Es. (6.8 del libro)

Si consideri il codice (lineare) binario $C(5,1)$ con matrice generatrice $G = [1\ 1\ 1\ 1\ 1]$

($C \subseteq \mathbb{F}_2^n$, n = 5, k = 1; $(\mathbb{F}_2^n, +)$)

Costruire le parole del codice e una tabella di Slepian.

$k = 1 \rightarrow$ I possibili messaggi sono in $\mathbb{F}_2^k = \mathbb{F}_2 = \{0, 1\}$

$x = u \cdot G \rightarrow u = 0 \rightarrow x = [0\ 0\ 0\ 0\ 0]$, $u = 1 \rightarrow x = [1\ 1\ 1\ 1\ 1]$

Le parole di codice sono 00000 e 11111; è un codice a ripetizione di lunghezza 5.

$\binom{5}{0} = 1$

$\binom{5}{1} = 5$ peso 1

$\binom{5}{2} = 10$ peso 2

q^n sequenze

2^5 seq.

Parole di codice (peso 0)		Sindromi
00000	11111	0000^T
00001	11110	0001^T
00010	11101	0010^T
00100	11011	0100^T
01000 ← e	10111 ← y	1000^T
10000	01111	1111^T
00011	11100	0011^T
00101	11010	
00110	11001	
01001	10110	
⋮	⋮	

laterale

Sindrome di $y \in \mathbb{F}_q^n$: $s(y) = H \cdot y^T \in \mathbb{F}_q^{n-k}$

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

$n - k = 4$ righe

$n = 5$ colonne

$rk(H) = n - k = 4$ ✓

$rk(H) = 4$

$H \cdot G^T = 0_{((n-k)\times k)}$ ✓

$((n-k)\times n)\ (n \times k)$

$H y^T = \sum_{i=1}^{n} h_i \cdot y_i$

$\hat{x} = y - e = 10111 - 01000$

h_i = i-esima colonna di H = 11111

Codici di Hamming

Nel caso binario, un codice di Hamming ha $n = 2^m - 1$ (per qualche $m \geq 2$) e $k = \underbrace{2^m - 1}_{n} - m$ $(m = n - k)$; la matrice di controllo contiene <u>tutte</u> le sequenze binarie di lunghezza m non nulle.

Esempio: $m = 3$ ($\rightarrow n = 7, k = 4$; $C(7,4)$); una <u>possibile</u> matrice di controllo H è:

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

$-A^T$ $\quad I_{n-k}$ $\quad$ (1) (2) (3) (4) (5) (6) (7)

$G = [I_k \mid A]$ $\qquad$ G

$$G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \qquad G = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \ \ldots\ldots$$

$$s(y) = H y^T = \sum_{i=1}^{n} \vec{h_i} \cdot y_i$$

($\vec{h_i}$: i-esima colonna di H)

$$s(y) = s(x+e) = s(x) + s(e) = s(e) = \sum_{i=1}^{n} \vec{h_i} \cdot e_i$$

(e: 0)

Distanza minima del codice è 3 $\rightarrow$ <u>corregge fino a 1 errore</u>

Possiamo assumere (ai fini della decodifica) che la config. di errore e abbia peso ≤ 1

$e_i \neq 0$ <u>al più</u> per <u>una</u> posizione

$$\rightarrow s(y) = s(e) = \boxed{\vec{h_i} \cdot e_i} \quad (i = 1, 2, \ldots, n) = \vec{h_i}$$

→ Correggi l'errore in posizione i : $\hat{x} = y - e_i$

Esempio. Seq. trasmessa : $x = 1\,0\,0\,1\,1\,0\,0$

Seq. ricevuta : $y = 1\,0\,0\,0\,1\,0\,0$

Calcolo $s(y) = Hy^T = \begin{bmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{bmatrix} \cdot \begin{bmatrix} 1\\0\\0\\0\\1\\0\\0 \end{bmatrix} = \begin{bmatrix} 0\\0\\1 \end{bmatrix} \cdot 1 + \begin{bmatrix} 1\\0\\1 \end{bmatrix} \cdot 1 = \begin{bmatrix} 1\\0\\0 \end{bmatrix} = (100)^T$

(① ② ③ ④)

$s(y) = s(e) = 100^T \Rightarrow \vec{h_i} = \begin{bmatrix} 1\\0\\0 \end{bmatrix} \Rightarrow i = 4 \Rightarrow e = (0001000)$

$e_i = 1$, $i = 4$

$\Rightarrow \hat{e} = \vec{h_4} \Rightarrow \hat{x} = y - \hat{e} = 1000100 - 0001000 = 1001100$

→ In questo caso, la decodifica è corretta.

Decodifica per un codice di Hamming:

1. Ricevi y dal canale e calcola $s(y) = Hy^T$
2. Se $s(y) = \vec{0}$, restituisci $\hat{x} = y$
3. Altrimenti, cerca la colonna $\vec{h_i}$ di H tale che $s(y) = e_i \cdot \vec{h_i}$; restituisci $\hat{x} = y - \hat{e}$ (correggi l'i-esima posizione di y con un pezza e_i)

Codici di Hamming generali (non necessariamente binari)

Alfabeto q-ario ($q \geq 2$); parametro $m \geq 2$

Un codice di Hamming q-ario con parametro m ha nella matrice di controllo $n = (q^m - 1)/(q-1)$ colonne, tutte <u>a coppie</u> linearmente indipendenti.

$\Rightarrow k = n - m = (q^m - 1)/(q-1) - m$

0. Poni $S = \mathbb{F}_q^m \setminus \{00\ldots0\}$

Operativamente, per costruire H:

1 - Scelgo un elemento $h_1 \in S$

2 - Elimina da S tutti i multipli di h_1:
(tutti gli elementi della forma $\alpha \cdot h_1$ con $\alpha \in \mathbb{F}_q$)

3 - Torna al punto e prosegui con $h_2, h_3, \ldots$.

$q = 3$

$0, 1, 2$

$\mathbb{F}_3$

$h_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = 2 \cdot h_1$

Esempio: $\mathbb{F}_q = \mathbb{F}_3$ — $q = 3$, $m = 3$; $d_{min} = 3$.

$\rightarrow n = (q^3 - 1)/(q-1) = 13$, $k = n - m = 10$;

codice di tipo $C(13, 10, 3)$.

Matrice di controllo

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

$$2 \cdot \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}$$

$\frac{q^m - 1}{q - 1}$ deriva dal fatto che ci sono $q^m - 1$ possibili sequenze non-nulle di lunghezza m;

ogni sequenza ha esattamente q multipli (includendo anche se stessa)

$\rightarrow q - 1$ multipli diversi che vengono esclusi.