Fondamenti di Telecomunicazioni – Esercitazione 10

Corso di Ingegneria Fisica e Matematica
A.A. 2025–2026

Convenzioni.

Usiamo il codice di Hamming binario sistematico $(7, 4)$, con parola di codice

$$\mathbf{c} = (u_1, u_2, u_3, u_4, p_1, p_2, p_3).$$

I bit di parità sono

$$p_1 = u_1 \oplus u_2 \oplus u_3, \qquad p_2 = u_2 \oplus u_3 \oplus u_4, \qquad p_3 = u_1 \oplus u_2 \oplus u_4.$$

Una parola ricevuta si indica con

$$\mathbf{x} = (x_1, x_2, x_3, x_4, x_5, x_6, x_7),$$

dove i primi quattro bit sono informativi e gli ultimi tre sono bit di parità.

La sindrome viene calcolata nella forma

$$\mathbf{s} = \mathbf{x}H,$$

dove

$$H \in \mathbb{F}_2^{7\times 3}$$

è la matrice di controllo

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

In questo modo

$$\mathbf{s} = (s_1, s_2, s_3),$$

con

$$\begin{cases} s_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_5, \\ s_2 = x_2 \oplus x_3 \oplus x_4 \oplus x_6, \\ s_3 = x_1 \oplus x_2 \oplus x_4 \oplus x_7. \end{cases}$$

La sindrome nulla indica che la parola ricevuta soddisfa le equazioni di parità. Se c'è un solo errore, la sindrome coincide con la riga di H corrispondente alla posizione del bit errato:

sindrome	bit errato	sindrome	bit errato
101	$x_1 = u_1$	011	$x_4 = u_4$
111	$x_2 = u_2$	100	$x_5 = p_1$
110	$x_3 = u_3$	010	$x_6 = p_2$
001	$x_7 = p_3$		

Quindi la procedura di correzione di un errore singolo è:

$$\boxed{\mathbf{s} = \mathbf{x}H \quad \Longrightarrow \quad \text{cerco la riga di } H \text{ uguale a } \mathbf{s} \quad \Longrightarrow \quad \text{inverto quel bit.}}$$

Esercizio 1 – Codifica Hamming $(7, 4)$ e correzione di un errore su un bit di parità

Si consideri il blocco informativo

$$\mathbf{u} = (u_1, u_2, u_3, u_4) = (1, 1, 0, 1).$$

a) Calcolare i bit di parità e la parola di codice $\mathbf{c}$.

b) Supponiamo che durante la trasmissione si corrompa il sesto bit, cioè il bit di parità p_2, e che il ricevitore osservi

$$\mathbf{x} = (1, 1, 0, 1, 0, 1, 1).$$

Calcolare la sindrome.

c) Usare la sindrome per identificare e correggere l'errore.

d) Ricavare i bit informativi corretti.

Soluzione.

a) Calcoliamo

$$p_1 = 1 \oplus 1 \oplus 0 = 0, \qquad p_2 = 1 \oplus 0 \oplus 1 = 0, \qquad p_3 = 1 \oplus 1 \oplus 1 = 1.$$

Quindi

$$\mathbf{c} = (1, 1, 0, 1, 0, 0, 1).$$

b) Per

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

si ha

$$s_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_5 = 1 \oplus 1 \oplus 0 \oplus 0 = 0,$$
$$s_2 = x_2 \oplus x_3 \oplus x_4 \oplus x_6 = 1 \oplus 0 \oplus 1 \oplus 1 = 1,$$
$$s_3 = x_1 \oplus x_2 \oplus x_4 \oplus x_7 = 1 \oplus 1 \oplus 1 \oplus 1 = 0.$$

Dunque

$$\mathbf{s} = (0, 1, 0).$$

c) La sindrome $(0, 1, 0)$ coincide con la sesta riga di H. Quindi l'errore è nella posizione 6, cioè nel bit di parità p_2.

Correggiamo invertendo il sesto bit:

$$(1, 1, 0, 1, 0, 1, 1) \longrightarrow (1, 1, 0, 1, 0, 0, 1).$$

Quindi

$$\widehat{\mathbf{c}} = (1, 1, 0, 1, 0, 0, 1).$$

d) Essendo il codice sistematico, i bit informativi sono i primi quattro:

$$\widehat{\mathbf{u}} = (1, 1, 0, 1).$$

Esercizio 2 – Decodifica di uno stream ricevuto tramite sindrome

Supponiamo che, durante la trasmissione di un flusso di bit codificato con il codice di Hamming $(7, 4)$, il ricevitore osservi i primi due blocchi codificati:

$$0110001\ 1011010.$$

Decodificare i due blocchi, ipotizzando che in ciascun blocco sia presente al più un errore.

a) Dividere lo stream ricevuto in blocchi di 7 bit.

b) Calcolare la sindrome del primo blocco e, se necessario, correggerlo.

c) Calcolare la sindrome del secondo blocco e, se necessario, correggerlo.

d) Ricavare i bit informativi associati ai due blocchi.

Soluzione.

a) Lo stream ricevuto è

$$0110001\ 1011010.$$

Dividiamolo nei due blocchi:

$$\mathbf{x}_1 = (0,1,1,0,0,0,1), \qquad \mathbf{x}_2 = (1,0,1,1,0,1,0).$$

b) **Primo blocco.**

Calcoliamo la sindrome:

$$s_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_5 = 0 \oplus 1 \oplus 1 \oplus 0 = 0,$$

$$s_2 = x_2 \oplus x_3 \oplus x_4 \oplus x_6 = 1 \oplus 1 \oplus 0 \oplus 0 = 0,$$

$$s_3 = x_1 \oplus x_2 \oplus x_4 \oplus x_7 = 0 \oplus 1 \oplus 0 \oplus 1 = 0.$$

Dunque

$$\mathbf{s}_1 = (0,0,0).$$

La sindrome è nulla, quindi il blocco ricevuto soddisfa le equazioni di parità. Assumendo al più un errore, non correggiamo nulla:

$$\widehat{\mathbf{c}}_1 = (0,1,1,0,0,0,1).$$

c) **Secondo blocco.**

Calcoliamo la sindrome di

$$\mathbf{x}_2 = (1,0,1,1,0,1,0).$$

Si ha

$$s_1 = 1 \oplus 0 \oplus 1 \oplus 0 = 0,$$

$$s_2 = 0 \oplus 1 \oplus 1 \oplus 1 = 1,$$

$$s_3 = 1 \oplus 0 \oplus 1 \oplus 0 = 0.$$

Quindi

$$\mathbf{s}_2 = (0,1,0).$$

La sindrome $(0,1,0)$ coincide con la sesta riga di H. Quindi l'errore è nella posizione 6, cioè nel bit di parità p_2.

Correggendo:

$$(1,0,1,1,0,1,0) \longrightarrow (1,0,1,1,0,0,0).$$

Quindi

$$\widehat{\mathbf{c}}_2 = (1,0,1,1,0,0,0).$$

d) Essendo il codice sistematico, i bit informativi sono i primi quattro bit di ciascun blocco corretto:

$$\widehat{\mathbf{u}}_1 = (0,1,1,0), \qquad \widehat{\mathbf{u}}_2 = (1,0,1,1).$$

Quindi la decodifica dei primi due blocchi produce

$$\boxed{\widehat{\mathbf{u}}_1 = 0110, \qquad \widehat{\mathbf{u}}_2 = 1011.}$$

Concatenando:

$$\boxed{01101011.}$$

Esercizio 3 – Potere correttore e potere rivelatore

Il codice di Hamming $(7,4)$ ha distanza minima

$$d_{\min} = 3.$$

Ricordiamo che la distanza minima $d_{\min}$ di un codice a blocco è la minima distanza di Hamming tra due parole di codice distinte:

$$d_{\min} = \min_{\mathbf{c}_1 \neq \mathbf{c}_2} d_H(\mathbf{c}_1, \mathbf{c}_2).$$

Essa misura quanto sono separate tra loro le parole lecite del codice.

Se una parola trasmessa subisce pochi errori, il vettore ricevuto rimane vicino alla parola trasmessa. Il codice può correggere in modo garantito fino a

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

errori, perché le sfere di raggio t centrate sulle parole di codice non si sovrappongono.

Invece un codice può rivelare fino a

$$d_{\min} - 1$$

errori, perché con meno di $d_{\min}$ cambiamenti non si può passare da una parola di codice a un'altra parola di codice.

a) Calcolare il potere correttore.

b) Dire quanti errori sono sicuramente rivelabili.

c) Considerare la parola di codice nulla

$$\mathbf{c} = (0,0,0,0,0,0,0).$$

Se avvengono due errori nelle posizioni 1 e 2, il ricevitore osserva

$$\mathbf{x} = (1,1,0,0,0,0,0).$$

Calcolare la sindrome e commentare.

d) Mostrare con un esempio che tre errori possono non essere rivelati.

Soluzione.

a)
$$t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1.$$

Quindi il codice corregge sicuramente un errore:

$$t = 1.$$

b) Un codice con distanza minima $d_{\min}$ rivela sicuramente fino a $d_{\min} - 1$ errori. Qui:

$$d_{\min} - 1 = 2.$$

Il codice rivela fino a due errori, ma non li corregge necessariamente.

c) Per
$$\mathbf{x} = (1, 1, 0, 0, 0, 0, 0)$$
si ha
$$\mathbf{s} = \mathbf{x}H = H_1 \oplus H_2,$$
dove H_i indica la riga i-esima di H. Quindi
$$\mathbf{s} = (1, 0, 1) \oplus (1, 1, 1) = (0, 1, 0).$$

Equivalentemente:
$$s_1 = 1 \oplus 1 \oplus 0 \oplus 0 = 0,$$
$$s_2 = 1 \oplus 0 \oplus 0 \oplus 0 = 1,$$
$$s_3 = 1 \oplus 1 \oplus 0 \oplus 0 = 0.$$

Dunque
$$\mathbf{s} = (0, 1, 0).$$

La sindrome è non nulla, quindi il ricevitore rivela la presenza di errore. Tuttavia, se assumesse che ci sia un solo errore, correggerebbe il sesto bit, ottenendo una parola diversa da quella trasmessa.

Due errori sono quindi rivelabili, ma non correggibili in modo affidabile.

d) Consideriamo ancora la parola nulla e supponiamo tre errori nelle posizioni $1, 3, 4$:
$$\mathbf{x} = (1, 0, 1, 1, 0, 0, 0).$$

La sindrome vale
$$\mathbf{s} = H_1 \oplus H_3 \oplus H_4.$$

Ora
$$H_1 = (1, 0, 1), \qquad H_3 = (1, 1, 0), \qquad H_4 = (0, 1, 1),$$
e quindi
$$H_1 \oplus H_3 \oplus H_4 = (0, 0, 0).$$

Dunque
$$\mathbf{s} = (0, 0, 0).$$

La parola ricevuta è una parola di codice valida, quindi i tre errori non vengono rivelati.

Infatti
$$(1, 0, 1, 1) \mapsto (1, 0, 1, 1, 0, 0, 0).$$

Questo è coerente con $d_{\min} = 3$: esistono parole di codice distanti esattamente tre posizioni.

Esercizio 4 – Probabilità di errata decodifica per il codice di Hamming $(7, 4)$

Si consideri un codice di Hamming $(7, 4)$, con distanza minima

$$d_{\min} = 3.$$

Il codice viene usato come codice correttore di errori tramite decodifica a sindrome. Si assuma che gli errori sui bit ricevuti siano indipendenti e che ogni bit sia errato con probabilità

$$p.$$

a) Determinare il potere correttore del codice.

b) Calcolare la probabilità che una parola ricevuta di 7 bit contenga più errori di quanti il codice riesca a correggere.

c) Approssimare tale probabilità per $p \ll 1$.

d) Stimare la probabilità di errore sul singolo bit dopo la decodifica a sindrome.

Soluzione.

a) Il potere correttore di un codice con distanza minima $d_{\min}$ è

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor.$$

Nel caso del codice di Hamming $(7, 4)$, $d_{\min} = 3$, quindi

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

Dunque il codice corregge tutti i pattern con al più un errore:

$$t = 1.$$

b) La decodifica è garantita corretta se nella parola ricevuta ci sono zero errori oppure un errore.

La probabilità di avere i errori in una parola di 7 bit è binomiale:

$$\Pr\{I = i\} = \binom{7}{i} p^i (1 - p)^{7-i}.$$

La probabilità di uscire dalla regione di correzione garantita è quindi

$$P_{\text{fail}} = \Pr\{I \geq 2\}.$$

Pertanto

$$P_{\text{fail}} = 1 - \Pr\{I = 0\} - \Pr\{I = 1\} = 1 - (1 - p)^7 - 7p(1 - p)^6.$$

Equivalentemente:

$$P_{\text{fail}} = \sum_{i=2}^{7} \binom{7}{i} p^i (1 - p)^{7-i}.$$

Quindi

$$P_{\text{fail}} = 1 - (1 - p)^7 - 7p(1 - p)^6.$$

c) Per $p \ll 1$, il termine dominante nella somma è quello con esattamente due errori:

$$\Pr\{I = 2\} = \binom{7}{2} p^2 (1-p)^5.$$

Poiché

$$(1-p)^5 \simeq 1,$$

si ottiene

$$\Pr\{I = 2\} \simeq \binom{7}{2} p^2 = 21 p^2.$$

Gli altri termini hanno potenze più alte di p:

$$\Pr\{I = 3\} \simeq \binom{7}{3} p^3, \qquad \Pr\{I = 4\} \simeq \binom{7}{4} p^4,$$

e così via. Per $p \ll 1$,

$$p^2 \gg p^3 \gg p^4 \gg \cdots .$$

Dunque

$$P_{\text{fail}} \simeq 21 p^2.$$

d) Vogliamo ora stimare la probabilità di errore sul singolo bit dopo la decodifica.

Il caso dominante, per $p \ll 1$, è ancora quello con esattamente due errori nella parola ricevuta. Supponiamo quindi che siano errati due bit, nelle posizioni i e j. Con la decodifica a sindrome:

$$\mathbf{s} = \mathbf{x} H.$$

Se gli errori sono nelle posizioni i e j, allora la sindrome è la somma modulo 2 delle due righe corrispondenti di H:

$$\mathbf{s} = H_i \oplus H_j.$$

Nel codice di Hamming, la somma modulo 2 di due righe non nulle e distinte di H coincide con una terza riga di H. Quindi il decodificatore interpreta la sindrome come se ci fosse un solo errore in una terza posizione k, e ribalta anche quel bit.

Di conseguenza, nel caso dominante di due errori:

$$\text{2 errori iniziali} \quad \longrightarrow \quad \text{3 bit errati dopo la decodifica.}$$

La probabilità che ci siano esattamente due errori è circa

$$\binom{7}{2} p^2.$$

Quando questo accade, i bit errati dopo decodifica sono circa 3 su 7. Quindi la probabilità di errore sul singolo bit dopo decodifica si stima come

$$P_{b,\text{dec}} \simeq \frac{3}{7} \binom{7}{2} p^2.$$

Poiché

$$\binom{7}{2} = 21,$$

si ottiene

$$P_{b,\mathrm{dec}} \simeq \frac{3}{7} \cdot 21p^2 = 9p^2.$$

Dunque

$$P_{b,\mathrm{dec}} \simeq 9p^2.$$

Osservazione. La probabilità

$$P_{\mathrm{fail}} \simeq 21p^2$$

è una probabilità di errore a livello di blocco, cioè misura la probabilità che la parola ricevuta contenga troppi errori per essere corretta con garanzia. Invece

$$P_{b,\mathrm{dec}} \simeq 9p^2$$

è una stima della probabilità di errore sul singolo bit dopo la decodifica a sindrome.

Esercizio 5 – Costruzione del codice di Hamming $(15, 11)$

Vogliamo costruire un codice di Hamming binario con $r = 4$ bit di parità.
Usiamo una codifica sistematica, cioè le parole di codice hanno la forma

$$\mathbf{c} = (u_1, \ldots, u_K, p_1, p_2, p_3, p_4),$$

e la matrice generatrice ha struttura

$$G = [I_{K\times K} \quad P_{K\times 4}].$$

Con la convenzione usata in questa esercitazione, la sindrome si calcola come

$$\mathbf{s} = \mathbf{x}H,$$

quindi la matrice di controllo ha dimensione

$$H \in \mathbb{F}_2^{N\times 4}$$

e ha struttura

$$H = \begin{pmatrix} P \\ I_{4\times 4} \end{pmatrix}.$$

a) Spiegare perché H deve contenere tutte le stringhe binarie non nulle di lunghezza 4.

b) Determinare il numero di righe di H, cioè la lunghezza N del codice.

c) Determinare il numero di bit informativi K.

d) Dire quali righe devono comparire in P.

e) Generalizzare il risultato al caso di r bit di parità.

Soluzione.

a) Nel codice di Hamming, la sindrome deve identificare univocamente la posizione di un eventuale errore singolo.

Infatti, se l'errore è nella posizione i, allora

$$\mathbf{s} = H_i,$$

dove H_i è la riga i-esima di H.

Quindi tutte le righe di H devono essere:

- non nulle;
- tutte diverse tra loro.

Poiché la sindrome ha 4 bit, le possibili sindromi non nulle sono

$$2^4 - 1 = 15.$$

b) Per usare tutte le sindromi non nulle, H deve avere

$$N = 2^4 - 1 = 15$$

righe. Dunque il codice ha lunghezza

$$\boxed{N = 15.}$$

c) Poiché ci sono 4 bit di parità,

$$N = K + 4.$$

Quindi

$$K = N - 4 = 15 - 4 = 11.$$

Il codice ottenuto è quindi

$$\boxed{(15, 11).}$$

d) La struttura della matrice di controllo è

$$H = \begin{pmatrix} P \\ I_{4\times 4} \end{pmatrix}.$$

La parte $I_{4\times 4}$ contiene le quattro righe

$$1000, \qquad 0100, \qquad 0010, \qquad 0001,$$

associate ai quattro bit di parità.

Per completare H, la matrice P deve contenere tutte le altre stringhe binarie non nulle di lunghezza 4, cioè tutte quelle che non sono già righe di I_4.

Quindi il numero di righe di P è

$$2^4 - 1 - 4 = 11.$$

Graficamente:

$$G = \left[\underbrace{I_{11\times 11}}_{\text{bit informativi}} \qquad \underbrace{P_{11\times 4}}_{\text{bit di parità}} \right],$$

e

$$H = \left[\frac{P_{11\times 4}}{I_{4\times 4}} \right].$$

Una possibile scelta è prendere in P tutte le stringhe di lunghezza 4 con peso almeno 2:

$$P = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

In questo modo H contiene esattamente tutte le 15 stringhe binarie non nulle di lunghezza 4.

e) In generale, se il numero di bit di parità è r, allora la sindrome ha r bit.

Le sindromi non nulle sono

$$2^r - 1.$$

Quindi la lunghezza del codice è

$$\boxed{N = 2^r - 1.}$$

Poiché i bit di parità sono r, il numero di bit informativi è

$$\boxed{K = N - r = 2^r - 1 - r.}$$

Per esempio:

r	N	K	codice
3	7	4	$(7, 4)$
4	15	11	$(15, 11)$
5	31	26	$(31, 26)$