ESERCITAZIONE 10

Codice sistematico di Hamming $\overset{N\ K}{(7,4)}$

$$c = (\underbrace{u_1, u_2, u_3, u_4}_{\text{bit informativi}}, \underbrace{p_1, p_2, p_3}_{\text{bit di parità}})$$

matrice generatrice

$$x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7) = u\,G$$

$$= (u_1, u_2, u_3, u_4) \left(\begin{array}{cccc|ccc} \multicolumn{4}{c|}{K} & \multicolumn{3}{c}{N-K} \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ \multicolumn{4}{c|}{I_K} & \multicolumn{3}{c}{P} \end{array} \right)$$

$p_1 = u_1 \oplus u_2 \oplus u_3$

$p_2 = u_2 \oplus u_3 \oplus u_4$

$p_3 = u_1 \oplus u_2 \oplus u_4$

Sindrome / Matrice controllo H

$$\underbrace{S = (s_1, s_2, s_3)}_{\text{Sindrome}} = x\,H = (x_1, \dots, x_7) \begin{pmatrix} P \\ I_{N-K} \end{pmatrix} = (x_1, \dots, x_7) \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Sindrome	bit errato
1 0 1	$x_1 \to u_1$
1 1 1	$x_2 \to u_2$
1 1 0	$x_3 \to u_3$
0 1 1	$x_4 \to u_4$
1 0 0	$x_5 \to u_5$
0 1 0	$x_6 \to u_6$
0 0 1	$x_7 \to u_7$

$s_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_5$

$s_2 = x_2 \oplus x_3 \oplus x_4 \oplus x_6$

$s_3 = x_1 \oplus x_2 \oplus x_4 \oplus x_7$

Esercizio 1

Blocco informativo

$u = (1, 1, 0, 1)$

a) Calcolare la parola di codice di Hamming

$c = (1, 1, 0, 1, p_1, p_2, p_3)$

$p_1 = 1 \oplus 1 \oplus 0 = 0$

$p_2 = 1 \oplus 0 \oplus 1 = 0$

$p_3 = 1 \oplus 1 \oplus 1 = 1$

$= (1, 1, 0, 1, 0, 0, 1)$

b) Il ricevitore osserva

errore 6° bit

$x = (1, 1, 0, 1, 0, 1, 1)$

$s = (s_1, s_2, s_3) = (1 \oplus 1 \oplus 0 \oplus 0,\ 1 \oplus 0 \oplus 1 \oplus 1,\ 1 \oplus 1 \oplus 1 \oplus 1)$

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

c'è almeno 1 errore

010 → errore 6° bit → correggerlo.

Esercizio 2

Al ricevitore arriva un flusso di bit codificato con Hamming e essendo i primi 2 blocchi

$$\overbrace{\underbrace{0110|001}_{7\text{ bit}}}^{x_1} \quad \overbrace{\underbrace{1011|010}_{7\text{ bit}}}^{x_2}$$

Ipotizzando che in ciascun blocco sia presente al più 1 errore.

a) Calcolare le sindromi per i 2 blocchi:

1° blocco

$$\underbrace{s'}_{(s_1, s_2, s_3)} = x_1 H \qquad s'' = x_2 H$$

$$= (0 \oplus 1 \oplus 1 \oplus 0,\ 1 \oplus 1 \oplus 0 \oplus 0,\ 0 \oplus 1 \oplus 0 \oplus 1)$$

$$= \boxed{(0, 0, 0)}$$

nessun errore o più di 2

per ipotesi

errore 6° bit

$$s'' = (1 \oplus 0 \oplus 1 \oplus 0,\ 0 \oplus 1 \oplus 1 \oplus 1,\ 1 \oplus 0 \oplus 1 \oplus 0) = (0, 1, 0)$$

$$\underbrace{x_2}_{\text{corretto}} = (1, 0, 1, 1, 0, \boxed{0}, 0)$$

b) Ricevuto : bit informativi :

$\hat{u}_1 = (0,1,1,0)$

$\hat{u}_2 = (1,0,1,1)$

Esercizio 3

Il codice di Hamming (7,4) ha distanza minima $d_{min} = 3$.

$$d_{min} = \min_{c_1 \neq c_2} \underbrace{d_H(c_1, c_2)}$$

distanza di Hamming
bit in cui differiscono
c_1 e c_2.

Corregge fino a t errori dove $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$

potere correttore

Rileva fino a $d_{min}-1$ errori

potere rivelatore

Oss. I codici di Hamming che vediamo hanno distanza minima 3.

a) $t = \frac{3-1}{2} = 1$ correggono un errore

ne rivela fino a 2 errori

Supponiamo di avere la parola nulla $c = (0,0,0,0,0,0,0)$

e emergono 2 errori nella prima e seconda posizione.

$$x = (1, 1, 0, 0, 0, 0, 0)$$

identifico 2 righe di H (H_1 e H_2)

$$\underline{s} = H_1 \oplus H_2 = H_6 = (1 \oplus 1 \oplus 0 \oplus 0,\ 1 \oplus 0 \oplus 0 \oplus 0,\ 1 \oplus 1 \oplus 0 \oplus 0)$$

sindrome

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

errore 6° bit (rivelato)

$\downarrow$ ricostruita

$$\hat{x} = (1, 1, 0, 0, 0, 1, 0)$$

$$\neq$$

$$c$$ (inviata)

d) Supponiamo di avere 3 errori adesso in c

$$x = (1, 0, 1, 1, 0, 0, 0)$$ → PAROLA VALIDA

$$s = H_1 \oplus H_3 \oplus H_4 = (1, 0, 1) \oplus (1, 1, 0) \oplus (0, 1, 1)$$

$$= (0, 0, 0)$$

nessun errore rilevato

Esercizio 4

Costruzione codice di Hamming sistematico con $r=4$ bit di parità.

$$C = (\underbrace{u_1, u_2, \dots, u_K}_{\text{bit informativi}}, \underbrace{p_1, p_2, p_3, p_4}_{\text{bit parità}})$$

$$G = [\underbrace{I_K}_{\substack{\text{matrice}\\\text{identità}\\K \times K}} \quad \underbrace{P}_{\substack{\text{parità}\\K \times 4}}] \qquad H = \begin{pmatrix} P_{K \times 4} \\ \underbrace{I_{N-K}}_{4} \end{pmatrix}$$

$N = K + 4$

a) Spiegare come si deve costruire H

la sindrome $s = H_i$ ← riga i-esima di H

deve identificare univocamente la posizione dell'errore (posizione i-esima)

- Righe di H tutte non nulle
- Tutte diverse tra loro

$r = 4$ bit $\Rightarrow$ sindrome 4 bit

$2^4 - 1 = 15$ sindromi possibili $\Rightarrow$ # righe di H è 15.

$\rightarrow$ # posizione $= N$

b) $N = \overset{K}{11} + \underset{r}{4} = 15$

d) Dire quali righe devono comparire in P

$$H = \begin{pmatrix} P_{11\times 4} \\ I_4 \end{pmatrix} \qquad I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Parole con esattamente 1 uno.

$$P_{11\times 4} = \begin{pmatrix} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \end{pmatrix}$$ = parole con 2 uni, 3 uni e quella che 4 uni.

$$P_{11\times 4} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

e) In generale se r è # bit di parità allora la sindrome ha r bit.

$$\#\text{sindromi} = 2^r - 1$$

lung. codice

$$N = 2^r - 1$$

$$K = N - r = 2^r - r - 1$$

bit informativi

r	N	K
3	7	4
4	15	11
5	31	26
⋮	⋮	⋮

Esercizio 5

Hamming (7,4). Si assume che errori sui bit ricevuti siano indipendenti e che ogni bit sia errato con probabilità p.

a) Calcolare la probabilità che una parola ricevuta di 7 bit contenga più errori di quanti possa correggere.

$t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$ potere correttore

Probabilità di avere esattamente i-errori è binomiale

$$\Pr(\overset{\#\text{errori}}{I}=i) = \binom{7}{i} p^i (1-p)^{7-i}$$

$$P_{errore} = \Pr(\underbrace{I \geq 2}_{\text{almeno 2 errori non riesco a correggerli}}) = 1 - \Pr(I=0) - \Pr(I=1)$$

$$= 1-(1-p)^7 - \underbrace{\binom{7}{1}}_{=7} p(1-p)^6 = 1-(1-p)^7 - p(1-p)^6$$

c) Se $p \ll 1$ un approssimazione è usare il termine dominante che è quello $\underline{I=2}$.

$$\Pr(I=2) = \binom{7}{2} p^2 \underbrace{(1-p)^5}_{p \ll 1 \rightarrow \sim 1} \sim 21 p^2$$

gli altri termini

$$\Pr(I=3) \simeq \binom{7}{3} p^3 \quad , \quad \Pr(I=4) \simeq \binom{7}{4} p^4, \dots$$

hanno potenze di p più alte.

$p \ll 1$

$$p^2 \gg p^3 \gg p^4 \gg \dots$$

Dunque

$$\boxed{P_{errore} \simeq 21 p^2}$$ blocco

d) Stimare probabilità sul singolo bit.

Come abbiamo visto l'errore dominante è quello di esattamente 2 errori.

$$S = xH = H_i \oplus H_j = H_k$$

$i \neq j \neq k$

terza riga diversa

Quindi la decodifica corregge 1 bit corretto.

2 errori $\longrightarrow$ 3 errori dopo decodifica

$$P_b = \frac{3}{7} P_{errore} \simeq \cancel{\frac{3}{7}} \cdot \cancel{21}^{3} p^2 = \boxed{9 p^2}$$

enumerazione prob. uniforme nei bit in decodifica,