

# Capitolo 14

## Codici lineari

### 14.1 Prime definizioni ed esempi

D'ora in avanti supporremo che  $q$  sia potenza di un primo  $p$  e che l'alfabeto  $F = F_q$  sia il campo di Galois con  $q$  elementi  $GF(q)$ , per cui  $F^n$  è lo spazio vettoriale  $V(n, q)$  di dimensione  $n$  su  $F$ . Un *codice lineare* è, per definizione, un sottospazio vettoriale di  $F^n$  e ogni matrice ad esso associata è una matrice sul campo  $F$ . Il codice *ASCII*, il codice *ASCII* esteso e quello associato al piano di Fano sono esempi di codici lineari su  $GF(2)$ .

Se  $C$  è un codice lineare di dimensione  $k$  e distanza minima  $d$ , parleremo di  $[n, k, d]$ -*codice*, o di  $[n, k]$ -*codice* e diremo che  $n$ ,  $k$  e  $d$  sono i suoi *parametri*. Un tale codice è chiaramente un  $(n, q^k, d)$ -*codice*.

Nel seguito riterremo fissato un  $[n, k, d]$ -codice  $C$  e denoteremo sempre con  $\mathbf{0}$  il vettore nullo (*parola nulla*).

**DEFINIZIONE 14.1.1.** Si chiama *peso*  $w(\mathbf{a})$  di una parola  $\mathbf{a} \in F^n$  il numero delle componenti di  $\mathbf{a}$  diverse da zero, cioè la distanza di  $\mathbf{a}$  dalla parola nulla. Il minimo  $w(C)$  dei pesi delle parole di  $C$  diverse da  $\mathbf{0}$  è per definizione il *peso minimo* di  $C$ , cioè

$$w(C) := \min\{w(\mathbf{a}) : \mathbf{a} \in C, \mathbf{a} \neq \mathbf{0}\}.$$

Quando non vi è possibilità di equivoci, scriveremo  $w$  in luogo di  $w(C)$ . □

**OSSERVAZIONE 14.1.2.** Se due parole  $\mathbf{a}$  e  $\mathbf{b}$  di  $C$  hanno distanza  $h$ , allora la parola  $\mathbf{a} - \mathbf{b}$ , che è ancora in  $C$ , ha peso  $h$ . Ne segue che in ogni  $[n, k, d]$ -codice risulta

$$d = w. \tag{14.1}$$

□

Per trovare la distanza minima del codice  $C$  basta dunque calcolare i pesi delle  $M - 1 = q^k - 1$  parole di  $C$  diverse da  $\mathbf{0}$ . Questo è un primo vantaggio offerto dalla proprietà di linearità di un

codice. Senza questa ipotesi, infatti, per determinare la distanza minima di un  $(n, M)$ -codice occorre calcolare  $M(M-1)/2$  distanze e tale numero è maggiore di  $M-1$  non appena è  $M > 2$ . Un secondo e importante vantaggio di un codice lineare è che esso può essere descritto completamente da una sua base. Pertanto, nello studio di un codice lineare  $C$ , risultano di particolare importanza le matrici le cui righe costituiscono una base di  $C$ . Tali matrici si chiamano *matrici generatrici* del codice e, se questo ha parametri  $[n, k, d]$ , sono di tipo  $k \times n$ .

L'equivalenza fra codici non conserva in generale la linearità; infatti, se  $C$  è lineare si vede subito che un codice  $C'$  ottenuto da  $C$  mediante operazioni di tipo  $(B)$  non è necessariamente lineare. Pertanto, per la classe dei codici lineari, conviene modificare la  $(B)$  in modo che partendo da un codice lineare si ottenga ancora un codice con questa proprietà. A tale scopo diciamo che due codici lineari su  $F_q$  sono *linearmente equivalenti* se due matrici ad essi rispettivamente associate si ottengono l'una dall'altra mediante una successione finita di operazioni del tipo  $(A)$  e del tipo  $(B')$  così definito:

$(B')$  moltiplicazione degli elementi di una fissata colonna per uno scalare non nullo.

Nel seguito, poiché considereremo esclusivamente codici lineari, diremo che due tali codici sono *equivalenti* quando sono linearmente equivalenti.

Con semplici argomenti di algebra lineare si può provare la seguente proposizione.

**PROPOSIZIONE 14.1.3.** *Due matrici  $G$  e  $G'$  su  $F$  generano codici lineari equivalenti se, e soltanto se, si ottengono l'una dall'altra mediante un numero finito di operazioni elementari del tipo seguente:*

$(R1)$  scambio di due righe,

$(R2)$  moltiplicazione di una riga per uno scalare non nullo,

$(R3)$  sostituzione di una riga con la somma di quest'ultima e di un'altra riga,

$(C1)$  scambio di due colonne,

$(C2)$  moltiplicazione di una colonna per uno scalare non nullo.

**ESEMPIO 14.1.4.** Il codice

$$C = \{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\}$$

è un  $[3, 2, 2]$ -codice binario con matrice generatrice

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

□

**ESEMPIO 14.1.5.** Il  $[7, 4, 3]$ -codice associato al piano di Fano  $PG(2, 2)$  (cfr. esempio 13.4.21) ha matrice generatrice

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

□

**ESEMPIO 14.1.6.** Il codice di ripetizione  $q$ -ario di lunghezza  $n$  é un  $[n, 1, n]$ -codice con matrice generatrice

$$G = [1 \quad 1 \quad 1 \quad \cdots \quad 1].$$

□

E' utile osservare che una matrice generatrice  $G$  di un  $[n, k, d]$ -codice  $C$ , mediante operazioni di cui alla prop.14.1.3, può sempre mettersi nella forma

$$[I_k, A], \tag{14.2}$$

ove  $I_k$  é la matrice identità d'ordine  $k$  e  $A$  una matrice di tipo  $k \times (n - k)$ . La (14.2), che rappresenta la matrice generatrice di un codice equivalente a  $C$ , prende il nome di *forma standard* di  $G$ .

**ESERCIZIO 14.1.7.** Usando la forma standard delle matrici generatrici, provare che ogni codice lineare di dimensione  $k$  é  $k$ -sistematico.

Ricordiamo che il *prodotto scalare (standard)* di due vettori  $\mathbf{a}, \mathbf{b}$  di  $V(n, q)$ , che denotiamo con  $\mathbf{ab}$ , é definito da

$$\mathbf{ab} = (a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

e verifica le seguenti proprietà:

$$\begin{cases} \mathbf{ab} = \mathbf{ba} \\ (\lambda\mathbf{a} + \mu\mathbf{b})\mathbf{c} = \lambda(\mathbf{ac}) + \mu(\mathbf{bc}) \end{cases} \tag{14.3}$$

per ogni  $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V(n, q)$  e  $\lambda, \mu \in F$ . Due vettori  $\mathbf{a}, \mathbf{b}$  per cui é  $\mathbf{ab} = 0$  si dicono *ortogonali* e, per ogni sottoinsieme  $A$  di  $V(n, q)$ ,  $A^\perp$  denota il sottospazio ortogonale ad  $A$ , cioè il sottospazio dei vettori ortogonali a tutti i vettori di  $A$ . Se  $W$  é un sottospazio  $k$ -dimensionale di  $V(n, q)$  con base

$$\{\mathbf{g}_i = (g_{i1}, g_{i2}, \dots, g_{in}), i = 1, 2, \dots, k\},$$

allora  $W^\perp$  é il sottospazio costituito dai vettori  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  tali che

$$\begin{cases} g_{11}x_1 + g_{12}x_2 + \cdots + g_{1n}x_n = 0 \\ g_{21}x_1 + g_{22}x_2 + \cdots + g_{2n}x_n = 0 \\ \vdots \\ g_{k1}x_1 + g_{k2}x_2 + \cdots + g_{kn}x_n = 0 \end{cases}$$

e quindi, avendo la matrice  $(g_{ij})$  rango  $k$ , risulta

$$\dim(W) + \dim(W^\perp) = n. \tag{14.4}$$

La (14.4) assicura che, se  $C$  é un  $[n, k]$ -codice, il sottospazio  $C^\perp$  ortogonale a  $C$  é un codice con parametri  $[n, n - k]$ . Esso prende il nome di *codice duale* di  $C$  e, detta  $G$  una matrice generatrice di  $C$ , risulta

$$\mathbf{a} \in C^\perp \Leftrightarrow \mathbf{a}G^t = \mathbf{0}.$$

Una matrice generatrice  $H$  di  $C^\perp$  prende il nome di *matrice di controllo (di paritá)* di  $C$  e gode delle seguenti proprietà:

$$\begin{cases} GH^t = 0, \\ C = \{\mathbf{x} \in V(n, q) : \mathbf{x}H^t = 0\}. \end{cases} \quad (14.5)$$

La (14.5) mostra che il codice  $C$  puó essere completamente descritto da una sua matrice controllo di paritá, cosa che risulterà molto utile nel seguito. Se supponiamo  $G = [I_k, A]$  in forma standard, allora é facile rendersi conto che

$$H = [-A^t, I_{n-k}]$$

é una matrice controllo di paritá di  $C$ .

**DEFINIZIONE 14.1.8.** Quando  $C$  é contenuto in  $C^\perp$ , diciamo che é un codice *autoortogonale*. Se un codice autoortogonale  $C$  coincide con  $C^\perp$ , diciamo che  $C$  é *autoduale*.  $\square$

**OSSERVAZIONE 14.1.9.** Per un codice autoortogonale, la (14.4) dice che

$$n = \dim(C) + \dim(C^\perp) \geq 2\dim(C),$$

da cui abbiamo

$$\begin{cases} C \text{ autoortogonale} & \Rightarrow \dim(C) \leq \frac{n}{2}, \\ C \text{ autoduale} & \Rightarrow \dim(C) = \frac{n}{2}. \end{cases} \quad (14.6)$$

$\square$

Per ogni parola  $\mathbf{a} = (a_1, a_2, \dots, a_n)$  su  $F_q$ , diciamo *controllo di paritá* di  $\mathbf{a}$  l'opposto della somma delle sue componenti, cioè  $a_0 = -(a_1 + a_2 + \dots + a_n)$ . Fissato allora l'  $[n, k, d]$ -codice  $C$ , possiamo considerare l'  $[n + 1, k]$ -codice  $\overline{C}$  definito da

$$\overline{C} = \{\mathbf{a}' = (a_0, a_1, a_2, \dots, a_n) : \mathbf{a} \in C\},$$

il quale prende il nome di *codice esteso* di  $C$ . Un'utile proprietà di  $\overline{C}$  é che tutte le sue parole hanno controllo di paritá nullo. E' chiaro quindi che ha senso prenderlo in considerazione solo quando le parole di  $C$  non hanno tutte controllo di paritá uguale a zero. Per esempio, il codice *ASCII* esteso é proprio il codice esteso di  $C = F_2^7$ . Osserviamo che, se  $C$  ha matrice controllo di paritá  $H$ , allora

$$\overline{H} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & & & \\ \vdots & & H & \\ 0 & & & \end{bmatrix}$$

é una matrice controllo di paritá per  $\overline{C}$ .

## 14.2 Codifica e decodifica di un codice lineare

Dedichiamo questo paragrafo ad una breve esposizione riguardante la codifica e la decodifica di un  $[n, k]$ -codice lineare  $C$   $e$ -correttore su  $F_q$ . A tale scopo premettiamo alcune osservazioni e definizioni.

**DEFINIZIONE 14.2.1.** Distribuiamo tutte le parole di  $V(n, q)$  in una matrice  $\Sigma = (\sigma_{ij})$  con  $q^{n-k}$  righe e  $q^k$  colonne in modo che siano soddisfatte le seguenti proprietà:

- (i) la prima riga contiene tutte le parole di  $C$  ed  $\sigma_{11} = \mathbf{0}$ ;
- (ii) per ogni indice di riga  $i$ , la parola  $\mathbf{a}_i = \sigma_{i1}$   $\acute{e}$  di peso minimo rispetto a quelle contenute nella riga scelta e nelle righe successive;
- (iii) per ogni coppia  $(i, j)$  di indici  $\acute{e}$   $\sigma_{ij} = \mathbf{a}_i + \sigma_{1j}$ .

Una matrice  $\Sigma$  cosí costruita prende il nome di *tabella standard* di  $C$  ed  $\acute{e}$  chiaro che la sua riga  $i$ -esima, per ogni indice  $i$ , contiene tutte le parole del laterale  $\mathbf{a}_i + C$  di  $C$ . Inoltre, ogni laterale di  $C$  ha le sue parole distribuite su una riga di  $\Sigma$ . La parola di un laterale di  $C$  che occupa la prima posizione nella corrispondente riga di  $\Sigma$  prende il nome di *direttrice* del laterale. □

Un semplice algoritmo per costruire una tabella standard  $\Sigma$  di  $C$   $\acute{e}$  il seguente:

- primo passo:** distribuire le parole di  $C$  sulla prima riga di  $\Sigma$  con l'unica condizione  $\sigma_{11} = \mathbf{0}$ ;
- secondo passo:** scegliere una parola  $\mathbf{a}_2$  di peso minimo in  $F_q^n \setminus C$  e porre  $\sigma_{21} = \mathbf{a}_2$ ;
- terzo passo:** distribuire sulla seconda riga di  $\Sigma$  le parole di  $\mathbf{a}_2 + C$  in modo che sia  $\sigma_{2j} = \mathbf{a}_2 + \sigma_{1j}$ ;
- quarto passo:** scegliere una parola  $\mathbf{a}_3$  di peso minimo in  $F_q^n \setminus \{C \cup (\mathbf{a}_2 + C)\}$  e porre  $\sigma_{31} = \mathbf{a}_3$ ;
- quinto passo:** distribuire sulla terza riga di  $\Sigma$  le parole di  $\mathbf{a}_3 + C$  in modo che sia  $\sigma_{3j} = \mathbf{a}_3 + \sigma_{1j}$ ;
- ..... continuare in questo modo fino all'esaurimento delle parole di  $F_q^n$ .

**DEFINIZIONE 14.2.2.** Per ogni vettore  $\mathbf{a} \in V(n, q)$ , diciamo *sindrome* di  $\mathbf{a}$  il vettore  $S(\mathbf{a}) \in V(n - k, q)$  definito da

$$S(\mathbf{a}) = \mathbf{a}H^t,$$

$H$  essendo una matrice controllo di paritá di  $C$ . □

**PROPOSIZIONE 14.2.3.** Se  $C$   $\acute{e}$  un  $[n, k]$ -codice, risulta

$$\mathbf{a} \in C \Leftrightarrow S(\mathbf{a}) = \mathbf{0}.$$

Inoltre, due vettori  $\mathbf{a}, \mathbf{b} \in V(n, q)$  hanno la stessa sindrome se, e soltanto se, appartengono ad uno stesso laterale di  $C$  in  $V(n, q)$ . Ne segue che le sindromi sono in corrispondenza biunivoca con i laterali di  $C$  in  $V(n, q)$ .

**DIMOSTRAZIONE.** La prima parte é ovvia. Per la seconda basta osservare che, detti  $\mathbf{a}$  e  $\mathbf{b}$  due vettori di  $V(n, q)$ , risulta

$$\begin{aligned}\mathbf{a} + C = \mathbf{b} + C &\Leftrightarrow \mathbf{b} - \mathbf{a} \in C \Leftrightarrow (\mathbf{b} - \mathbf{a})H^t = \mathbf{0} \Leftrightarrow \\ &\mathbf{a}H^t = \mathbf{b}H^t \Leftrightarrow S(\mathbf{a}) = S(\mathbf{b}).\end{aligned}$$

□

Torniamo ora al problema della codifica e della decodifica. L'operazione di codifica consiste nel porre in corrispondenza biunivoca  $q^k$  messaggi assegnati con le parole di  $C$  e ovviamente non é restrittivo supporre che l'insieme dei messaggi sia l'insieme dei vettori di  $V(k, q)$ , lo spazio vettoriale  $k$ -dimensionale su  $F_q$ .

Se  $G$  é una matrice generatrice di  $C$ , della quale denotiamo con  $\mathbf{g}_i$  i vettori riga, si sceglie come *funzione di codifica* l'applicazione

$$\mathbf{a} = (a_1, a_2, \dots, a_k) \in V(k, q) \rightarrow a_1\mathbf{g}_1 + a_2\mathbf{g}_2 + \dots + a_k\mathbf{g}_k \in C,$$

che é un isomorfismo di spazi vettoriali. Allora, avendosi

$$a_1\mathbf{g}_1 + a_2\mathbf{g}_2 + \dots + a_k\mathbf{g}_k = \mathbf{a}G,$$

l'*algoritmo di codifica* é semplicemente il prodotto (righe per colonne) di vettori numerici di lunghezza  $k$  per la matrice  $G$ . Di solito la matrice  $G$  é data in forma standard  $G = [I_k, A]$ . In questo caso, le prime  $k$  lettere di  $\mathbf{a}G$  coincidono ordinatamente con le componenti di  $\mathbf{a}$ , rappresentano cioè il messaggio, mentre le rimanenti  $n - k$  sono quelle che abbiamo chiamato lettere di controllo.

Sia dunque

$$\mathbf{x} = \mathbf{a}G$$

la parola di  $C$  con la quale é stato codificato il messaggio  $\mathbf{a}$  e supponiamo che questa venga trasmessa e ricevuta in errore; il decodificatore riceva cioè una parola  $\mathbf{y} \neq \mathbf{x}$ . Supponiamo inoltre  $d(\mathbf{x}, \mathbf{y}) \leq e$ . In questo caso  $\mathbf{y} \notin C$  e il decodificatore deve risalire in modo automatico a  $\mathbf{x}$  secondo il principio del *nearest neighbour decoding*; deve quindi usare un algoritmo di decodifica che gli permetta di trovare la parola  $\mathbf{z}$  di  $C$  a distanza minima da  $\mathbf{y}$ . Ricordiamo che, essendo  $d(\mathbf{x}, \mathbf{y}) \leq e$ , risulta  $\mathbf{z} = \mathbf{x}$ . Assegnata una tabella standard di  $C$ , un possibile schema di decodifica é il seguente: se  $i$  é l'indice della riga della tabella cui  $\mathbf{y}$  appartiene, si decodifica  $\mathbf{y}$  come  $\mathbf{z} = \mathbf{y} - \mathbf{a}_i$ . Poiché il peso di  $\mathbf{a}_i = \mathbf{y} - \mathbf{z}$ , che é uguale alla distanza fra  $\mathbf{y}$  e  $\mathbf{z}$ , é per costruzione il piú piccolo possibile, al variare di  $\mathbf{z} \in C$ , siamo sicuri di aver usato uno schema di decodifica secondo il principio del *nearest neighbour decoding*. L'algoritmo corrispondente a questo schema é semplice a descriversi e consta dei seguenti passi:

**primo passo:** scorrere la tabella standard, iniziando dal primo elemento della prima riga e continuando in successione, fino a trovare la parola ricevuta  $\mathbf{y}$ ;

**secondo passo:** decodificare  $\mathbf{y}$  come la prima parola della colonna della tabella cui  $\mathbf{y}$  appartiene.

Osserviamo esplicitamente che lo schema di decodifica descritto si fonda sostanzialmente su due fatti:

- (1) l'errore  $e = \mathbf{y} - \mathbf{x}$ , che il decodificatore non conosce e deve scoprire, e la parola  $\mathbf{y}$  ricevuta sono nello stesso laterale di  $C$ ;
- (2) la speranza che durante la trasmissione non si siano verificati troppi errori; cioè il peso di  $e$  sia abbastanza piccolo in modo che  $e$  abbia buona probabilità di coincidere con la direttrice del laterale  $\mathbf{y} + C$ .

Quando il numero delle parole di  $C$  è molto grande, il primo passo del nostro algoritmo di decodifica può richiedere molto tempo, così l'intero sistema di comunicazione corre il rischio di essere troppo lento. Se ciò accade, conviene servirsi di sistemi di decodifica più veloci. Uno di questi si basa sulla cosiddetta *decodifica a sindromi*, che funziona nel seguente modo:

- (1) si estende una tabella standard di  $C$  aggiungendo la colonna delle sindromi, cioè la colonna il cui elemento generico è la sindrome delle parole del laterale corrispondente alla riga cui l'elemento stesso appartiene (cfr. prop. 14.2.3);
- (2) si calcola la sindrome  $S(\mathbf{y})$  di  $\mathbf{y}$  e, scorrendo la colonna delle sindromi, si trova l'indice  $i$  della riga cui  $S(\mathbf{y})$  e  $\mathbf{y}$  appartengono;
- (3)  $\mathbf{y}$  si decodifica come  $\mathbf{z} = \mathbf{y} - \mathbf{a}_i$ .

Questo schema di decodifica necessita quindi di una matrice  $M$  con due sole colonne, la prima delle quali coincida con la prima colonna di una tabella standard  $\Sigma$  di  $C$ , la seconda con la colonna delle sindromi di  $\Sigma$ . Allora anche in questo caso l'algoritmo di decodifica è molto semplice e, detta  $H$  una matrice controllo di parità di  $C$ , consiste dei seguenti passi:

**primo passo:** calcolare la sindrome  $S(\mathbf{y}) = \mathbf{y}H^t$  della parola ricevuta  $\mathbf{y}$ ;

**secondo passo:** scorrere la colonna delle sindromi fino a trovare  $S(\mathbf{y})$ ;

**terzo passo:** decodificare  $\mathbf{y}$  come la differenza  $\mathbf{z}$  tra  $\mathbf{y}$  e la parola che si trova a sinistra di  $S(\mathbf{y})$  nella matrice  $M$ .

Si noti che la parola  $\mathbf{z}$  ottenuta alla fine dell'algoritmo è la stessa che si otterrebbe usando il primo schema di decodifica descritto. Si noti ancora che, al fine della decodifica di  $\mathbf{y}$ , il primo algoritmo deve scorrere una tabella con  $q^{n-k}$  righe e  $q^k$  colonne, mentre il secondo soltanto la colonna delle sindromi, che ha  $q^{n-k}$  elementi. È chiaro quindi che, se  $C$  è abbastanza grande, il secondo algoritmo è molto più veloce del primo.

**ESEMPIO 14.2.4.** Consideriamo il  $[4, 2]$ -codice binario

$$C = \{(0, 0, 0, 0), (1, 0, 1, 1), (0, 1, 0, 1), (1, 1, 1, 0)\}$$

avente come matrice controllo

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Una tabella standard di  $C$ , ampliata mediante la colonna delle sindromi, é data da

$$\begin{array}{cccc|c} (0, 0, 0, 0) & (1, 0, 1, 1) & (0, 1, 0, 1) & (1, 1, 1, 0) & (0, 0) \\ (1, 0, 0, 0) & (0, 0, 1, 1) & (1, 1, 0, 1) & (0, 1, 1, 0) & (1, 1) \\ (0, 1, 0, 0) & (1, 1, 1, 1) & (0, 0, 0, 1) & (1, 0, 1, 0) & (0, 1) \\ (0, 0, 1, 0) & (1, 0, 0, 1) & (0, 1, 1, 1) & (1, 1, 0, 0) & (1, 0) \end{array} .$$

□

Gli algoritmi descritti sono applicabili a tutti i codici lineari. C'è da osservare che essi possono essere modificati e resi più efficienti in presenza di particolari classi di tali codici.

### 14.3 Il problema fondamentale della teoria dei codici lineari

**PROPOSIZIONE 14.3.1.** *Siano  $C$  un  $[n, n-m]$ -codice su  $F_q$ ,  $H = (a_{ij})$  una sua matrice controllo di parità e denotiamo con*

$$\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^n$$

*i vettori colonna della matrice  $H$ . Valgono le seguenti proprietà:*

(1) *Se  $\mathbf{x}$  é una parola di  $C$  di peso  $t$  e se  $x_{i_1}, x_{i_2}, \dots, x_{i_t}$  sono le sue componenti diverse da zero, allora le colonne  $\mathbf{a}^{i_1}, \mathbf{a}^{i_2}, \dots, \mathbf{a}^{i_t}$  di  $H$  sono linearmente dipendenti di  $F_q^m$ .*

(2) *Se  $x_{i_1}, x_{i_2}, \dots, x_{i_t}$  sono elementi di  $F_q$  non tutti nulli tali che*

$$\sum_{j=1}^t x_{i_j} \mathbf{a}^{i_j} = \mathbf{0},$$

*allora il vettore  $\mathbf{a} \in F_q^n$  di componenti*

$$a_s = \begin{cases} 0 & \text{se } s \neq i_1, i_2, \dots, i_t, \\ x_{i_j} & \text{se } s = i_j, \text{ con } j = i_1, i_2, \dots, i_t. \end{cases}$$

*é una parola del codice  $C$  di peso al piú  $t$ .*

**DIMOSTRAZIONE.** Nell'ipotesi (1), osservato che

$$\begin{aligned} \mathbf{x}H^t &= \left( \sum_{j=1}^n x_j a_{1j}, \sum_{j=1}^n x_j a_{2j}, \dots, \sum_{j=1}^n x_j a_{mj} \right) \\ &= \left( \sum_{j=1}^t x_{i_j} a_{1i_j}, \sum_{j=1}^t x_{i_j} a_{2i_j}, \dots, \sum_{j=1}^t x_{i_j} a_{mi_j} \right), \end{aligned}$$

l'asserto segue dalle seguenti implicazioni:

$$\mathbf{x}H^t = \mathbf{0} \Rightarrow \left( \sum_{j=1}^t x_{i_j} a_{1i_j}, \sum_{j=1}^t x_{i_j} a_{2i_j}, \dots, \sum_{j=1}^t x_{i_j} a_{mi_j} \right) = \mathbf{0} \Rightarrow \\ x_{i_1} \mathbf{a}^{i_1} + x_{i_2} \mathbf{a}^{i_2} + \dots + x_{i_t} \mathbf{a}^{i_t} = \mathbf{0}.$$

Con un ragionamento analogo si prova la seconda parte della proposizione.  $\square$

Conseguenza immediata dell'ultima proposizione é il seguente teorema.

**PROPOSIZIONE 14.3.2.** *Siano  $C$  un  $[n, n - m]$ -codice su  $F_q$  e  $H$  una sua matrice controllo di parit . Allora  $C$  ha distanza minima  $d$  se, e soltanto se, le colonne di  $H$  generano  $F_q^m$  e verificano le seguenti due propriet :*

$$\begin{cases} \text{ogni sottoinsieme di } d - 1 \text{ colonne   indipendente,} \\ \text{esistono } d \text{ colonne dipendenti.} \end{cases} \quad (14.7)$$

Inoltre, per ogni fissato  $[n, n - m, d]$ -codice su  $F_q$ , risulta

$$d \leq m + 1. \quad (14.8)$$

Osserviamo esplicitamente che la (14.8) segue dal fatto che  $m$    il massimo numero di vettori indipendenti di  $V(m, q)$ .

**COROLLARIO 14.3.3.** *Sia  $C$  un  $[n, n - m]$ -codice su  $F_q$  e  $H$  una sua matrice controllo di parit . Allora  $C$  ha distanza minima  $d > 2$  se, e soltanto se, le colonne di  $H$  sono le coordinate proiettive dei punti di una calotta di specie  $d - 2$  in  $PG(m - 1, q)$ .*

**DIMOSTRAZIONE.** Basta osservare che, se    $d > 2$ , le colonne di  $H$  sono a due a due non proporzionali e, quindi, rappresentano punti distinti di  $PG(m - 1, q)$ .  $\square$

**DEFINIZIONE 14.3.4.** I codici lineari per i quali la (14.8)   un'uguaglianza, cio  i codici con parametri  $[n, n - m, m + 1]$  si chiamano *codici MDS*, o *MDS-codici* (*MDS* sta per *maximum distance separable*).  $\square$

Fissati  $m, d, q$ , con  $d \leq m + 1$ , il problema di calcolare il pi  grande intero  $n$  per cui esiste un codice su  $F_q$  con parametri  $[n, n - m, d]$    noto come *problema fondamentale della teoria dei codici lineari*. Tale problema, nel caso  $d \geq 2$ ,   equivalente al *packing problem* che abbiamo introdotto nel paragrafo 2.2.5. Il corollario 14.3.3, infatti, prova anche il seguente teorema.

**PROPOSIZIONE 14.3.5.** *Fissati  $m, d, q$ , con  $d \leq m + 1$ , il massimo intero  $n$  per cui esiste un codice su  $F_q$  con parametri  $[n, n - m, d]$    uguale al massimo numero di punti di una calotta di specie  $d - 2$  in  $PG(m - 1, q)$ , cio  a  $M_{d-2}(m - 1, q)$ .*

**ESERCIZIO 14.3.6.** *Siano  $n, d$  interi tali che  $M_{d-2}(m - 2, q) < n \leq M_{d-2}(m - 1, q)$ . Allora  $n - m$    la massima dimensione di un codice lineare di lunghezza  $n$  e distanza minima  $d$  su  $F_q$ .*

**ESEMPIO 14.3.7.** Le colonne della matrice

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 1 & -1 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix}$$

sono a quattro a quattro indipendenti sul campo  $F_3 = \{0, 1, -1\}$ . Allora il codice lineare su  $F_3$  avente  $H$  come matrice di controllo, in forza della prop.14.3.2, ha parametri  $[11, 6, 5]$  e si verifica senza difficoltà che é perfetto:

$$3^6 \left[ \binom{11}{0} + \binom{11}{1}2 + \binom{11}{2}2^2 \right] = 3^6 [1 + 22 + 220] = 3^6 3^5 = 3^{11}.$$

Tale codice é noto come *codice (ternario) di Golay* e si denota con  $\mathcal{G}_{11}$ . □

**ESEMPIO 14.3.8.** Ricordiamo che i  $q + 1$  punti di una curva razionale normale di  $PG(m - 1, q)$  sono a  $m$  a  $m$  indipendenti e denotiamo con  $H$  una matrice le cui colonne sono le coordinate di tali punti. Allora il codice lineare su  $F_q$  avente  $H$  come matrice di controllo, in forza della prop.14.3.2, ha parametri  $[q + 1, q + 1 - m, m + 1]$  e, quindi, é un codice MDS. □

**ESERCIZIO 14.3.9.** Trovare il piú grande intero  $n$  per cui esistono:

- un  $[n, n - 3, 4]$ -codice su  $F_q$  (si noti che questi codici sono MDS);
- un  $[n, n - 4, 4]$ -codice su  $F_q$ .

## 14.4 I codici di Hamming

Consideriamo la famiglia

$$\{V_i(1, q) : i = 1, 2, \dots, n = q^{m-1} + q^{m-2} + \dots + q + 1\}$$

di tutti i sottospazi 1-dimensionali di  $V(m, q)$ ,  $m > 2$ , e in ognuno di essi scegliamo un vettore non nullo  $\mathbf{a}^i = (a_{1i}, a_{2i}, \dots, a_{mi})$ . Osserviamo che i sottospazi  $V_i(1, q)$  possono pensarsi come i punti dello spazio proiettivo  $PG(m - 1, q)$  e, in questo caso, i vettori  $\mathbf{a}^i$  diventano coordinate proiettive di tali punti.

Denotata con

$$H = H_{m,q} = (a_{ij})$$

la matrice di tipo  $m \times n$  avente come vettori colonna  $\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^n$ , possiamo considerare l'  $[n, n - m]$ -codice lineare avente  $H$  come matrice controllo di paritá. Tale codice, che denotiamo con  $Ham(m, q)$ , si chiama  $(m, q)$ -codice di Hamming ed é definito da

$$Ham(m, q) = \{\mathbf{a} \in F_q^n : \mathbf{a}H^t = \mathbf{0}\}.$$

Poiché  $H$  ha le colonne a due a due indipendenti (cioé distinte) e ne contiene tre dipendenti, abbiamo, in forza della prop.14.3.2, che la distanza minima di  $Ham(m, q)$  é 3 e di conseguenza esso é un  $[n, n-m, 3]$ -codice 1-correttore. Ne segue che le sfere di centro le parole di  $Ham(m, q)$  e raggio 1 sono a due a due disgiunte e, poiché ognuna di esse contiene esattamente  $n(q-1)+1$  parole di  $F_q^n$ , risulta

$$q^{n-m}[1+n(q-1)] = q^n = |F_q^n|,$$

il che assicura che  $Ham(m, q)$  é un codice perfetto. Osserviamo che (cfr. prop.14.3.1) una parola non nulla  $\mathbf{a}$  di  $H(m, q)$  ha peso  $c$  e presenta lettere diverse da zero nelle posizioni  $i_1, i_2, \dots, i_c$  se, e soltanto se, le colonne di posto  $i_1, i_2, \dots, i_c$  in  $H$  sono linearmente dipendenti. Osserviamo, ancora, che  $Ham(3, 2)$  é equivalente al codice associato al piano di Fano.  $\square$

## 14.5 L'enumeratore dei pesi

Uno dei problemi centrali nello studio di un codice lineare  $C$  di lunghezza  $n$  é il calcolo, per ogni  $i = 1, 2, \dots, n$ , del numero  $w_i = w_i(C)$  di tutte le parole di  $C$  di peso  $i$  e, a tale proposito, spesso si considera il polinomio

$$W(x, y) = W_C(x, y) = \sum_{\mathbf{a} \in C} x^{w(\mathbf{a})} y^{n-w(\mathbf{a})} = \sum_{i=0}^n w_i x^i y^{n-i}, \quad (14.9)$$

che prende il nome di *enumeratore dei pesi* di  $C$ . Il teorema successivo, che riportiamo senza dimostrazione, fornisce una importante relazione fra  $W(x, y)$  e l'enumeratore dei pesi  $W^\perp(x, y)$  del codice duale di  $C$ .

**PROPOSIZIONE 14.5.1.** (F.J.MacWilliams, 1963). *Siano  $W(x, y)$  e  $W^\perp(x, y)$  gli enumeratori dei pesi rispettivamente di un  $[n, k]$ -codice  $C$  su  $F_q$  e del suo duale. Allora risulta*

$$W^\perp(x, y) = q^{-k} W(y - x, y + (q-1)x)$$

e quindi, se  $C$  é autoduale, risulta

$$W(x, y) = q^{-n/2} W(y - x, y + (q-1)x).$$

**OSSERVAZIONE 14.5.2.** In alcuni casi la conoscenza dei pesi delle parole di una matrice generatrice  $A$  di un codice lineare dá informazioni sui coefficienti del polinomio enumeratore dei pesi. Per esempio, se due parole  $\mathbf{a}, \mathbf{b}$  di un codice binario  $C$  hanno peso pari  $2s$  e  $2t$ , rispettivamente, detto  $m$  il numero degli indici  $j$  tali che  $a_j = b_j = 1$ , risulta

$$w(\mathbf{a} + \mathbf{b}) = 2s - m + 2t - m = 2(s + t - m).$$

Ne segue che, se le parole di  $A$  hanno tutte peso pari, allora  $C$  é un codice *pari*, cioé tutte le sue parole hanno peso pari. Analogamente si prova che, se  $C$  é autoortogonale e tutte le parole di  $A$  hanno peso divisibile per 4, la stessa proprietá é vera per tutte le parole di  $C$ . In questo caso  $C$  si dice *doppiamente pari*.  $\square$

## 14.6 Codici ciclici

Un  $[n, k]$ -codice  $C$  su  $F_q$  si dice *ciclico* se verifica la seguente proprietà

$$(a_0, a_1, \dots, a_{n-2}, a_{n-1}) \in C \Leftrightarrow (a_{n-1}, a_0, \dots, a_{n-3}, a_{n-2}) \in C. \quad (14.10)$$

Nello studio dei codici ciclici conviene, e vedremo subito perché, indicare le lettere che formano una parola  $\mathbf{a}$  con  $a_0, a_1, \dots, a_{n-1}$  invece che con  $a_1, a_2, \dots, a_n$ . Possiamo, infatti, pensare di identificare la parola

$$\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in F_q^n$$

con il polinomio

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} \in F_q^n[x].$$

Tenendo presente che:

- i polinomi che si ottengono in corrispondenza degli elementi di  $F_q^n$  sono tutti e soli quelli di grado minore di  $n$ ,
- ogni laterale proprio dell'ideale  $(x^n - 1)$  di  $F_q[x]$  generato da  $x^n - 1$  contiene un unico polinomio di grado minore di  $n$ ,

la funzione

$$\mathbf{a} \rightarrow a(x)$$

può essere considerata come una biiezione fra  $F_q^n$  e l'anello quoziente

$$Pol_q(n, x) = F_q[x]/(x^n - 1).$$

In questo modo, ogni polinomio a coefficienti in  $F_q$  viene sostanzialmente identificato col resto della sua divisione per  $x^n - 1$ .

Per ogni sottoinsieme  $S$  di  $F_q^n$ , denoteremo con  $S(x)$  il corrispondente sottoinsieme in  $Pol_q(n, x)$ .

Se si riguarda  $Pol_q(n, x)$  come spazio vettoriale su  $F_q$ , la biiezione precedente è chiaramente un isomorfismo di spazi vettoriali e,  $C(x)$  è un sottospazio vettoriale di  $Pol_q(n, x)$ . Con queste posizioni si ha subito che la (14.10) equivale a

$$a(x) \in C(x) \Rightarrow xa(x) \in C(x) \quad (14.11)$$

e ciò, come vedremo, porta immediatamente ad una caratterizzazione algebrica dei codici ciclici.

**PROPOSIZIONE 14.6.1.** *Un codice lineare  $C$  su  $F_q$  è ciclico se, e soltanto se,  $C(x)$  è un ideale di  $Pol_q(n, x)$ .*

**DIMOSTRAZIONE.** Se  $C$  è lineare e ciclico,  $C(x)$  è sottospazio vettoriale di  $Pol_q(n, x)$  e, per ogni  $a(x) \in C(x)$  e  $q(x) = q_0 + q_1x + \dots + q_{n-1}x^{n-1}$  in  $Pol_q(n, x)$ , risulta

$$q(x)a(x) = q_0a(x) + q_1xa(x) + \dots + q_{n-1}x^{n-1}a(x).$$

Ne segue che  $q(x)a(x)$  é in  $C(x)$  perché, in forza della (14.11),  $x^s a(x)$  é in  $C(x)$ , per ogni intero non negativo  $s$ .

Se  $C(x)$  é un ideale di  $Pol_q(n, x)$ , allora  $C$  é sottospazio vettoriale di  $F_q^n$  e, per ogni parola  $\mathbf{a} \in C$ ,  $x\mathbf{a}(x)$  é un elemento di  $C(x)$ ; cioè  $C(x)$  é ciclico.  $\square$

Ricordiamo che l'anello  $F_q[x]$  é ad ideali principali e, quindi, ogni suo ideale  $J$  contiene qualche polinomio

$$c(x) = c_0 + c_1x + \cdots + c_{m-1}x^{m-1} + c_mx^m$$

che lo genera. I generatori di  $J$  sono, allora, tutti e soli i polinomi che differiscono da  $c(x)$  per una costante moltiplicativa non nulla e, tra essi, ve ne é uno solo monico, il *polinomio minimo* di  $J$ . Inoltre, se  $J_1 = (c_1(x))$  e  $J_2 = (c_2(x))$  sono ideali di  $F_q[x]$ , risulta  $J_1 \subseteq J_2$  se, e solo se,  $c_2(x)$  divide  $c_1(x)$ . Osserviamo, ora, che ogni ideale  $C(x)$  di  $Pol_q(n, x)$  é un quoziente  $J/(x^n - 1)$ , con  $J$  ideale di  $F_q[x]$  contenente l'ideale  $(x^n - 1)$ , e ogni generatore  $c(x)$  di  $J$ , che puó identificarsi con un generatore di  $C(x)$  e si chiama *polinomio generatore* di  $C$ , deve dividere  $x^n - 1$ . Ne segue, in forza della prop.14.6.1, che il numero degli  $[n, k]$ -codici ciclici su  $F_q$  é uguale al numero dei polinomi di  $F_q[x]$  che dividono  $x^n - 1$ , a meno di una costante moltiplicativa non nulla. Cosí, se  $x^n - 1$  possiede  $s$  fattori irriducibili distinti in  $F_q[x]$ , il numero degli  $[n, k]$ -codici ciclici su  $F_q$  é  $2^s$ , in tale numero essendo compresi anche il codice nullo  $\{\mathbf{0}\}$  e  $F_q^n$ .

Se  $c(x)$  é un polinomio generatore di un codice ciclico  $C$ , il polinomio  $h(x) \in F_q[x]$ , definito da

$$x^n - 1 = c(x)h(x),$$

prende il nome di *polinomio di controllo* di  $C$ .

**ESEMPIO 14.6.2.** Il polinomio  $x^4 - 1 \in F_3[x]$ , ha la seguente decomposizione in fattori irriducibili

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

e quindi abbiamo otto polinomi a coefficienti in  $F_3$  che dividono  $x^4 - 1$ :  $1, x - 1, x + 1, x^2 + 1, (x - 1)(x + 1), (x - 1)(x^2 + 1), (x + 1)(x^2 + 1), x^4 - 1$ . Esistono, pertanto, otto codici ciclici di lunghezza 4 su  $F_3$ .  $\square$

**PROPOSIZIONE 14.6.3.** Sia  $C$  un  $[n, k]$ -codice ciclico su  $F_q$  con polinomio generatore di grado  $m$

$$c(x) = c_0 + c_1x + \cdots + c_{m-1}x^{m-1} + c_mx^m$$

e relativo polinomio di controllo  $h(x)$ . Allora la matrice di tipo  $(n - m) \times n$

$$G_c = \begin{bmatrix} c_0 & c_1 & \cdots & c_m & & & 0 \\ & c_0 & c_1 & \cdots & c_m & & \\ & & \ddots & & & & \\ & 0 & & c_0 & \cdots & c_{m-1} & c_m \end{bmatrix}$$

é una matrice generatrice di  $C$  e, di conseguenza, é

$$k = n - m.$$

Inoltre, una parola  $\mathbf{a} \in F_q^n$  appartiene al codice  $C$  se, e soltanto se, risulta

$$a(x)h(x) = 0 \text{ in } Pol_q(n, x).$$

**DIMOSTRAZIONE.** Le righe di  $G_c$  sono chiaramente linearmente indipendenti e sono tutte parole di  $C$  perché i polinomi corrispondenti sono  $c(x), xc(x), \dots, x^{n-m-1}c(x)$  e  $\mathbf{c} \in C$ . Resta da provare che ogni parola di  $C$  è combinazione lineare delle righe di  $G_c$ . Ora, se  $\mathbf{a} \in C$ , il polinomio  $a(x)$  è in  $C(x)$  e quindi esiste un polinomio  $q(x)$  di grado minore di  $n - m$  tale che

$$a(x) = q(x)c(x). \quad (14.12)$$

Essendo i gradi di  $a(x), q(x), c(x)$  non superiori ad  $n$ , l'uguaglianza precedente è una uguaglianza in  $F_q[x]$  e così abbiamo

$$a(x) = q_0c(x) + q_1xc(x) + \dots + q_{n-m-1}x^{n-m-1}c(x),$$

cioè  $\mathbf{a}$  è combinazione lineare delle righe di  $G_c$  mediante gli scalari  $q_0, q_1, \dots, q_{n-m-1}$ . Inoltre, dalla 14.6.3, abbiamo

$$a(x)h(x) = q(x)c(x)h(x) = (x^n - 1)q(x) = 0 \text{ in } Pol_q(n, x).$$

Supponiamo ora che per un polinomio  $a(x)$  di grado minore di  $n$ , sia

$$a(x)h(x) = 0 \text{ in } Pol_q(n, x)$$

e sia

$$a(x) = q(x)c(x) + r(x),$$

con  $r(x)$  di grado minore di  $m = n - k$ . Allora

$$r(x)h(x) = r(x)h(x) + (x^n - 1)q(x) =$$

$$r(x)h(x) + c(x)h(x)q(x) = h(x)a(x) = 0 \text{ in } Pol_q(n, x).$$

Poiché il grado di  $r(x)h(x)$  è minore di  $n$ , l'ultima uguaglianza assicura che  $r(x)h(x)$  è il polinomio nullo; di conseguenza  $r(x)$  è il polinomio nullo e  $a(x)$  appartiene a  $C(x)$ . L'asserto è così completamente provato.  $\square$

Osserviamo che il polinomio di controllo di  $C$  è anche il polinomio generatore di un codice avente la stessa dimensione di  $C^\perp$ . Tale codice non coincide con  $C^\perp$  perché la relazione  $a(x)h(x) = 0$  in  $Pol_q(n, x)$  non equivale all'annullarsi del prodotto scalare  $\mathbf{a}\mathbf{h}$ .

**PROPOSIZIONE 14.6.4.** Sia  $C$  un  $[n, k]$ -codice lineare ciclico su  $F_q$  con polinomio di controllo

$$h(x) = h_0 + h_1x + \dots + h_{k-1}x^{k-1} + h_kx^k.$$

Allora la matrice di tipo  $(n - k) \times n$



In questa rappresentazione di  $Ham(m, 2)$ , il sottospazio vettoriale di  $Pol_2(n, x)$  ad esso associato é un ideale, avendosi

$$Ham(m, 2)(x) = \{a(x) \in Pol_2(n, x) : a(\alpha) = 0\}.$$

Si ha cosí che *ogni codice binario di Hamming é equivalente ad un codice ciclico.*

□