

Capitolo 15

Codici lineari e disegni

15.1 Generalit 

Sia $q = p^h$ una potenza di un primo p , $F = F_q$ il campo di Galois con q elementi e $\mathcal{P} = \{p_1, p_2, \dots, p_v\}$ un insieme finito con v elementi.

Per ogni parola $\mathbf{a} = (a_1, a_2, \dots, a_v)$ di lunghezza v su F , definiamo *supporto di \mathbf{a}* l'insieme dei punti p_i di \mathcal{P} tali che $a_i \neq 0$. Il supporto di una parola \mathbf{a} , che denoteremo con $\text{supp}(\mathbf{a})$,   quindi un sottoinsieme di \mathcal{P} e chiaramente risulta

$$\text{supp}(\mathbf{a}) = \emptyset \Leftrightarrow \mathbf{a} = \mathbf{0},$$

$$|\text{supp}(\mathbf{a})| = w(\mathbf{a}),$$

$$\text{supp}(\mathbf{a}) = \mathcal{P} \Leftrightarrow w(\mathbf{a}) = v.$$

Osserviamo che, se denotiamo con \star l'operazione di differenza simmetrica, risulta

$$q = 2 \Rightarrow \begin{cases} \text{supp}(\mathbf{a} + \mathbf{b}) = \text{supp}(\mathbf{a}) \star \text{supp}(\mathbf{b}) \\ d(\mathbf{a}, \mathbf{b}) = |\text{supp}(\mathbf{a}) \star \text{supp}(\mathbf{b})| \\ \mathbf{a}\mathbf{b} = 0 \Leftrightarrow |\text{supp}(\mathbf{a}) \cap \text{supp}(\mathbf{b})| \text{   pari} \end{cases} \quad (15.1)$$

per ogni due parole \mathbf{a} e \mathbf{b} . Inoltre, sempre nell'ipotesi $q = 2$, ogni parola \mathbf{a} pu  riguardarsi come la funzione caratteristica di $\text{supp}(\mathbf{a})$.

Il teorema che segue fornisce un primo esempio dello stretto legame esistente tra la teoria dei codici e quella dei disegni. Esso permette, infatti, di costruire un disegno a partire da un codice perfetto binario.

PROPOSIZIONE 15.1.1. *Sia C un (v, M, d) -codice binario e-correttore. Allora, se C   perfetto e non banale, i supporti delle sue parole di peso $d = 2e + 1$ formano i blocchi di un $(e + 1) - (v, d, 1)$ disegno.*

DIMOSTRAZIONE. Se prendiamo come alfabeto $F_2 = \{0, 1\}$, non é restrittivo supporre che la parola $\mathbf{0}$ appartenga a C e si puó in modo ovvio definire il peso delle parole di C , pur non essendo C necessariamente lineare. Risulta cosí $w(\mathbf{a}) \geq d$, per ogni parola \mathbf{a} di C diversa da $\mathbf{0}$. Poiché C é perfetto, abbiamo che é $d = 2e + 1$ e che le sfere con centro le parole di C e raggio e formano una partizione di F_2^v . Allora, detta \mathbf{y} una parola di F_2^v di peso $e + 1$, esiste un'unica parola \mathbf{a} di C tale che $\mathbf{y} \in S(\mathbf{a}, e)$, cioè tale che

$$d(\mathbf{a}, \mathbf{y}) \leq e.$$

Inoltre, se é

$$h = |\text{supp}(\mathbf{a}) \cap \text{supp}(\mathbf{y})|,$$

abbiamo

$$e \geq d(\mathbf{a}, \mathbf{y}) = |\text{supp}(\mathbf{a}) \star \text{supp}(\mathbf{y})| = (w(\mathbf{a}) - h) + (e + 1 - h) =$$

$$w(\mathbf{a}) + e - 2h + 1 \geq w(\mathbf{a}) + e - 2|\text{supp}(\mathbf{y})| + 1 =$$

$$w(\mathbf{a}) + e - 2(e + 1) + 1 = w(\mathbf{a}) - e - 1$$

e, essendo $w(\mathbf{a}) \geq 2e + 1$, le disuguaglianze precedenti sono delle uguaglianze e risulta

$$w(\mathbf{a}) = 2e + 1 = d \quad e \quad d(\mathbf{a}, \mathbf{y}) = 3e - 2h + 2.$$

A questo punto abbiamo

$$e = d(\mathbf{a}, \mathbf{y}) = 3e - 2h + 2 \geq 3e - 2(e + 1) + 2 = e$$

e cioè

$$h = e + 1.$$

L'ultima uguaglianza implica che il supporto di \mathbf{y} é contenuto nel supporto di \mathbf{a} . Ne segue che ogni insieme di $e + 1$ punti di \mathcal{P} é contenuto nel supporto di un'unica parola di peso d e l'asserto é cosí completamente provato. \square

ESEMPIO 15.1.2. Ogni codice lineare binario C con gli stessi parametri di un codice di Hamming binario, cioè un $[2^m - 1, 2^m - 1 - m, 3]$ -codice su F_2 , é perfetto. Allora, usando la prop.15.1.1, é possibile provare che il disegno associato a C é quello dei punti e delle rette dello spazio proiettivo $PG(m - 1, 2)$. \square

15.2 Il teorema di Assmus-Mattson

Per completezza espositiva riportiamo l'enunciato di uno dei piú importanti teoremi che permettono di costruire t -disegni a partire da codici lineari.

PROPOSIZIONE 15.2.1. (E.F. Assmus - H.F. Mattson, 1969). Sia C un $[n, k, d]$ -codice su F_q e denotiamo con w_j il numero delle parole di peso j di C e con d^\perp la distanza minima di C^\perp . Siano inoltre:

- t un intero minore di $d + 1$;
- v il piú grande intero tale che

$$v - \frac{v + q - 2}{q - 1} < d, \text{ se } q \neq 2, \text{ e } v = n, \text{ se } q = 2.$$

Supponiamo, infine, che il polinomio

$$W^\perp(x, y) = \sum_{i=0}^n w_i^\perp x^i y^{n-i},$$

enumeratore dei pesi di C^\perp , abbia al piú $d - t$ coefficienti diversi da zero tra $w_1^\perp, w_2^\perp, \dots, w_{n-t}^\perp$.

Allora, per ogni intero j tale che

$$w_j \neq 0 \text{ e } d \leq j \leq v,$$

il supporto delle parole di C di peso j costituiscono la famiglia dei blocchi di un t -disegno. Analogamente, per ogni intero s tale che

$$w_s^\perp \neq 0 \text{ e } d^\perp \leq s \leq \min\{n - t, v^\perp\},$$

il supporto delle parole di C^\perp di peso s costituiscono la famiglia dei blocchi di un t -disegno.

Il teorema precedente é stato utilizzato per la costruzione di diversi nuovi 5-disegni. Stranamente, esso non ha dato luogo a nuovi t -disegni con $t > 5$.

15.3 Codice lineare associato ad un disegno

Vediamo ora come é possibile costruire dei codici a partire da un t -disegno. A tale scopo, supponiamo che $\mathbf{D} = (\mathcal{P}, \mathcal{B})$ sia un $t - (v, k, \lambda)$ disegno e, posto $\mathcal{B} = \{B_1, B_2, \dots, B_b\}$, denotiamo con $A = (a_{ij})$ una matrice di tipo $b \times v$ che sia la trasposta di una matrice d'incidenza di \mathbf{D} . Le colonne e le righe di A sono dunque in corrispondenza biunivoca con i punti ed i blocchi di \mathbf{D} , rispettivamente. Il codice lineare $C_q(\mathbf{D})$ su F_q generato dalle righe di A prende il nome di *codice di \mathbf{D}* su F_q ed é chiaramente indipendente dalla matrice d'incidenza considerata.

Poiché A é ad elementi 0 e 1, la dimensione $\dim_q(\mathbf{D})$ di $C_q(\mathbf{D})$ corrisponde al rango $\text{rank}_p(A)$ di A sul sottocampo fondamentale F_p di F_q e, per questo motivo, prende il nome di p -rango di A o del disegno \mathbf{D} .

Il codice intersezione di $C_q(\mathbf{D})$ e del suo duale $C_q(\mathbf{D})^\perp$ si chiama q -involucro di \mathbf{D} e si denota con $\text{Hull}_q(\mathbf{D})$. In questo modo al t -disegno \mathbf{D} rimangono associati i tre codici $C_q(\mathbf{D})$, $C_q(\mathbf{D})^\perp$

e $Hull_q(\mathbf{D})$, la cui conoscenza spesso permette di descrivere agevolmente molte proprietà di \mathbf{D} . Per esempio, è di grande utilità conoscere la distribuzione dei pesi di tali codici, cioè i coefficienti del polinomio (14.9). Viceversa, a volte è possibile trovare dei buoni codici partendo dalla conoscenza di particolari disegni.

Osserviamo esplicitamente che le righe della matrice A sono parole del codice $C_q(\mathbf{D})$ i cui supporti sono esattamente i blocchi di \mathbf{D} . Nel seguito denoteremo sempre con $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_b$ le righe di A e così con le nostre notazioni, abbiamo

$$\text{supp}(\mathbf{a}_i) = B_i, \quad \text{per ogni } i = 1, 2, \dots, b. \quad (15.2)$$

I sottoinsiemi di \mathcal{P} che risultano supporti di parole $C_q(\mathbf{D})$, con abuso di linguaggio, saranno chiamati q -parole o semplicemente parole nel caso $q = 2$. È chiaro che, se X è una q -parola non vuota, esistono diverse parole di $C_q(\mathbf{D})$ aventi come supporto X . Nel caso $q = 2$ la corrispondenza tra parole di $C_2(\mathbf{D})$ e le parole di \mathcal{P} è biunivoca. Pertanto, quando è $q = 2$, le parole di \mathcal{P} sono tutti e soli gli insiemi di punti che risultano differenza simmetrica di blocchi (cfr. (15.1)). In altri termini questo significa che X è una parola di \mathcal{P} se, e soltanto se, esiste un insieme \mathcal{F} di blocchi con le seguenti proprietà:

- (1) ogni punto di X appartiene ad un numero dispari di blocchi di \mathcal{F} ,
- (2) ogni punto di $\mathcal{P} \setminus X$ appartiene ad un numero pari di blocchi di \mathcal{F} .

ESEMPIO 15.3.1. Il determinante, calcolato sui razionali, di una matrice d'incidenza del piano di Fano $PG(2, 2)$ è uguale a $24 (= 2^3 \cdot 3)$ e quindi risulta

$$\dim_q(PG(2, 2)) < 7, \quad \text{per } p = 2, 3,$$

$$\dim_q(PG(2, 2)) = 7, \quad \text{per ogni } p \neq 2, 3.$$

Il codice C di $PG(2, 2)$ su F_2 è quello descritto in 13.4.21 e abbiamo già visto che esso è equivalente al codice di Hamming $Ham(3, 2)$. C'è da osservare che i supporti delle parole di C di peso 3 sono tutte e sole le rette. Analogamente, i supporti delle parole di C di peso 4 sono tutti e soli i complementari delle rette che, in questo caso, coincidono con le iperovali. Queste due famiglie individuano dunque rispettivamente $PG(2, 2)$ e il suo disegno complementare.

Non è difficile verificare che il codice di $PG(2, 2)$ su F_3 è il codice duale di $\{\mathbf{0}, \mathbf{j}, -\mathbf{j}\}$, ove $\mathbf{j} = (1, 1, 1, 1, 1, 1, 1)$. Quest'ultima proprietà è caso particolare di un teorema sui codici dei disegni simmetrici. Il codice di $PG(2, 2)$ su F_q , con $q \neq 2, 3$, è F_q^7 . \square

Nello studio di un t -disegno \mathbf{D} , oltre alla conoscenza del codice di \mathbf{D} su F_q è spesso determinante la conoscenza del suo involucro. Questo problema non si pone quando $C_q(\mathbf{D})$ è autoortogonale perché, in questo caso, risulta evidentemente $Hull_q(\mathbf{D}) = C_q(\mathbf{D})$. Per esempio, usando la (15.1) si prova immediatamente la seguente proposizione.

PROPOSIZIONE 15.3.2. *Il codice binario associato ad un $t - (v, k, \lambda)$ disegno è autoortogonale se, e soltanto se, sono verificate le seguenti proprietà:*

- (i) k è pari;
- (ii) ogni due blocchi distinti di \mathbf{D} s'intersecano in un numero pari di punti.

ESEMPIO 15.3.3. Il codice binario associato al disegno di Mathieu \mathcal{M}_{24} é di lunghezza 24 e, in forza della 15.3.2, risulta autoortogonale. Ne segue che la sua dimensione é al piú 12. Questo codice, che studieremo nel prossimo paragrafo, si denota con \mathcal{G}_{24} ed é noto come *codice binario di Golay esteso*. A titolo di informazione, ricordiamo che \mathcal{G}_{24} é uno dei codici utilizzati dalla NASA agli inizi degli anni '80 nel programma aerospaziale *Voyager* ed é stato usato per trasmettere sulla terra immagini di Giove e di Saturno. \square

PROPOSIZIONE 15.3.4. Sia $\mathbf{D} = (\mathcal{P}, \mathcal{B})$ un $2 - (v, k, \lambda)$ disegno simmetrico e q la potenza di un primo p che non divide l'ordine $n = k - \lambda$ di \mathbf{D} . Allora

$$\text{rank}_p(\mathbf{D}) \geq v - 1, \tag{15.3}$$

l'uguaglianza avendosi se, e solo se, p divide k . In quest'ultimo caso $C_q(\mathbf{D})$ coincide con $C(q, v)^\perp$, ove

$$C(q, v) = \{(a, a, \dots, a) : a \in F_q\}$$

é il codice di ripetizione q -ario di lunghezza v su F_q .

DIMOSTRAZIONE. Per ogni $i = 1, 2, \dots, v$, consideriamo le seguenti parole del codice $C_q(\mathbf{D})$

$$\mathbf{a}^i = \sum_{p_i \in B_j} \mathbf{a}_j = (\lambda, \dots, \lambda, r, \lambda, \dots, \lambda),$$

ove l'unica componente di \mathbf{a}^i uguale ad r é quella di posto i , r essendo il numero dei blocchi di \mathbf{D} contenenti un fissato punto. Posto $\mathbf{j} = (1, 1, \dots, 1)$, se \mathbf{x} é una parola di F_q^v ortogonale a \mathbf{j} , abbiamo

$$x_1 + x_2 + \dots + x_v = 0$$

e

$$\begin{aligned} x_1 \mathbf{a}^1 + x_2 \mathbf{a}^2 + \dots + x_v \mathbf{a}^v = \\ \left(rx_1 + \lambda \sum_{j \neq 1} x_j, rx_2 + \lambda \sum_{j \neq 2} x_j, \dots, rx_v + \lambda \sum_{j \neq v} x_j \right) = \\ (rx_1 - \lambda x_1, rx_2 - \lambda x_2, \dots, rx_v - \lambda x_v) = (r - \lambda) \mathbf{x} = n \mathbf{x}. \end{aligned}$$

Ne segue che \mathbf{x} appartiene al codice $C_q(\mathbf{D})$ perché n é diverso da zero su F_p , cioè

$$C(q, v)^\perp \subseteq C_q(\mathbf{D})$$

e

$$v - 1 = \dim(C(q, v)^\perp) \leq \dim_q(\mathbf{D}) = \text{rank}_p(\mathbf{D}).$$

Chiaramente, l'ultima disuguaglianza si riduce ad un'uguaglianza se, e soltanto se, risulta $C(q, v)^\perp = C_q(\mathbf{D})$ e ciò equivale a dire che

$$\mathbf{j} \mathbf{a}_i = k = 0, \text{ per ogni } i = 1, 2, \dots, v,$$

ció p divide k . L'asserto é cosí completamente provato. \square

Notiamo che la (15.3) é una generalizzazione della disuguaglianza di Fisher.

15.4 Codice binario associato ad un piano proiettivo

Sia $\pi_n = (\mathcal{P}, \mathcal{B})$ un piano proiettivo d'ordine n e ricordiamo che una tale struttura é null'altro che un $2 - (v, n + 1, 1)$ disegno simmetrico con $v = n^2 + n + 1$. Denotate con L_1, L_2, \dots, L_v le rette di π_n , sia \mathbf{a}_i la riga corrispondente alla retta L_i nella matrice A , trasposta di una matrice di incidenza di π_n .

Applicando a π_n la prop.15.3.4, abbiamo

$$p \nmid n(n+1) \Rightarrow \text{rank}_p(\pi_n) = \text{dim}_q(\pi_n) = n^2 + n + 1 \quad (15.4)$$

e

$$p|(n+1) \Rightarrow \begin{cases} \text{rank}_p(\pi_n) = \text{dim}_q(\pi_n) = n^2 + n \\ C_q(\pi_n) = C(q, n^2 + n + 1)^\perp \end{cases} \quad (15.5)$$

Osserviamo esplicitamente che dalla (15.5) segue

$$n \text{ dispari} \Rightarrow \text{rank}_2(\pi_n) = \text{dim}_2(\pi_n) = n^2 + n \quad (15.6)$$

e $C_2(\pi_n)$ é il codice binario formato da tutte le parole di F_2^v aventi peso pari.

DEFINIZIONE 15.4.1. Un insieme \mathcal{F} di rette di π_n si dice *pari* (risp. *dispari*) se ogni punto del piano appartiene ad un numero pari (risp. dispari) di rette di \mathcal{F} . Dualmente, un insieme X di punti di π_n si dice *pari* (risp. *dispari*) se ogni retta del piano interseca X in un numero pari (risp. dispari) di punti. \square

OSSERVAZIONE 15.4.2. Nel caso n dispari, come conseguenza della (15.6) e della successiva osservazione, abbiamo che un insieme pari e non vuoto di rette (risp. punti) di π_n deve necessariamente coincidere con \mathcal{B} (risp. \mathcal{P}). \square

Mettiamoci ora nell'ipotesi che n sia pari e, posto $C = C_2(\pi_n)$, consideriamo il codice esteso \overline{C} di C . Poiché $n + 1$ é dispari, la parola \mathbf{a}'_i di \overline{C} corrispondente ad \mathbf{a}_i é data da $\mathbf{a}'_i = (\mathbf{a}_i, 1)$ e, poiché due rette distinte s'intersecano in esattamente un punto, abbiamo

$$\mathbf{a}'_i \mathbf{a}'_j = 0, \text{ per ogni } i, j = 1, 2, \dots, v.$$

Ne segue che \overline{C} é autoortogonale e, in forza della (14.6), abbiamo

$$n^2 + n + 2 \geq 2\text{dim}(\overline{C}) = 2\text{dim}(C),$$

cioé

$$n \text{ pari} \Rightarrow \text{rank}_2(\pi_n) = \text{dim}_2(\pi_n) \leq \frac{n^2 + n + 2}{2}. \quad (15.7)$$

La prop.15.3.4 e le considerazioni svolte nel precedente paragrafo mostrano che é interessante studiare il codice su F_q di un disegno simmetrico solo nel caso che questo abbia ordine n divisibile per p . Questo studio, che in generale presenta non poche difficoltà, verrà ora affrontato nel caso dei piani proiettivi d'ordine $n \equiv 2 \pmod{4}$ e $q = 2$. I risultati che esporremo saranno utili per comprendere il supporto teorico alla base della ricerca esaustiva che ha portato alla dimostrazione della non esistenza di un piano proiettivo d'ordine 10.

PROPOSIZIONE 15.4.3. *Sia π_n un piano proiettivo finito d'ordine n , con $n \equiv 2 \pmod{4}$. Allora risulta*

$$\dim_2(\pi_n) = \frac{n^2 + n + 2}{2}. \quad (15.8)$$

Ne segue che il codice esteso di $C_2(\pi_n)$ é autoduale.

DIMOSTRAZIONE. Sia A la trasposta di una matrice di incidenza di π_n e, posto,

$$n = 4h + 2,$$

$$\dim_2(\pi_n) = k,$$

$$\dim(C_2(\pi_n)^\perp) = n^2 + n + 1 - k = r,$$

non é restrittivo supporre che una matrice H generatrice di $C_2(\pi_n)^\perp$, cioé una matrice controllo di parità di $C_2(\pi_n)$, sia della forma standard

$$H = [I_r, P].$$

In queste ipotesi, introduciamo la matrice ausiliaria B definita da

$$B = \left[\begin{array}{c|c} I_r & P \\ \hline 0 & I_k \end{array} \right]$$

e osserviamo che, essendo ogni riga di A ortogonale a tutte le righe di H , le prime r colonne di AB^t sono nulle su F_2 . Questo significa che AB^t , considerata come matrice sui razionali, é ad elementi interi e i suoi primi r vettori colonna sono divisibili per 2. Abbiamo cosí che 2^r divide il determinante di AB^t . D'altra parte, ricordando la 10.10, abbiamo

$$\begin{aligned} |AB^t| &= |A||B| = |A||I_r||I_k| = |A| = \\ &= (1+n)n^{\frac{n^2+n}{2}} = (1+n)2^{\frac{n^2+n}{2}}(2h+1)^{\frac{n^2+n}{2}} \end{aligned}$$

e, essendo $1+n$ e $2h+1$ dispari e $|AB^t|$ divisibile per 2^r , risulta che 2^r divide

$$2^{\frac{n^2+n}{2}},$$

cioé

$$r = n^2 + n + 1 - k \leq \frac{n^2 + n}{2},$$

o, equivalentemente

$$k \geq \frac{n^2 + n + 2}{2}.$$

L'asserto segue allora dalla 15.7

□

PROPOSIZIONE 15.4.4. *Sia π_n un piano proiettivo finito d'ordine n , con $n \equiv 2 \pmod{4}$. Allora la distanza minima di $C = C_2(\pi_n)$ é*

$$d = n + 1, \quad (15.9)$$

le parole di π_n di cardinalità $n + 1$ essendo tutte e sole le rette di π_n . Inoltre, le parole di π_n di cardinalità $n + 2$ sono tutte e sole le iperovali di π_n , cioè gli insiemi di $n + 2$ punti a tre a tre non allineati.

DIMOSTRAZIONE. Se \mathbf{a} é una parola di C , denotiamo con \mathbf{a}' la corrispondente parola di \overline{C} , codice esteso di C . Osserviamo poi che d non supera $n + 1$ perché le righe \mathbf{a}_i della matrice A , corrispondenti alle rette di π_n , hanno peso $n + 1$.

Supponiamo che d sia pari e minore di $n + 1$ e diciamo \mathbf{a} una parola di C di peso d . Poiché risulta

$$\mathbf{a}'_i \mathbf{a}' = 0, \quad \mathbf{a}' = (\mathbf{a}, 0),$$

per ogni $i = 1, 2, \dots, n^2 + n + 1$, deve essere anche

$$\mathbf{a}_i \mathbf{a} = 0.$$

Ne segue che ogni retta ad intersezione non vuota con $\text{supp}(\mathbf{a})$ ha almeno due punti in comune con esso. Allora $\text{supp}(\mathbf{a})$ deve contenere almeno $n + 2$ punti e ciò é contro le ipotesi. Resta così provato che d é dispari.

Sia dunque \mathbf{a} una parola di C di peso $d \leq n + 1$ e osserviamo che questa volta é $\mathbf{a}' = (\mathbf{a}, 1)$. Allora da

$$0 = \mathbf{a}'_i \mathbf{a}' = \mathbf{a}_i \mathbf{a} + 1, \quad i = 1, 2, \dots, n^2 + n + 1,$$

segue che ogni retta di π_n contiene almeno un punto di $\text{supp}(\mathbf{a})$ e di conseguenza é $d \geq n + 1$, cioè

$$d = n + 1.$$

D'altra parte, poiché $\text{supp}(\mathbf{a})$ contiene esattamente $n + 1$ punti ed é ad intersezione non vuota con ogni retta di π_n , si ha subito che $\text{supp}(\mathbf{a})$ deve essere una retta e la prima parte dell'asserto é provata.

Con argomentazioni simili alle precedenti si prova facilmente che il supporto di una parola di C di peso $n + 2$ é necessariamente una iperovale. Supponiamo dunque che Ω sia una iperovale e osserviamo che per ogni punto non su Ω passa un numero pari ($= (n + 2)/2$) di rette incidenti Ω , mentre per ogni punto su Ω passa un numero dispari ($= n + 1$) di tali rette. Ne segue che Ω é la differenza simmetrica delle rette che la incidono e, in forza delle 15.1 é una parola di π_n . L'asserto é così completamente provato. \square

15.5 Non esistenza di un piano proiettivo d'ordine 10

In questo paragrafo riportiamo la *storia* della dimostrazione della non esistenza di un piano proiettivo d'ordine 10. Tale dimostrazione é stata ottenuta sfruttando essenzialmente la potenza

raggiunta negli anni '80 dagli elaboratori elettronici e, pertanto, é tuttora aperta la questione della ricerca di metodi adeguati per la soluzione del problema senza l'uso di strumenti di calcolo.

Denotiamo, dunque, con C il codice su F_2 di un ipotetico piano proiettivo π d'ordine 10 e con w_i i coefficienti del relativo polinomio enumeratore dei pesi. Le parole a'_i del codice esteso \overline{C} hanno peso (= 12) divisibile per 4 e ciò, essendo \overline{C} autoduale, implica che \overline{C} é doppiamente pari.

Mediante l'uso di elaboratori elettronici sono stati provati i seguenti risultati:

$$w_{12} = 0 \quad (\text{C.W.H.Lam, L.Thiel, S.Swiercz, J.McKay, 1983}),$$

$$w_{15} = 0 \quad (\text{R.H.F.Denniston, 1969 e indipendentemente F.J.MacWilliams, N.J.A.Sloane, J.C.Thompson, 1973}),$$

$$w_{16} = 0 \quad (\text{C.W.H.Lam, S.Swiercz, L.Thiel, 1986}).$$

Sono dunque noti i valori di w_i , per ogni $i = 0, 1, 2, \dots, 18$, che riportiamo nella seguente tabella.

w_0	$w_i \quad i = 1, 2, \dots, 10$	w_{11}	$w_j \quad j = 12, 13, \dots, 18$
1	0	11	0

Nel 1970, *E.F.Assmus* e *H.F.Mattson* hanno osservato che, usando i valori riportati nella tabella precedente e la relazione 14.5.1, é possibile trovare tutti i coefficienti del polinomio enumeratore dei pesi di C . In particolare, si ha

$$w_{19} = 24.675$$

e quindi, se esiste un piano proiettivo l'ordine 10, esso deve contenere delle configurazioni di 19 punti che risultino differenza simmetrica di rette. Queste configurazioni sono state studiate da *M.Hall Jr*, il quale nel 1980 ha provato che, se a é una parola di C di peso 19, allora, delle 111 rette di π , 6 intersecano $w(a)$ in 5 punti, 37 in 3 punti e 68 in un solo punto. In sostanza, le configurazioni in questione possono pensarsi come strutture geometriche aventi 19 punti e 43 blocchi tali che: 6 blocchi hanno 5 punti, 37 blocchi hanno 3 punti e due punti distinti appartengono ad un unico blocco. Inoltre, si può provare che, a meno di isomorfismi, il numero di tali strutture é 66 e ovviamente una almeno di queste, se esiste π , deve avere matrice di incidenza estendibile ad una matrice di incidenza di π . E' appunto questo il dato di partenza delle ricerche dei matematici che negli ultimi anni si sono occupati del problema del piano proiettivo d'ordine 10.

In un lavoro del 1985 *Lam, Crossfiel e Thiel* hanno provato che 21 configurazioni delle 66 possibili hanno matrice di incidenza non estendibile a quella di un piano proiettivo d'ordine 10. Finalmente, nel 1988, *Lam, Thiel e Swiercz* [57], usando dei programmi da loro elaborati (parte di questi hanno girato per 83 giorni su un *CRAY supercomputer* e per 160 giorni su cinque *VAX* collegati in rete) hanno esteso il precedente risultato alle rimanenti 45 configurazioni, giungendo così a provare che *non esiste un piano proiettivo d'ordine 10*.

15.6 Codici perfetti

Ricordiamo che abbiamo definito perfetto un (n, M, d) -codice e -correttore C su F_q quando per esso la disuguaglianza di Hamming (13.6) é un'uguaglianza. Come già osservato, ciò equivale a dire che le sfere di centro le parole di C e raggio e costituiscono una partizione di F_q^n . Notiamo esplicitamente che la proprietà di un codice di essere perfetto dipende esclusivamente dai suoi parametri.

Abbiamo anche costruito una classe infinita di codici lineari perfetti non banali: i codici di Hamming $Ham(m, q)$. Inoltre il corollario 14.3.3 assicura che un codice lineare perfetto con i parametri di $Ham(m, q)$ é equivalente a $Ham(m, q)$.

Nel 1949, *M.J.E. Golay* trovó che le terne $(23, 2^{12}, 7)$ e $(90, 2^{78}, 5)$ per $q = 2$ e $(11, 3^6, 5)$ per $q = 3$ verificano l'uguaglianza nella (13.6), fornendo anche un modello di codice lineare perfetto nel primo e terzo caso e dimostrando la non esistenza di un $[90, 78, 5]$ -codice binario. I due nuovi codici perfetti dovuti a Golay si denotano rispettivamente con \mathcal{G}_{23} e \mathcal{G}_{11} e furono da questi definiti mediante la presentazione di una loro matrice generatrice.

Solo nel 1973, grazie ai lavori di *J.H. van Lint* e *A. Tietavainen*, si giunse al seguente fondamentale risultato, che riportiamo senza dimostrazione.

PROPOSIZIONE 15.6.1. *Se q é potenza di un primo, ogni codice q -ario perfetto non banale ha i parametri di un codice di Hamming o di uno dei due codici di Golay.*

Nel caso lineare la precedente proposizione porta alla seguente caratterizzazione dei codici perfetti.

PROPOSIZIONE 15.6.2. *Ogni codice lineare perfetto non banale é equivalente ad un codice di Hamming o ad uno dei due codici di Golay.*

Abbiamo già dato una costruzione del codice \mathcal{G}_{11} (cfr. esempio 14.3.7). Ci proponiamo, ora, di dare una costruzione ed una interpretazione geometrica del codice di Golay \mathcal{G}_{23} e, a tale scopo, faremo riferimento a tutte le notazioni e convenzioni introdotte nei paragrafi precedenti.

Fissata la trasposta A di una matrice d'incidenza del $5 - (24, 8, 1)$ disegno di Mathieu $\mathcal{M}_{24} = (\mathcal{P}, \mathcal{B})$, consideriamo il codice lineare binario di \mathcal{M}_{24} , cioè il codice di Golay esteso \mathcal{G}_{24} . Abbiamo visto che esso é autoortogonale, doppiamente pari, cioè il peso di ogni sua parola é divisibile per 4, e

$$\dim(\mathcal{G}_{24}) \leq 12.$$

Inoltre, i supporti di due sue qualsiasi parole s'intersecano in un numero pari di punti (cfr. 12.5.5). Poiché ogni punto di \mathcal{M}_{24} appartiene ad un numero dispari di blocchi (cfr. 12.5.5), la differenza simmetrica di tutti i suoi blocchi coincide con \mathcal{P} e ciò equivale a dire che la parola $\mathbf{j} = (1, 1, \dots, 1)$ appartiene a \mathcal{G}_{24} . Allora, per ogni parola \mathbf{a} di F_2^{24} , abbiamo

$$\mathbf{a} \in \mathcal{G}_{23} \Leftrightarrow \mathbf{j} + \mathbf{a} \in \mathcal{G}_{24},$$

cioé

$$w_i = w_{24-i}, \quad \text{per ogni } i = 1, 2, \dots, 12,$$

avendo denotato con w_j il numero delle parole di \mathcal{G}_{24} di peso j . Quanto finora detto assicura che la distribuzione dei pesi delle parole di \mathcal{G}_{24} é completamente determinata dalla conoscenza di w_4 , w_8 e w_{12} .

PROPOSIZIONE 15.6.3. *In \mathcal{G}_{24} risulta*

$$w_4 = 0.$$

DIMOSTRAZIONE. Sia \mathbf{a} una parola di \mathcal{G}_{24} di peso 4 e supponiamo $\text{supp}(\mathbf{a}) = \{x, y, z, t\}$. Dei 21 blocchi di \mathcal{M}_{24} passanti per a, b, c (cfr.12.5.5) scegliamone uno B non contenente t . Allora l'intersezione di $\text{supp}(\mathbf{a})$ e B contiene solo i tre punti a, b, c e ciò é assurdo perché i supporti di due parole di \mathcal{G}_{24} hanno un numero pari di punti in comune. \square

Poiché ogni blocco di \mathcal{M}_{24} contiene esattamente otto punti e \mathcal{G}_{24} non contiene parole non nulle di peso minore di 8, per la distanza minima di \mathcal{G}_{24} , abbiamo

$$d = d(\mathcal{G}_{24}) = 8. \quad (15.10)$$

PROPOSIZIONE 15.6.4. *Una parola \mathbf{a} di \mathcal{G}_{24} ha peso 8 se, e soltanto se, il supporto di \mathbf{a} é un blocco di \mathcal{M}_{24} . Ne segue che w_8 é uguale al numero di blocchi di \mathcal{M}_{24} , cioè*

$$w_8 = b = 759.$$

DIMOSTRAZIONE. E' chiaro che ogni blocco di \mathcal{M}_{24} é supporto di una parola di peso 8 di \mathcal{G}_{24} . Sia dunque \mathbf{a} una parola di \mathcal{G}_{24} di peso 8 e sia B un blocco di \mathcal{M}_{24} contenente cinque punti del supporto di \mathbf{a} . Allora, la differenza simmetrica di B e $\text{supp}(\mathbf{a})$ contiene meno di 8 punti e di conseguenza, in forza della 15.10, deve essere vuota, cioè $\text{supp}(\mathbf{a}) = B$. \square

Passiamo ora a studiare il supporto di una parola di peso 12 di \mathcal{G}_{24} . Un insieme di dodici punti di \mathcal{M}_{24} di questo tipo prende il nome di *dodecade*. Esempi di dodecadi si ottengono considerando le differenze simmetriche di coppie di blocchi di \mathcal{M}_{24} che s'intersecano in esattamente due punti. Ci proponiamo di provare che tutte le dodecadi sono necessariamente di questo tipo.

Sia \mathbf{a} una parola di \mathcal{G}_{24} di peso 12 e B_i un blocco contenente cinque punti di $\text{supp}(\mathbf{a})$. Il blocco B_i non può essere contenuto nel supporto di \mathbf{a} , altrimenti avremmo $w(\mathbf{a} + \mathbf{a}_i) = 4$ e ciò non é possibile. Abbiamo allora che

$$w(\mathbf{a} + \mathbf{a}_i) = |\text{supp}(\mathbf{a} + \mathbf{a}_i)| = |\text{supp}(\mathbf{a}) \star \text{supp}(\mathbf{a}_i)| = 8$$

e, per la 15.6.4, $\text{supp}(\mathbf{a} + \mathbf{a}_i)$ é un blocco B_j . Resta così provata la seguente proposizione.

PROPOSIZIONE 15.6.5. *Se una dodecade X ha cinque punti in comune con un blocco B_i , allora*

$$|X \cap B_i| = 6$$

ed esiste un unico blocco B_j tale che

$$X = B_i \star B_j.$$

Ne segue che le dodecadi di \mathcal{M}_{24} sono tutte e sole le differenze simmetriche di due blocchi che s'intersecano in esattamente due punti.

Siamo ora in grado di calcolare w_{12} , cioè il numero di tutte le dodecadi di \mathcal{M}_{24} .

PROPOSIZIONE 15.6.6. *In \mathcal{G}_{24} risulta*

$$w_{12} = 2.576.$$

DIMOSTRAZIONE. Cominciamo col valutare i seguenti interi:

- n_1 = numero dei blocchi di \mathcal{M}_{24} che incidono in esattamente due punti un fissato blocco B_i ;
- n_2 = numero delle coppie (X, B_i) , con X dodecade e B_i blocco di \mathcal{M}_{24} , tali che $|X \cap B_i| = 6$.

Utilizzando il principio di inclusione-esclusione e la 12.5.5, fissati due punti distinti p_s, p_t di B_i , abbiamo

$$\begin{aligned} |B_j : B_j \cap B_i = \{p_s, p_t\}| &= (\lambda_2 - 1) - 6(\lambda_3 - 1) + \binom{6}{2}(\lambda_4 - 1) = \\ &= 76 - 120 + 60 = 16 \end{aligned}$$

e quindi

$$n_1 = \binom{8}{2} 16 = 448.$$

Ora osserviamo che, in forza della proposizione precedente, esistono esattamente n_1 dodecadi incidenti un fissato blocco B_i in esattamente 6 punti e

$$\frac{1}{6} \binom{12}{5}$$

blocchi incidenti una fissata dodecade X in esattamente 6 punti. Ne segue che

$$n_2 = \frac{1}{6} \binom{12}{5} w_{12} = bn_1 = 448.759$$

e quindi

$$w_{12} = 2.576.$$

□

A questo punto conosciamo la distribuzione dei pesi delle parole di \mathcal{G}_{24} , che riassumiamo nella seguente tabella.

$w_0 = w_{24}$	$w_8 = w_{16}$	w_{12}	$w_i, i \neq 0, 8, 12, 16, 24$
1	759	2.576	0

Si ha allora che

$$|\mathcal{G}_{24}| = w_0 + w_8 + w_{12} + w_{16} + w_{24} = 4.096 = 2^{12},$$

cioé \mathcal{G}_{24} ha dimensione 12. Possiamo dunque concludere con la seguente proposizione.

PROPOSIZIONE 15.6.7. *Il codice \mathcal{G}_{24} é un $[24, 12, 8]$ -codice binario autoduale.*

Se ad ogni parola di \mathcal{G}_{24} cancelliamo la prima componente, il codice che otteniamo é un $[23, 12, 7]$ -codice lineare 3-correttore il cui codice esteso é ovviamente \mathcal{G}_{24} . Esso prende il nome di *codice binario di Golay* e si denota con \mathcal{G}_{23} . I supporti delle sue parole di peso 7 costituiscono i blocchi del disegno di Mathieu \mathcal{M}_{23} (ricordiamo che \mathcal{M}_{23} é il derivato di \mathcal{M}_{24} rispetto ad un suo punto) per il quale la trasposta di una sua matrice d'incidenza A^- si ottiene cancellando da A la prima colonna. Inoltre, poiché le righe \mathbf{a}_i^- di A^- generano \mathcal{G}_{23} , si ha che \mathcal{G}_{23} stesso é il codice di \mathcal{M}_{23} su F_2 .

La distribuzione dei pesi w_i^- delle parole di \mathcal{G}_{23} si ricava facilmente da quella relativa a \mathcal{G}_{24} ed é riportata nella seguente tabella.

$w_0^- = w_{23}^-$	$w_7^- = w_{16}^-$	$w_8^- = w_{15}^-$	$w_{11}^- = w_{12}^-$
1	253	506	1.288

Inoltre, poiché \mathcal{G}_{23} corregge 3 errori, le sfere di raggio 3 con centro nelle sue parole sono a due a due disgiunte. Allora, poiché una sfera di raggio 3 e centro una parola di F_2^{23} contiene esattamente 2^{11} parole ed é

$$2^{11}|\mathcal{G}_{23}| = 2^{11}2^{12} = 2^{23} = |F_2^{23}|,$$

abbiamo la seguente proposizione.

PROPOSIZIONE 15.6.8. *Il codice di Golay \mathcal{G}_{23} é perfetto.*

Osserviamo che ogni $[23, 12, 7]$ -codice binario C é necessariamente perfetto e quindi i supporti delle sue parole di peso 7 formano i blocchi di un $4 - (23, 7, 1)$ disegno (cfr.15.1.1), cioè del disegno di Mathieu \mathcal{M}_{23} . Ne segue che é $C = \mathcal{G}_{23}$ e, in forza delle precedenti considerazioni, é facile rendersi conto che ogni $[24, 12, 8]$ -codice binario é equivalente a \mathcal{G}_{24} . Abbiamo così la seguente proposizione.

PROPOSIZIONE 15.6.9. *Il codice di Golay \mathcal{G}_{23} , a meno di equivalenze, é l'unico $[23, 12, 7]$ -codice binario perfetto.*

