RADICI DELL'UNITÀ

GIOVANNI FELDER

In queste lezioni considereremo le *radici dell'unità* ovvero le soluzioni dell'equazione $x^n = 1$, per un numero intero positivo n dato, in vari contesti. Dopo aver ricordato il contesto più classico dei numeri complessi, studieremo *matrici* che soddisfano quest'equazione, il che ci porterà alla teoria delle *matrici circolanti*, le cui righe sono le permutazioni cicliche della prima riga. Mostreremo che gli zeri del polinomio caratteristico di una matrice circolante di dimensione n sono i valori alle radici n-esime dell'unità del suo polinomio presentatore. Questo ci permetterà di trovare una generalizzazione a gradi più alti della formula di risoluzione

$$x = \frac{-b + \epsilon\sqrt{b^2 - 4ac}}{2a}, \qquad \epsilon^2 = 1,$$

dell'equazione di secondo grado $ax^2 + bx + c = 0$, in cui le diverse soluzioni sono ottenute inserendo diverse radici dell'unità. In particolare otterremo formule di risoluzione per equazioni generali di terzo e quarto grado. Infine studieremo le radici dell'unità nei campi finiti o di Galois. Il risultato principale, dovuto essenzialmente a Galois, è che gli elementi diversi da zero di un campo finito di q elementi sono soluzioni di $x^n = 1$ dove $n = q - 1$ e formano un gruppo ciclico di ordine n. Vedremo come questa osservazione è fondamentale per i codici correttori di Reed–Solomon, utilizzati per la memorizzazione di informazione su CD e DVD, nella comunicazione con le sonde Voyager, nei codici Quick Response (fig. 1) leggibili dai telefonini intelligenti e in molte altre applicazioni.

1. Le radici complesse dell'unità

Questo è il contesto più classico. Le n soluzioni

$$e^{\frac{2\pi i j}{n}} = \cos\left(\frac{2\pi j}{n}\right) + i\sin\left(\frac{2\pi j}{n}\right), \quad j = 0, \dots, n-1, \tag{1}$$

dell'equazione $x^n = 1$ nel campo $\mathbb{C}$ dei numeri complessi sono chiamate radici n-esime complesse dell'unità e formano un gruppo ciclico μ_n di ordine n. In altre parole, l'insieme delle soluzioni è della forma $\mu_n = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. Le radici α per cui vale questo si chiamano *primitive*. Sono della forma (1) dove j e n hanno massimo comun divisore uguale a 1, per esempio $j = 1$.

2. Matrici circolanti e formule di risoluzione

2.1. **Matrici circolanti.** Una matrice quadrata di ordine n a coefficienti in un campo K (per esempio $\mathbb{R}$ o $\mathbb{C}$) si chiama *circolante* se ognuna delle sue righe a partire dalla seconda si ottiene dalla precedente per spostamento ciclico a destra dei coefficienti, per esempio

$$\begin{pmatrix} 1 & 0 & 3 & 4 \\ 4 & 1 & 0 & 3 \\ 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}.$$

Queste matrici hanno proprietà notevoli e lo sviluppo della teoria delle matrici circolanti a coefficienti complessi ci porterà a una formula di risoluzione che mette in corrispondenza biunivoca radici n-esime dell'unità e soluzioni di equazioni algebriche di grado $n \leq 4$.

Una matrice circolante è unicamente definita dalla sua prima riga. È quindi utile introdurre la notazione

$$C(a_0, \dots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

per indicare la matrice circolante la cui prima riga è $(a_0, \dots, a_{n-1})$.

Teorema 2.1. *La matrice identità è circolante. Multipli, somme e prodotti di matrici circolanti sono circolanti. Il prodotto di matrici circolanti è commutativo.*

In altre parole, le matrici circolanti a coefficienti in K formano un'algebra commutativa con unità su K. Le tesi del teorema, ad eccezione di quelle sul prodotto, sono piuttosto ovvie: la matrice identità è $C(1, 0, \dots, 0)$ e per ogni $c \in K$ vale

$$\begin{aligned} C(a_0, \dots, a_{n-1}) + C(b_0, \dots, b_{n-1}) &= C(a_0 + b_0, \dots, a_{n-1} + b_{n-1}), \\ cC(a_0, \dots, a_{n-1}) &= C(ca_0, \dots, ca_{n-1}). \end{aligned}$$

Per capire le proprietà del prodotto di matrici circolanti e la struttura dell'algebra di queste matrici consideriamo la semplice matrice circolante $X = C(0, 1, 0, \cdots, 0)$:

$$X = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Questa matrice corrisponde all'applicazione lineare che manda il vettore $v = (v_0, \dots, v_{n-1})^t$ nel vettore $Xv = (v_1, v_2, \dots, v_{n-1}, v_0)^t$. Se iteriamo questa trasformazione n volte ritroviamo il vettore di partenza.

Quindi X è soluzione dell'equazione

$$X^n = \mathbf{1}$$

nelle matrici quadrate di ordine n, dove $\mathbf{1}$ è la matrice identità. Inoltre vediamo che $X^2 = C(0, 0, 1, 0, \ldots, 0)$ e in generale per $0 \leq k \leq n-1$, $X^k = C(0, \ldots, 1, \ldots, 0)$. Concludiamo che

$$C(a_0, a_1, \ldots, a_{n-1}) = a_0\mathbf{1} + a_1X + a_2X^2 + \cdots a_{n-1}X^{n-1},$$

ovvero: *le matrici circolanti sono i polinomi di grado* $\leq n-1$ *della matrice* X. Da questa rappresentazione segue che il prodotto di matrici circolanti è circolante e che il prodotto di matrici circolanti è commutativo. Il teorema è così dimostrato.

Nel linguaggio dell'algebra si può formulare il risultato nel modo seguente.

L'algebra delle matrici circolanti di ordine n *a coefficienti in* K *è isomorfa all'algebra* $K[x]/(x^n - 1)K[x]$ *generata da una variabile* x *soggetta all'unica relazione* $x^n - 1 = 0$.

L'isomorfismo manda x nella matrice X.

2.2. **Autovettori di matrici circolanti.** Ricordiamo che un vettore $v \in K^n$ non nullo si chiama *autovettore* della matrice $n \times n$ A di *autovalore* $\lambda \in K$ se $Av = \lambda v$.

Vedremo che le matrici circolanti a coefficienti in $K = \mathbb{C}$ (o in un campo algebricamente chiuso) hanno tutte gli stessi autovettori.

Cominciamo a determinare gli autovettori di $X = C(0, 1, 0, \ldots, 0)$. Per le coordinate di un autovettore $v = (v_0, \ldots, v_{n-1})^t$ di autovalore λ deve valere che $v_1 = \lambda v_0, v_2 = \lambda v_1, \ldots, v_0 = \lambda v_{n-1}$. Segue che v è un autovettore se e solo se $\lambda^n = 1$ e $v_j = \lambda^j v_0$ per $j = 0, \ldots, n-1$ e $v_0 \neq 0$.

Quindi per λ radice ennesima dell'unità abbiamo un autovettore di autovalore λ, che normalizziamo ponendo $v_0 = 1$. L'algebra lineare ci insegna che autovettori corrispondenti ad autovalori diversi sono linearmente indipendenti. Abbiamo quindi n autovettori linearmente indipendenti che perciò costituiscono una base dello spazio $\mathbb{C}^n$. Una matrice con una base di autovettori si chiama diagonalizzabile: una tale matrice definisce un'applicazione che espressa nella base di autovettori è data da una matrice diagonale.

Più esplicitamente, ponendo

$$\epsilon = e^{\frac{2\pi i}{n}}$$

abbiamo:

La matrice $X = C(0,1,0,\dots,0)$ *ha autovalori* $1, \epsilon, \epsilon^2, \dots, \epsilon^{n-1}$. *Un autovettore corrispondente all'autovalore* ϵ^j *è*

$$b_j = \begin{pmatrix} 1 \\ \epsilon^j \\ \epsilon^{2j} \\ \vdots \\ \epsilon^{(n-1)j} \end{pmatrix},$$

Questa descrizione ci consente di determinare gli autovettori e autovalori di tutte le matrici circolanti. Per formulare il risultato introduciamo una definizione.

Definizione 2.2. Il *polinomio presentatore*[1] della matrice circolante $C = C(a_0, \dots, a_{n-1})$ è il polinomio

$$P_C(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

Teorema 2.3. *Per ogni matrice circolante* C *di ordine* n *e polinomio presentatore* P_C *vale l'identità*

$$C\, b_j = P_C(\epsilon^j) b_j, \qquad j = 0, \dots, n-1.$$

In altre parole, per ogni j *il vettore* b_j *è autovettore di ogni matrice circolante* C *e il corrispondente autovalore è il valore del polinomio presentatore nella radice dell'unità* ϵ^j.

Dimostrazione. È chiaro che da $Xb_j = \epsilon^j b_j$ segue che $X^p b_j = (\epsilon^j)^p b_j$ e quindi

$$(a_0\mathbf{1} + a_1 X + \cdots + a_{n-1} X^{n-1}) b_j = (a_0 + a_1\epsilon^j + \cdots + (\epsilon^j)^{n-1}) b_j = P_C(\epsilon^j) b_j.$$

□

Esempio 1. Per $n = 1$, $\epsilon = -1$. La matrice circolante $C = C(a,b) = \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ ha polinomio presentatore $P_C(x) = a + bx$ e vale

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = (a+b) \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$
$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = (a-b) \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

il che si può anche facilmente verificare direttamente.

Corollario 2.4. *Il determinante di una matrice circolante è il prodotto dei valori del suo polinomio presentatore nelle radici dell'unità:*

$$\det C(a_0, \dots, a_{n-1}) = P_C(1) P_C(\epsilon) P_C(\epsilon^2) \cdots P_C(\epsilon^{n-1}).$$

[1] Il termine inglese è "representer" .

Infatti il determinante di una matrice complessa è il prodotto dei suoi autovalori.

Osserviamo che si può considerare questa formula come una generalizzazione del prodotto notevole

$$a^2 - b^2 = (a + b)(a - b)$$

che si ritrova nel caso $n = 2$ dell'esempio 1.

Per $n = 3$, il determinante di $C(a, b, c)$ è $a^3 + b^3 + c^3 - 3abc$ e quindi deduciamo l'identità

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a + b\epsilon + c\epsilon^{-1})(a + b\epsilon^{-1} + c\epsilon),$$

$$\epsilon = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

2.3. **Formule di risoluzione.** Ricordiamo che il *polinomio caratteristico* di una matrice quadrata $n \times n$ C

$$\chi_C(z) = \det(z\mathbf{1} - C)$$

Osserviamo che se $C = C(a_0, \ldots, a_{n-1})$ è circolante allora $z\mathbf{1} - C$ è la matrice circolante $C(z - a_0, -a_1, \ldots, -a_{n-1})$. Il corollario 2.4 fornisce una relazione tra il polinomio caratteristico e il polinomio presentatore di una matrice circolante:

Teorema 2.5. *Il polinomio caratteristico di una matrice circolante C di ordine n e polinomio presentatore P_C è*

$$\chi_C(z) = (z - P_C(1))(z - P_C(\epsilon))(z - P_C(\epsilon^2)) \cdots (z - P_C(\epsilon^{n-1})).$$

Dimostrazione. Un modo di dimostrare il teorema è di osservare che il polinomio presentatore di $z\mathbf{1} - C$ è $z - P_C(x)$ (visto come polinomio di variabile x) e applicare il corollario 2.4. L'altro modo è di utilizzare il fatto che le radici del polinomio caratteristico di una matrice sono gli autovalori della matrice, che nel nostro caso sono dati dal teorema 2.3. □

La formula del teorema 2.5 dà una formula di risoluzione per polinomi caratteristici di matrici circolanti. Il polinomio presentatore stabilisce una corrispondenza $\epsilon^j \mapsto P_C(\epsilon^j)$ tra le radici ennesime dell'unità e le radici del polinomio caratteristico $\chi_C(z)$.

Il fatto che le equazioni di grado inferiore o uguale al quarto hanno una formula risolutiva generale esprimibile tramite radicali si può formulare in modo efficace utilizzando matrici circolanti.

Teorema 2.6. *Ogni polinomio di grado ≤ 4 è polinomio caratteristico di una matrice circolante i cui coefficienti si esprimono a partire dai coefficienti del polinomio tramite radicali.*

Vediamo prima come si realizza quest'idea nel caso dell'equazione di secondo grado:

$$z^2 + pz + q = 0$$

Si cerca quindi una matrice circolante $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ il cui polinomio caratteristico $(z-a)^2 - b^2$ è $z^2 + pz + q$.

$$-2a = p, \qquad a^2 - b^2 = q.$$

Una soluzione è $a = -p/2$, $b = \sqrt{p^2/4 - c}$. Le radici sono quindi i valori del polinomio presentatore $P_C(x) = a + bx$ per $x = \pm 1$:

$$z_1 = P_C(1) = a + b, \qquad z_2 = P_C(-1) = a - b.$$

Per $n = 3$ consideriamo l'equazione

$$z^3 + pz + q = 0 \tag{2}$$

Si può ricondurre l'equazione generale di terzo grado a una di questa forma con una sostituzione $z \mapsto z + m$. Il polinomio caratteristico della matrice circolante $C(0, a, b)$ è

$$\det \begin{pmatrix} z & -a & -b \\ -b & z & -a \\ -a & -b & z \end{pmatrix} = z^3 - 3abz - a^3 - b^3$$

Per applicare il risultato alla risoluzione dell'equazione cerchiamo una matrice circolante di polinomio caratteristico dato (2). Dobbiamo quindi trovare una soluzione (a, b) del sistema

$$3ab = -p, \quad a^3 + b^3 = -q$$

Eliminando b si ottiene un'equazione di secondo grado per $c = a^3$:

$$c^2 + qc - p^3/27 = 0$$

Otteniamo quindi una soluzione (per qualsiasi scelta delle radici cubiche e quadrate)

$$a = \left(-\frac{q}{2} + \frac{1}{2} \left(q^2 + \frac{4p^3}{27} \right)^{\frac{1}{2}} \right)^{\frac{1}{3}}, \quad b = -\frac{p}{3a}.$$

La divisione per a presuppone che $a \neq 0$ che vale se $p \neq 0$. Se $p = 0$, scegliamo più semplicemente $a = 0$, $b = -q^{1/3}$.

Il polinomio presentatore è $P_C(x) = az + bz^2$ e le radici cercate sono quindi

$$z_1 = a + b, \quad z_2 = a\epsilon + b\epsilon^2, \quad z_3 = a\epsilon^2 + b\epsilon,$$

dove

$$\epsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \quad \epsilon^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Il calcolo delle radici di un polinomio di quarto grado

$$z^4 + pz^2 + qz + r \tag{3}$$

è un po' più complicato. Il polinomio caratteristico di $C(0,a,b,c)$ è della forma (3) dove

$$\begin{aligned} p &= -2b^2 - 4ac, \\ q &= -4b(a^2+c^2) \\ r &= -a^4 + b^4 - c^4 - 4ab^2c + 2a^2c^2 \\ &= -(a^2+c^2)^2 + b^4 - 4acb^2 + 4(ac)^2 \end{aligned}$$

Le prime due equazioni ci permettono di eliminare le espressioni $4ac = -p - 2b^2$ $a^2 + c^2 = -q/(4b)$ da r per ottenere un'equazione di terzo grado per b^2:

$$64b^6 + 32pb^4 + (4p^2 - 16r)b^2 + q^2 = 0$$

Data una soluzione b di quest'equazione, ottenuta prendendo la radice quadrata di una soluzione per b^2 data dalla formula di Cardano, si possono esprimere anche a, c in funzione di p, q, r risolvendo equazioni di grado 2. Otteniamo quindi a, b, c espressi nei termini di p, q, r utilizzando le quattro operazioni e l'estrazione di radice quadrata e cubica. Le quattro soluzioni di (3) sono infine ottenute valutando il polinomio presentatore nelle radici $1, i, -1, -i$:

$$\begin{aligned} z_1 &= a + b + c, \\ z_2 &= a\,i - b - c\,i, \\ z_3 &= -a + b - c, \\ z_4 &= -a\,i - b + c\,i. \end{aligned}$$

2.4. **Esercizi.**

(1) La trasposta A^t di una matrice $A = (a_{ij})$ è la matrice i cui coefficienti sono $a^t_{ij} = a_{ji}$. Dimostrare che la trasposta di una matrice $n \times n$ circolante C è circolante e che $P_C(x) = x^n P_{C^t}(x^{-1})$. Per $K = \mathbb{C}$ trovare un'affermazione analoga per l'aggiunta C^* (trasposta coniugata) di una matrice circolante C.

(2) Una matrice A a coefficienti complessi si chiama *normale* se è $AA^* = A^*A$. Mostrare che le matrici circolanti complesse sono normali. Il teorema spettrale asserisce che le matrici normali hanno una base *ortonormata* di autovettori per il prodotto scalare $(v, w) = \sum v_i \bar{w}_i$. Si verifichi questo teorema per le matrici circolanti costruendo una base ortonormata di autovettori.

3. L'equazione $x^n = 1$ nei campi di Galois

Ricordiamo che un *campo* è un insieme K munito di un'addizione $+\colon K \times K \to K$ e una moltiplicazione $\cdot\colon K \times K \to K$ tali che (i) $(K, +)$ è un gruppo abeliano, chiamato gruppo additivo del campo. Denotiamo l'elemento neutro con 0 e l'inverso di a con $-a$. (ii) $(K \smallsetminus \{0\}, \cdot)$ è un

gruppo abeliano, chiamato gruppo moltiplicativo del campo, con elemento neutro 1 e inversione $a \mapsto a^{-1}$. (iii) Vale la proprietà distributiva $a \cdot (b + c) = a \cdot b + a \cdot c$, $a, b, c \in K$.

Gli esempi classici sono $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Qui ci occuperemo dei campi finiti, chiamati anche campi di Galois, che ne aveva già implicitamente descritto le proprietà fondamentali nel suo lavoro *Sur la théorie des nombres* del 1830 [2]. La nozione di campo astratto come sopra fu introdotta più tardi, da Dedekind e Weber.

I campi di Galois più semplici sono i campi $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ delle classi di resto modulo un numero primo p. Un elemento di $\mathbb{F}_p$ è la classe di equivalenza $[n]$ di un numero intero n, dove due interi sono equivalenti se e solo se la loro differenza è un multiplo di p. Addizione e moltiplicazione sono indotte dalle operazioni sui numeri interi. La particolarità di $\mathbb{Z}/p\mathbb{Z}$ con p primo è che tutti gli elementi diversi da $0 = [0]$ hanno un inverso per la moltiplicazione. Per semplificare la notazione scriveremo j invece di $[j]$ per indicare la classe del numero intero j, che possiamo scegliere tra 0 e $p - 1$.

Esempio 2. Le operazioni del campo $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ di ordine 5 sono date dalle seguenti tabelle:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Enunciamo due risultati fondamentali sui campi di Galois, per la cui dimostrazione rimandiamo a un libro di algebra.

Teorema 3.1. *Per ogni potenza $q = p^m$, $m = 1, 2, \ldots$ di un numero primo esiste un campo finito $\mathbb{F}_q$ con q elementi. Ogni campo finito è isomorfo a uno di questi.*

Il campo $\mathbb{F}_q$ con $q = p^m$ è un estensione galoisiana di grado m di $\mathbb{F}_p$ e può essere definito come il campo di spezzamento dell'equazione $x^q = x$. Per le applicazione è utile avere una costruzione più esplicita: $\mathbb{F}_q$ è ottenuta aggiungendo un numero immaginario (che Galois chiamò i), radice di un (arbitrario) polinomio irriducibile F di grado m a coefficienti in $\mathbb{F}_p$. Nelle parole di Galois [2],

> Soit une pareille équation ou congruence, $\mathrm{F}x = 0$, et p le module. Supposons d'abord, pour plus de simplicité, que la congruence en question n'admette aucun facteur commensurable, c'est-à-dire qu'on ne puisse pas trouver trois fonctions $\varphi x, \psi x, \chi x$ telles que
>
> $$\varphi x.\psi x = \mathrm{F}x + p.\chi x.$$

> Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions des nombres entiers, symboles dont l'emploi, dans le calcul, sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.

In notazione moderna $\mathbb{F}_q$ è l'anello quoziente $\mathbb{F}_q = \mathbb{F}_p[x]/F(x)\mathbb{F}_p[x]$. Per esempio per costruire $\mathbb{F}_4$ si può prendere $F(x) = x^2 - x - 1$ e definire $\mathbb{F}_4$ come l'insieme delle espressioni $a + b\ i$ dove $a, b \in \mathbb{F}_2 = \{0, 1\}$ e vale la relazione $i^2 = i + 1$. Un altro esempio, presentato da Galois, è $\mathbb{F}_{343} = \mathbb{F}_7[x]/(x^3 - 2)\mathbb{F}_7[x]$, consistente delle $343 = 7^3$ espressioni $a + b\,i + c\,i^2$ con coefficienti $a, b, c \in \mathbb{F}_7$ dove il numero immaginario i è soggetto alla relazione $i^3 = 2$. Sulla base di questa costruzione, Galois dimostra il

Teorema 3.2. *Il gruppo moltiplicativo di $\mathbb{F}_q$ è ciclico di ordine $q - 1$. In altre parole esiste un generatore $\alpha \in \mathbb{F}_q$ tale che*

$$\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$$

e $\alpha^{q-1} = 1$.

Un tale generatore α è chiamato *radice primitiva dell'unità*.

Esempio 3. In $\mathbb{F}_5$ possiamo prendere $\alpha = 2$: le sue potenze $1, 2$, $\alpha^2 = 4$, $\alpha^3 = 3$ esauriscono $\mathbb{F}_5 \smallsetminus \{0\}$. Oppure $\alpha = 3$, ma non $\alpha = 4$, il cui quadrato modulo 5 è 1.

Esempio 4. Galois mostra che $\alpha = i - i^2$ è una radice primitiva dell'unità di $\mathbb{F}_{343}$, costruito come sopra.

3.1. **Esercizi.**

(1) Quali sono le radici primitive in $\mathbb{F}_7$?
(2) Quali sono le radici primitive in $\mathbb{F}_{2^{31}}$? [Suggerimento: i numeri primi della forma $2^p - 1$ sono chiamati numeri primi di Mersenne. I numeri primi più grandi conosciuti sono di questa forma. Nel 1772 Eulero scoprì l'ottavo numero primo di Mersenne $2^{31} - 1 = 131071$]
(3) Si dia una formula per la somma e il prodotto in $\mathbb{F}_4$, realizzato come il campo delle espressioni $a + bi$ con $a, b \in \mathbb{F}^2$ e $i^2 = i + 1$. Si compilino le tabelle di addizione e moltiplicazione.

4. Codici di Reed–Solomon

4.1. **Codici correttori.** La teoria dei codici correttori tratta il problema di trasmettere informazione in modo affidabile attraverso un canale disturbato. L'idea è di codificare l'informazione da trasmettere in modo tale che il ricevente sia in grado di rilevare e correggere entro certi

limiti gli errori di trasmissione. Un modo semplice (ma non molto efficiente) di realizzare quest'idea è di utilizzare un codice di ripetizione: per trasmettere un messaggio, consistente di una successione finita di simboli di un certo alfabeto, ripetiamo ogni carattere un certo numero di volte, per esempio cinque volte. Quindi per mandare il messaggio di nove simboli 'mi senti?' trasmetteremo

```
mmmmmiiiii      sssssseeeeennnnnttttttiiiii?????
```

Questo codice può rilevare fino a quattro errori di trasmissione e correggerne due: se sappiamo che il messaggio è trasmesso con al massimo due simboli sbagliati possiamo correggerlo prendendo in ogni blocco di cinque lettere quella che appare più spesso. Se invece ci fossero fino a quattro simboli sbagliati, per esempio se l'inizio del messaggio fosse corrotto in 'mcmcc', il ricevente capirebbe che ci sono stati errori di trasmissione ma non sarebbe in grado di correggerli.

Vediamo che con questo codice dobbiamo inviare il quintuplo dell'informazione, in questo caso 45 simboli per poter correggere due errori. Il *tasso* di trasmissione del codice, ovvero il rapporto tra numero di simboli nel messaggio e il numero di simboli trasmessi è quindi $R = 1/5$. Questo tasso ci permette di tollerare fino a $2/45 \approx 4\%$ di errori. Descriveremo con l'aiuto della teoria dei gruppi di Galois dei codici con un tasso molto più vicino a $R = 1$ in grado di correggere più errori.

4.2. **Codici a blocchi.** Nella teoria dei *codici a blocchi* supponiamo di voler inviare dei messaggi che scomponiamo in blocchi di k simboli tratte da un un insieme finito di q elementi che chiamiamo alfabeto. Ognuno dei q^k blocchi possibili viene codificato in un blocco diverso di lunghezza $n \geq k$ che sarà trasmesso. Abbiamo quindi un'applicazione iniettiva $A^k \to A^n$ chiamata *codifica*. La sua immagine C, un sottoinsieme di A^n, è chiamato *codice* e i suoi q^k elementi sono chiamati *parole di codice* (codewords).

La *distanza di Hamming* tra due elementi di A^n è il numero di coordinate in cui differiscono: se $a = (a_1, \ldots, a_n)$ e $b = (b_1 \ldots, b_n) \in A^n$ la loro distanza $\delta(a, b)$ è il numero di indici $i \in \{1, \ldots, n\}$ per cui $a_i \neq b_i$. Per esempio, se A è l'alfabeto italiano, abbiamo δ(Galois,Geloso)$= 3$ per la distanza di Hamming tra parole di sei lettere in A^6. La *distanza minima di Hamming* di un codice $C \subset A^n$ è il valore minimo della distanza di Hamming tra due parole di codice diverse. In altre parole se la distanza minima è d occorre modificare almeno d simboli di una parola di codice per ottenerne un'altra. Di conseguenza un codice di distanza minima d può rilevare fino a $d-1$ errori e correggerne $\lfloor \frac{d-1}{2} \rfloor$, la parte intera di $\frac{d-1}{2}$. Più precisamente, se trasmettiamo una parola di codice attraverso un canale di cui sappiamo che il numero di errori di trasmissione è al massimo $d-1$, il ricevente può capire se ci sono stati errori, e chiedere di rispedire il messaggio. Se questo numero è al massimo $\lfloor \frac{d-1}{2} \rfloor$, il ricevente può addirittura correggere gli errori: può

ricostruire la parola inviata cercando tra le parole di codice quella *più vicina* per la distanza di Hamming a quella ricevuta, ovvero quella che ha più lettere in comune nelle stesse posizioni.

Vogliamo quindi rendere la distanza minima d più grande possibile. Un semplice ragionamento mostra che c'è un limite superiore per d, valida per tutti i codici a blocchi:

Lemma 4.1. *Per la distanza minima di un codice $C \subset A^n$ costituito da q^k parole di codice di lunghezza n scritte in un alfabeto A di q simboli vale la disuguaglianza di Singleton*

$$d \leq n - k + 1$$

Dimostrazione. Supponiamo che la distanza di Hamming minima tra le parole di codice sia d. Questo implica che se cancelliamo i primi $d-1$ simboli di ogni parola di codice otteniamo ancora q^k parole distinte in A^{n-d+1}. Siccome quest'ultimo insieme ha q^{n-d+1} elementi, deve valere

$$k \leq n - d + 1$$

□

Costruiremo ora dei codici col valore ottimale $d = n - k + 1$ della distanza minima utilizzando l'algebra lineare su un campo di Galois. Questi codici hanno come alfabeto il campo $\mathbb{F}_q$ e la particolarità che la somma di parole di codice, viste come elementi dello spazio vettoriale $\mathbb{F}_q^n$ sul campo $\mathbb{F}_q$, è ancora una parola di codice.

Definizione 4.2. Un *codice lineare* di alfabeto $\mathbb{F}_q$, lunghezza n e dimensione k è un sottospazio vettoriale di $\mathbb{F}_q^n$ di dimensione k. Una *codifica lineare* di alfabeto $\mathbb{F}_q$, lunghezza n e dimensione k è un'applicazione lineare iniettiva

$$\mathbb{F}_q^k \to \mathbb{F}_q^n.$$

Chiaramente l'immagine di una codifica lineare è un codice lineare. Un codice lineare di alfabeto $\mathbb{F}_q$, lunghezza n, dimensione k e distanza minima d è anche chiamato codice $[n, k, d]_q$. I codici $[n, k, n - k + 1]_q$, che saturano la disuguaglianza di Singleton, sono chiamati codici MDS (*Maximum Distance Separable*).

4.3. **Codici di Reed–Solomon.** Il codice di Reed–Solomon $\mathrm{RS}(n, k)$ è un codice lineare di lunghezza n, dimensione k e alfabeto $\mathbb{F}_q$ dove $n = q - 1$. È quindi dato da un sottospazio di dimensione k dello spazio vettoriale $\mathbb{F}_q^n$ sul campo $\mathbb{F}_q$. Diamo due definizioni diverse di questo codice, dando due codifiche (applicazioni lineari iniettive)

$$\mathbb{F}_q^k \to \mathbb{F}_q^n$$

diverse. Il codice è l'immagine di queste applicazioni. Per la prima codifica, che risale alla definizione originale di Reed e Solomon, è facile calcolare la distanza di Hamming minima tra due parole di codice. La

seconda è quella utilizzata nelle applicazioni perché per essa esistono efficienti algoritmi di decodifica e correzione degli errori.

Per descrivere le codifiche è utile pensare a un blocco da codificare o una parola di codice, consistente di un gruppo di simboli dell'alfabeto $\mathbb{F}_q$ come la lista dei coefficienti di un polinomio. Quindi a un blocco $(p_0, \dots, p_{k-1}) \in \mathbb{F}_q^k$ da codificare corrisponde il polinomio di grado $\leq k-1$

$$p(x) = p_0 + p_1 x + \cdots p_{k-1} x^{k-1}.$$

Utilizzeremo più volte questa rappresentazione. La prima codifica è data dall'applicazione di valutazione alle radici dell'unità

$$p(x) \mapsto (p(1), p(\alpha), p(\alpha^2), \dots, p(\alpha^{n-1}))$$

dove α è una radice primitiva. Il risultato seguente mostra non solo che questa codifica è un'applicazione iniettiva ma che la distanza di Hamming minima tra l'immagine di due elementi diversi è almeno $n-k+1$.

Teorema 4.3. *Il codice di Reed–Solomon RS(n,k) è un codice $[n,k,n-k+1]_q$ con $n = q-1$. È quindi un codice lineare MDS consistente di q^k parole di codice composte da n simboli di un alfabeto di q simboli; è in grado di rilevare $n-k$ errori e correggerne $\lfloor \frac{n-k}{2} \rfloor$.*

Dimostrazione. Dobbiamo mostrare che la distanza minima è $n-k+1$, cioè che se $a(x), b(x)$ sono polinomi diversi di grado minore di k, allora la distanza di Hamming tra le loro immagini $(a(1), \dots, a(\alpha^{n-1}))$, $(b(1), \dots, b(\alpha^{n-1}))$ è almeno $n-k+1$. Ciò significa che le immagini differiscono almeno in $n-k+1$ posizioni. Supponiamo per assurdo che a e b siano diversi ma che differiscano in meno di $n-k+1$ posizioni, ovvero che $a(x) = b(x)$ per almeno k valori diversi $x_1, \dots, x_k$ di x presi tra le radici dell'unità. Allora il polinomio $p(x) = a(x) - b(x)$ di grado $k-1$ ha k zeri diversi, il che è possibile solo se p è il polinomio nullo quindi se a e b coincidono. □

Esempio 5. Il codice RS$(4,2)$ è costituito da 25 parole di lunghezza 4 e alfabeto $\mathbb{F}_5 = \{0,1,2,3,4\}$. Negli esercizi qui sotto si propone di calcolarlo. La risposta è:

$$\{0000, 3410, 1320, 4230, 2140, 0341, 3201, 1111, 4021, 2431,$$
$$0132, 3042, 1402, 4312, 2222, 0423, 3333, 1243, 4103, 2013,$$
$$0214, 3124, 1034, 4444, 2304\},$$

dove utilizziamo la notazione abbreviata *abcd* per indicare un elemento (a,b,c,d) di $\mathbb{F}_5^4$. Il teorema implica che la distanza minima di Hamming di questo codice è $d = 3$: ogni coppia di parole diverse differisce in almeno 3 simboli, il che si può anche verificare direttamente.

FIGURA 1. Un esempio di codice QR (marchio registrato della DENSO Corporation) rappresentante una celebre citazione di Galois. L'area al di fuori dei tre grandi quadrati di posizionamento è divisa in gruppi di otto quadrati bianchi o neri e rappresentano ciacuno un byte, o elemento di $\mathbb{F}_{256}$. La sequenza di questi byte sono una parola di un codice di Reed–Solomon. Il meccanismo di correzione degli errori permette di leggere il messaggio anche se è parzialmente coperto.

Esempio 6. Gli alfabeti $\mathbb{F}_{128}$ e $\mathbb{F}_{256}$ sono usati comunemente in informatica, perché in essi sono rappresentati i caratteri ASCII e UTF-8 tradotti in sequenze di 7 bit (ASCII) o 8 bit (UTF-8) utilizzate dai computer e da internet. Per esempio la lettera A è rappresentata dalla sequenza 01000001 nel sistema di codifica UTF-8. Il codice di Reed–Solomon RS(255,223) codifica blocchi di 223 caratteri in blocchi di lunghezza 255, quindi con un tasso di $223/255 \approx 87\%$, e corregge fino a $(255-223)/2 = 16$ errori ossia tollera un numero di errori fino al 6% del numero di caratteri trasmessi.

Osservazione 4.4. I codici di Reed–Solomon hanno la particolarità di avere lunghezza uguale al numero di simboli dell'alfabeto meno 1. Vedremo negli esercizi che con una semplice procedura di *accorciamento* si possono costruire codici MDS più generali.

Proponiamo ora una descrizione delle parole del codice $\mathrm{RS}(n,k)$ indipendente dalla codifica. Se identifichiamo anche $\mathbb{F}_q^n$ con lo spazio dei polinomi di grado al massimo $n-1$, possiamo interpretare la prima codifica come un'applicazione che manda un polinomio di grado $\leq k-1$ in un polinomio di grado $\leq n-1$:

$$p(x) \mapsto p(1) + p(\alpha)x + p(\alpha^2)x^2 + \cdots + p(\alpha^{n-1})x^{n-1}. \tag{4}$$

Teorema 4.5. *Il codice di Reed–Solomon $RS(n,k)$, visto come l'immagine dell'applicazione* (4)*, consiste dei polinomi di grado $n-1$ che si annullano in $\alpha, \ldots, \alpha^{n-k}$.*

Dimostrazione. Dimostriamo prima che i polinomi del codice si annullano in questi punti. La dimostrazione utilizza una proprietà basilare delle soluzioni dell'equazione $x^m = 1$:

Se per un elemento $a \neq 1$ di un campo K vale $a^m = 1$ allora $1 + a + a^2 + \cdots + a^{m-1} = 0$.

Questa proprietà segue dall'identità elementare

$$1 + x + x^2 + \cdots x^{m-1} = \frac{1 - x^m}{1 - x},$$

che vale in ogni anello quando $1 - x$ è invertibile.

Visto che la codifica di Reed–Solomon è un'applicazione lineare, è sufficiente dimostrare che l'immagine di ciascuno dei monomi $p(x) = 1, x, \ldots, x^{k-1}$ si annulla in $\alpha, \ldots, \alpha^{n-k}$. L'immagine di x^ℓ è il polinomio

$$f(x) = \sum_{j=0}^{n-1} \alpha^{j\ell} x^j$$

Abbiamo quindi che per $r = 1, \ldots, n - k$

$$f(\alpha^r) = \sum_{j=0}^{n-1} \alpha^{j\ell} \alpha^{jr} = \sum_{j=0}^{n-1} (\alpha^{\ell+r})^j = 0,$$

perché $\ell + r$, con $0 \leq \ell \leq k-1$ e $1 \leq r \leq n-k$, è compreso tra 1 e $n-1$ e quindi $\alpha^{\ell+r} \neq 1$. Questo dimostra che i polinomi nell'immagine della codifica si annullano in $\alpha, \ldots, \alpha^{n-k}$. Quindi i polinomi di grado $n - 1$ che si annullano in questi punti formano un sottospazio V del codice, che è a sua volta un sottospazio di dimensione k di $\mathbb{F}_q^n$. Per dimostrare che V coincide con il codice basta mostrare che ha anch'esso dimensione k. Ma questo è ovvio perché i polinomi di V sono i polinomi di grado $n - 1$ divisibili per

$$g(x) = (x - \alpha) \cdots (x - \alpha^{n-k}), \tag{5}$$

ovvero quelli della forma

$$(a_0 + a_1 x + \cdots a_{k-1} x^k) g(x), \quad a_0, \ldots, a_{k-1} \in \mathbb{F}_q.$$

□

La dimostrazione suggerisce una seconda codifica $\mathbb{F}_q^k \to \mathbb{F}_q^n$, che è quella usata nella pratica, con immagine uguale al codice di Reed–Solomon. Come sopra associamo a $p = (p_0, \ldots, p_{k-1}) \in \mathbb{F}_q^k$ il polinomio $p(x) = p_0 + p_1 x + \cdots p_{k-1} x^{k-1}$. La codifica manda p nei coefficienti $(f_0, \ldots, f_{n-1})$ del polinomio $p(x)g(x)$ di grado $\leq n-1$ dove $g(x)$ è data dalla (5). Quindi la seconda codifica è data dall'applicazione

$$p(x) \mapsto f(x) = p(x) \prod_{j=1}^{n-k} (x - \alpha^j),$$

dallo spazio dei polinomi di grado $\leq k - 1$ allo spazio dei polinomi di grado $\leq n-1$. Il polinomio $g(x) = \prod_{j=1}^{n-k} (x - \alpha^j)$ è chiamato *polinomio generatore* del codice.

Supponiamo di trasmettere il blocco dei coefficienti di $f(x)$ e che ci siano al massimo $\lfloor (n-k)/2 \rfloor$ errori di trasmissione. Il ricevente del messaggio può facilmente verificare se ci sono stati degli errori di trasmissione valutando il polinomio ricevuto $r(x)$ in $\alpha, \ldots, \alpha^{n-k}$. Se $r(\alpha) = \cdots = r(\alpha^{n-k}) = 0$, il ricevente concluderà che non ci sono stati errori di trasmissione e potrà ottenere il messaggio $p(x)$ dividendo per $g(x) = \prod_{j=1}^{n-k}(x - \alpha^j)$. Se invece ci sono stati errori, avremo

$$r(x) = f(x) + e(x) = p(x)g(x) + e(x),$$

dove $e(x)$ è il polinomio i cui coefficienti sono gli errori nei simboli corrotti. Il compito di un algoritmo di correzione è di trovare $e(x)$, per sottrarlo da $r(x)$ e ottenere $p(x)$ dividendo per $g(x)$. Gli algoritmi di correzione, per cui rimandiamo alla bibliografia, utilizzano il fatto che $e(x)$ è unicamente determinato dai suoi valori $e(\alpha), \ldots, e(\alpha^{n-k})$, chiamati sindromi. Visto che g si annulla in questi punti, il ricevente può calcolare le sindromi direttamente valutando il polinomio ricevuto: $e(\alpha^j) = f(\alpha^j)$, per $j = 1, \ldots, n-k$.

4.4. **Esercizi.**

(1) Indichiamo come calcolare il codice RS$(4, 2)$ (Esempio 5).
   (a) Mostrare che $\alpha = 2$ è una radice dell'unità in $\mathbb{F}_5$ e calcolare il polinomio generatore $g(x) = (x - \alpha)(x - \alpha^2)$. [Risposta: $g(x) = 2 + 4x + x^2$].
   (b) Mostrare che la seconda codifica $\mathbb{F}_5^2 \to \mathbb{F}_5^4$ manda $(1, 0)$ in $(3, 4, 1, 0)$ e $(0, 1)$ in $(0, 3, 4, 1)$.
   (c) Calcolare (preferibilmente con l'aiuto di un computer) l'immagine di tutti gli altri vettori utilizzando la linearità.

(2) Mostrare che il tasso R di un codice e la percentuale e di errori tollerati per simbolo trasmesso sono legati dalla formula $e \cong (1 - R)/2$ (con uguaglianza esatta se la distanza minima di Hamming d è dispari).

(3) Sia $0 < \ell < k$. Mostrare che la seconda codifica di RS(n, k) manda polinomi di grado al più $\ell - 1$ in polinomi di grado al più $m - 1$ con $m = n - k + \ell$. Otteniamo quindi una codifica $\mathbb{F}_q^\ell \to \mathbb{F}_q^m$. Mostrare che la sua immagine è un codice MDS di tipo $[m, \ell, m - \ell + 1]_q$. Questi codici sono chiamati codici di Reed–Solomon *accorciati*.

(4) Dimostrare che i codici RS$(n, 1)$ sono codici di ripetizione.

Riferimenti bibliografici

[1] Dan Kalman and James E. White, *Polynomial equations and circulant matrices*, Amer. Math. Monthly **108** (2001), no. 9, 821–840, DOI 10.2307/2695555. MR1864053 (2002h:15031)

[2] Évariste Galois, *Sur la théorie des nombres*, Œuvres mathématiques, Gauthier-Villars, 1897, pp. 15–23.
`http://fr.wikisource.org/wiki/Œuvres_mathématiques/5`.

[3] Luca Giuzzi, *Codici correttori*: *Un'introduzione*, UNITEXT, Springer, Milano, 2006.
[4] Jacobus Hendricus van Lint, *Introduction to coding theory*, 3rd ed., Graduate Texts in Mathematics, vol. 86, Springer-Verlag, Berlin, 1999. MR1664228 (2000a:94001)

Dipartimento di matematica, ETH, CH-8092 Zurigo

felder@math.ethz.ch