Consequences of Arithmetic for Set Theory

Lorenz HALBEISEN [1]
Department of Mathematics,
ETH Zürich, Switzerland

Saharon SHELAH [2]
Institute of Mathematics,
Hebrew University Jerusalem, Israel

Abstract

In this paper, we consider certain cardinals in ZF (set theory without AC, the Axiom of Choice). In ZFC (set theory with AC), given any cardinals $\mathcal{C}$ and $\mathcal{D}$, either $\mathcal{C} \leq \mathcal{D}$ or $\mathcal{D} \leq \mathcal{C}$. However, in ZF this is no longer so. For a given infinite set A consider $\mathit{seq}^{\mathit{1\text{-}1}}(A)$, the set of all sequences of A without repetition. We compare $\big|\mathit{seq}^{\mathit{1\text{-}1}}(A)\big|$, the cardinality of this set, to $\big|\mathcal{P}(A)\big|$, the cardinality of the power set of A. What is provable about these two cardinals in ZF? The main result of this paper is that $\mathrm{ZF} \vdash \forall A(\big|\mathit{seq}^{\mathit{1\text{-}1}}(A)\big| \neq \big|\mathcal{P}(A)\big|)$ and we show that this is the best possible result. Furthermore, it is provable in ZF that if B is an infinite set, then $\big|\mathit{fin}(B)\big| < \big|\mathcal{P}(B)\big|$, even though the existence for some infinite set B^* of a function f from $\mathit{fin}(B^*)$ onto $\mathcal{P}(B^*)$ is consistent with ZF.

§0 Introduction, Definitions and Basic Theorems

Introduction: In ZFC the cardinality of ordinal numbers plays an important role, since by AC each set has the cardinality of some ordinal.
We use "alephs" for the cardinalities of ordinals. Thus in ZFC each cardinal number is an aleph. However this need not be the case in ZF.
If we have a model M of ZF in which the axiom of choice fails, then we have more cardinals in M than in a model V of ZFC, even if we have fewer sets in M than in V. (This occurs when the choice-functions are not all in M). This is because the ordinals are in M and hence the alephs as well.

[1] Parts of this work are of the first author's Diplomarbeit at the ETH Zürich. He is grateful to his supervisor, Professor H. Läuchli.

[2] Research partially supported by the Basic Research Fund, Israeli Academy; Publ. No. 488

In this paper we are interested in the relation between three cardinals arising in connection with a set S, namely,

1) the cardinality of the power set of S
2) the cardinality of the finite subsets of S
3) the cardinality of the finite sequences without repetition of S

This section contains definitions and basic theorems provable in ZF.
In the next section we present two relative consistency proofs illustrating possible relations between these cardinals.
The last two sections contain three results provable in ZF. The proofs of these are based on the same idea originally from E. Specker, who used it to prove that the axiom of choice follows from the generalised continuum hypothesis [Sp1]. Assuming the existence of a function we derive a contradiction to Hartogs' Theorem.

Because we do not use AC, our proofs are constructive. But we will see that sometimes arithmetic is powerful enough for our constructions, making it an adequate substitute for AC.

Cardinals: A *cardinal number* $\mathcal{C}$ is the equvalence class of all sets which have the *same size.* (Two sets are said to have the same size *iff* there is a bijection between them.)

Alephs: A cardinal number $\mathcal{C}$ is an *aleph* if it contains a well-ordered set.

We use calligraphic letters to denote cardinals and $\aleph$'s to denote the alephs.
We denote the cardinality of the set s by $|s|$.

Relations between cardinals: We say that the cardinal number $\mathcal{C}$ is less than or equal to the cardinal number $\mathcal{D}$ *iff* there are sets $c \in \mathcal{C}$, $d \in \mathcal{D}$ and a 1-1 function from c into d.
In this case we write $\mathcal{C} \leq \mathcal{D}$. We write $\mathcal{C} < \mathcal{D}$ for $\mathcal{C} \leq \mathcal{D}$ and $\mathcal{C} \neq \mathcal{D}$.
If $c \in \mathcal{C}$, $d \in \mathcal{D}$ and we have a function from d onto c, then we write $\mathcal{C} \leq^* \mathcal{D}$.

We also need some well-known facts provable in ZF:

Hartogs' Theorem: Given a cardinal $\mathcal{C}$ there is a least aleph, $\aleph(\mathcal{C})$, such that $\aleph(\mathcal{C}) \not\leq \mathcal{C}$.
Proof: See [Je1] p.25 ■

Cantor-Bernstein Theorem: If $\mathcal{C}$ and $\mathcal{D}$ are cardinals with $\mathcal{C} \leq \mathcal{D}$ and $\mathcal{D} \leq \mathcal{C}$, then $\mathcal{C} = \mathcal{D}$.

Proof: See [Je1] p.23 ■

Cantor Normal Form Theorem: Any ordinal α can be written as

$$\alpha = \sum_{i=0}^{j} \omega^{\alpha_i} \cdot k_i$$

with $\alpha \geq \alpha_0 > \alpha_1 > \ldots > \alpha_j \geq 0$, $1 \leq k_i < \omega$, $0 \leq j < \omega$.
Proof: See [Ba] p.57*ff* ■

Corollary 1: The Cantor Normal Form does not depend on AC.
Proof: The proof of the Cantor Normal Form requires no infinite choices. ■

Corollary 2: If $\alpha = \sum_{i=0}^{j} \omega^{\alpha_i} \cdot k_i$ is a Cantor Normal Form, then define $\overleftrightarrow{\alpha}$ by

$$\overleftrightarrow{\alpha} := \sum_{i=j}^{0} \omega^{\alpha_i} \cdot k_i = \omega^{\alpha_0} \cdot k_0.$$

Then (in ZF) $\left|\alpha\right| = \left|\overleftrightarrow{\alpha}\right|$
Proof: See [Ba] p.60 ■

Corollary 3: For any ordinal α, ZF implies the existence of the following bijections.

$$\begin{array}{llll} F^{\alpha}_{\mathit{seq}^{\mathit{1\text{-}1}}} & : & \alpha \longrightarrow \mathit{seq}^{\mathit{1\text{-}1}}(\alpha) & (=: \text{finite sequences of } \alpha \text{ without repetition}) \\ F^{\alpha}_{\mathit{seq}} & : & \alpha \longrightarrow \mathit{seq}(\alpha) & (=: \text{finite sequences of } \alpha\,) \\ F^{\alpha}_{\mathit{fin}} & : & \alpha \longrightarrow \mathit{fin}(\alpha) & (=: \text{finite subsets of } \alpha\,) \end{array}$$

Proof: Use the Cantor Normal Form Theorem, Corollary 2, order the finite subsets of α and then use the Cantor-Bernstein Theorem. ■

§1 Consistency results

In this section we work in the Mostowski permutation model to derive some relative consistency results. The permutation models are models of ZFA, set theory with atoms, (see [Je2] p.44*ff*).

The atoms $x \in A$ may also be considered to be sets which contain only themselves, this means: $x \in A \Rightarrow x = \{x\}$ (see [Sp2] p.197 or [La] p.2).
Thus the permutation models are models for ZF without the axiom of foundation.

However, the Jech-Sochor Embedding Theorem (see [Je] p.208*ff*) implies consistency results for ZF.

In the permutation models we have a set of atoms A and a group $\mathcal{G}$ of permutations of A. Let $\mathcal{F}$ be a normal filter on $\mathcal{G}$ (see [Je] p.199). We say that x is *symmetric* if the group $\operatorname{sym}_{\mathcal{G}}(x) := \{\pi \in \mathcal{G} : \ \pi(x) = x \ \}$ belongs to $\mathcal{F}$.

Let us further assume that $\operatorname{sym}_{\mathcal{G}}(a) \in \mathcal{F}$ for every atom a, that is, that all atoms are symmetric (with respect to $\mathcal{G}$ and $\mathcal{F}$) and let $\mathcal{B}$ be the class of all hereditarily symmetric objects.

The class $\mathcal{B}$ is both a permutation model and a transitive class: all atoms are in $\mathcal{B}$ and $A \in \mathcal{B}$. Moreover, $\mathcal{B}$ is a transitive model of ZFA.

Given a finite set $E \subset A$, let $\operatorname{fix}_{\mathcal{G}}(E) := \{\pi \in \mathcal{G} : \ \pi a = a \text{ for all } a \in E\}$ and let $\mathcal{F}$ be the filter on $\mathcal{G}$ generated by $\{\operatorname{fix}_{\mathcal{G}}(E) : \ E \subset A \text{ is finite}\}$.

$\mathcal{F}$ is a normal filter and x is symmetric *iff* there is a finite set of atoms E_x such that $\pi(x) = x$ whenever $\pi \in \mathcal{G}$ and $\pi a = a$ for each $a \in E_x$. Such an E_x is called a support for x.

Now the Mostowski model is constructed as follows: (see also [Je2] p.49*ff*)

1) The set of atoms A is infinite.
2) R is an order-relation on A.
3) With respect to R, A is a dense linear ordered set without endpoints.
4) Let Aut_R be the group of all permutations of A such that for all atoms $x, y \in A$ and each $\pi \in \operatorname{Aut}_R$, if Rxy then $R\pi(x)\pi(y)$.
5) Let $\mathcal{F}$ be generated by $\{\operatorname{fix}(E) : \ E \subset A \text{ is finite } \}$.

We will write $x < y$ instead of Rxy.

The subsets of A (in the Mostowski model) are symmetric sets. Hence each subset of A has a finite support.

If $x \subseteq A$ (in the Mostowski model) and x has non-empty support E_x, then an $a \in E_x$ may or may not belongs to x.

Fact: If $b \notin x \cup E_x$ and there are two elements $a_0, a_1 \in E_x$ with $a_0 < b < a_1$ such that $\forall c(a_0 < c < a_1 \to c \notin E_x)$, then $\forall c(a_0 < c < a_1 \to c \notin x)$.

Otherwise we construct a $\pi \in \operatorname{Aut}_R$ such that $\pi a_i = a_i$ for all $a_i \in E_x$ and $\pi c = b$. Then $\pi(x) \neq x$, which is a contradiction.

We can similarly show that if $a_0 < b < a_1$ and $b \in x \setminus E_x$, then $\forall c(a_0 < c < a_1 \to c \in x)$. The cases when $\neg\exists a_1(a_1 \in E_x \ \wedge \ b < a_1)$ or $\neg\exists a_0(a_0 \in E_x \ \wedge \ b > a_0)$ are similar.

Hence, given a finite set $E \subset A$ ($\big|E\big| =: n$), we can construct $2^n \cdot 2^{n+1} = 2^{2n+1}$ subsets $x \subseteq A$ such that E is a support of x.

Given a finite subset E of A, consider the set $\mathcal{E}$ of subsets of A with support E. We use R to order $\mathcal{E}$ as follows. Given $E_1 = \{a_1, \ldots, a_n\}$ and $E_2 = \{a_1, \ldots, a_n, \ldots, a_{n+k}\}$ with $a_i < a_j$ whenever $i < j$ and given $x \in \mathcal{E}$, if x is the l^{th} subset with support E_1, then x is also the l^{th} subset with support E_2.

Finally, we define the function F: $\mathit{fin}(A) \longrightarrow \mathcal{P}(A)$ by
$E \longmapsto \left|E\right|^{th}$ subset of A
constructible with support E.

It is easy to see that F is onto.

If $E \subset A$ is finite, then use R to order the subsets of E and use the corresponding lexicographic order on the set of permutations of subsets of E. The set of permutations of subsets of E is isomorphic to $\mathit{seq}^{\mathit{1\text{-}1}}(E)$. In fact we can order $\mathit{seq}^{\mathit{1\text{-}1}}(E)$ for each finite $E \subset A$.

For each subset $x \subseteq A$ there is exactly one smallest support E_x (=:supp(x)).

If $\left|\text{supp}(x)\right| = n$, then put $\overline{x} := \left|\{y \subseteq A : \text{supp}(y) = \text{supp}(x)\}\right| \leq 2^{2n+1}$ and for $l \leq \overline{x}$ define as above the l^{th} element of $\{y \subseteq A : \text{supp}(y) = \text{supp}(x)\}$.

We say that: "$y \subseteq A$ is the l^{th} subset of A with support supp(x)".

Now choose 24 distinct elements $a_0, \ldots, a_{23} \in A$ and define $A_{24} := \{a_0, \ldots, a_{23}\}$. A simple calculation shows that

$$\text{if } n \geq 12, \text{ then } 2 \cdot 2^{2n+1} < n! \tag{$*$}$$

Take a finite subset E of A and let $y \subseteq A$ be the l^{th} subset of A with $\text{supp}(y) = E$. Put $D := \text{supp}(y)\Delta A_{24}$ (where Δ denotes symmetric difference) and $d := \left|D\right|$.

Define the function $\mathit{Seq}_A : \mathcal{P}(A) \longrightarrow \mathit{seq}^{\mathit{1\text{-}1}}(A)$ by

$$\mathit{Seq}_A(y) := \begin{cases} \text{the } l^{th} \text{ permutation of supp}(y) & \text{if } \left|\text{supp}(y)\right| \geq 12, \\ \text{the } (d! - l - 1)^{th} \text{ permutation of supp}(y) & \text{otherwise.} \end{cases}$$

Seq_A is well defined because of $(*)$ and $d \geq 13$.

It is easy to see that Seq_A is 1-1. If there is a bijection between $\mathcal{P}(A)$ and $\mathit{seq}^{\mathit{1\text{-}1}}(A)$, then we find an ω-sequence$^{\mathit{1\text{-}1}}$ in A using an analogous construction. But this is a contradiction (see section 3).

Even more is true in the Mostowski model, ($\mathcal{A} := \left|\text{Atoms}\right|$),

$$\mathcal{A} < \mathit{fin}(\mathcal{A}) < \mathcal{P}(\mathcal{A}) < \mathit{seq}^{\mathit{1\text{-}1}}(\mathcal{A}) < \mathit{fin}(\mathit{fin}(\mathcal{A})) < \mathit{seq}(\mathcal{A}) < \mathcal{P}(\mathcal{P}(\mathcal{A})).$$

(We omit the proof).

Our interest here is in the following result.

Theorem 1: The following theories are equiconsistent:
(i) ZF
(ii) $\mathrm{ZF} + \exists\mathcal{A}(\mathcal{P}(\mathcal{A}) < \mathit{seq}^{\mathit{1\text{-}1}}(\mathcal{A}))$
(iii) $\mathrm{ZF} + \exists\mathcal{A}(\mathcal{P}(\mathcal{A}) \leq^* \mathit{fin}(\mathcal{A}))$

Proof: It was shown above that in the Mostowski model there is a cardinal $\mathcal{A}$, namely the cardinality of the set of atoms, for which both (ii) and (iii) hold. Unfortunately, the Mostowski model is only a model of ZFA. But it is well-known that Con(ZF)⇒Con(ZFC) and the Jech-Sochor Embedding Theorem provides a model of (ii) and (iii). ■

Theorem 2: The following theories are equiconsistent:
(i) ZF
(ii) $\mathrm{ZF} + \exists\mathcal{A}(\mathit{seq}(\mathcal{A}) < \mathit{fin}(\mathcal{A}))$

Proof:
By the Jech-Sochor Embedding Theorem it is enough to construct a permutation model $\mathcal{B}$ in which there is a set A, such that:

(a) there is a 1-1 function from $\mathit{seq}(A)$ into $\mathit{fin}(A)$,
(b) there is no bijection between $\mathit{seq}(A)$ and $\mathit{fin}(A)$.

We construct by induction on $n \in \omega$ the following:

(α) $A_0 := \{\{\emptyset\}\}$; $Sq_0(\{\emptyset\})$:=the empty sequence;
$G_0 :=$ the group of all permutations of A_0.

Let k_n be the number of elements of G_n, and $\mathcal{E}_n$ be the set of sequences of A_n in length less or equal than n which are not in range(Sq_n), then

(β) $A_{n+1} := A_n \mathbin{\dot\cup} \{(n+1, \zeta, i) : \ \zeta \in \mathcal{E}_n \text{ and } i < k_n + k_n\}$.

(δ) Sq_{n+1} is a function from A_{n+1} to $\mathit{seq}(A_n)$ defined as follows:

$$Sq_{n+1}(x) = \begin{cases} Sq_n(x) & \text{if } x \in A_n, \\ \zeta & \text{if } x = (n+1, \zeta, i) \in A_{n+1} \setminus A_n. \end{cases}$$

(γ) 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

$$h(x) = \begin{cases} g_h(x) & \text{if } x \in A_n, \\ (n+1, g_h(\zeta), i +_n j_h) & \text{if } x = (n+1, \zeta, i) \in A_{n+1} \setminus A_n. \end{cases}$$

Where $g_h(\zeta)(m) := g_h(\zeta(m))$ and $+_n$ is the addition modulo $k_n + k_n$.

Let $A := \bigcup\{A_n : \ n \in \omega\}$ and $Sq := \bigcup\{Sq_n : \ n \in \omega\}$, then Sq is a function from A onto $\mathit{seq}(A)$.

Further define for each natural number n partial functions f_n from A to $A \cup \{\emptyset\}$ as follows. If $lg(x)$ denotes the length of $Sq(x)$ and $n < lg(x)$, then $f_n(x) := Sq(x)(n)$, otherwise let $f_n(x) = \emptyset$.

Let $\mathrm{Aut}(A)$ be the group of all permutations of A.
Then $\mathcal{G} := \{H \in \mathrm{Aut}(A) : \forall n \in \omega(H|_{A_n} \in G_n)\}$ is a group of permutations of A.
Let $\mathcal{F}$ be the normal filter on $\mathcal{G}$ generated by $\{\mathrm{fix}(E) : E \subset A \text{ is finite}\}$ and $\mathcal{B}$ be the class of all hereditarily symmetric objects.
Now $A \in \mathcal{B}$ and for each $n \in \omega$, $\mathrm{supp}(f_n) = \emptyset$, hence f_n belongs to $\mathcal{B}$, too.

Now define on A a equivalence relation as follows,

$$x \sim y \quad \textit{iff} \quad \forall n(f_n(x) = f_n(y)).$$

Facts:

1. Every equivalence class of A is finite.
(Because of each A_n is finite, hence each k_n).

2. $\mathit{seq}(A) = \{\varsigma_x : x \in A\}$ where $\varsigma_x(n) := f_n(x)$, (if $f_n(x) \neq \emptyset$).

3. For every finite subset B of A, there are finite subsets C, Y of A and a natural number $k > 1$ such that $B \subseteq C$, $\forall x \in A \backslash C$ $(\big|\{H(x) : H \in \mathrm{fix}_{\mathcal{G}}(C)\}\big| > k)$ and $\big|\{H[Y] : H \in \mathrm{fix}_{\mathcal{G}}(C)\}\big| = k$.
(Choose A_n $(n \geq 1)$ such that $B \subseteq A_n$ and let $C := A_n$. Let $k := k_n + k_n$ and $Y := \{(n+1, \zeta, i) \in A_{n+1} : \ i \text{ is even}\}$. Then Y has exactly two images under $\{h : h \in \mathrm{fix}_{\mathcal{G}}(C)\}$ and $\forall x \in A \setminus C(\ \big|\{h(x) : \ h \in \mathrm{fix}_{\mathcal{G}}(C)\}\big| \geq k_{n+1} + k_{n+1}).$)

Now the function

$$\begin{array}{rccc} \Psi : & \mathit{seq}(A) & \longrightarrow & \mathit{fin}(A) \\ & \varsigma & \longmapsto & \{x : \ \varsigma_x = \varsigma\} \end{array}$$

is a 1-1 function in $\mathcal{B}$ from $\mathit{seq}(A)$ into $\mathit{fin}(A)$ (by the facts 1 and 2).
Hence (a) holds in $\mathcal{B}$.

To prove (b), assume there is a 1-1 function $\Phi \in \mathcal{B}$ from $\mathit{fin}(A)$ into $\mathit{seq}(A)$.

Let B be a support of Φ and let C, Y, k be as in fact 3.

If the sequence $\Phi(Y)$ belongs to $\mathit{seq}(C)$, then for some $H \in \mathrm{fix}_{\mathcal{G}}(C)$, $H[Y] \neq Y$, hence $\Phi(H[Y]) \neq \Phi(Y)$. But this contradicts that H maps Φ to itself, (by definition of C, Y and H).

Otherwise there exists an $m \in \omega$ such that $x := \Phi(Y)(m)$ does not belong to the set C.

Hence $\big|\{H(x) :\ H \in \mathrm{fix}_{\mathcal{G}}(C)\}\big| > k$ and $\big|\{H[Y] :\ H \in \mathrm{fix}_{\mathcal{G}}(C)\}\big| = k$, (by fact 3). Every $H \in \mathrm{fix}_{\mathcal{G}}(C)$ maps Φ to itself, hence $\Phi(Y)$ to $\Phi(H[Y])$. So we have a mapping from a set with k members onto a set with more than k members.
But this is a contradiction. ■

§2 ZF $\vdash$ ($\big|\mathit{fin}(S)\big| < \big|\mathcal{P}(S)\big|$) for any infinite set S.

Theorem 3: ZF $\vdash \mathit{fin}(\mathcal{C}) < \mathcal{P}(\mathcal{C})$

Proof: Take $S \in \mathcal{C}$. The natural map from $\mathit{fin}(S)$ into $\mathcal{P}(S)$ is a 1-1 function, hence $\big|\mathit{fin}(S)\big| \leq \big|\mathcal{P}(S)\big|$ is always true.
Assume that there is a bijective function $B :\ \mathit{fin}(S) \longrightarrow \mathcal{P}(S)$. Then, given any ordinal α, we can construct an α-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{fin}(S)$. But this contradicts Hartogs' Theorem.

First we construct an ω-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{fin}(S)$ as follows:
$S \in \mathcal{P}(S)$ and, because S is infinite, $S \notin \mathit{fin}(S)$.
But $B^{-1}(S) \in \mathit{fin}(S)$. So put $s_0 := B^{-1}(S)$ and $s_{n+1} := B^{-1}(s_n)$ $(n \in \omega)$.
Then the set $\{s_i :\ i < \omega\}$ is an infinite set of finite subsets of S and the sequence $\langle s_0, s_1, \ldots, s_n, \ldots\rangle_\omega$ is an ω-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{fin}(S)$.

If we have already constructed an α-sequence$^{\mathit{1\text{-}1}}$ $\langle s_0, s_1, \ldots, s_\beta, \ldots\rangle_\alpha$ in $\mathit{fin}(S)$ (with $\alpha \geq \omega$), then we define an equivalence relation on S by

$$x \sim y \quad \mathit{iff} \quad \forall\beta < \alpha(x \in s_\beta \leftrightarrow y \in s_\beta)$$

Take $x \in S$ and suppose that $\mu < \alpha$. Define

$$\begin{aligned} D_{x,\mu} &:= \bigcap_{\iota<\mu}\{s_\iota :\ x \in s_\iota\} \\ g(x) &:= \{\mu < \alpha :\ x \in s_\mu \wedge (s_\mu \cap D_{x,\mu} \neq D_{x,\mu})\}. \end{aligned}$$

Fact: Given $x, y \in S$, $g(x) = g(y) \Leftrightarrow x \sim y$.
(In other words $x^\sim = y^\sim$ whenever $g(x) = g(y)$).
Hence there is a bijection between $\{x^\sim :\ x \in S\}$ and $\{g(x) :\ x \in S\}$.
Furthermore, $g(x) \in \mathit{fin}(\alpha)$.

Since $\{g(x) :\ x \in S\} \subseteq \mathit{fin}(\alpha)$, apply F^α_{fin} to obtain $F^\alpha_{\mathit{fin}}[\{g(x) :\ x \in S\}] \subseteq \alpha$.
Let γ be the order-type of $F^\alpha_{\mathit{fin}}[\{g(x) :\ x \in S\}]$. Then $\gamma \leq \alpha$ and for each $g(x)$ we obtain an ordinal number $\eta(g(x)) < \gamma$.
Each s_ι $(\iota < \alpha)$ is the union of at most finitely many equivalence classes. Thus there is a 1-1 function

$$\begin{aligned} h :\quad \alpha &\longrightarrow \mathit{fin}(\gamma) \\ \iota &\longmapsto \{\xi :\ \eta(g(x)) = \xi\ \wedge\ x \in s_\iota\}. \end{aligned}$$

Since $F^{\gamma}_{\mathit{fin}}$ is a bijection between $\mathit{fin}(\gamma)$ and γ, $F^{\gamma}_{\mathit{fin}}\circ h$ is a 1-1 function from α into γ and because $\gamma \leq \alpha$ we also have a 1-1 function from γ into α.

The Cantor-Bernstein Theorem yields a bijection between γ and α and hence a bijection G from $\{\eta(g(x)) : \ x \in S\}$ onto $\{s_\iota : \ \iota < \alpha\}$.

Now consider the function $\Gamma := B\circ G\circ\eta\circ g$ from S into P(S):

$$\Gamma : \ S \xrightarrow{g} \{g(x) : \ x \in S\} \xrightarrow{\eta} \{\eta(g(x)) : \ x \in S\} \xrightarrow{G} \{s_\iota : \ \iota < \alpha\} \xrightarrow{B} \mathcal{P}(S)$$

Fact: $S_\alpha := \ \{x \in S : \ x \notin \Gamma(x)\} \notin \{B(s_\iota) : \ \iota < \alpha\}$.

Otherwise Take $S_\alpha = B(s_\beta)$ (for some $\beta < \alpha$).
We identify each $x^\sim$ with $g(x)$ using the bijection above.
Then there is a $g(x)$ such that $G\circ\eta((g(x)) = s_\beta$.
Now if $y \in x^\sim$ then $\Gamma(y) = S_\alpha$.
But $y \in S_\alpha \Leftrightarrow y \notin \Gamma(y) \Leftrightarrow y \notin S_\alpha$, which is a contradiction.

But $S_\alpha \subseteq S$ and $B^{-1}(S_\alpha) =: s_\alpha \in \mathit{fin}(S)$ with $s_\alpha \notin \{s_\iota : \ \iota < \alpha\}$ and we have an $(\alpha + 1)$-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{fin}(S)$, namely $\langle s_0, s_1, \ldots, s_\beta, \ldots, s_\alpha\rangle_{\alpha+1}$.

We now see that for an infinite set S there is no bijection between $\mathit{fin}(S)$ and $\mathcal{P}(S)$ and this completes the proof. ■

We note the following facts.

Given a natural number n, $\quad$ ZF $\vdash (n \times \mathit{fin}(\mathcal{C}) = \mathcal{P}(\mathcal{C}) \rightarrow n = 2^k$ for a $k \in \omega)$.
Moreover, for each $k \in \omega$ $\quad$ Con(ZF) $\Rightarrow$ Con(ZF $+ \exists\mathcal{C}(2^k \times \mathit{fin}(\mathcal{C}) = \mathcal{P}(\mathcal{C}))$
(If $k = 0$, then this is obvious for finite cardinals.)

Sketch of the proof:

For the consistency result, consider the permutation model with an infinite set of atoms A and the empty relation. Then the automorphism group is the complete permutation group. It is not hard to see that any subset of A in this model is either finite or has a finite complement. Take a natural number k and consider (in this model) the set $k \times A$. The cardinality of the set $\mathcal{P}(k \times A)$ is the same as that of the set $2^k \times \mathit{fin}(A)$.

To prove the other fact, assume that n is a natural number which is not a power of 2 and that for some infinite set S there is a bijection B between $n \times \mathit{fin}(S)$ and $\mathcal{P}(S)$. Use the function B to construct an ω-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{fin}(S)$. Then, using Theorem 3, $\omega \leq \mathit{fin}(S) < \mathcal{P}(S)$ and it is easy to see that $n \times \mathit{fin}(S) \leq \mathit{fin}(S) \times \mathit{fin}(S) \ =: \mathit{fin}(S)^2$.
Then $\omega < \mathcal{P}(S) = n \times \mathit{fin}(S) \leq \mathit{fin}(S)^2$ contradicts the fact that if $\aleph_0 \leq \mathcal{P}(\mathcal{C})$, then for any natural number n, $\mathcal{P}(\mathcal{C}) \not\leq \mathit{fin}(\mathcal{C})^n$. (Here $\aleph_0$ denotes the cardinality of ω). The proof of this fact is similar to the proof of Theorem 3. ■

§3 $\mathit{seq}^{\mathit{1\text{-}1}}(S)$, $\mathit{seq}(S)$ and $\mathcal{P}(S)$ when S is an arbitrary set.

We show that ZF $\vdash \mathit{seq}^{\mathit{1\text{-}1}}(\mathcal{C}) \neq \mathcal{P}(\mathcal{C})$ for every cardinal $\mathcal{C} \geq 2$. But we first need the following result.

Lemma: ZF $\vdash \aleph_0 \leq \mathcal{P}(\mathcal{C}) \to \mathcal{P}(\mathcal{C}) \not\leq \mathit{seq}^{\mathit{1\text{-}1}}(\mathcal{C})$.

Proof:
Take $S \in \mathcal{C}$. Then, because $\aleph_0 \leq \mathcal{P}(\mathcal{C})$, we have a 1-1 function $f_\omega : \omega \longrightarrow \mathcal{P}(S)$.
Assume that there is a 1-1 function $J : \mathcal{P}(S) \longrightarrow \mathit{seq}^{\mathit{1\text{-}1}}(S)$.
Then $J \circ f_\omega$: $\omega \longrightarrow \mathit{seq}^{\mathit{1\text{-}1}}(S)$ is also 1-1 and we get an ω-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{seq}^{\mathit{1\text{-}1}}(S)$.
Using this ω-sequence$^{\mathit{1\text{-}1}}$ in $\mathit{seq}^{\mathit{1\text{-}1}}(S)$ we can easily construct an ω-sequence$^{\mathit{1\text{-}1}}$ in S.
If we already have constructed an α-sequence$^{\mathit{1\text{-}1}}$ $\langle s_0, s_1, \ldots, s_\beta, \ldots \rangle_\alpha$ $(\alpha \geq \omega)$ in S, put $T := \{s_\iota : \ \iota < \alpha\}$. This gives rise to bijective functions,

$$\begin{array}{rrcl} h_0 : & T & \longrightarrow & \alpha \\ h_1 : & \mathit{seq}^{\mathit{1\text{-}1}}(\alpha) & \longrightarrow & \mathit{seq}^{\mathit{1\text{-}1}}(T). \end{array}$$

Let J^{-1} be the inverse of J and denote the inverse of F^α_{seq} by invF^α_{seq}.
Further define

$$\Gamma := J^{-1} \circ h_1 \circ \mathrm{inv} F^\alpha_{\mathit{seq}} \circ h_0$$

Note: dom$(\Gamma) \subseteq T$ and range$(\Gamma) \subseteq \mathcal{P}(S)$ (because J is 1-1).

Fact: $S_\alpha := \{x \in S : \ x \notin \Gamma(x)\} \notin J^{-1}[\mathit{seq}^{\mathit{1\text{-}1}}(T)]$.
Assume not, then $x \in S$ such that $J(S_\alpha) = h_1 \circ \mathrm{inv} F^\alpha_{\mathit{seq}} \circ h_0(x)$ yields a contradiction.

Because $J(S_\alpha) \notin \mathit{seq}^{\mathit{1\text{-}1}}(T)$, the sequence $J(S_\alpha)$ has a first element which is not in T, say s_α. Finally, the sequence $\langle s_0, s_1, \ldots, s_\alpha \rangle_{\alpha+1}$ is an $(\alpha+1)$-sequence$^{\mathit{1\text{-}1}}$ in S.
So the existence of a 1-1 function $J : \ \mathcal{P}(S) \longrightarrow \mathit{seq}^{\mathit{1\text{-}1}}(S)$ contradicts Hartogs' Theorem. ■

Theorem 4: If $\mathcal{C} \geq 2$ is any cardinal, then ZF $\vdash (\mathit{seq}^{\mathit{1\text{-}1}}(\mathcal{C}) \neq \mathcal{P}(\mathcal{C}))$

Proof:
By the Lemma it is enough to prove that if $\mathcal{C} \geq 2$, then $\mathit{seq}^{\mathit{1\text{-}1}}(\mathcal{C}) = \mathcal{P}(\mathcal{C}) \Rightarrow \aleph_0 \leq \mathcal{C}$.
For finite cardinals $\mathcal{C} \geq 2$ the statement is obvious. So let $S \in \mathcal{C}$ be an infinite set and assume that there is a bijective function

$$B : \mathit{seq}^{\mathit{1\text{-}1}}(S) \longrightarrow \mathcal{P}(S).$$

We use this function to construct an ω-sequence$^{\mathit{1\text{-}1}}$ in S.

Let $n^\star$ $(n < \omega)$ be the cardinality of $\mathit{seq}^{\mathit{1\text{-}1}}(n)$.
Then $0^\star = 1$; $1^\star = 2$; $2^\star = 5$; ... $16^\star = 56,874,039,553,217$; ... (see [Sl], No. 589), and, in general

$$n^\star = \sum_{i=0}^{n} \frac{n!}{i!}$$

We begin by choosing four distinct elements of S, $S_4 := \{s_0, s_1, s_2, s_3\}$ and use these elements to construct a 4-sequence$^{\mathit{1\text{-}1}}$ $\langle s_0, s_1, s_2, s_3\rangle_4$ in S. This sequence will give us an order on the set $\mathit{seq}^{\mathit{1\text{-}1}}(S_4)$ (e.g. we order $\mathit{seq}^{\mathit{1\text{-}1}}(S_4)$ by length and lexicographically).

If we have already constructed an n-sequence$^{\mathit{1\text{-}1}}$ $\langle s_0, s_1, \ldots, s_{n-1}\rangle_n$ in S $(n \geq 4)$, put $S_n := \{s_i : \ i < n\}$. Then $B[\mathit{seq}^{\mathit{1\text{-}1}}(S_n)] \subseteq \mathcal{P}(S)$ has cardinality $n^\star$.

We now define an equivalence relation on S by

$$x \sim y \quad \mathit{iff} \quad \forall q \in \mathit{seq}^{\mathit{1\text{-}1}}(S_n)(x \in B(q) \leftrightarrow y \in B(q)).$$

It is easy to see that for each $q \in \mathit{seq}^{\mathit{1\text{-}1}}(S_n)$

$$B(q) \text{ is the } \textit{disjoint union} \text{ of } \textit{less} \text{ than } n^\star \text{ equivalence classes.} \tag{1}$$

Take the above order on $\mathit{seq}^{\mathit{1\text{-}1}}(S_n)$. This induces an order on the set of equivalence classes eq:= $\{x^\sim : \ x \in S\}$ and also an order on $\mathcal{P}(\text{eq})$.

If there is a first $r \in \mathcal{P}(\text{eq})$ such that $r \notin B[\mathit{seq}^{\mathit{1\text{-}1}}(S_n)]$, then $q_r := B^{-1}(r)$ is a "new" sequence in S. This is $q_r \notin \mathit{seq}^{\mathit{1\text{-}1}}(S_n)$ and we choose the first element s_n of q_r which is not in S_n.
Hence, the sequence $\langle s_0, s_1, \ldots, s_n\rangle_{n+1}$ is now an $(n+1)$-sequence$^{\mathit{1\text{-}1}}$ in S.

If there is an $s_i \in S_n$ such that $\{s_i\} \notin B[\mathit{seq}^{\mathit{1\text{-}1}}(S_n)]$, then use $B^{-1}(\{s_i\})$ to construct an $(n+1)$-sequence$^{\mathit{1\text{-}1}}$ in S.

Otherwise our construction stops at S_n and we write stop(S_n).

Our construction only stops if

$$\begin{array}{ll} \text{for each } s_i \in S_n : & \{s_i\} \in \text{eq and} \\ \text{for each } r \in \mathcal{P}(\text{eq}) & \text{there is a } q_r \in \mathit{seq}^{\mathit{1\text{-}1}}(S_n) \text{ such that } B(q_r) = r. \end{array}$$

If κ $(\kappa < \omega)$ is the cardinality of eq, then 2^κ is the cardiniality of $\mathcal{P}(\text{eq})$ and because of (1) we have stop$(S_n) \ \Rightarrow \ 2^\kappa = n^\star$.
It is known that $0^\star = 1 = 2^0$; $1^\star = 2 = 2^1$; $3^\star = 16 = 2^4$ and $n^\star$ is a power of 2 for some $n > 3$, then n has to be bigger than 10^8.

If there are only finitely many $k, n < \omega$ such that $2^k = n^\star$, then there is a least n_0 such that $2^k = {n_0}^\star$ and $\forall n > n_0(\neg\text{stop}(S_n))$.

Refining our construction removes the need for this strong arithmetic condition.

Assume $\mathrm{stop}(S_n)$.
If $x \notin S_n$ then let $S^x_{n+1} := S_n \dot{\cup} \{x\}$ and $S^x_{n+k} := S^x_{n+1} \dot{\cup} \{Y\}$ with Y of cardinality $k-1$. Because (n is even)$\Leftrightarrow$ ($n^\star$ is odd) and $\mathrm{stop}(S_n)$, we cannot have $\mathrm{stop}(S^x_{n+1})$ for any $x \notin S_n$.

Now we recommence our construction with the set S^x_{n+1} and construct an $(n+k)$-sequence*1-1* $\langle s_0, s_1, \ldots, s_{n+k-1}\rangle_{n+k}$ $(k \geq 2)$ in S.
If the construction also stops at the $(n+\mathrm{stop})^{th}$ stage at the set $S^x_{n+\mathrm{stop}}$ $(\mathrm{stop} \geq 2)$, then we write S^x instead of $S^x_{n+\mathrm{stop}}$.

If there is an $x \in S$ such that S^x is infinite, then our construction does not stop when we recommence with S^x_{n+1} and we can construct an ω-sequence*1-1* in S. But this contradicts our Lemma.

So there cannot be such an x and each $x \in S$ is in exactly one *finite* set S^x. If for each $x \in S$, S^x is the union of some elements of eq, then S must be finite, because eq is finite. But this contradicts our assumption that S is infinite.

A subset of S is called *good* if it cannot be written as the union of elements of eq.

Consider the set $T_{\min} := \{x : \ S^x \text{ is good and of least cardinality}\}$ and let m_{T} be the cardinality of S^x for some x in $T_{\min}$. Further for $x \in T_{\min}$ let $x_= := \{y : S^y = S^x\}$ (these elements of S^x we cannot distinguish) and $m_=$ denote the least cardinality of the sets $x_=$.
If $T_{\min}$ is good, use $B^{-1}(T_{\min})$ to construct an $(n+1)$-sequence*1-1* in S.
Otherwise take $x \in T_{\min}$. Because S^x is good

$$B^{-1}(S^x) \notin \mathit{seq}^{\mathit{1\text{-}1}}(S_n).$$

Thus there is a first y in $B^{-1}(S^x)$ which is not in S_n. It is easy to see that $S^y \subseteq S^x$ and if $S^y \neq S^x$ then S^y is not good (because of $x \in T_{\min}$).
But then $B^{-1}(S^x \setminus S^y) \notin \mathit{seq}^{\mathit{1\text{-}1}}(S^y)$ and we may proceed.

So for each $x \in T_{\min}$ construct an m_{T}-sequence*1-1* SEQ^x in S^x such that

$$S^x = S^y \implies \mathrm{SEQ}^x = \mathrm{SEQ}^y.$$

For $i < m_{\mathrm{T}}$ define

$$Q_i := \{s \in S : \ s \text{ is the } i^{th} \text{ element in } \mathrm{SEQ}^x \text{ for some } x \in S\}$$

Assume there is some $j < m_{\mathrm{T}}$ such that Q_j is good. Then $B^{-1}(Q_j) \notin \mathit{seq}^{\mathit{1\text{-}1}}(S_n)$. But $B^{-1}(Q_j) \in \mathit{seq}^{\mathit{1\text{-}1}}(S)$ and we get an $(n+1)$-sequence*1-1* in S.

It remains to justify our assumption.

Note that if for some $i \neq j$, $z \in Q_i \cap Q_j$, then S^z cannot be good. Furthermore for each $x \in T_{\min}$ there is exactly one i_x such that $x \in Q_{i_x}$ and if $z, y \in x_=$, $z \neq y$, then $i_x \neq i_y$. If there are no good Q_i's, $m_=$ cannot exceed κ, (the cardinality of eq). But by the following this is a contradiction:

An easy calculation modulo 2^r $(r \leq 4)$ shows that for each n, if $2^r|n^\star$, then $2^r|(n+2^r)^\star$ and $2^r\not|(n+t)^\star$ if $0 < t < 2^r$.

Assume there is a smallest k $(k \geq 4)$ such that $2^{k+1}|n^\star$ and $2^{k+1}|(n+t)^\star$ for some t with $0 < t < 2^{k+1}$.

Then, because $2^k|2^{k+1}$, we have $2^k|n^\star$ and $2^k|(n+t)^\star$. Since k is by definition the smallest such number, we know that t must be 2^k.

$$\begin{array}{rlr}
(n+2^k)^\star = \sum\limits_{i=0}^{n+2^k} \frac{(n+2^k)!}{i!} = & 1\cdot 2\cdot\ \dots\ \cdot 2^k\cdot (2^k+1)\cdot\ \dots\ \cdot(2^k+n) & {\scriptstyle (1)} \\
+ & 2\cdot\ \dots\ \cdot 2^k\cdot\ \qquad \dots \qquad \cdot(2^k+n) & {\scriptstyle (2)} \\
 & \qquad \ddots & \vdots \\
+ & \qquad 2^k\cdot \qquad \dots \qquad \cdot(2^k+n) & {\scriptstyle (2^k)} \\
 & \qquad\qquad\qquad \ddots & \vdots \\
+ & \qquad\qquad\qquad\qquad (2^k+n) & {\scriptstyle (2^k+n)} \\
+ & \qquad\qquad\qquad\qquad\qquad 1 & {\scriptstyle (2^k+n+1)}
\end{array}$$

It is easy to see that 2^{k+1} divides rows ${\scriptstyle (1)} - {\scriptstyle (2^k)}$ since $k \geq 2$ and $n \geq 2$.

If we calculate the products of rows ${\scriptstyle (2^k+1) - (2^k+n+1)}$, then we only have to consider sums which are not obiviously divisible by 2^{k+1}. So, for a suitable natural number ε we have

$$(n+2^k)^\star = 2^k \cdot (\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i\cdot j!}) + n^\star + 2^{k+1}\cdot \varepsilon. \tag{2}$$

We know that $2^{k+1}|n^\star$ with $n \geq 3,\ k \geq 4$. And because $n^\star$ is even n has to be odd. If j is $n-1,\ n-2$ or $n-3$, then $\sum\limits_{i>j}^{n} \frac{n!}{i\cdot j!}$ is odd. Moreover, if $0 \leq j \leq (n-4)$, then $\sum\limits_{i>j}^{n} \frac{n!}{i\cdot j!}$ is even. So $\sum\limits_{j=0}^{n-1} \sum\limits_{i>j}^{n} \frac{n!}{i\cdot j!}$ is odd. Hence $2^{k+1}\not|(n+2^k)^\star$, (by (2) and $2^{k+1}|n^\star$).

We return to the proof.

We know that if $2^\kappa = n^\star$ and $(n+t)^\star$ is a power of 2, then 2^κ divides t. $(**)$

Take $x \in T_{\text{min}}$ such that $\Big|x_=\Big| = m_=$. If $y \in S^x$, then

(i) $\Big|S^y\Big| = n + t_y$ with 2^κ divides t_y,
(ii) either $y \in x_=$ or S^y is not good.

This is because $2^\kappa = n^\star$ and $(**)$.

Hence (for a suitable natural number ε) $m_{\text{T}} = \Big|S^x\Big| = n + 2^\kappa \cdot \varepsilon + m_=$ (by (ii)), and 2^κ divides $m_=$ (by (i)).

But this implies that $m_=$ must be larger than κ, which justifies our assumption. $\blacksquare$

The statement obtained when *seq*$^{1\text{-}1}$ is replaced by *seq* is much easier to prove:

Theorem 5: ZF $\vdash$ $seq(\mathcal{C}) \neq \mathcal{P}(\mathcal{C})$ for all cardinals such that $\emptyset \notin \mathcal{C}$.

Proof: Take $S \in \mathcal{C}$. First note the fact that if $\aleph_0 \leq \mathcal{C}$, then $seq(\mathcal{C}) \ngeq \mathcal{P}(\mathcal{C})$.

(The proof is the same as the proof of the Lemma, except that we can skip the first lines of the proof of the Lemma).

Assume there is a bijection B from $seq(S)$ onto $\mathcal{P}(S)$. Choose an $s_0 \in S$, and define a 1-1 function f_{s_0} from ω into $\mathcal{P}(S)$ by $i \mapsto \xi_i := B(\langle s_0, s_0, \dots, s_0\rangle)$ (i-times). Use the ξ_i's to construct pairwise disjoint subsets $c_i \subseteq S$ ($i < \omega$).
Given an n-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \dots, s_{n-1}\rangle_n$ in S, let $S_n := \{s_i : i < n\}$ and the natural order on S_n induce a well-ordering on the set $seq(S_n)$ with order type ω. Then there is a bijection $h : \omega \longrightarrow seq(S_n)$. Now the function $\Gamma := B \circ h$ is a 1-1 function from ω into $\mathcal{P}(S)$ and $t := \dot{\bigcup}\{c_i : c_i \subseteq \Gamma(i)\} \notin \{\Gamma(k) : k \in \omega\}$.
Hence $B^{-1}(t)$ is a sequence in S which does not belongs to S_n. Choose $s_n \in S$ to be the first element of $B^{-1}(t)$ not in S_n. Then $\langle s_0, s_1, \dots, s_n\rangle_{n+1}$ is an $(n+1)$-sequence$^{1\text{-}1}$ in the set S.

Thus, we can construct an ω-sequence$^{1\text{-}1}$ in S, which is a contradiction to the previous fact. $\blacksquare$

References

[Ba] H. Bachmann, Transfinite Zahlen, Springer-Verlag, Berlin (1967).

[Je1] T. Jech, Set Theory, Academic Press, New York (1978).

[Je2] T. Jech, The Axiom of Choice, North-Holland Publ. Co., Amsterdam (1973).

[La] H. Läuchli, Auswahlaxiom in der Algebra, Comment. Math. Helv., vol.37, 1962, 1–18.

[Sl] N.J.A. Sloane, A Handbook of Integer Sequences, Academic Press, New York (1973).

[Sp1] E. Specker, Verallgemeinerte Kontinuumshypothese und Auswahlaxiom, Archiv der Mathematik 5, 1954, 332–337.

[Sp2] E. Specker, Zur Axiomatik der Mengenlehre, Zeitschr. f. math. Logik und Grundl. der Math. 3, 1957, 173–210.