an $\mathbb{M}$-condition and let φ be a sentence of the forcing language. Then there exists a $q \in M$ with $p \leq^0 q$ such that either $q \Vdash_{\mathbb{M}} \varphi$ or $q \Vdash_{\mathbb{M}} \neg\varphi$.

In order to get familiar with this notation we prove the following fact. Notice that this fact was already used implicitly in the previous chapter (*e.g.*, in the proof of COROLLARY 24.8).

FACT 25.3. *Let $\underset{\sim}{g}$ be an $\mathbb{M}$-name for a function $g \in {}^\omega\omega$ and let $n_0 \in \omega$ be a fixed integer. Further, let $p \in M$ and $k \in \omega$ be such that*

$$p \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) \in k .$$

Then there are $q \in M$ and $l_0 \in k$ such that $p \leq^0 q$ and

$$q \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l_0 .$$

Proof. Since Mathias forcing has pure decision (see THEOREM 24.3), there is a $q_0 \in M$ with $p \leq^0 q_0$ such that

$$q_0 \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = 0 \qquad \text{or} \qquad q_0 \Vdash_{\mathbb{M}} \bigvee_{0<l<k} \underset{\sim}{g}(n_0) = l ,$$

where $\bigvee_{0<l<k} \varphi_l$ is an abbreviation for $\varphi_1 \vee \cdots \vee \varphi_{k-1}$. In the latter case, by pure decision we find a $q_1 \in M$ with $q_0 \leq^0 q_1$ such that

$$q_1 \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = 1 \qquad \text{or} \qquad q_1 \Vdash_{\mathbb{M}} \bigvee_{1<l<k} \underset{\sim}{g}(n_0) = l\,.$$

Proceeding this way, we finally find a $q \in M$ with $p \leq^0 q$ and an $l_0 \in k$ such that $q \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l_0$. ⊣

To prove the following lemma, we just have to iterate this procedure.

LEMMA 25.4. *Let $\underset{\sim}{g}$ be an $\mathbb{M}$-name for a function $g \in {}^\omega\omega$ and let $n_0 \in \omega$ be a fixed integer. Further, let $p \in M$ and $k \in \omega$ be such that*

$$p \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) \in k\,.$$

Then, for every $i \in \omega$, there are $q_i \in M$ and $I_i \subseteq k$ such that $p \leq^i q_i$, $|I_i| \leq i+1$, and

$$q_i \Vdash_{\mathbb{M}} \bigvee_{l \in I_i} \underset{\sim}{g}(n_0) = l\,.$$

Proof. The proof is by induction on i: For $i = 0$, this is just FACT 25.3. So, let us assume that the lemma holds for some $i \in \omega$. In other words, there are $q_i \in M$ and $I_i \subseteq k$ such that $p \leq^i q_i$, $|I_i| \leq i+1$, and $q_i \Vdash_{\mathbb{M}} \bigvee_{l \in I_i} \underset{\sim}{g}(n_0) = l$. Let $p = (s, x)$ and $q_i = (s, y_i)$, where $x = \{a_0 < a_1 < \cdots\}$ and $y_i = \{b_0 < b_1 < \cdots\}$ respectively. Notice that for all $j \in i$, $a_j = b_j$. If $a_i = b_i$, then, for $I_{i+1} := I_i$ and $q_{i+1} := q_i$, we get

$$q_{i+1} \Vdash_{\mathbb{M}} \bigvee_{l \in I_{i+1}} \underset{\sim}{g}(n_0) = l\,.$$

Otherwise, we have $a_i < b_i$ (since $p \leq^i q_i$), and by FACT 25.3, we find $y' \subseteq y \setminus a_i$ and $l_{i+1} \in k$ such that

$$\big(s \cup \{a_j : j \leq i\}, y'\big) \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l_{i+1}\,.$$

Now, for $I_{i+1} := I_i \cup \{l_{i+1}\}$ and $q_{i+1} := \big(s \cup \{a_j : j \leq i\}, y'\big)$ we get

$$q_{i+1} \Vdash_{\mathbb{M}} \bigvee_{l \in I_{i+1}} \underset{\sim}{g}(n_0) = l\,,$$

where by construction, $p \leq^{i+1} q_{i+1}$ and $|I_{i+1}| \leq i+2$. ⊣

The next result uses the fact that Mathias forcing is proper (see COROLLARY 24.7).

LEMMA 25.5. *Let* $\mathbf{V}$ *be a model of* ZFC, *let* $\{\underset{\sim}{\alpha}_k : k \in \omega\}$ *be a countable set of* $\mathbb{M}$*-names for ordinals, such that for some* $p \in M$ *we have*

$$p \Vdash_{\mathbb{M}} \forall k \in \omega \, (\underset{\sim}{\alpha}_k \in \omega_2) \, .$$

Then, for every $i \in \omega$, *there is a countable set* $A \subseteq \omega_2$ *in* $\mathbf{V}$, *as well as a* $q \in M$ *with* $p \leq^i q$, *such that*

$$q \Vdash_{\mathbb{M}} \forall k \in \omega \, (\underset{\sim}{\alpha}_k \in A) \, .$$

Proof. Let $\mathbf{N} = (N, \in)$ be a countable elementary submodel of $(\mathrm{H}_\chi, \in)$ which contains $\mathbb{M}$, $\{\underset{\sim}{\alpha}_k : k \in \omega\}$, and p, where $p = (s, x)$. Since N is countable (in $\mathbf{V}$), there exists a Mathias real $m_G \in [s, x]^\omega \cap \mathbf{V}$ over $\mathbf{N}$. Notice that $(s, m_G \setminus s) \geq (s, x)$ and that $(s, m_G \setminus s)$ belongs to $\mathbf{V}$. By COROLLARY 24.6, every $m'_G \in [s, m_G \setminus s]^\omega$ is a Mathias real over $\mathbf{N}$, and hence, the $\mathbb{M}$-condition $q = (s, m_G \setminus s)$ is $\mathbf{N}$-generic. Now, for $A := N \cap \omega_2$, which is countable in $\mathbf{V}$, we get that $q \Vdash_{\mathbb{M}} \forall k \in \omega \, (\underset{\sim}{\alpha}_k \in A)$, which proves the lemma in the case when $i = 0$. For $i > 0$, we can proceed as in the proof of LEMMA 25.4 — the details are left as an exercise to the reader. ⊣

In the following result we introduce what is called a *fusion argument*:

FACT 25.6. *Let* $\langle p_n : n \in \omega \rangle$ *be a sequence of* $\mathbb{M}$*-conditions such that for all* $n \in \omega$, $p_n \leq p_{n+1}$. *Further assume that there is an* $m_0 \in \omega$ *such that for all* $n \geq m_0$, $p_n \leq^n p_{n+1}$. *Then there exists an* $\mathbb{M}$*-condition* p_ω *such that for all* $n \geq m_0$, $p_n \leq^n p_\omega$.

Proof. For $n \in \omega$, let $p_n = (s_n, x_n)$ where $x_n = \{x_n(0) < x_n(1) < \cdots\}$, and define

$$p_\omega = \big(s_{m_0} \cup \{x_{m_0}(i) : i \in m_0\}, \{x_i(i-1) : m_0 \in i \in \omega\}\big) \, .$$

We leave it as an exercise to the reader to show that p_ω has the required properties. ⊣

Below we shall generalise the previous results to countable support iterations of Mathias forcing, but first let us introduce some notations: Let $\mathbf{V}$ be a model of ZFC, let $\mathbb{P}_{\omega_2} = \langle \mathbb{Q}_\gamma : \gamma \in \omega_2 \rangle$ be the countable support iteration of length ω_2 of Mathias forcing $\mathbb{M}$, and let $G = \langle G(\gamma) : \gamma \in \omega_2 \rangle$ be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$. Furthermore, for $\beta \leq \omega_2$, $K \in \mathrm{fin}(\beta)$, $\mathbb{P}_\beta$-conditions p and q, and $n \in \omega$, define

$$p \leq^n_K q \iff p \leq q \wedge \forall \gamma \in K \, \big(q|_\gamma \Vdash_{\mathbb{P}_\gamma} p(\gamma) \leq^n q(\gamma)\big) \, .$$

The next result shows how fusion arguments work in countable support iterations of Mathias forcing.

LEMMA 25.7. *Let β be an ordinal with $1 \leq \beta \leq \omega_2$ and let $\langle p_n : n \in \omega\rangle$ be a sequence of $\mathbb{P}_\beta$-conditions. Furthermore, let $\langle K_n : n \in \omega\rangle$ be an increasing chain of finite subsets of β (i.e., $n < n' \to K_n \subseteq K_{n'}$) such that*

$$\bigcup_{n\in\omega} K_n = \bigcup_{n\in\omega} \operatorname{supp}(p_n) \qquad \textit{and} \qquad \forall n \in \omega\, (p_n \leq^n_{K_n} p_{n+1})\,.$$

Then there is a $\mathbb{P}_\beta$-condition p_ω such that for each $n \in \omega$, $p_n \leq^n_{K_n} p_\omega$.

Proof. For every $\gamma \in \beta$, $p_n(\gamma)$ is a $\mathbb{P}_\gamma$-name for an $\mathbb{M}$-condition. Thus, $p_n(\gamma) = (\underset{\sim}{s}_n, \underset{\sim}{x}_n)$ where $\underset{\sim}{x}_n = \{\underset{\sim}{x}_n(0) < \underset{\sim}{x}_n(1) < \cdots\}$. For $\gamma \in \bigcup_{n\in\omega} K_n$, let $m_0 = \min\{n \in \omega : \gamma \in K_n\}$ and define

$$p_\omega(\gamma) = \big(\underset{\sim}{s}_{m_0} \cup \{\underset{\sim}{x}_{m_0}(i) : i \in m_0\}, \{\underset{\sim}{x}_i(i-1) : m_0 \in i \in \omega\}\big)\,.$$

In the case when $\gamma \notin \bigcup_{n\in\omega} K_n$ define $p_\omega(\gamma) = \mathbf{0}_\gamma$. We leave it as an exercise to the reader to show that p_ω has the required properties. $\dashv$

In order to state the next result, we have to introduce again some notation: For ordinals $\alpha < \beta \leq \omega_2$ we say that q is a $\mathbb{P}_{\alpha\beta}$-condition *iff* there is a $\mathbb{P}_{\omega_2}$-condition $p = \langle p(\gamma) : \gamma \in \omega_2\rangle$ such that $q = \langle p(\gamma) : \alpha \leq \gamma < \beta\rangle$. In particular, $\mathbb{P}_{0\beta}$-conditions are the same as $\mathbb{P}_\beta$-conditions.

LEMMA 25.8. *Let β be an ordinal with $1 \leq \beta \leq \omega_2$ and let p be a $\mathbb{P}_\beta$-condition. Furthermore, let $K = \{\alpha_1 < \cdots < \alpha_i\}$ be a finite subset of β (i.e., $i \in \omega$) and let $n \in \omega$.*

(a) Let $\{\underset{\sim}{\alpha}_k : k \in \omega\}$ be a countable set of $\mathbb{P}_\beta$-names for ordinals such that

$$p \Vdash_{\mathbb{P}_\beta} \forall k \in \omega\, (\underset{\sim}{\alpha}_k \in \omega_2)\,.$$

Then there is a countable set $A \subseteq \omega_2$ in $\mathbf{V}$ and a $\mathbb{P}_\beta$-condition p' with $p \leq^n_K p'$ such that

$$p' \Vdash_{\mathbb{P}_\beta} \forall k \in \omega\, (\underset{\sim}{\alpha}_k \in A)\,.$$

(b) Let δ be an ordinal, where $\beta < \delta \leq \omega_2$, and assume that for some $\mathbb{P}_\beta$-name $\underset{\sim}{r}$ we have

$$p \Vdash_{\mathbb{P}_\beta} \text{“}\underset{\sim}{r} \textit{ is a } \mathbb{P}_{\beta\delta}\textit{-condition”}.$$

Then there is a $\mathbb{P}_\beta$-condition p' with $p \leq^n_K p'$ and a $\mathbb{P}_{\beta\delta}$-condition q such that

$$p' \Vdash_{\mathbb{P}_\beta} \underset{\sim}{r} = q\,.$$

In particular, $p' \cup q$ is a $\mathbb{P}_\delta$-condition (which is in general not the case for $p' \cup \underset{\sim}{r}$).

(c) Let $\underset{\sim}{g}$ be a $\mathbb{P}_\beta$-name for a function $g \in {}^\omega\omega$ and let $n_0 \in \omega$ be a fixed integer. Further, assume that for some $k \in \omega$,

$$p \Vdash_{\mathbb{P}_\beta} \underset{\sim}{g}(n_0) \in k\,.$$

Then there is an $I \subseteq k$ with $|I| \leq (n+1)^i$ and a $\mathbb{P}_\beta$-condition p_0 with $p \leq_K^n p_0$ such that

$$p_0 \Vdash_{\mathbb{P}_\beta} \bigvee_{l \in I} \underset{\sim}{g}(n_0) = l\,.$$

Proof. (a) Firstly recall that since Mathias forcing is proper, also $\mathbb{P}_\delta$, as a countable support iteration of proper forcing notions, is proper (see THEOREM 20.3.(b)). Thus, let $\mathbf{N} = (N, \in)$ be a countable elementary submodel of $(\mathrm{H}_\chi, \in)$ which contains $\mathbb{P}_\delta$, $\{\underset{\sim}{\alpha}_k : k \in \omega\}$, p, and $\underset{\sim}{r}$. Now, by similar arguments as in the proof of LEMMA 25.5 we can construct a $\mathbb{P}_\beta$-condition p' with the required properties — the details are left as an exercise to the reader.

(b) As a consequence of (a), there is a $\mathbb{P}_\beta$-condition p' with $p \leq_K^n p'$ as well as a countable set $A \subseteq [\beta, \delta)$ in $\mathbf{V}$ such that

$$p' \Vdash_{\mathbb{P}_\beta} \mathrm{supp}(\underset{\sim}{r}) \subseteq A\,.$$

For $\gamma \in [\beta, \delta) \setminus A$, let $q(\gamma) := \mathbf{0}_\gamma$. Otherwise, for $\gamma \in A$, let $q(\gamma) := \underset{\sim}{r}(\gamma)$. Then $q \in \mathbb{P}_{\beta\delta}$ and $p' \Vdash_{\mathbb{P}_\beta} \underset{\sim}{r} = q$, as required.

(c) The proof is by induction on β, where $1 \leq \beta \leq \omega_2$: Thus, we have to consider the case when $\beta = 1$, which we have already done in LEMMA 25.4, the case when β is a successor ordinal, and the case when β is a limit ordinal.

For $\beta = \delta + 1$, where $1 \leq \delta$, we just consider the case when $\delta = \alpha_i$ and leave the other case — which is similar to the case when β is a limit ordinal — as an exercise to the reader. For $p(\delta) = (\underset{\sim}{s}, \underset{\sim}{x})$, where $\underset{\sim}{x} = \{\underset{\sim}{x}(0) < \underset{\sim}{x}(1) < \cdots\}$, and for every $j \leq n$ let

$$\underset{\sim}{r}_j = \big(\underset{\sim}{s} \cup \{\underset{\sim}{x}(i) : i \in j\}, \{\underset{\sim}{x}(i) : j \leq i \in \omega\}\big)\,.$$

Notice that $\underset{\sim}{r}_j$ is a $\mathbb{P}_\delta$-name for an $\mathbb{M}$-condition. In particular, if $p|_\delta \in G|_\delta$, where $G|_\delta$ is $\mathbb{P}_\delta$-generic over $\mathbf{V}$, then $\mathbf{V}[G|_\delta] \vDash$ "$\underset{\sim}{r}_j[G|_\delta]$ is an $\mathbb{M}$-condition". Since LEMMA 25.4 holds in $\mathbf{V}[G|_\delta]$, there is a $\mathbb{P}_\delta$-name $\underset{\sim}{r}'_j$ for an $\mathbb{M}$-condition such that

$$p|_\delta \Vdash_{\mathbb{P}_\delta} \Big(\underset{\sim}{r}_j \leq^0 \underset{\sim}{r}'_j \wedge \exists l \in k\big(\underset{\sim}{r}'_j \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l\big)\Big)\,.$$

In particular, if $p|_\delta \in G|_\delta$, then, for some $l \in k$, $\mathbf{V}[G|_\delta] \vDash \underset{\sim}{r}'_j[G|_\delta] \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l$. Now, by induction on j, where $0 \leq j \leq n$, we can construct $\mathbb{P}_\delta$-conditions q_j, $\mathbb{P}_\delta$-names for $\mathbb{M}$-conditions $\underset{\sim}{r}'_j$, as well as subsets $I_j \subseteq k$, which satisfy the following conditions:

- $p|_\delta \leq_{K \cap \delta}^n q_0 \leq_{K \cap \delta}^n \cdots \leq_{K \cap \delta}^n q_n$,
- for each $j \leq n$ we have $|I_j| \leq (n+1)^{i-1}$,
- for each $j \leq n$, $q_j \Vdash_{\mathbb{P}_\delta} \underset{\sim}{r}'_j \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) \in I_j$ (for this, encode $\underset{\sim}{r}'_j \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l$ by a function $\underset{\sim}{g}_{\underset{\sim}{r}'_j}$, stipulating $\underset{\sim}{g}_{\underset{\sim}{r}'_j}(n_0) = l \Leftrightarrow \underset{\sim}{r}'_j \Vdash_{\mathbb{M}} \underset{\sim}{g}(n_0) = l$, and apply LEMMA 25.4),
- $\underset{\sim}{r}'_n$ is such that $q_n \cup \underset{\sim}{r}'_n \Vdash_{\mathbb{P}_\beta} \underset{\sim}{g}(n_0) \in \bigcup_{j \leq n} I_j$.

Then, for $p_0 := q_n \cup \underset{\sim}{r}'_n$ and $I := \bigcup_{j \leq n} I_j$ we have $p \leq^n_K p_0$, $|I| \leq (n+1)^i$, and $p_0 \Vdash_{\mathbb{P}_\beta} \bigvee_{l \in I} \underset{\sim}{g}(n_0) = l$, as required.

Assume now that β is a limit ordinal and that the lemma is true for $\alpha_i + 1$ (notice that $\alpha_i + 1 < \beta$). Let $\underset{\sim}{r}$ be a $\mathbb{P}_{\alpha_i+1}$-name for some $\mathbb{P}_{\alpha_i+1\beta}$-condition such that

$$p|_{\alpha_i+1} \Vdash_{\mathbb{P}_{\alpha_i+1}} \Big(p|_{[\alpha_i+1\beta)} \leq \underset{\sim}{r} \wedge \exists l \in k\big(\underset{\sim}{r} \Vdash_{\mathbb{P}_{\alpha_i+1\beta}} \underset{\sim}{g}(n_0) = l\,\big)\Big)\,.$$

Applying part (b) of the lemma to $\alpha_i + 1$, we get a $\mathbb{P}_{\alpha_i+1}$-condition p' with $p|_{\alpha_i+1} \leq^n_K p'$ and a $\mathbb{P}_{\alpha_i+1\beta}$-condition q such that

$$p' \Vdash_{\mathbb{P}_{\alpha_i+1}} \underset{\sim}{r} = q\,.$$

By induction hypothesis, there is a $\mathbb{P}_{\alpha_i+1}$-condition q' with $p' \leq^n_K q'$ and an $I \subseteq k$ with $|I| \leq (n+1)^i$, such that

$$q' \Vdash_{\mathbb{P}_{\alpha_i+1}} \exists l \in I\big(q \Vdash_{\mathbb{P}_{\alpha_i+1\beta}} \underset{\sim}{g}(n_0) = l\,\big)\,.$$

Finally, let $p_0 = q' \cup q$. Then p_0 has the required properties. $\dashv$

The next result, which will be crucial in the proof that there are no rapid filters in Mathias' model, concludes our investigation of ω_2-stage countable support iterations of Mathias forcing.

LEMMA 25.9. *Let* $\mathbf{V}$ *be a model of* ZFC, *let* $\mathbb{P}_{\omega_2}$ *be the countable support iteration of length* ω_2 *of Mathias forcing* $\mathbb{M}$, *and let* $G = \langle G(\gamma) : \gamma \in \omega_2 \rangle$ *be* $\mathbb{P}_{\omega_2}$*-generic over* $\mathbf{V}$. *Furthermore, let* $\underset{\sim}{f}$ *be an* $\mathbb{M}$*-name for the first Mathias real, more precisely,* $\underset{\sim}{f}$ *is the name for a strictly increasing function in* ${}^\omega\omega$ *such that*

$$\mathbf{0}_{\omega_2} \Vdash_{\mathbb{P}_{\omega_2}} \big\{\underset{\sim}{f}(i) : i \in \omega\big\} = \bigcup \big\{s : \exists x \in [\omega]^\omega \big((s,x) \in \underset{\cdot}{G}(0)\big)\big\}\,.$$

If $\underset{\sim}{g}$ *is a* $\mathbb{P}_{\omega_2}$*-name for a strictly increasing function in* ${}^\omega\omega$ *such that for some* $\mathbb{P}_{\omega_2}$*-condition* p *we have*

$$p \Vdash_{\mathbb{P}_{\omega_2}} \forall i \in \omega\big(\underset{\sim}{f}(i) < \underset{\sim}{g}(i)\big)\,,$$

then there are infinite sets $\mathscr{I}_0, \mathscr{I}_1 \subseteq \omega$ *in* $\mathbf{V}$, *where* $\mathscr{I}_0 \cap \mathscr{I}_1$ *is finite, and* $\mathbb{P}_{\omega_2}$*-conditions* $\hat{p}_0, \hat{p}_1$, *where* $\hat{p}_0 \geq p \leq \hat{p}_1$, *such that*

$$\hat{p}_0 \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_0 \qquad \textit{and} \qquad \hat{p}_1 \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_1\,.$$

Proof. Before we can start the proof, we have to introduce some notations: Firstly notice that if q is a $\mathbb{P}_{\omega_2}$-condition, then $q(0)$ is an $\mathbb{M}$-condition, *i.e.*, $q(0) = (s,x)$ where $s \in \operatorname{fin}(\omega)$ and $x \in [\omega]^\omega$. We call s the *stem* of $q(0)$ and write $s = \operatorname{stem}\big(q(0)\big)$. Let q be a $\mathbb{P}_{\omega_2}$-condition such that the stem of $q(0)$ is empty, *i.e.*, $q(0) = (\emptyset, x)$ for some $x \in [\omega]^\omega$. For every $t \in \operatorname{fin}(x)$ let

$q(0)_t := (t, x \setminus \bar{t}^+)$, where $\bar{t}^+ = \max(t)+1$. Notice that $q(0)_t$ is an $\mathbb{M}$-condition, $\operatorname{stem}\big(q(0)_t\big) = t$, and $q(0) \leq q(0)_t$.

Now, let us begin with the proof: Assume that for some $\mathbb{P}_{\omega_2}$-condition p we have

$$p \Vdash_{\mathbb{P}_{\omega_2}} \forall i \in \omega\big(\underset{\sim}{f}(i) < \underset{\sim}{g}(i)\big)\,.$$

By induction on n we shall construct an infinite sequence $\langle p_n : n \in \omega\rangle$ of $\mathbb{P}_{\omega_2}$-conditions such that $p = p_0$ and for every $n \in \omega$ we have $p_n \leq^n_{K_n} p_{n+1}$, where the finite sets $K_n \subseteq \omega_2$ are such that $0 \in K_0$, $n < n' \to K_n \subseteq K_{n'}$, and $\bigcup_{n\in\omega} K_n = \bigcup_{n\in\omega} \operatorname{supp}(p_n)$ (the construction of the K_n's with the required properties is left as an exercise to the reader).

For the sake of simplicity, let us assume that the stem of $p(0)$ is empty (*i.e.*, $p = (\emptyset, x)$ for some $x \in [\omega]^\omega$), which implies that the stems of the p_n's are empty, too. This way we even get infinite sets $\mathscr{I}_0, \mathscr{I}_1 \subseteq \omega$ such that $\mathscr{I}_0 \cap \mathscr{I}_1 = \emptyset$. We leave it as an exercise to the reader to verify that the case when the stem of $p(0)$ is non-empty yields infinite sets $\mathscr{I}_0$ and $\mathscr{I}_1$ such that the intersection $\mathscr{I}_0 \cap \mathscr{I}_1$ is still finite.

The goal is that for each $n \in \omega$ and for each $t = \{k_0 < \dots < k_{n+1}\} \subseteq x_{n+1}$, where $p_{n+1}(0) = (\emptyset, x_{n+1})$, we have

$$p_{n+1}(0)_t{}^\frown p_{n+1}|_{[1,\omega_2)} \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \cap [k_n, k_{n+1}) \subseteq I_t\,,$$

where $I_t \subseteq [k_n, k_{n+1})$ is such that $|I_t| \leq (n+1)\cdot(n+1)^{|K_n|}$. The infinite sequence $\langle p_n : n \in \omega\rangle$ is constructed as follows: Assume that we have already constructed p_n for some $n \in \omega$ (recall that $p_0 = p$). So, $p_n = (\emptyset, x_n)$ for some $x_n \in [\omega]^\omega$. Let $t = \{k_0 < \dots < k_{n+1}\} \subseteq x_n$ be an arbitrary but fixed subset of x_n of cardinality $n+2$ and let $p_t := p_n(0)_t{}^\frown p_n|_{[1,\omega_2)}$. Then, for each $i \leq n$, we obviously have

$$p_t \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}(i) \geq k_{n+1} \;\vee \bigvee_{l \in k_{n+1}} \underset{\sim}{g}(i) = l\,.$$

Notice that since $p_t \Vdash_{\mathbb{P}_{\omega_2}} \forall i \leq n+1\big(\underset{\sim}{f}(i) = k_i\big)$, and since $\underset{\sim}{g}$ is strictly increasing, $p_t \Vdash_{\mathbb{P}_{\omega_2}} \forall i > n\,\big(\underset{\sim}{g}(i) > k_{n+1}\big)$. Hence, by applying LEMMA 25.8.(c) $(n+1)$-times (for each $i \leq n$), we find a $\mathbb{P}_{\omega_2}$-condition q_t with $p_t \leq^n_{K_n} q_t$, as well as a set $I_t \subseteq [k_n, k_{n+1})$, such that $|I_t| \leq (n+1)\cdot(n+1)^{|K_n|}$ and

$$q_t \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \cap [k_n, k_{n+1}) \subseteq I_t\,.$$

Since t was arbitrary, for each $t \in \operatorname{fin}(x_n)$ of cardinality $n+2$ we find a q_t with $p_t \leq^n_{K_n} q_t$ such that $q_t \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \cap [k_n, k_{n+1}) \subseteq I_t$, where I_t is as above. Moreover, by induction on $\max(t)$ (similar to the proof of CLAIM below), we can construct a $\mathbb{P}_{\omega_2}$-condition p_{n+1} such that $p_{n+1}(0) = (\emptyset, x_{n+1})$ and $p_n \leq^n_{K_n} p_{n+1}$, and for every finite set $t = \{k_0 < \dots < k_{n+1}\} \subseteq x_{n+1}$ of cardinality $n+2$ we have

$$p_{n+1}(0)_t \Vdash_{\mathbb{M}} p_{n+1}|_{[1,\omega_2)} = q_t|_{[1,\omega_2)}$$

and

$$p_{n+1}(0)_t{}^\frown p_{n+1}|_{[1,\omega_2)} \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \cap [k_n, k_{n+1}) \subseteq I_t .$$

Thus, p_{n+1} has the required properties, which completes the construction of the sequence $\langle p_n : n \in \omega \rangle$.

By LEMMA 25.7, let p_ω be the fusion of the p_n's. Since $p \leq^0 p_\omega$, the stem of p_ω is empty, and therefore $p_\omega = (\emptyset, z)$ for some $z \in [\omega]^\omega$. By construction, for each $t = \{k_0 < \cdots < k_{m+1}\} \in \operatorname{fin}(z)$, where $m \in \omega$, we have

$$p_\omega(0)_t{}^\frown p_\omega|_{[1,\omega_2)} \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \cap [k_m, k_{m+1}) \subseteq I_t .$$

It remains to construct infinite sets $\mathscr{I}_0, \mathscr{I}_1 \subseteq \omega$ in $\mathbf{V}$, where $\mathscr{I}_0 \cap \mathscr{I}_1$ is finite, and $\mathbb{P}_{\omega_2}$-conditions $\hat{p}_0, \hat{p}_1$, where $\hat{p}_0 \geq p_\omega \leq \hat{p}_1$, such that $\hat{p}_0 \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_0$ and $\hat{p}_1 \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_1$. For this, we first prove the following

CLAIM. *Let* $p_\omega(0) = (\emptyset, z)$ *(for some* $z \in [\omega]^\omega$*), and for every* $x \in [z]^\omega$*, let* $\mathscr{I}_x := \bigcup \{I_t : t \in \operatorname{fin}(x)\}$*, where* I_t *is as above. Then there are infinite sets* $\hat{x}, \hat{y} \in [z]^\omega$ *such that* $\mathscr{I}_{\hat{x}} \cap \mathscr{I}_{\hat{y}}$ *is finite. Moreover, since we assumed that* stem$\big(p_\omega(0)\big) = \emptyset$*, we even get* $\mathscr{I}_{\hat{x}} \cap \mathscr{I}_{\hat{y}} = \emptyset$*.*

Proof of Claim. By construction, for every $t = \{k_0 < \cdots < k_{n+1}\} \in \operatorname{fin}(z)$, $I_t \subseteq [k_n, k_{n+1})$ and $|I_t| \leq (n+1)^{|K_n|+1}$. Notice that the size of I_t depends on $|t|$, but not on the particular set t. For every $n \in \omega$, let $F(n) := (n+1)^{|K_n|+1}$. Then, for every non-empty $t \in \operatorname{fin}(z)$ we have $|I_t| \leq F(|t|)$ (notice that for every $k_0 \in z$, $I_{\{k_0\}} = \emptyset$). For each non-empty set $s = \{k_0 < \cdots < k_n\} \in \operatorname{fin}(z)$ let

$$succ_z(s) = \big\{t \in \operatorname{fin}(z) : t = \{k_0 < \cdots < k_n < k_{n+1}\}\big\} ,$$

i.e., $t \in succ_z(s)$ *iff* $t = s \cup \{k_{n+1}\}$ for some $k_{n+1} \in z$ with $k_{n+1} > k_n$. Then, for each non-empty set $s = \{k_0 < \cdots < k_n\} \in \operatorname{fin}(z)$ we get that $\mathscr{E}_s = \big\{I_t : t \in succ_z(s)\big\}$ is an infinite set of finite subsets of $[k_n, \omega)$, where the cardinality of the finite sets $I_t \in \mathscr{E}_s$ is bounded by $F\big(|s|+1\big)$. By similar arguments as in the proof of the Δ-System Lemma 13.2, for each non-empty set $s = \{k_0 < \cdots < k_n\} \in \operatorname{fin}(z)$ we can construct an infinite set $z' \in [z]^\omega$ and a finite set $\Delta_s \subseteq [k_n, \omega)$, such that for any distinct $t, t' \in succ_{z'}(s)$ we have $I_t \cap I_{t'} \subseteq \Delta_s$. In other words, for any distinct $t, t' \in succ_{z'}(s)$, $I_t \setminus \Delta_s$ and $I_{t'} \setminus \Delta_s$ are disjoint. Moreover, we can construct an infinite set $z_0 \in [z]^\omega$, and for every non-empty $s = \{k_0 < \cdots < k_n\} \in \operatorname{fin}(z_0)$ a finite set $\Delta_s \subseteq [k_n, \omega)$, such that for any distinct $t, t' \in succ_{z_0}(s)$ we have

$$I_t \cap I_{t'} \subseteq \Delta_s . \qquad (\Delta)$$

Now, we are ready to construct the sets $\hat{x}$ and $\hat{y}$ in $[z]^\omega$ with the required properties: Firstly, let x_0 and y_0 be two disjoint infinite subsets of z_0. Let $k_0 = \min(x_0)$ and let $l_0 \in y_0$ be such that $l_0 > \max\big(\Delta_{\{k_0\}}\big)$. By (Δ) we find sets $x_1 \in [x_0]^\omega$ and $y_1 \in [y_0]^\omega$ such that for all $t \in succ_{x_1}(\{k_0\})$ and all $t' \in succ_{y_1}(\{l_0\})$, $I_t \cap I_{t'} = \emptyset$. Now, choose $k_1 \in x_1$ such that $k_1 > k_0$, and $l_1 \in y_1$ such that $l_1 > \max\big\{\max(\Delta_{\{k_1\}}), \max(\Delta_{\{k_0,k_1\}})\big\}$. Again by (Δ) we find sets

$x_2 \in [x_1]^\omega$ and $y_2 \in [y_1]^\omega$ such that for all $t \in succ_{x_2}(\{k_1\}) \cup succ_{x_2}(\{k_0, k_1\})$ and all $t' \in succ_{y_2}(\{l_1\}) \cup succ_{y_2}(\{l_0, l_1\})$, $I_t \cap I_{t'} = \emptyset$. Proceeding this way, we finally get $\hat{x}, \hat{y} \in [z_0]^\omega$ such that for all $t \in \text{fin}(\hat{x})$ and all $t' \in \text{fin}(\hat{y})$ we have $I_t \cap I_{t'} = \emptyset$, and hence, $\mathscr{I}_{\hat{x}} \cap \mathscr{I}_{\hat{y}} = \emptyset$. $\dashv_{\text{Claim}}$

Now, let $\hat{p}_0 := (\emptyset, \hat{x})^\frown p_\omega|_{[1\omega_2)}$ and $\hat{p}_1 := (\emptyset, \hat{y})^\frown p_\omega|_{[1\omega_2)}$. Then $\hat{p}_0 \geq p \leq \hat{p}_1$, and by construction of $\hat{x}$ and $\hat{y}$ we have

$$\hat{p}_0 \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_{\hat{x}} \qquad \text{and} \qquad \hat{p}_1 \Vdash_{\mathbb{P}_{\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_{\hat{y}}\,,$$

where $\mathscr{I}_{\hat{x}} \cap \mathscr{I}_{\hat{y}} = \emptyset$, which completes the proof. $\dashv$

Before we show that every Ramsey ultrafilter is rapid, let us briefly recall the notion of rapid filters (given in Chapter 10 | Related Result 70), as well as the notion of Q-points (also given in Chapter 10):

A free filter $\mathscr{F} \subseteq [\omega]^\omega$ is called a **rapid filter** if for each $f \in {}^\omega\omega$ there exists an $x \in \mathscr{F}$ such that for all $n \in \omega$, $\big|x \cap f(n)\big| \leq n$. Furthermore, a free ultrafilter $\mathscr{U} \subseteq [\omega]^\omega$ is a ***Q*-point** if for each partition of ω into finite pieces $\{I_n \subseteq \omega : n \in \omega\}$, (*i.e.*, for each $n \in \omega$, I_n is finite), there is an $x \in \mathscr{U}$ such that for each $n \in \omega$, $|x \cap I_n| \leq 1$. The following fact is just a consequence of these definitions.

Fact 25.10. *Every Q-point is a rapid filter.*

Proof. Let $\mathscr{U} \subseteq [\omega]^\omega$ be a Q-point and let $f \in {}^\omega\omega$ be any strictly increasing function. Let $I_0 := \big[0, f(0)\big)$, and for $n \in \omega$ let $I_{n+1} := \big[f(n), f(n+1)\big)$. Then $\{I_n \subseteq \omega : n \in \omega\}$ is obviously a partition of ω into finite pieces. Since $\mathscr{U}$ is a Q-point (in particular a free ultrafilter), there is an $x \in \mathscr{U}$ such that $x \cap f(0) = \emptyset$ and for each $n \in \omega$, $|x \cap I_n| \leq 1$, *i.e.*, for all $n \in \omega$, $|x \cap f(n)| \leq n$. Thus, $\mathscr{U}$ is a rapid filter. $\dashv$

By Fact 10.10 we know that every Ramsey ultrafilter is a Q-point, and therefore, every Ramsey ultrafilter is rapid.

Now, we are ready to prove the main result of this section.

Proposition 25.11. *It is consistent with* $\mathsf{ZFC} + \mathfrak{h} = \mathfrak{c}$ *that there are no rapid filters. In particular, since every Ramsey ultrafilter is rapid, it is consistent with* $\mathsf{ZFC} + \mathfrak{h} = \mathfrak{c}$ *that there are no Ramsey ultrafilters.*

Proof. Since $\mathfrak{h} = \mathfrak{c}$ in Mathias' model, it is obviously enough to prove that there are no rapid filters in Mathias' model. So, let $\mathbb{P}_{\omega_2} = \langle \mathbb{Q}_\gamma : \gamma \in \omega_2 \rangle$ be the countable support iteration of length ω_2 of Mathias forcing $\mathbb{M}$, starting in a model $\mathbf{V}$ of $\mathsf{ZFC} + \mathsf{CH}$. Furthermore, let $\underset{\sim}{\mathscr{F}}$ be a $\mathbb{P}_{\omega_2}$-name for a filter in the $\mathbb{P}_{\omega_2}$-generic extension of $\mathbf{V}$ (*i.e.*, $\mathbf{0}_{\omega_2} \Vdash_{\mathbb{P}_{\omega_2}}$ "$\underset{\sim}{\mathscr{F}}$ is a filter") and let G be $\mathbb{P}_{\omega_2}$-generic over $\mathbf{V}$. Then, similar to Claim 2 in the proof of Proposition 24.12, there is an $\alpha < \omega_2$ such that $\underset{\sim}{\mathscr{F}}[G] \cap \mathbf{V}[G|_\alpha] \in \mathbf{V}[G|_\alpha]$.

Let us work in the model $\mathbf{V}[G|_\alpha]$, *i.e.*, we consider $\mathbf{V}[G|_\alpha]$ as the ground model: In $\mathbf{V}[G|_\alpha]$, let $\underset{\sim}{f}$ be an $\mathbb{M}$-name in $\mathbf{V}[G|_\alpha]$ for the next Mathias real, *i.e.*, $\underset{\sim}{f}$ is the $\mathbb{M}$-name for a strictly increasing function in ${}^\omega\omega$ such that

$$\mathbf{0}_{\alpha\omega_2} \Vdash_{\mathbb{P}_{\alpha\omega_2}} \big\{\underset{\sim}{f}(n) : n \in \omega\big\} = \bigcup \big\{s : \exists x \in [\omega]^\omega \big((s,x) \in \underset{\cdot}{G}(\alpha)\big)\big\}\,.$$

Assume towards a contradiction that $\mathscr{F}$ is rapid. Then there is a $\mathbb{P}_{\alpha\omega_2}$-name $\underset{\sim}{g}$ for a strictly increasing function in ${}^\omega\omega$ and a $\mathbb{P}_{\alpha\omega_2}$-condition p, such that

$$p \Vdash_{\mathbb{P}_{\alpha\omega_2}} \forall n \in \omega\big(\underset{\sim}{g}(n) > \underset{\sim}{f}(n)\big) \wedge \underset{\sim}{g}[\omega] \in \mathscr{F}\,. \qquad (*)$$

By Lemma 25.9 (with respect to the ground model $\mathbf{V}[G|_\alpha]$), there are $\mathbb{P}_{\alpha\omega_2}$-conditions $\hat{p}_0$ and $\hat{p}_1$ with $\hat{p}_0 \geq p \leq \hat{p}_1$, and almost disjoint sets $\mathscr{I}_0, \mathscr{I}_1 \in [\omega]^\omega$ in $\mathbf{V}[G|_\alpha]$, such that

$$\hat{p}_0 \Vdash_{\mathbb{P}_{\alpha\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_0 \qquad \text{and} \qquad \hat{p}_1 \Vdash_{\mathbb{P}_{\alpha\omega_2}} \underset{\sim}{g}[\omega] \subseteq \mathscr{I}_1\,.$$

In particular, if $\hat{p}_0 \Vdash_{\mathbb{P}_{\alpha\omega_2}} \underset{\sim}{g}[\omega] \in \mathscr{F}[G|_\alpha]$, then $\hat{p}_1 \Vdash_{\mathbb{P}_{\alpha\omega_2}} \underset{\sim}{g}[\omega] \notin \mathscr{F}[G|_\alpha]$, and vice versa. Hence, $p \not\Vdash_{\mathbb{P}_{\alpha\omega_2}} \underset{\sim}{g}[\omega] \in \mathscr{F}[G|_\alpha]$, which is a contradiction to $(*)$. Thus, since $\mathscr{F}$ was arbitrary, there are no rapid filters in $\mathbf{V}[G]$. $\dashv$

Notes

Using results of Laver's ([7, Lemmata 5 & 6]), Miller [8] showed that there are no rapid filters in Laver's model (*cf.* Related Result 146). In the proof that there are no rapid filters in Mathias' model given above, we essentially followed Miller's proof by translating the corresponding results of Laver's to iterations of Mathias forcing.

Related Results

144. *Ultrafilter forcing* $\mathbb{U}$ *collapses* $\mathfrak{c}$ *to* $\mathfrak{h}$. By Lemma 25.1 we already know that ultrafilter forcing $\mathbb{U}$ does not collapse $\mathfrak{c}$ to any cardinal $\kappa < \mathfrak{h}$, *i.e.*, if G is $\mathbb{U}$-generic over $\mathbf{V}$, then $\mathbf{V}[G] \models \mathfrak{c} \geq \mathfrak{h}^{\mathbf{V}}$. Thus, in order to show that $\mathbf{V}[G] \models \mathfrak{c} = \mathfrak{h}^{\mathbf{V}}$, it is enough to show that $\mathbf{V}[G] \models \mathfrak{c} \leq \mathfrak{h}^{\mathbf{V}}$. In particular, it is enough to show that there is a surjection in $\mathbf{V}[G]$ which maps $\mathfrak{h}^{\mathbf{V}}$ onto $\mathfrak{c}$: Let us work in the model $\mathbf{V}$. By the Base Matrix Lemma 2.11 of Balcar, Pelant, and Simon [1] (see Chapter 8 | Related Result 51), there exists a shattering family $\mathscr{H}_0 = \big\{\mathscr{A}_\xi \subseteq [\omega]^\omega : \xi \in \mathfrak{h}\big\}$ which has the property that for each $x \in [\omega]^\omega$ there is a $\xi \in \mathfrak{h}$ and an $A \in \mathscr{A}_\xi$ such that $A \subseteq^* x$. Now, for each $A \in [\omega]^\omega$ let $\mathscr{C}_A \subseteq [A]^\omega$ be an almost disjoint family of cardinality $\mathfrak{c}$ and let $h_A : \mathscr{C}_A \twoheadrightarrow \mathfrak{c}$ be a surjection. Furthermore, we define the $\mathbb{U}$-name $\underset{\sim}{f}$ for a function from some subset of $\mathfrak{h}$ to $\mathfrak{c}$ by stipulating

$$\underset{\sim}{f} = \Big\{\big\langle\langle \underset{\cdot}{\xi}, \gamma\rangle, [x]^{\tilde{}}\big\rangle : \xi \in \mathfrak{h} \wedge \gamma \in \mathfrak{c} \wedge \exists A \in \mathscr{A}_\xi \big(x \in \mathscr{C}_A \wedge h_A(x) = \gamma\big)\Big\}\,.$$

In particular, if $\big\langle\langle \underset{\cdot}{\xi}, \gamma\rangle, [x]^{\tilde{}}\big\rangle \in \underset{\sim}{f}$, then

$$[x]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{f}(\xi) = \gamma\,.$$

By the properties of $\mathscr{H}_0$, for every $y \in [\omega]^\omega$ there is a $\xi \in \mathfrak{h}$ and an $A \in \mathscr{A}_\xi$ such that $A \subseteq^* y$. Thus, there exists an $x \in \mathscr{C}_A$ (in particular, $x \subseteq^* y$), such that $h_A(x) = \gamma$. In other words, for every $y \in [\omega]^\omega$ and each $\gamma \in \mathfrak{c}$, there are $x \subseteq^* y$ and $\xi \in \mathfrak{h}$ such that $[x]^{\tilde{}} \Vdash_{\mathbb{U}} \underset{\sim}{f}(\xi) = \gamma$. Hence,

$$D_\gamma = \left\{[x]^{\tilde{}} : [x]^{\tilde{}} \Vdash_{\mathbb{U}} \exists \xi \in \mathfrak{c}\big(\underset{\sim}{f}(\xi) = \gamma\big)\right\}$$

is an open dense subset of $[\omega]^\omega/\,\mathrm{fin}$, and therefore, $\underset{\sim}{f}[G]$ is a surjection from some subset of $\mathfrak{h}$ onto $\mathfrak{c}$, which shows that $\mathbf{V}[G] \vDash \mathfrak{c} \leq \mathfrak{h}^{\mathbf{V}}$.

145. *A model in which there are no Ramsey ultrafilters.* The first model in which there are no Ramsey ultrafilters was constructed by Kunen [6] using measure algebras (see also Jech [4, Theorem 91]).

146. *There are no rapid ultrafilters in Laver's model.* Miller [8] showed that there are no rapid ultrafilters in Laver's model (*i.e.*, the model we get after a countable support iteration of length ω_2 of Laver forcing starting in a model of $\mathsf{ZFC}+\mathsf{CH}$). However, like in Mathias' model, there are still P-points in Laver's model (see Roitman [10]).

147. *There are no Q-points in Miller's model.* According to Miller [9, p. 156], there are no Q-points in Miller's model (*i.e.*, the model we get after a countable support iteration of length ω_2 of Miller forcing starting in a model of $\mathsf{ZFC}+\mathsf{CH}$). On the other hand, since Miller forcing preserves P-points (by LEMMA 23.5), there are still P-points in Miller's model. Further notice that in Miller's model we have $\mathfrak{d} = \mathfrak{c}$ (*cf.* THEOREM 10.16).

148. *Models without rapid ultrafilters and large continuum.* We have seen that there exists a model of ZFC in which there are no rapid ultrafilters and $\mathfrak{c} = \omega_2$. It is natural to ask whether the continuum can be further increased without adding rapid ultrafilters; this is indeed the case: For any cardinal κ there exists a model of ZFC in which there are no rapid ultrafilters and $\mathfrak{c} \geq \kappa$ (see Judah and Shelah [5, Theorem 2.0], or Bartoszyński and Judah [2, Theorem 4.6.7]).

149. *Borel's conjecture and the existence of Ramsey ultrafilters.* Judah [3] showed that Borel's conjecture holds in the model constructed in the proof of PROPOSITION 25.2 (see Bartoszyński and Judah [2, Theorem 8.3.14]). Thus, Borel's conjecture does not contradict the existence of a Ramsey ultrafilter (compare with Chapter 23 | RELATED RESULT 131 and RELATED RESULT 146).

REFERENCES

1. BOHUSLAV BALCAR, JAN PELANT, AND PETR SIMON, *The space of ultrafilters on N covered by nowhere dense sets*, ***Fundamenta Mathematicae***, vol. 110 (1980), 11–24.
2. TOMEK BARTOSZYŃSKI AND HAIM JUDAH, ***Set Theory: on the structure of the real line***, A. K. Peters, Wellesley, 1995.
3. JAIME I. IHODA, *Strong measure zero sets and rapid filters*, ***The Journal of Symbolic Logic***, vol. 53 (1988), 393–402.
4. THOMAS JECH, ***Set Theory***, [Pure and Applied Mathematics], Academic Press, London, 1978.

5. Haim Judah and Saharon Shelah, *Q-sets, Sierpinski sets, and rapid filters*, ***Proceedings of the American Mathematical Society***, vol. 111 (1991), 821–832.
6. Kenneth Kunen, *Some points in βN*, ***Mathematical Proceedings of the Cambridge Philosophical Society***, vol. 80 (1976), 385–398.
7. Richard Laver, *On the consistency of Borel's conjecture*, ***Acta Mathematica***, vol. 137 (1976), 151–169.
8. Arnold W. Miller, *There are no Q-points in Laver's model for the Borel conjecture*, ***Proceedings of the American Mathematical Society***, vol. 78 (1980), 103–106.
9. ———, *Rational perfect set forcing*, in ***Axiomatic Set Theory*** (James E. Baumgartner, Donald A. Martin, and Saharon Shelah, eds.), Contemporary Mathematics, vol. 31, American Mathematical Society, Providence, RI, 1984, pp. 143–159.
10. Judy Roitman, *p-points in iterated forcing extensions*, ***Proceedings of the American Mathematical Society***, vol. 69 (1978), 314–318.

26

Combinatorial Properties of Sets of Partitions

In this chapter we shall investigate combinatorial properties of sets of partitions of ω, where we try to combine as many topics or voices (to use a musical term) as possible. As explained in Chapter 11, ***partitions*** of ω are to some extent the dual form of ***subsets*** of ω. Thus, we shall use the term "dual" to denote the partition forms of Mathias forcing, of Ramsey ultrafilters, of cardinal characteristics, *et cetera*. Firstly, we shall investigate combinatorial properties of a dual form of unrestricted Mathias forcing (which was introduced in Chapter 24). In particular, by using the PARTITION RAMSEY THEOREM 11.4, which is a dual form of RAMSEY'S THEOREM 2.1 (and which was the main result of Chapter 11), we shall prove that dual Mathias forcing has pure decision. Secondly, we shall dualise the shattering number $\mathfrak{h}$ (introduced in Chapter 8 and further investigated in Chapter 9), and show how it can be increased by iterating dual Mathias forcing (*cf.* PROPOSITION 24.12). Finally, we shall dualise the notion of Ramsey ultrafilters (introduced and investigated in Chapter 10), and show — using the methods developed in Part II and the previous chapter — that the existence of these dual Ramsey ultrafilters is consistent with $\mathsf{ZFC} + \mathsf{CH}$ as well as with $\mathsf{ZFC} + \neg\mathsf{CH}$.

A Dual Form of Mathias Forcing

Firstly, let us recall some terminology — for more detailed definitions see Chapter 11: The set of all infinite partitions of ω is denoted by $(\omega)^\omega$, and $(\mathbb{N})$ denotes the set of all (finite) partitions of natural numbers. For $P \in (\mathbb{N})$ or $P \in (\omega)^\omega$, let $\mathrm{Min}(P) := \big\{\min(p) : p \in P\big\}$ and $\mathrm{Dom}(P) := \bigcup P$. For partitions P and Q (*e.g.*, $P \in (\mathbb{N})$ and $Q \in (\omega)^\omega$) we write $P \sqsubseteq Q$ if Q restricted to $\mathrm{Dom}(P)$ is finer than P. Furthermore, for partitions P and Q, let $P \sqcap Q$ $(P \sqcup Q)$ denote the finest (coarsest) partition R such that $\mathrm{Dom}(R) = \mathrm{Dom}(P) \cup \mathrm{Dom}(Q)$ and R is coarser (finer) than P and Q. Let $S \in (\mathbb{N})$ and $X \in (\omega)^\omega$. If for each $s \in S$ there exists an $x \in X$ such that $x \cap \mathrm{Dom}(S) = s$, then we write $S \preccurlyeq X$. Similarly, for $S, T \in (\mathbb{N})$, where

$\mathrm{Dom}(S) \subseteq \mathrm{Dom}(T)$, we write $S \preccurlyeq T$ if for each $s \in S$ there exists a $t \in T$ such that $t \cap \mathrm{Dom}(S) = s$. Finally, for $S \in (\mathbb{N})$ and $X \in (\omega)^\omega$ with $S \sqsubseteq X$, let

$$(S, X)^\omega = \left\{ Y \in (\omega)^\omega : S \preccurlyeq Y \sqsubseteq X \right\}.$$

A set $(S, X)^\omega$, where S and X are as above, is called a **dual Ellentuck neighbourhood**.

Now, we are ready to define a dual form of Mathias forcing (*i.e.*, a form of Mathias forcing in terms of partitions): Similar to Mathias forcing $\mathbb{M}$, introduced in Chapter 24, we define **dual Mathias forcing** $\mathbb{M}^* = (M^*, \leq)$ by stipulating:

$$M^* = \left\{ (S, X) : S \in (\mathbb{N}) \ \wedge \ X \in (\omega)^\omega \ \wedge \ S \preccurlyeq X \right\}$$

$$(S, X) \leq (T, Y) \iff (T, Y)^\omega \subseteq (S, X)^\omega$$

Notice that $(S, X) \leq (T, Y) \iff S \preccurlyeq T \wedge Y \sqsubseteq X$. Thus, we get dual Mathias forcing from Mathias forcing by replacing subsets of ω with partitions of ω. However, as we shall see below, dual Mathias forcing is much stronger than Mathias forcing (see also RELATED RESULT 151), but first, let us show that dual Mathias forcing is at least as strong as Mathias forcing:

FACT 26.1. *Dual Mathias forcing adds Mathias reals and consequently it also adds dominating reals.*

Proof. Firstly, let M_0 be the set of all $\mathbb{M}$-conditions (s, x) for which we have $0 \in s$, or, in case $s = \emptyset$, $0 \in x$, and let $\mathbb{M}_0 = (M_0, \leq)$. Obviously, the forcing notions $\mathbb{M}_0$ and $\mathbb{M}$ are equivalent. Secondly, define the function $h : M^* \to M_0$ by stipulating

$$\begin{array}{rccc} h: & M^* & \longrightarrow & M_0 \\ & (S, X) & \longmapsto & \big(\mathrm{Min}(S), \mathrm{Min}(X) \setminus \mathrm{Min}(S) \big). \end{array}$$

Then, the function h satisfies the following conditions:

- for all $q_0, q_1 \in M^*$, if $q_0 \leq_{\mathbb{M}^*} q_1$ then $h(q_0) \leq_{\mathbb{M}} h(q_1)$,
- for all $q \in M^*$ and each $p \in M_0$ with $h(q) \leq_{\mathbb{M}} p$, there is a $q' \in M^*$ with $q \leq_{\mathbb{M}^*} q'$ such that $p \leq_{\mathbb{M}} h(q')$.

We leave it as an exercise to the reader to verify that this implies that whenever G^* is $\mathbb{M}^*$-generic, then $\left\{ \big(\mathrm{Min}(S), \mathrm{Min}(X) \setminus \mathrm{Min}(S) \big) \in M_0 : (S, X) \in G^* \right\}$ is $\mathbb{M}_0$-generic. Thus, dual Mathias forcing $\mathbb{M}^*$ adds Mathias reals, and since Mathias reals are dominating, it also adds dominating reals. $\dashv$

One of the main features of Mathias forcing is that it has pure decision. This is also the case for dual Mathias forcing and the proof is essentially the same as the proof for the corresponding result for Mathias forcing. However, at a crucial point we have to use the PARTITION RAMSEY THEOREM 11.4 — a dual form of RAMSEY'S THEOREM 2.1 — which will serve as a kind of Pigeon-Hole Principle.

THEOREM 26.2. *Let (S_0, X_0) be an $\mathbb{M}^*$-condition and let φ be a sentence of the forcing language. Then there exists an $\mathbb{M}^*$-condition $(S_0, Y_0) \geq (S_0, X_0)$ such that either $(S_0, Y_0) \Vdash_{\mathbb{M}^*} \varphi$ or $(S_0, Y_0) \Vdash_{\mathbb{M}^*} \neg\varphi$ (i.e., (S_0, Y_0) decides φ).*

Proof. We follow the proof of THEOREM 24.3: For any set $\mathcal{O} \subseteq M^*$ which is open with respect to the dual Ellentuck topology, let

$$\bar{\mathcal{O}} := \bigcup \left\{ (S, X)^\omega : (S, X) \in \mathcal{O} \right\}.$$

With respect to a fixed open set $\mathcal{O} \subseteq M^*$, we call the condition (S, X) **good** if there is a $Y \in (S, Y)^\omega$ such that $(S, X)^\omega \subseteq \bar{\mathcal{O}}$; otherwise, we call it **bad**. Furthermore, we call (S, X) **ugly** if (T^*, X) is bad for all $S \preccurlyeq T^* \sqsubseteq X$ with $|T| = |S|$, where $T^* := T \cup \left\{ \mathrm{Dom}(T) \right\}$.

CLAIM 1. *If the condition (S, X) is bad, then there is a $Y \in (S, X)^\omega$ such that (S, Y) is ugly.*

Proof of Claim 1. We follow the proof of LEMMA 24.4: Let $Z_0 := X$ and let $T_0 := S$. Assume we have already defined $Z_{n-1} \in (\omega)^\omega$ and $T_{n-1} \in (\mathbb{N})$ for some positive integer n. Let T_n be such that $S \preccurlyeq T_n$, $|T_n| = |S| + n$, and $T_n^* \preccurlyeq Z_{n-1}$. Let $\{U_i : i \leq m\}$ be an enumeration of all T such that $S \preccurlyeq T \sqsubseteq T_n$, $|T| = |S|$ and $\mathrm{Dom}(T) = \mathrm{Dom}(T_n)$. Further, let $Z^{-1} := Z_{n-1}$. Now, choose for each $i \leq m$ a partition $Z^i \in (\omega)^\omega$ such that $Z^i \sqsubseteq Z^{i-1}$, $T_n^* \preccurlyeq Z^i$ and either $(U_i^*, U_i \sqcap Z^i)$ is bad or $(U_i^*, Z^i)^\omega \subseteq \bar{\mathcal{O}}$, and let $Z_{n+1} := Z^m$. Finally, let $Z \in (\omega)^\omega$ be the only partition such that for all $n \in \omega$, $T_n \preccurlyeq Z$. By construction of Z, for all $T \in (S, Z)^{(|S|)^*}$, where

$$(S, Z)^{(|S|)^*} = \left\{ T \in (\mathbb{N}) : |T| = |S| \wedge S \preccurlyeq T \wedge T^* \sqsubseteq Z \right\},$$

we have either $(T^*, Z)^\omega \subseteq \bar{\mathcal{O}}$ or (T^*, Z) is bad. Now, for $n = |S|$, define the sets $C_0 := \left\{ T \in (S, Z)^{(n)^*} : (T^*, Z) \text{ is bad} \right\}$ and $C_1 := \left\{ T \in (S, Z)^{(n)^*} : (T^*, Z)^\omega \subseteq \bar{\mathcal{O}} \right\}$. Then, by the properties of Z, $C_0 \cup C_1 = (S, Z)^{(n)^*}$. Hence, by the PARTITION RAMSEY THEOREM 11.4, there exists a $Y \in (S, Z)$ such that either $(S, Y)^{(n)^*} \subseteq C_0$ or $(S, Y)^{(n)^*} \subseteq C_1$. Thus, since (S, X) is bad, (S, Y) is ugly. $\dashv_{\text{Claim 1}}$

Moreover, by a similar construction as in the proof of LEMMA 24.5 we can prove the following

CLAIM 2. *If the condition (S, X) is bad, then there is a $Y \in (S, X)^\omega$ such that $(S, Y)^\omega \cap \bar{\mathcal{O}} = \emptyset$.*

Proof of Claim 2. By CLAIM 1, there is a $Z_0 \in (S, X)^\omega$ such that (S, Z_0) is ugly, *i.e.*, for all $T \in (\mathbb{N})$ with $S \preccurlyeq T^* \sqsubseteq Z_0$ and $|T| = |S|$, (T^*, Z_0) is bad. Let $T_0 \in (\mathbb{N})$ be such that $T_0^* \preccurlyeq Z_0$ and $|T_0| = |S|$. Then, since (S, Z_0) is ugly, (T_0^*, Z_0) is bad. Assume that for some $n \in \omega$ we have already constructed $(T_n, Z_n) \geq (T_0, Z_0)$ with $T_n^* \preccurlyeq Z_n$ and $|T_n| = |S| + n$, such that for all $T \in (\mathbb{N})$ with $T_0 \preccurlyeq T \sqsubseteq T_n$ and $\mathrm{Dom}(T) = \mathrm{Dom}(T_n)$ we have either $(T^*, T \sqcap Z_n)$ is bad or $(T, Z_n)^\omega \subseteq \bar{\mathcal{O}}$. Let T_{n+1} be such that $T_n^* \preccurlyeq T_{n+1}^* \preccurlyeq Z_n$

and $|T_{n+1}| = |T_n| + 1$. By applying CLAIM 1 to every $T \in (\mathbb{N})$ with $T_0 \preccurlyeq T \sqsubseteq T_{n+1}$ and $\mathrm{Dom}(T) = \mathrm{Dom}(T_{n+1})$, we find a $Z_{n+1} \in (T^*_{n+1}, Z_n)^\omega$ such that for all $T \in (\mathbb{N})$ with $T_0 \preccurlyeq T \sqsubseteq T_{n+1}$ and $\mathrm{Dom}(T) = \mathrm{Dom}(T_{n+1})$, we have either $(T^*, T \sqcap Z_{n+1})$ is bad or $(T, Z_{n+1})^\omega \subseteq \bar{\mathcal{O}}$. Let $Y = \bigcup_{n\in\omega} T_n$, *i.e.*, Y is the only (infinite) partition such that for all $n \in \omega$, $T_n \preccurlyeq Y$.

Assume towards a contradiction that $(S, Y)^\omega \cap \bar{\mathcal{O}} \neq \emptyset$. Then there are $T \in (\mathbb{N})$ with $S \preccurlyeq T \sqsubseteq Y$ such that $(T, Y)^\omega \subseteq \bar{\mathcal{O}}$, *i.e.*, $(T, T \sqcap Y)$ is good. Choose T_0 (with $S \preccurlyeq T_0 \sqsubseteq Y$) of least cardinality such that $(T_0, T_0 \sqcap Y)$ is good. Since (S, Y) is ugly, $|T_0| > |S|$. Hence, we find a $T_1 \sqsubseteq Y$ with $S \preccurlyeq T_1^* \preccurlyeq T_0$ and $|T_1| = |T_0| - 1$. By construction of Y, $(T_1, T_1 \sqcap Y)$ is either ugly or good. In the former case, $(T_0, T_0 \sqcap Y)$ would be bad (a contradiction to the choice of T_0), and in the latter case, T_0 would not be of least cardinality (again a contradiction to the choice of T_0). Thus, $(S, Y)^\omega \cap \bar{\mathcal{O}} = \emptyset$, which completes the proof. $\dashv_{\text{Claim 2}}$

Now, let φ be a sentence of the forcing language. With respect to φ we define $\mathcal{O}_1 := \{q \in M^* : q \Vdash_{\mathbb{M}^*} \varphi\}$ and $\mathcal{O}_2 := \{q \in M^* : q \Vdash_{\mathbb{M}^*} \neg\varphi\}$. Notice that $\mathcal{O}_1 \cup \mathcal{O}_2$ is an open dense subset of M^*. If the $\mathbb{M}^*$-condition (S_0, X_0) is good with respect to $\bar{\mathcal{O}}_1$, there is a $Y_0 \in (S_0, X_0)^\omega$ such that $(S_0, Y_0)^\omega \subseteq \bar{\mathcal{O}}_1$. Otherwise, if (S_0, X_0) is bad with respect to $\bar{\mathcal{O}}_1$, by CLAIM 2 there is a $Y_0 \in (S_0, X_0)^\omega$ such that $(S_0, Y_0)^\omega \cap \bar{\mathcal{O}}_1 = \emptyset$. In the former case we have $(S_0, Y_0) \Vdash_{\mathbb{M}^*} \varphi$ and we are done. In the latter case we proceed as follows: Since $(S_0, Y_0)^\omega \cap \bar{\mathcal{O}}_1 = \emptyset$ and $\mathcal{O}_1 \cup \mathcal{O}_2$ is dense, for every $(S_0, Z_0) \geq (S_0, Y_0)$ there exists a $(T, Z) \geq (S_0, Z_0)$ such that $(T, Z) \in \mathcal{O}_2$. This implies that (S_0, Y_0) cannot be bad with respect to $\bar{\mathcal{O}}_2$, since otherwise, by CLAIM 2 we would find an $(S_0, Z_0) \geq (S_0, Y_0)$ such that $(S_0, Z_0)^\omega \cap (\overline{\mathcal{O}_1 \cup \mathcal{O}_2}) = \emptyset$. Thus, (S_0, Y_0) is good with respect to $\bar{\mathcal{O}}_2$ and we find $(S_0, Y_0') \geq (S_0, Y_0)$ such that $(S_0, Y_0')^\omega \subseteq \bar{\mathcal{O}}_2$, *i.e.*, $(S_0, Y_0') \Vdash_{\mathbb{M}^*} \neg\varphi$. $\dashv$

Now, having THEOREM 26.2 at hand, it is not hard to show that dual Mathias forcing is proper and has the Laver property: Firstly, notice that to each $G \subseteq M^*$ which is $\mathbb{M}^*$-generic over some model $\mathbf{V}$ there exists a unique infinite partition $X_G \in (\omega)^\omega$ with the property that for all $S \in (\mathbb{N})$,

$$S \preccurlyeq X_G \iff \exists Y \in (\omega)^\omega \big((S, Y) \in G\big)\,.$$

Thus, every $\mathbb{M}^*$-generic set $G \subseteq M^*$ corresponds to a unique $\mathbb{M}^*$-generic partition $X_G \in (\omega)^\omega$, which we call **Mathias partition**. Following the proof of COROLLARY 24.6 we can show that if X_G is a Mathias partition over $\mathbf{V}$ and $Y \sqsubseteq X_G$ is an infinite partition, then Y is a Mathias partition over $\mathbf{V}$, too. Furthermore, by similar arguments as in the proofs of COROLLARIES 24.7 & 24.8, one can show that dual Mathias forcing is proper and has the Laver property, in particular, dual Mathias forcing does not add Cohen reals (the details are left as an exercise to the reader).

A feature of Mathias forcing is that it can be written as a two-step iteration. More precisely, $\mathbb{M} \approx \mathbb{U} * \mathbb{M}_{\underset{\sim}{\mathscr{U}}}$, where $\underset{\sim}{\mathscr{U}}$ is the canonical $\mathbb{U}$-name for the $\mathbb{U}$-generic ultrafilter (see LEMMA 24.10). Before we can prove the corresponding result with respect to dual Mathias forcing, we have to introduce a dual form of $\mathbb{U}$ and have to define restricted dual Mathias forcing: Firstly, for $X, Y \in (\omega)^\omega$ let $Y \sqsubseteq^* X \iff \exists F \in \text{fin}(\omega)\big(Y \sqcap \{F\} \sqsubseteq X\big)$; notice that $\{F\}$ is a one-block partition with domain F. Now, let $\mathbb{U}^* = \big((\omega)^\omega, \leq\big)$, where

$$X \leq Y \iff Y \sqsubseteq^* X .$$

Strictly speaking, $\big((\omega)^\omega, \leq\big)$ is not a partially ordered set since "$\leq$" is not anti-symmetric (*i.e.*, $X \leq Y$ and $Y \leq X$ does not imply $X = Y$). However, it is slightly easier to drop anti-symmetry than to work with equivalence classes.

Furthermore, for any family of infinite partitions $\mathscr{F}^* \subseteq (\omega)^\omega$, let $\mathbb{M}^*_{\mathscr{F}^*} = (M^*_{\mathscr{F}^*}, \leq)$, where $M^*_{\mathscr{F}^*}$ is the set of all $\mathbb{M}^*$-conditions (S, X) such that $X \in \mathscr{F}^*$. Now, the dual form of LEMMA 24.10 reads as follows.

LEMMA 26.3. *$\mathbb{M}^* \approx \mathbb{U}^* * \mathbb{M}^*_{\underset{\cdot}{\mathscr{U}}^*}$, where $\underset{\cdot}{\mathscr{U}}^*$ is the canonical $\mathbb{U}^*$-name for the $\mathbb{U}^*$-generic filter.*

Before we prove LEMMA 26.3, we first show that the forcing notion $\mathbb{U}^*$ is σ-closed and that it adds Ramsey ultrafilters.

LEMMA 26.4. *The forcing notion $\mathbb{U}^*$ is σ-closed, and whenever $\mathscr{U}^*$ is $\mathbb{U}^*$-generic over $\mathbf{V}$, then there is a Ramsey ultrafilter in $V[\mathscr{U}^*]$.*

Proof. $\mathbb{U}^*$ is σ-closed: Let $X_0 \leq X_1 \leq \cdots$ be an increasing sequence of infinite partitions (*i.e.*, for all $i \in \omega$, $X_{i+1} \sqsubseteq^* X_i$). Choose a sequence $\langle F_i : i \in \omega\rangle$ of finite sets of natural numbers such that for all $i \in \omega$, $X_{i+1} \sqcap \{F_i\} \sqsubseteq X_i$. For every $X \in (\omega)^\omega$, order the blocks of X by their least element, and for $k \in \omega$, let $X(k)$ denote the k^{th} block with respect to this ordering. Define $y_0 := X_0(0)$, and for positive integers n, let $y_n := X_n(k)$, where $k := n + \bigcup_{i\in n}(\bigcup F_i)$. Now, let $Y := \{y_i : i \in \omega\} \cup (\omega \setminus \bigcup_{i\in\omega} y_i)$. Then, for each $i \in \omega$ we have $Y \sqsubseteq^* X_i$, which shows that $\mathbb{U}^*$ is σ-closed.

$\mathbb{U}^*$ adds Ramsey ultrafilters: We show that the set $\big\{\text{Min}(X) \setminus \{0\} : X \in \mathscr{U}^*\big\}$ is a Ramsey ultrafilter over $\omega \setminus \{0\}$: Firstly, recall that a forcing notion which is σ-closed does not add new reals to the ground model (see LEMMA 14.17). Let $\pi : [\omega]^2 \to 2$ be an arbitrary colouring and let $Y \in (\omega)^\omega$. Then, by RAMSEY'S THEOREM 2.1, there exists an infinite set $x \subseteq \text{Min}(Y)$ with $0 \notin x$ such that π is constant on $[x]^2$. Now, let

$$X = \big\{b : b \in Y \wedge \min(b) \in x\big\} \cup \bigcup \big\{b : b \in Y \wedge \min(b) \notin x\big\} .$$

Then $X \sqsubseteq Y$, $X \in (\omega)^\omega$, and $\text{Min}(X) \setminus \{0\} = x$. Consequently we get that

$$D_\pi := \big\{X \in (\omega)^\omega : \pi|_{[\text{Min}(X)\setminus\{0\}]^2} \text{ is constant}\big\}$$

is open dense, which implies that $D_\pi \cap \mathscr{U}^* \neq \emptyset$. Finally, since the colouring π was arbitrary, this shows that $\big\{\text{Min}(X) \setminus \{0\} : X \in \mathscr{U}^*\big\}$ is a Ramsey ultrafilter over $\omega \setminus \{0\}$. $\dashv$

As a consequence we get the following

FACT 26.5. *Forcing with $\mathbb{U}^*$ does not add new partitions to the ground model.*

Proof. First, notice that partitions X can be encoded by real numbers $r_X \subseteq \omega$, for example let

$$r_X = \big\{k \in \omega : \exists n, m \in \omega\big(k = \eta\{n,m\} \wedge \exists l\big(\{n,m\} \subseteq X(l)\big)\big)\big\},$$

where η is a bijection between $\omega \times \omega$ and ω, and $X(l)$ is as above.

Now, by LEMMA 14.17 we know that σ-closed forcing notions do not add new reals — and therefore no new partitions — to the ground model. ⊣

Now we are ready to give the

Proof of LEMMA 26.3. Since $\mathbb{U}^*$ does not add new partitions, for every $\mathbb{U}^*$-name $\underset{\sim}{(T,Y)}$ for an $\mathbb{M}^*_{\underset{\sim}{\mathscr{U}^*}}$-condition, and for every partition $Z \in (\omega)^\omega$, there is an $\mathbb{M}^*$-condition (S,X) in the ground model as well as a partition $Z' \sqsubseteq^* Z$ such that

$$Z' \Vdash_{\mathbb{U}^*} \underset{\cdot}{(S,X)} = \underset{\sim}{(T,Y)}\,.$$

We leave it as an exercise to the reader to show that

$$\begin{aligned} h:\quad M^* \quad &\longrightarrow \quad (\omega)^\omega \times M^*_{\underset{\sim}{\mathscr{U}^*}} \\ (S,X) \quad &\longmapsto \quad \big\langle X, \underset{\cdot}{(S,X)}\big\rangle \end{aligned}$$

is a dense embedding. Hence, by FACT 14.3, dual Mathias forcing $\mathbb{M}^*$ is equivalent to the two-step iteration $\mathbb{U}^* * \mathbb{M}^*_{\underset{\sim}{\mathscr{U}^*}}$. ⊣

At this point, we would like to say a few words about the two-step iterations $\mathbb{U} * \mathbb{M}_{\underset{\cdot}{\mathscr{U}}}$ and $\mathbb{U}^* * \mathbb{M}^*_{\underset{\cdot}{\mathscr{U}^*}}$ respectively: At first glance, the iterations look very similar and in both cases we start with a forcing notion which is σ-closed. However, $\mathbb{M}_{\mathscr{U}}$ satisfies *ccc*, which is not the case for $\mathbb{M}^*_{\underset{\cdot}{\mathscr{U}^*}}$. The reason for this is that partitions of ω — in contrast to subsets of ω — do not have "complements", which changes the situation drastically, especially when we work with partition ultrafilters (see below).

In order to investigate dual Mathias forcing in greater details, we have to define first a dual form of the shattering cardinal $\mathfrak{h}$: Two partitions $X, Y \in (\omega)^\omega$ are called **almost orthogonal**, denoted $X \perp_* Y$, if $X \sqcap Y \notin (\omega)^\omega$, otherwise they are called **compatible**. A family $\mathscr{A}^* \subseteq (\omega)^\omega$ is called **maximal almost orthogonal** (*mao*) if $\mathscr{A}^*$ is a maximal family of pairwise almost orthogonal partitions. Furthermore, a family $\mathscr{H}^*$ of *mao* families of partitions **shatters** a partition $X \in (\omega)^\omega$, if there are $\mathscr{A}^* \in \mathscr{H}^*$ and two distinct partitions $Y, Y' \in \mathscr{A}^*$ such that X is compatible with both Y and Y'. Finally, a family of *mao* families of partitions is **shattering**, if it shatters each member of $(\omega)^\omega$. Now, the **dual shattering number $\mathfrak{H}$** is the smallest cardinality of a shattering family; more formally

$$\mathfrak{H} = \min\left\{|\mathscr{H}^*| : \mathscr{H}^* \text{ is shattering}\right\}.$$

What can we say about the size of $\mathfrak{H}$? Now, like for $\mathfrak{h}$ we can show that the cardinal $\mathfrak{H}$ is uncountable and less than or equal to $\mathfrak{c}$.

FACT 26.6. $\omega_1 \leq \mathfrak{H} \leq \mathfrak{c}$.

Proof. $\omega_1 \leq \mathfrak{H}$: Let $\mathscr{H}^*_\omega = \{\mathscr{A}^*_n : n \in \omega\}$ be a countable set of *mao* families. We construct a partition $X \in (\omega)^\omega$ which is not shattered by $\mathscr{H}^*_\omega$: Let $X_0 \in \mathscr{A}^*_0$, and for $n \in \omega$, let $X_{n+1} = X_n \sqcap Y_{n+1}$, where $Y_n \in \mathscr{A}^*_{n+1}$ is such that $X_n \sqcap Y_{n+1} \in (\omega)^\omega$. Then, by the first part of LEMMA 26.4, there exists an X such that for all $n \in \omega$, $X \sqsubseteq^* X_n$.

$\mathfrak{H} \leq \mathfrak{c}$: Recall that each partition $X \in (\omega)^\omega$ can be encoded by a real r_X. Now, for each $X \in (\omega)^\omega$ choose a *mao* family $\mathscr{A}^*_X$ which contains two distinct partitions $Y_0, Y_1 \in (\omega)^\omega$ such that both, Y_0 and Y_1, are compatible with X. Then $\left\{\mathscr{A}^*_X : X \in (\omega)^\omega\right\}$ is a shattering family of cardinality less than or equal to $\mathfrak{c}$. ⊣

Compared to other cardinal characteristics of the continuum, $\mathfrak{H}$ is quite small, in fact we get

PROPOSITION 26.7. $\mathfrak{H} \leq \mathfrak{h}$.

Proof. Notice first that for every *mad* family $\mathscr{A} \subseteq [\omega]^\omega$ there is a *mao* family $\mathscr{A}^* \subseteq (\omega)^\omega$ consisting of partitions $X \in (\omega)^\omega$ such that $\mathrm{Min}(X) \setminus \{0\}$ is contained in some element of $\mathscr{A}$. Let $\mathscr{H} = \{\mathscr{A}_\xi : \xi \in \mathfrak{h}\}$ be a shattering family of *mad* families and let $\mathscr{H}^* = \{\mathscr{A}^*_\xi : \xi \in \mathfrak{h}\}$ be the corresponding family of *mao* families. By contraposition we show that if $\mathscr{H}^*$ is not shattering, then also $\mathscr{H}$ is not shattering: So, suppose that $\mathscr{H}^*$ is not shattering. Then there is a partition $X \in (\omega)^\omega$ which is not shattered by $\mathscr{A}^*_\xi$ (for any $\xi \in \mathfrak{h}$). Thus, for every $\xi \in \mathfrak{h}$, we find an $X_\xi \in \mathscr{A}^*_\xi$ such that $X \sqsubseteq^* X_\xi$, and therefore, $\mathrm{Min}(X) \subseteq \mathrm{Min}(X_\xi)$. Hence, $\mathrm{Min}(X)$ is not shattered by any $\mathscr{A}_\xi$, which shows that $\mathscr{H}$ is not a shattering family. ⊣

Another small cardinal characteristic which is less than or equal to $\mathfrak{h}$ is $\mathfrak{p}$. So, it is natural to compare $\mathfrak{H}$ with $\mathfrak{p}$. On the one hand, one can show that $\mathfrak{p} = \mathfrak{H} < \mathfrak{h}$ is consistent with ZFC (see RELATED RESULT 151). On the other hand, one can show that also $\mathfrak{H} < \mathfrak{h} = \mathfrak{p}$ is consistent with ZFC (see RELATED RESULT 152). Hence, $\mathfrak{H}$ can be small even in the case when $\mathfrak{p}$ or $\mathfrak{h}$ is large. However, by a countable support iteration of dual Mathias forcing we can enlarge $\mathfrak{H}$ without changing the size of $\mathfrak{p}$ and show that also $\mathfrak{p} < \mathfrak{H} = \mathfrak{h}$ is consistent with ZFC.

PROPOSITION 26.8. $\mathfrak{p} = \mathit{cov}(\mathcal{M}) < \mathfrak{H} = \mathfrak{h}$ *is consistent with* ZFC.

Proof (Sketch). Since $\mathfrak{p} \leq \mathit{cov}(\mathcal{M})$ (by THEOREM 21.5), and since $\omega_1 \leq \mathfrak{p}$, it is enough to show that $\omega_1 = \mathit{cov}(\mathcal{M}) < \mathfrak{H} = \omega_2$ is consistent with ZFC.

We can just follow PROPOSITION 24.12 (replacing Mathias forcing with dual Mathias forcing). Thus, let $\mathbb{P}_{\omega_2} = \langle \underset{\sim}{\mathbb{Q}}_\alpha : \alpha \in \omega_2 \rangle$ be a countable support iteration of dual Mathias forcing and let G be $\mathbb{P}_{\omega_2}$-generic over some model $\mathbf{V}$ of $\mathsf{ZFC} + \mathsf{CH}$.

Firstly, show that $\mathbf{V}[G] \vDash \mathfrak{H} = \mathfrak{h} = \omega_2$: For this, use the fact that dual Mathias forcing, like Mathias forcing, is proper, that $\mathbb{M}^* \approx \mathbb{U}^* * \mathbb{M}^*_{\underset{\sim}{\mathscr{U}}^*}$, and that $\mathfrak{H} \leq \mathfrak{h}$.

Secondly, show that $\mathbf{V}[G] \vDash \omega_1 = cov(\mathcal{M})$: For this, use the fact that dual Mathias forcing, like Mathias forcing, has the Laver property and therefore does not add Cohen reals. Furthermore, recall that the Laver property is preserved under countable support iteration of proper forcing notions and that $cov(\mathcal{M})$ remains unchanged if no Cohen reals are added. Thus, since $\mathbf{V} \vDash \mathsf{CH}$, we get $\mathbf{V}[G] \vDash \omega_1 = cov(\mathcal{M})$. $\dashv$

A Dual Form of Ramsey Ultrafilters

In Chapter 10 we have seen several equivalent definitions of Ramsey ultrafilters. For example, a filter $\mathscr{U} \subseteq [\omega]^\omega$ is a Ramsey ultrafilter if for every colouring $\pi : [\omega]^2 \to 2$ there is an $x \in \mathscr{U}$ such that $\pi|_{[x]^2}$ is constant, which is equivalent to saying that the MAIDEN does not have a winning strategy in the game $\mathcal{G}_{\mathscr{U}}$, defined by

$$\mathcal{G}_{\mathscr{U}}: \quad \begin{array}{lccccccccccccc} \text{MAIDEN} & x_0 & & \supseteq & & x_1 & & \supseteq & & x_2 & & \supseteq & & \\ & & \searrow^{\ni} & & \nearrow & & \searrow^{\ni} & & \nearrow & & \searrow^{\ni} & & \nearrow & \cdots \\ \text{DEATH} & & & a_0 & & < & & a_1 & & < & & a_2 & & < \end{array}$$

in which DEATH wins the game $\mathcal{G}_{\mathscr{U}}$ if and only if $\{a_i : i \in \omega\}$ belongs to $\mathscr{U}$.

Moreover, by Chapter 10 | RELATED RESULT 71, $\mathscr{U} \subseteq [\omega]^\omega$ is a Ramsey ultrafilter *iff* the MAIDEN does not have a winning strategy in the game $\mathcal{G}'_{\mathscr{U}}$, defined by

$$\mathcal{G}'_{\mathscr{U}}: \quad \begin{array}{lccccccccccc} \text{MAIDEN} & (a_0, x_0) & & & & (a_1, x_1) & & & & (a_2, x_2) & & \\ & & \searrow & & \nearrow & & \searrow & & \nearrow & & \searrow & \nearrow \cdots \\ \text{DEATH} & & & y_0 & & & & y_1 & & & & y_2 \end{array}$$

in which the MAIDEN wins the game $\mathcal{G}'_{\mathscr{U}}$ if and only if $\{a_i : i \in \omega\}$ does *not* belong to $\mathscr{U}$. The dual form of the latter game is in fact just the game $\mathcal{G}_{\mathscr{U}^*}$ which we introduced in Chapter 11:

$$\mathcal{G}_{\mathscr{U}^*}: \quad \begin{array}{lccccccccccc} \text{MAIDEN} & (S_0, X_0) & & & & (S_1, X_1) & & & & (S_2, X_2) & & \\ & & \searrow & & \nearrow & & \searrow & & \nearrow & & \searrow & \nearrow \cdots \\ \text{DEATH} & & & Y_0 & & & & Y_1 & & & & Y_2 \end{array}$$

In that game, we require that the first move (S_0, X_0) of the MAIDEN is such that $X_0 \in \mathscr{U}^*$ and that $(S_0^*, X_0)^\omega$ is a dual Ellentuck neighbourhood. Furthermore, we require that for each $n \in \omega$, the n^{th} move of DEATH Y_n is such that $Y_n \in (S_n^*, X_n)^\omega$ and $Y_n \in \mathscr{U}^*$, and that the MAIDEN plays (S_{n+1}, X_{n+1}) such that

- $S_n^* \preccurlyeq S_{n+1}$, $|S_{n+1}| = |S_n| + 1$, $S_{n+1}^* \sqsubseteq Y_n$, and
- $X_{n+1} \in (S_{n+1}^*, Y_n)^\omega \cap \mathscr{U}^*$.

Finally, the MAIDEN wins the game $\mathcal{G}_{\mathscr{U}^*}$ if and only if the (unique) infinite partition $X \in (\omega)^\omega$ such that $S_n \preccurlyeq X$ (for all $n \in \omega$) does *not* belong to the family $\mathscr{U}^*$.

With respect to the game $\mathcal{G}_{\mathscr{U}^*}$ we define dual Ramsey ultrafilters as follows (for another dual form of Ramsey ultrafilters see RELATED RESULT 158): A family $\mathscr{F}^* \subseteq (\omega)^\omega$ is a **partition-filter** if $\mathscr{F}^*$ is closed under refinement and finite coarsening, and if for all $X, Y \in \mathscr{F}^*$ we have $X \sqcap Y \in \mathscr{F}^*$. Furthermore, a partition-filter $\mathscr{U}^* \subseteq (\omega)^\omega$ is a **partition-ultrafilter** if $\mathscr{U}^*$ is not properly contained in any partition-filter. Finally, a partition-ultrafilter $\mathscr{U}^* \subseteq (\omega)^\omega$ is a **Ramsey partition-ultrafilter** if the MAIDEN does not have a winning strategy in the game $\mathcal{G}_{\mathscr{U}^*}$.

It is easy to show that every Ramsey partition-ultrafilter $\mathscr{U}^* \subseteq (\omega)^\omega$ generates a Ramsey ultrafilter $\mathscr{U} \subseteq [\omega]^\omega$. In fact, if $\mathscr{U}^*$ is a Ramsey partition-ultrafilter, then $\{\operatorname{Min}(X) \setminus \{0\} : X \in \mathscr{U}^*\} \subseteq [\omega]^\omega$ is a Ramsey ultrafilter over $\omega \setminus \{0\}$. On the other hand, it is not at all clear whether Ramsey ultrafilters also generate Ramsey partition-ultrafilters — in fact it seems that Ramsey partition-ultrafilters are much stronger than Ramsey ultrafilters. However, the following result shows that the existence of Ramsey partition-ultrafilters is consistent with ZFC.

THEOREM 26.9. *If $\mathscr{U}^*$ is $\mathbb{U}^*$-generic over $\mathbf{V}$, then $\mathscr{U}^*$ is a Ramsey partition-ultrafilter in $\mathbf{V}[\mathscr{U}^*]$.*

Proof. Because $\mathscr{U}^*$ is $\mathbb{U}^*$-generic over $\mathbf{V}$, $\mathscr{U}^* \subseteq (\omega)^\omega$ is a partition-filter in $\mathbf{V}[\mathscr{U}^*]$. Furthermore, since $\mathbb{U}^*$ is σ-closed (by LEMMA 26.4), $\mathbb{U}^*$ does not add new partitions which implies that $\mathscr{U}^*$ is a partition-ultrafilter in $\mathbf{V}[\mathscr{U}^*]$.

It remains to show that in $\mathbf{V}[\mathscr{U}^*]$, the MAIDEN does not have a winning strategy in the game $\mathcal{G}_{\mathscr{U}^*}$. For this, let $\underset{\sim}{\sigma}$ be a $\mathbb{U}^*$-name for a strategy for the MAIDEN in the game $\mathcal{G}_{\underset{\sim}{\mathscr{U}}^*}$, *i.e.*,

$$\mathbf{0} \Vdash_{\mathbb{U}^*} \text{“}\underset{\sim}{\sigma} \text{ is a strategy for the MAIDEN in the game } \mathcal{G}_{\underset{\sim}{\mathscr{U}}^*}\text{”},$$

where $\underset{\sim}{\mathscr{U}}^*$ is the canonical $\mathbb{U}^*$-name for the $\mathbb{U}^*$-generic filter. Let us assume that the MAIDEN follows the strategy $\underset{\sim}{\sigma}[\mathscr{U}^*]$ in the model $\mathbf{V}[\mathscr{U}^*]$. Furthermore, let $Z_0 \in (\omega)^\omega$ be such that

$$Z_0 \Vdash_{\mathbb{U}^*} \underset{\sim}{\sigma}(\emptyset) = (\underset{\sim}{S}_0, \underset{\sim}{X}_0).$$

In particular, since $\underset{\sim}{\sigma}$ is the $\underset{\sim}{\mathscr{U}}$-name for a strategy,

$$Z_0 \Vdash_{\mathbb{U}^*} \underset{\sim}{X}_0 \in \underset{\sim}{\mathscr{U}}^*.$$

Assume that for some $n \in \omega$ we have already constructed an $\mathbb{M}^*$-condition $Z_n \geq Z_0$ such that

$$Z_n \Vdash_{\mathbb{U}^*} \underset{\sim}{\sigma}\big((\underset{\sim}{S}_0, \underset{\sim}{X}_0), \underset{\sim}{Y}_0, \dots, (\underset{\sim}{S}_{n-1}, \underset{\sim}{X}_{n-1}), \underset{\sim}{Y}_{n-1}\big) = (\underset{\sim}{S}_n, \underset{\sim}{X}_n)\,.$$

Then, since does not add new partitions, we find a $\mathbb{U}^*$-condition $Z'_n \geq Z_n$ (*i.e.*, $Z'_n \sqsubseteq^* Z_n$) and a dual Ellentuck neighbourhood (S_n, X_n) in $\mathbf{V}$ such that

$$Z'_n \Vdash_{\mathbb{U}^*} (\underset{\sim}{S}_n, \underset{\sim}{X}_n) = (S_n, X_n)\,.$$

Because $Z'_n \geq Z_n$, we have

$$Z'_n \Vdash_{\mathbb{U}^*} \underset{\sim}{\sigma}\big((\underset{\sim}{S}_0, \underset{\sim}{X}_0), \underset{\sim}{Y}_0, \dots, (\underset{\sim}{S}_{n-1}, \underset{\sim}{X}_{n-1}), \underset{\sim}{Y}_{n-1}\big) = (S_n, X_n)\,.$$

In particular, $Z'_n \Vdash_{\mathbb{U}^*} X_n \in \underset{\sim}{\mathscr{U}}^*$, which implies that Z'_n and X_n are compatible. Finally, Death plays a partition Y_n such that $Y_n \sqsubseteq^* (Z'_n \sqcap X_n)$ and $Y_n \in (S^*_n, X_n)^\omega$. Proceeding this way, we get an increasing sequence $S_0 \preccurlyeq S_1 \preccurlyeq \cdots$ of partitions of $(\mathbb{N})$.

Now, let $W \in (\omega)^\omega$ be the unique partition such that for all $n \in \omega$, $S_n \preccurlyeq W$. Notice that W belongs to $\mathbf{V}$. Then W is an infinite partition (*i.e.*, an $\mathbb{U}^*$-condition), $W \Vdash_{\mathbb{U}^*} W \in \underset{\sim}{\mathscr{U}}^*$, and for each $n \in \omega$, $W \sqsubseteq^* (Z'_n \sqcap X_n)$. Thus, by construction we get

$$W \Vdash_{\mathbb{U}^*} \text{“}\underset{\sim}{\sigma} \text{ is not a winning strategy for the Maiden in the game } \mathcal{G}_{\underset{\sim}{\mathscr{U}}^*}\text{”},$$

and since $\underset{\sim}{\sigma}$ was an arbitrary strategy, the Maiden does not have a winning strategy at all. ⊣

As a consequence we get that the existence of Ramsey partition-ultrafilters is consistent with $\mathsf{ZFC} + \mathsf{CH}$ (just force with $\mathbb{U}^*$ over a model in which CH holds). Unlike for Ramsey ultrafilters, it is not known whether CH implies the existence of Ramsey partition-ultrafilters. On the other hand, replacing $\mathbb{U}$ with $\mathbb{U}^*$ in the proof that ultrafilter forcing $\mathbb{U}$ collapses $\mathfrak{c}$ to $\mathfrak{h}$ (see Chapter 25 | Related Result 144), one can show that the forcing notion $\mathbb{U}^*$ collapses $\mathfrak{c}$ to $\mathfrak{H}$, and since $\mathfrak{H} > \omega_1$ is consistent with ZFC (by Proposition 26.8), we get that the existence of Ramsey partition-ultrafilters is also consistent with $\mathsf{ZFC} + \neg\mathsf{CH}$.

Notes

Dual Mathias forcing was introduced and investigated by Carlson and Simpson in [4] (*e.g.*, they showed that dual Mathias forcing has pure decision). The dual shattering number was introduced and investigated by Cichoń, Krawczyk, Majcher-Iwanow, and Węglorz in [5] (*e.g.*, they showed that $\mathfrak{H} \leq \mathfrak{h}$). However, most of the results presented in this chapter are taken from Halbeisen [6, 7].

Related Results

150. *Dualising cardinal characteristics of the continuum.* The first who studied systematically the dual forms of cardinal characteristics of the continuum were Cichoń, Krawczyk, Majcher-Iwanow, and Węglorz. For example they showed that $\mathfrak{H}$ is regular, that $\mathfrak{H} \leq \mathfrak{h}$, and that $\mathfrak{R} \leq \mathfrak{r}$. Before their work [5] was published in 2000, the paper was already available as a preprint in 1994 and motivated for example the work of Brendle [2], Spinas [15] and Halbeisen [6].

151. *On the consistency of* $\mathfrak{p} = \mathfrak{H} < \mathfrak{h}$. Spinas [15, Theorem 4.2] showed that in Mathias' model, which is the model we get after a countable support iteration of length ω_2 of Mathias forcing starting in a model of $\mathsf{ZFC} + \mathsf{CH}$, we have $\mathfrak{p} = \mathfrak{H} < \mathfrak{h}$. In particular, this shows that Mathias forcing does not add Mathias partitions; otherwise, by the proof of Proposition 26.8 (originally proved in Halbeisen [6]), we would have $\mathfrak{H} = \mathfrak{h}$ in Mathias' model.

152. *On the consistency of* $\mathfrak{H} < \mathfrak{p}$. Brendle [2] showed that $\mathfrak{H} < \mathfrak{h}$ is consistent with $\mathsf{ZFC} + \mathsf{MA}$. In particular, also $\mathfrak{H} < \mathfrak{p} = \mathfrak{h}$ is consistent with ZFC. To some extent this shows that dual Mathias forcing is far away from being a *ccc* forcing notion, even in the case when we restrict dual Mathias forcing to a partition-ultrafilter.

153. *Dualisations of* $\mathfrak{a}$ *and* $\mathfrak{t}$. We have seen above how one could dualise the shattering cardinal $\mathfrak{h}$, and we have seen that both statements, $\mathfrak{H} = \omega_1 = \mathfrak{H}$ and $\mathfrak{H} = \omega_2$, are consistent with ZFC. Now, it is somewhat surprising that the dual forms of $\mathfrak{a}$ and $\mathfrak{t}$ are absolute (*i.e.*, they cannot be moved). In particular, Krawczyk proved in [5] that the size of a maximal almost orthogonal family (*i.e.*, the dualisation of a *mad* family) is always equal to $\mathfrak{c}$, and Carlson proved that the dual tower number is always equal to ω_1 (see Matet [13, Proposition 43]).

154. *Converse dual cardinal characteristics.* If we replace the ordering "$\sqsubseteq$" on $(\omega)^\omega$ with "$\sqsupseteq$", we obviously get other kinds of dual cardinal characteristics: The so-called *converse dual cardinal characteristics* were first introduced and investigated by Majcher-Iwanow [12], whose work was continued by Brendle and Zhang in [3], where it is shown for example that the converse dual tower number is equal to $\mathfrak{p}$.

155. *The dual Ramsey property.* In Chapter 9 we have seen that the shattering cardinal $\mathfrak{h}$ is closely related to the Ramsey property. Now, one can show in a similar way that the dual shattering cardinal $\mathfrak{H}$ is closely related to the so-called *dual Ramsey property*, which was introduced and investigated by Carlson and Simpson in [4], and further investigated by Halbeisen in [6, 7] and by Halbeisen and Löwe in [9].

156. *Ultrafilter spaces on the semilattice of partitions.* There is essentially just one way to define a topology on the set of ultrafilters over ω. This topological space is usually denoted by $\beta\omega$ (*cf.* Chapter 9 | Related Result 63). On the other hand, there are four natural ways to define a topology on the set of partition-ultrafilters. Moreover, one can show that the corresponding four spaces of partition-ultrafilters are pairwise non-homeomorphic, but still have some of the nice properties of $\beta\omega$ (see Halbeisen and Löwe [10]).

157. *Partition-filters.* In [14], Matet introduced partition-filters associated with Hindman's Theorem and the Milliken-Taylor Theorem respectively (see

Chapter 2 | Related Result 3) and investigated the existence as well as combinatorial properties of these partition-filters. For a slightly different approach to filters associated to Hindman's Theorem see Blass [1].

158. *Ramsey partition-ultrafilters versus Ramseyan ultrafilters*.* Above, we have introduced Ramsey partition-ultrafilters in terms of the game $\mathcal{G}_{\mathscr{U}^*}$, which is, by Chapter 10 | Related Result 71, related to Ramsey ultrafilters $\mathscr{U} \subseteq [\omega]^\omega$. Furthermore, we have seen that the existence of these Ramsey partition-ultrafilters is consistent with ZFC (see also Halbeisen [7, Theorem 5.1]). Ramsey partition-ultrafilters have very strong combinatorial properties (see for example Halbeisen and Matet [11]), and it seems that they are significantly stronger than Ramsey ultrafilters. For example it is not known whether CH implies the existence of Ramsey partition-ultrafilters, whereas CH implies the existence of $2^{\mathfrak{c}}$ mutually non-isomorphic Ramsey ultrafilters (see Chapter 10 | Related Result 64). Now, instead of defining Ramsey partition-ultrafilters in terms of the game $\mathcal{G}_{\mathscr{U}^*}$, we could equally well take another approach: In Chapter 10 we defined Ramsey ultrafilters in terms of colourings of $[\omega]^2$, *i.e.*, $\mathscr{U} \subseteq [\omega]^\omega$ is a Ramsey ultrafilter if for every colouring $\pi : [\omega]^2 \to 2$ there is an $x \in \mathscr{U}$ such that $\pi|_{[x]^2}$ is constant. Dualising — and slightly strengthening — this property, we get what is called a Ramseyan ultrafilter. A partition-ultrafilter $\mathscr{U}^* \subseteq (\omega)^\omega$ is a *Ramseyan ultrafilter* if for every finite colouring of $(\omega)^{(n)}$, there is an $X \in \mathscr{U}^*$ such that $(X)^{(n)^*}$ is monochromatic. Unlike for Ramsey partition-ultrafilters, it is known that CH implies that there are $2^{\mathfrak{c}}$ mutually non-isomorphic Ramseyan ultrafilters (see Halbeisen [8, Theorem 2.2.1]). Thus, it seems that Ramseyan ultrafilters are somewhat weaker than Ramsey partition-ultrafilters — but it is also possible that they are equivalent.

References

1. Andreas Blass, *Ultrafilters related to Hindman's finite-unions theorem and its extensions*, in ***Logic and Combinatorics*** (Stephen G. Simpson, ed.), Contemporary Mathematics, vol. 65, [Proceedings of a Summer Research Conference held August 4–10, 1985], American Mathematical Society, Providence, RI, 1987, pp. 89–124.
2. Jörg Brendle, *Martin's axiom and the dual distributivity number*, ***Mathematical Logic Quarterly***, vol. 46 (2000), 241–248.
3. Jörg Brendle and Shuguo Zhang, *Converse dual cardinals*, ***The Journal of Symbolic Logic***, vol. 71 (2006), 22–34.
4. Timothy J. Carlson and Steve G. Simpson, *A dual form of Ramsey's Theorem*, ***Advances in Mathematics***, vol. 53 (1984), 265–290.
5. Jacek Cichoń, Adam Krawczyk, Barbara Majcher-Iwanow, and Bogdan Węglorz, *Dualization of the van Douwen diagram*, ***The Journal of Symbolic Logic***, vol. 65 (2000), 959–968.
6. Lorenz Halbeisen, *On shattering, splitting and reaping partitions*, ***Mathematical Logic Quarterly***, vol. 44 (1998), 123–134.
7. ———, *Symmetries between two Ramsey properties*, ***Archive for Mathematical Logic***, vol. 37 (1998), 241–260.
8. ———, *Ramseyan ultrafilters*, ***Fundamenta Mathematicae***, vol. 169 (2001), 233–248.

9. Lorenz Halbeisen and Benedikt Löwe, *Techniques for approaching the dual Ramsey property in the projective hierarchy*, ***Pacific Journal of Mathematics***, vol. 200 (2001), 119–145.
10. ———, *Ultrafilter spaces on the semilattice of partitions*, ***Topology and its Applications***, vol. 115 (2001), 317–332.
11. Lorenz Halbeisen and Pierre Matet, *A generalization of the dual Ellentuck theorem*, ***Archive for Mathematical Logic***, vol. 42 (2003), 103–128.
12. Barbara Majcher-Iwanow, *Cardinal invariants of the lattice of partitions*, ***Commentationes Mathematicae Universitatis Carolinae***, vol. 41 (2000), 543–558.
13. Pierre Matet, *Partitions and filters*, ***The Journal of Symbolic Logic***, vol. 51 (1986), 12–21.
14. ———, *Some filters of partitions*, ***The Journal of Symbolic Logic***, vol. 53 (1988), 540–553.
15. Otmar Spinas, *Partition numbers*, ***Annals of Pure and Applied Logic***, vol. 90 (1997), 243–262.

27

Suite

In this chapter we shall demonstrate how the tools we developed in the previous chapters can be used to shed new light on a classical problem in Measure Theory.

Assuming the Continuum Hypothesis, Banach and Kuratowski proved a combinatorial theorem which implies that a finite measure defined for each subset of $\mathbb{R}$ vanishes identically if it is zero for points (for the notion of *measure* we refer the reader to Oxtoby [3, p. 14]). We shall consider this result — which will be called BANACH-KURATOWSKI THEOREM — from a set-theoretical point of view, and among others it will be shown that the BANACH-KURATOWSKI THEOREM is equivalent to the existence of a K-Lusin set of size $\mathfrak{c}$ and that the existence of such a set is independent of $\mathsf{ZFC} + \neg\mathsf{CH}$.

The original proof of the BANACH-KURATOWSKI THEOREM is due to Banach and Kuratowski [1], THEOREM 27.1 is due to Halbeisen, and the non-classical results of this chapter are all due to Bartoszyński. References and some more results related to the BANACH-KURATOWSKI THEOREM can be found in Bartoszyński and Halbeisen [2].

Prelude

Historical background. In a paper of 1929, Banach and Kuratowski investigated the following problem in Measure Theory: *Does there exist a non-vanishing finite measure defined for each subset of* $\mathbb{R}$ *which is zero for points?* They showed that such a measure does not exist if one assumes CH. In fact, assuming CH, they proved the following combinatorial theorem and showed that it implies the non-existence of such a measure (notice that it is sufficient to consider just measures on subsets of the unit interval $[0,1]$).

THEOREM OF BANACH AND KURATOWSKI. *If* CH *holds, then there is an infinite matrix* $A^i_k \subseteq [0,1]$, *where* $i,k \in \omega$, *such that:*

(a) *For each* $i \in \omega$, $[0,1] = \bigcup_{k\in\omega} A^i_k$.

(b) *For each $i \in \omega$, if $k \neq k'$ then $A^i_k \cap A^i_{k'} = \emptyset$.*

(c) *For every infinite sequence $\langle k_0, k_1, \dots, k_i, \dots\rangle$ of natural numbers,*

$$\bigcap_{i\in\omega} \left(A^i_0 \cup A^i_1 \cup \ldots \cup A^i_{k_i}\right) \quad \textit{is countable}.$$

Below, we call an infinite matrix $A^i_k \subseteq [0,1]$ (where $i, k \in \omega$) for which (a), (b), and (c) hold a **BK-Matrix**.

Concerning the measure-theoretical problem we would like to mention that Ulam [4] proved the following generalisation of the BANACH-KURATOWSKI THEOREM: *If no cardinal less than or equal to $\mathfrak{c}$ is weakly inaccessible, then every finite measure defined for all subset of $\mathbb{R}$ which is zero for points vanishes identically.* For further results in this context we refer the reader to Oxtoby [3, Chapter 5].

Allemande

A cardinal characteristic called $\mathfrak{l}$. Before we give a slightly modified version of the original proof of the BANACH-KURATOWSKI THEOREM we introduce the following notion.

Recall that for functions $f, g \in {}^\omega\omega$, $f \leq g \iff f(n) \leq g(n)$ for all $n \in \omega$. Now, for $\mathscr{F} \subseteq {}^\omega\omega$, let $\lambda(\mathscr{F})$ denote the least cardinality such that for each $g \in {}^\omega\omega$, the cardinality of the set $\{f \in \mathscr{F} : f \leq g\}$ is strictly less than $\lambda(\mathscr{F})$. For any family $\mathscr{F} \subseteq {}^\omega\omega$ we obviously have $\lambda(\mathscr{F}) \leq \mathfrak{c}^+$. Furthermore, for families $\mathscr{F} \subseteq {}^\omega\omega$ of size $\mathfrak{c}$ one can easily show that $\omega_1 \leq \lambda(\mathscr{F})$. Thus, for families $\mathscr{F} \subseteq {}^\omega\omega$ of size $\mathfrak{c}$ we have $\omega_1 \leq \lambda(\mathscr{F}) \leq \mathfrak{c}^+$, which leads to the following definition:

$$\mathfrak{l} = \min\left\{\lambda(\mathscr{F}) : \mathscr{F} \subseteq {}^\omega\omega \wedge |\mathscr{F}| = \mathfrak{c}\right\}$$

If one assumes CH, then one can easily construct a family $\mathscr{F} \subseteq {}^\omega\omega$ of cardinality $\mathfrak{c}$ such that $\lambda(\mathscr{F}) = \omega_1$, hence, CH implies $\mathfrak{l} = \omega_1$.

In our notation, the crucial point in the original proof of Banach and Kuratowski reads as follows.

THEOREM 27.1. *The existence of a BK-Matrix is equivalent to $\mathfrak{l} = \omega_1$.*

Proof. ($\Leftarrow$) Let $\mathscr{F} \subseteq {}^\omega\omega$ be a family of cardinality $\mathfrak{c}$ with $\lambda(\mathscr{F}) = \omega_1$. In particular, for each $g \in {}^\omega\omega$, the set $\{f \in \mathscr{F} : f \leq g\}$ is at most countable. Since the interval $[0,1]$ has cardinality $\mathfrak{c}$, there is a one-to-one function h from $[0,1]$ onto $\mathscr{F}$. For $x \in [0,1]$, let $n^x_i := h(x)(i)$. Now, for $i, k \in \omega$, define the sets $A^i_k \subseteq [0,1]$ as follows:

$$x \in A^i_k \iff k = n^x_i\,.$$

We leave it as an exercise to the reader to check that these sets satisfy the conditions (a) and (b) of a BK-Matrix. For (c), take any sequence $\langle k_0, k_1, \ldots, k_i, \ldots\rangle$ of ω and pick an arbitrary $x \in \bigcap_{i\in\omega}(A^i_0 \cup A^i_1 \cup \ldots \cup A^i_{k_i})$. By definition, for each $i \in \omega$, x is in $A^i_0 \cup A^i_1 \cup \ldots \cup A^i_{k_i}$. Hence, for each $i \in \omega$ we get $n^x_i \leq k_i$, which implies that for $g \in {}^\omega\omega$ with $g(i) := k_i$ we have $h(x) \leq g$. Now, since $\lambda(\mathscr{F}) = \omega_1$, $h(x) \in \mathscr{F}$ and x was arbitrary, the set $\{x \in [0,1] : h(x) \leq g\} = \bigcap_{i\in\omega}\left(A^i_0 \cup A^i_1 \cup \ldots \cup A^i_{k_i}\right)$ is at most countable.

$(\Rightarrow)$ Let $A^i_k \subseteq [0,1]$, where $i, k \in \omega$, be a BK-Matrix and let $\mathscr{F} \subseteq {}^\omega\omega$ be the family of all functions $f \in {}^\omega\omega$ such that $\bigcap_{i\in\omega} A^i_{f(i)}$ is non-empty. Is is easy to see that $\mathscr{F}$ has cardinality $\mathfrak{c}$. Now, for any sequence $\langle k_0, k_1, \ldots, k_i, \ldots\rangle$ of natural numbers, the set $\bigcap_{i\in\omega}(A^i_0 \cup A^i_1 \cup \ldots \cup A^i_{k_i})$ is at most countable, which implies that for $g \in {}^\omega\omega$ with $g(i) := k_i$, the set $\{f \in \mathscr{F} : f \leq g\}$ is at most countable. Hence, $\lambda(\mathscr{F}) = \omega_1$. ⊣

Courante

Lusin and K-Lusin sets. Before we can define the notions of *Lusin* and *K-Lusin* sets respectively, we have to introduce the notion of a *compact* set (for the notions *open*, *closed*, *dense*, and *meagre* we refer the reader to Chapter 21). A set $X \subseteq {}^\omega\omega$ is **compact** if for every set $\mathscr{S} \subseteq \mathrm{seq}(\omega)$ of finite sequences in ω such that $X \subseteq \bigcup_{s\in\mathscr{S}} O_s$, there exists a *finite* subset $\{s_0, \ldots s_{m-1}\} \subseteq \mathscr{S}$ such that $X \subseteq \bigcup_{i\in m} O_{s_i}$. In other words, $X \subseteq {}^\omega\omega$ is compact if every open cover of X has a finite subcover.

The following lemma gives a combinatorial characterisation of compact subsets of ${}^\omega\omega$.

LEMMA 27.2. *The closure of a set $A \subseteq {}^\omega\omega$ is compact if and only if there is a function $f_0 \in {}^\omega\omega$ such that $A \subseteq \{f \in {}^\omega\omega : f \leq f_0\}$.*

Proof. For $A \subseteq {}^\omega\omega$ let $T_A = \{g|_n : g \in A \wedge n \in \omega\}$. Then $(T_A, \subseteq)$ is obviously a tree. Notice that if $\bar{A}$ denotes the closure of A, then $T_A = T_{\bar{A}}$. Now, $(T_A, \subseteq)$ is finitely branching if and only if for each $n \in \omega$, $\{g(n) : g \in A\}$ is finite; in which case we can define $f_0 \in {}^\omega\omega$ by stipulating $f_0(n) := \max\{g(n) : g \in A\}$ (and get that for all $g \in A$, $g \leq f_0$). Thus, it is enough to prove that a closed set A is compact if and only if $(T_A, \subseteq)$ is finitely branching.

$(\Rightarrow)$ If $(T_A, \subseteq)$ is not finitely branching, then there is an $n_0 \in \omega$ such that $\mathscr{S}_{n_0} = \{g|_{n_0} : g \in A\}$ is infinite. On the one hand, $A \subseteq \bigcup\{O_s : s \in \mathscr{S}_{n_0}\}$, but on the other hand, for any finite subset $\{s_0, \ldots s_{m-1}\} \subseteq \mathscr{S}_{n_0}$ we have $A \nsubseteq \bigcup_{i\in m} O_{s_i}$, hence, A is not compact.

$(\Leftarrow)$ Assume that $(T_A, \subseteq)$ is finitely branching. Let $\mathscr{S} \subseteq \mathrm{seq}(\omega)$ be such that $A \subseteq \bigcup_{s\in\mathscr{S}} O_s$ and let $\tilde{T}_A = \{g|_n : g \in A \wedge n \in \omega \wedge \forall k \leq n(g|_k \notin \mathscr{S})\}$. First we show that $\tilde{T}_A$ is finite: Assume towards a contradiction that $\tilde{T}_A$ is infinite. Then, by König's Lemma, $(\tilde{T}_A, \subseteq)$ contains an infinite branch, say $g_0 \in {}^\omega\omega$. Now, g_0 belongs to A (since A is closed), but by construction $g_0 \notin \bigcup_{s\in\mathscr{S}} O_s$, a contradiction. We say that $t \in \tilde{T}_A$ is a *leaf* of $\tilde{T}_A$ if for all $n \in \omega$, $t^\frown n \notin \tilde{T}_A$. Let $L(\tilde{T}_A)$ denote the finite set of leaves of $\tilde{T}_A$. Now, let $\mathscr{S}_0 = \{t^\frown n : t \in \tilde{T}_A \wedge n \in \omega \wedge t^\frown n \in T_A\}$. Notice that $\mathscr{S}_0 \cap \tilde{T}_A = \emptyset$. Then, since $(T_A, \subseteq)$ is finitely branching, $\mathscr{S}_0$ is finite, and by definition we get $\mathscr{S}_0 \subseteq \{t^\frown n : t \in \tilde{T}_A \wedge n \in \omega \wedge t^\frown n \in \mathscr{S}\}$. Moreover, $A \subseteq \bigcup\{O_s : s \in \mathscr{S}_0\}$, which shows that A is compact. ⊣

An uncountable set $X \subseteq {}^\omega\omega$ is a **Lusin set** if for each meagre set $M \subseteq {}^\omega\omega$, $X \cap M$ is countable; and an uncountable set $X \subseteq {}^\omega\omega$ is a ***K*-Lusin set** if for each compact set $K \subseteq {}^\omega\omega$, $X \cap K$ is countable.

FACT 27.3. *Every Lusin set is a K-Lusin set.*

Proof. By LEMMA 27.2, every compact set $K \subseteq {}^\omega\omega$ is meagre (even nowhere dense), and therefore, every Lusin set is a K-Lusin set. ⊣

Let Q be a countable dense subset of ${}^\omega\omega$. Then $X \subseteq {}^\omega\omega$ is **concentrated on *Q*** if every open subset of ${}^\omega\omega$ containing Q, contains all but countably many elements of X. Finally, a subset of ${}^\omega\omega$ is called **concentrated** if it is concentrated on some countable dense subset of ${}^\omega\omega$.

PROPOSITION 27.4. *The following statements are equivalent:*

(a) There exists a K-Lusin set of cardinality $\mathfrak{c}$.

(b) There exists a concentrated set of cardinality $\mathfrak{c}$.

Proof. (b)⇒(a) Let $X \subseteq {}^\omega\omega$ be concentrated on some countable dense set $Q \subseteq {}^\omega\omega$. One can show that there exists a homeomorphism between ${}^\omega\omega \setminus Q$ and ${}^\omega\omega$, *i.e.*, there exists a bijection $h : {}^\omega\omega \setminus Q \to {}^\omega\omega$ which maps open sets to open sets and closed sets to closed sets (the details are left to the reader). Let K be an arbitrary compact subset of ${}^\omega\omega$. Then $h^{-1}[K]$ is also compact, and therefore ${}^\omega\omega \setminus h^{-1}[K]$ is an open set containing Q. Thus, since X is concentrated on Q, ${}^\omega\omega \setminus h^{-1}[K]$ contains all but countably many elements of X and consequently $h[X] \cap K$ is countable; and since K was arbitrary, this implies that the image under h of a set concentrated on Q of cardinality $\mathfrak{c}$ is a K-Lusin set of the same cardinality.

(a)⇒(b) Similarly, if $Q \subseteq {}^\omega\omega$ is a countable dense set and $h : {}^\omega\omega \setminus Q \to {}^\omega\omega$ is a homeomorphism, then the pre-image under h of a K-Lusin set of cardinality $\mathfrak{c}$ is a concentrated set of the same cardinality. ⊣

Sarabande

The cardinal $\mathfrak{l}$ and the existence of large K-Lusin sets. The following result — even though it follows quite easily from the definitions — is in fact the heart of our set-theoretical investigation of the BANACH-KURATOWSKI THEOREM.

THEOREM 27.5. $\mathfrak{l} = \omega_1$ *if and only if there is a* K*-Lusin set of cardinality* $\mathfrak{c}$.

Proof. ($\Rightarrow$) Assume $\mathfrak{l} = \omega_1$ and let $\mathscr{F} \subseteq {}^\omega\omega$ be a set of cardinality $\mathfrak{c}$ such that for each $g \in {}^\omega\omega$, $\{f \in \mathscr{F} : f \leq g\}$ is countable. By LEMMA 27.2, for each closed and compact set $K \subseteq {}^\omega\omega$ there is a function $g_K \in {}^\omega\omega$ such that $K \subseteq \{g \in {}^\omega\omega : g \leq g_K\}$. Thus, for every closed and compact set K we have $\mathscr{F} \cap K \subseteq \{f \in \mathscr{F} : f \leq g_K\}$ is countable, hence, $\mathscr{F}$ is a K-Lusin set of cardinality $\mathfrak{c}$.

($\Leftarrow$) Let $X \subseteq {}^\omega\omega$ be a K-Lusin set of cardinality $\mathfrak{c}$. By LEMMA 27.2, for each $g \in {}^\omega\omega$ the set $K_g = \{f \in {}^\omega\omega : f \leq g\}$ is closed and compact. Thus, $X \cap K_g = \{f \in X : f \leq g\}$ is countable. Hence, $\lambda(X) = \omega_1$ and since $|X| = \mathfrak{c}$ we have $\mathfrak{l} = \omega_1$. ⊣

Gavotte I & II

***K*-Lusin sets and the cardinals $\mathfrak{b}$ and $\mathfrak{d}$.**

PROPOSITION 27.6. *The existence of a* K*-Lusin set of cardinality* $\mathfrak{c}$ *implies* $\mathfrak{b} = \omega_1$ *and* $\mathfrak{d} = \mathfrak{c}$.

Proof. Let $X \subseteq {}^\omega\omega$ be a K-Lusin set of cardinality $\mathfrak{c}$. On the one hand, every uncountable subset of X is unbounded, so, $\mathfrak{b} = \omega_1$. On the other hand, every function $g \in {}^\omega\omega$ dominates only countably many elements of X. Hence, no family $\mathscr{F} \subseteq {}^\omega\omega$ of cardinality strictly less than $\mathfrak{c}$ can dominate all elements of X, and thus, $\mathfrak{d} = \mathfrak{c}$. ⊣

By the definition of K-Lusin sets we get that K-Lusin sets are exactly those (uncountable) subsets of ${}^\omega\omega$ all whose uncountable subsets are unbounded, which explains that K-Lusin sets are also called *strongly unbounded*; K-Lusin sets play an important role in preserving unbounded families in iterations of proper forcing notions.

The existence of *K*-Lusin sets of cardinality $\mathfrak{c}$.

LEMMA 27.7. *If* G *is* $\mathbb{C}_\mathfrak{c}$*-generic over* $\mathbf{V}$, *then*

$$\mathbf{V}[G] \vDash \text{“there is a Lusin set of cardinaltiy } \mathfrak{c}\text{”}.$$

Proof. With G we can construct a set $C = \{c_\alpha : \alpha \in \mathfrak{c}\}$ of Cohen reals of cardinality $\mathfrak{c}$. Further, let $\underset{\sim}{r}$ be a $\mathbb{C}_\mathfrak{c}$-name for the code of a meagre F_σ set $A_r \in \mathbf{V}[G]$ and let $I = \text{supp}(\underset{\sim}{r})$ (*cf.* Chapter 21). Clearly, $I \subseteq \mathfrak{c}$ is countable, and by PROPOSITION 21.7, for each $\alpha \in \mathfrak{c} \setminus I$ we have $\mathbf{V}[G] \vDash c_\alpha \notin A_r$. Hence, $C \cap A_r$ is countable in $\mathbf{V}[G]$, and since $\mathbb{C}_\mathfrak{c}$ preserves cardinalities and A_r was arbitrary, $\mathbf{V}[G] \vDash$ “*C is a Lusin set of cardinaltiy* $\mathfrak{c}$”.

THEOREM 27.8. *The existence of a* K*-Lusin set of cardinality* $\mathfrak{c}$ *is independent of* $\mathsf{ZFC} + \neg\mathsf{CH}$. *Equivalently, the existence of a BK-Matrix is independent of* $\mathsf{ZFC} + \neg\mathsf{CH}$.

Proof. Firstly, notice that by THEOREM 27.1 and THEOREM 27.5 the existence of a BK-Matrix is equivalent to the existence of a K-Lusin set of cardinality $\mathfrak{c}$. Now, by LEMMA 27.7 and FACT 27.3 it is consistent with ZFC that there is a K-Lusin set (even a Lusin set) of cardinality $\mathfrak{c}$. On the other hand, it is consistent with ZFC that $\mathfrak{b} > \omega_1$ or that $\mathfrak{d} < \mathfrak{c}$ (*cf.* Chapter 18). Therefore, by PROPOSITION 27.6, it is consistent with ZFC that there are no K-Lusin sets of cardinality $\mathfrak{c}$. ⊣

***K*-Lusin sets and the cardinals $\mathfrak{b}$ and $\mathfrak{d}$.** As an immediate consequence of PROPOSITION 27.6 and THEOREM 27.8 we get that $\omega_1 = \mathfrak{b} < \mathfrak{d} = \mathfrak{c}$ is consistent with ZFC. Since Cohen reals are unbounded and since Cohen forcing does not add dominating reals (see Chapter 21), PROPOSITION 27.6 is in fact just a consequence of LEMMA 27.7.

In the next section, a very similar construction will be used to show that the converse of PROPOSITION 27.6 is not provable in ZFC.

Gigue

A model without K-Lusin sets in which $\mathfrak{b} = \omega_1$ and $\mathfrak{d} = \mathfrak{c}$.

PROPOSITION 27.9. *It is consistent with* ZFC *that* $\mathfrak{b} = \omega_1$ *and* $\mathfrak{d} = \mathfrak{c}$, *but there is no K-Lusin set of cardinality* $\mathfrak{c}$.

Proof. Let $\mathbf{V}$ be a model of ZFC in which $\mathfrak{p} = \mathfrak{c} = \omega_2$. Let $G = \langle c_\alpha : \alpha \in \omega_1 \rangle$ be $\mathbb{C}^{\omega_1}$-generic over $\mathbf{V}$. In the resulting model $\mathbf{V}[G]$ we have $\mathfrak{b} = \omega_1$ and $\mathfrak{d} = \omega_2$ (see PROPOSITION 21.13). On the other hand, there is no K-Lusin set of cardinality $\mathfrak{c}$ in $\mathbf{V}[G]$. Why? Suppose $X \subseteq {}^\omega\omega$ has cardinality ω_2. Take a countable ordinal α and a subset $X' \subseteq X$ of cardinality ω_2 such that $X' \subseteq \mathbf{V}[G|_\alpha]$, where $G|_\alpha = \langle c_\beta : \beta \in \alpha \rangle$. Now, $\mathbf{V}[G|_\alpha] = \mathbf{V}[c]$ for some Cohen real c (by FACT 18.4), and $\mathbf{V}[c] \vDash \mathfrak{p} = \mathfrak{c}$ (by THEOREM 19.4), and since $\mathfrak{p} \leq \mathfrak{b}$ we have $\mathbf{V}[c] \vDash \mathfrak{b} = \omega_2$. Thus, there is a function which dominates uncountably many elements of X'. Hence, by the remark after PROPOSITION 27.6, X cannot be a K-Lusin set. ⊣

One after another, the bells jangled into silence,
lowered their shouting mouths and were at peace.

DOROTHY L. SAYERS
The Nine Tailors, 1934

References

1. Stefan Banach and Kazimierz Kuratowski, *Sur une généralisation du problème de la mesure*, ***Fundamenta Mathematicae***, vol. 14 (1929), 127–131.
2. Tomek Bartoszyński and Lorenz Halbeisen, *On a theorem of Banach and Kuratowski and K-Lusin sets*, ***Rocky Mountain Journal of Mathematics***, vol. 33 (2003), 1223–1231.
3. John C. Oxtoby, ***Measure and Category***, 2nd ed., [Graduate Texts in Mathematics 2], Springer-Verlag, New York, 1980.
4. Stanisław Ulam, *Zur Masstheorie in der allgemeinen Mengenlehre*, ***Fundamenta Mathematicae***, vol. 16 (1930), 140–150.
5. Dorothy L. Sayers, ***The Nine Tailors, Changes Rung on an Old Theme in Two Short Touches and Two Full Peals***, Harcourt, Brace and Company, New York, 1934.

Index

Symbols

Names

A page number is given in italics when that page contains a biographical note about the person being indexed.

Subjects

Proper definitions as well as theorems with their proofs are indicated by boldface page numbers, theorems without proofs are indicated by page numbers without serifs, and historical notes are indicated by page numbers given in italics.