Proprietà dei codici a blocco

Peso di Hamming e distanza minima di un codice

- Il peso di Hamming $w(\mathbf{x})$ di una parola di codice $\mathbf{x}$ è costituito dal numero di '1' presenti in $\mathbf{x}$.
- Il peso di una parola di codice $\mathbf{x} \in \mathcal{C}(k, n)$ è la sua distanza dalla n-upla di tutti '0'

$$w(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0}_{1,n}) \tag{2}$$

- Per i codici lineari vale la proprietà che ciascuna parola di codice ha lo stesso insieme di distanze dalle altre parole di codice.
- La distanza minima di un codice si può calcolare a partire da una qualsiasi parola di codice.

Peso di Hamming e distanza minima di un codice

Teorema 3: La distanza minima del codice a blocco $\mathcal{C}(k, n)$ si può calcolare come il peso di Hamming minimo tra tutte le parole di codice

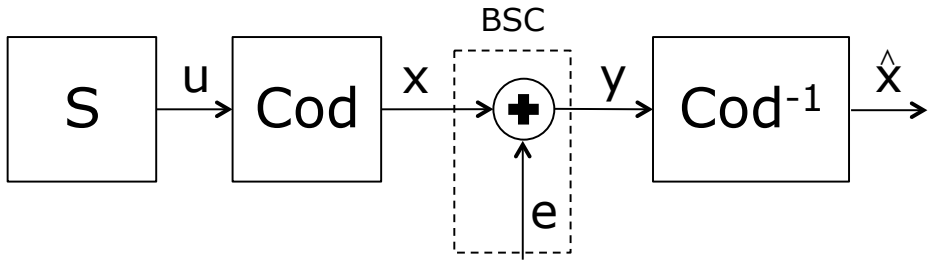
$$
\begin{aligned}
d_{min}(\mathcal{C}) &= \min_{\mathbf{x}_i, \mathbf{x}_j \in \mathcal{C}} d_H(\mathbf{x}_i, \mathbf{x}_j) \\
&= \min_{\mathbf{x}_i, \mathbf{x}_j \in \mathcal{C}} d_H(\mathbf{x}_i + \mathbf{x}_j, \mathbf{x}_j + \mathbf{x}_j) = \min_{\mathbf{x}_i, \mathbf{x}_j \in \mathcal{C}} d_H(\mathbf{x}_i + \mathbf{x}_j, \mathbf{0}_{1,n}) \\
&\qquad [\mathbf{x}_i + \mathbf{x}_j \in \mathcal{C}(k, n)] \\
&= \min_{\mathbf{x}_i \in \mathcal{C}} w(\mathbf{x}_i)
\end{aligned}
\tag{3}
$$

Rivelazione e decodifica degli errori

- Su un canale BSC senza memoria, la n-upla $\mathbf{y}$ a valle del decisore può essere rappresentata

$$\mathbf{y} = \mathbf{x} + \mathbf{e} \tag{4}$$

dove $\mathbf{e}$ è il vettore di errori introdotto dal canale.



- Se il canale non introduce errori $\Longrightarrow$ $\mathbf{e} = \mathbf{0}_{1,n}$.

Capacità di rivelare errori (*error detection*)

Sia $\mathbf{x}$ la parola di codice trasmessa e $\mathbf{y} = \mathbf{x} + \mathbf{e}$ la corrispondente sequenza di n bit ricevuta. Supponiamo che il canale introduca un certo numero di errori, i.e. $w(\mathbf{e}) > 0$.

- Se $\mathbf{y}$ non è una parola di codice, si è verificato un errore *rivelabile*;
- Se $\mathbf{y}$ è una parola di codice ma non quella trasmessa, si è verificato un errore *non rivelabile* ($w(\mathbf{e}) \geq d_{min}$).

Capacità di rivelare errori (*error detection*)

Il codice $\mathcal{C}(k, n)$ rivela un errore quando la parola ricevuta $\mathbf{y} \notin \mathcal{C}(k, n)$.

Teorema 4: Il codice $\mathcal{C}(k, n)$ è in grado di rivelare con certezza fino a $d_{min} - 1$ errori.

- Se $d_H(\mathbf{x}, \mathbf{y}) < d_{min} \implies \mathbf{y}$ non può essere una parola di codice, perché altrimenti vorrebbe dire che esistono due parole di codice la cui distanza è minore di d_{min}.
- Viceversa, se $d_H(\mathbf{x}, \mathbf{y}) = d_{min} \implies$ esiste almeno una parola di codice $\mathbf{c} \in \mathcal{C}(k, n), \mathbf{c} \neq \mathbf{x}$ tale che $d_H(\mathbf{x}, \mathbf{c}) = d_{min}$ e se $\mathbf{y} = \mathbf{c}$, l'errore non può essere rivelato.

Strategia di decodifica a massima verosimiglianza

- Sia $\mathbf{y}$ il vettore ricevuto a seguito della trasmissione su BSC, la strategia di decodifica a massima verosimiglianza (ML,*maximum likelihood*) consiste nel trovare il vettore $\hat{\mathbf{x}}$ che, fra tutte le 2^k possibili parole di codice $\mathbf{x}$, massimizza la probabilità condizionata $P(\mathbf{y}|\mathbf{x})$, ie

$$\hat{\mathbf{x}} = \arg \max_{\mathbf{x} \in \mathcal{C}(k,n)} P(\mathbf{y}|\mathbf{x}) \tag{5}$$

- Poichè gli eventi di errore sono indipendenti da bit a bit, si può scrivere la probabilità condizionata come il prodotto delle probabilità condizionate ottenute per ciascun bit trasmesso

$$P(\mathbf{y}|\mathbf{x}) = \prod_{\ell=1}^{n} P(y_\ell|x_\ell) \tag{6}$$

Strategia di decodifica a massima verosimiglianza

- Poiché siamo in GF(2), la probabilità $P(y_\ell|x_\ell)$ può assumere due soli valori

$$P(y_\ell|x_\ell) = \begin{cases} 1-p & \text{if } P(y_\ell = x_\ell|x_\ell) \\ p & \text{if } P(y_\ell \neq x_\ell|x_\ell) \end{cases}. \tag{7}$$

- La distanza di Hamming $d_H(\mathbf{x}, \mathbf{y})$ misura il numero di posizioni diverse tra $\mathbf{x}$ e $\mathbf{y}$ e quindi $n - d_H(\mathbf{x}, \mathbf{y})$ misura il numero posizioni uguali tra $\mathbf{x}$ e $\mathbf{y}$.
- La probabilità $P(\mathbf{y}|\mathbf{x})$ si calcola

$$P(\mathbf{y}|\mathbf{x}) = p^{d_H(\mathbf{x},\mathbf{y})}(1-p)^{n-d_H(\mathbf{x},\mathbf{y})} = (1-p)^n \left(\frac{p}{1-p}\right)^{d_H(\mathbf{x},\mathbf{y})} \tag{8}$$

Decisione a massima verosimiglianza

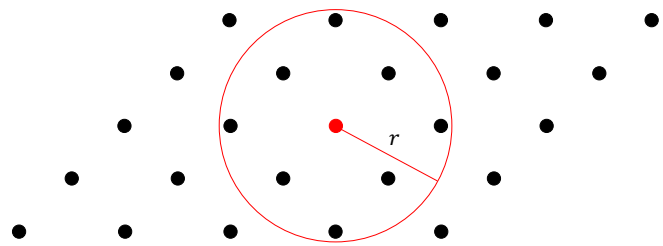
La parola di codice decisa $\hat{\mathbf{x}}$ è quella che che minimizza la distanza dalla parola $\mathbf{y}$ ricevuta

$$\hat{\mathbf{x}} = \arg \max_{\mathbf{x} \in \mathcal{C}(k,n)} P(\mathbf{y}|\mathbf{x}) = \arg \min_{\mathbf{x} \in \mathcal{C}(k,n)} d_H(\mathbf{y}, \mathbf{x}) \tag{9}$$

- Il ricevitore ML ottimo è il ricevitore a *distanza minima*: il ricevitore che associa alla sequenza di n bit ricevuta $\mathbf{y}$, la parola di codice $\mathbf{x}$ che minimizza la $d_H(\mathbf{x}, \mathbf{y})$.
- Il ricevitore ML è in grado di correggere *con successo* tutti quegli errori $\mathbf{e}$ per cui la parola ricevuta $\mathbf{y} = \mathbf{x} + \mathbf{e}$ è comunque più vicina alla parola trasmessa $\mathbf{x}$ che a qualsiasi altra parola del codice.

Decisione a massima verosimiglianza

- Per ogni vettore $\mathbf{v} \in \mathcal{V}_n$ e un raggio r esiste una 'sfera' di raggio r i cui elementi sono tutti quei vettori in $\mathcal{V}_n$ che hanno distanza di Hamming da $\mathbf{v}$ minore o uguale a r.

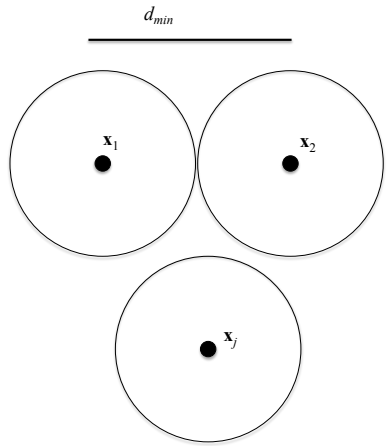


- Assumendo di adottare un ricevitore ML, il numero massimo t di errori che il codice $\mathcal{C}(k, n)$ è in grado di correggere è il massimo raggio t per cui le sfere centrate nelle parole di codice di $\mathcal{C}(k, n)$ sono tutte tra loro disgiunte.

Capacità di correggere errori (*error correction*)

Teorema 5: Un codice lineare a blocco può correggere fino a $t_{max} = \lfloor \frac{d_{min}-1}{2} \rfloor$ errori, i.e. $2t_{max} + 1 \leq d_{min} \leq 2t_{max} + 2$.

La condizione per cui le sfere di raggio t che circondano le parole di codice siano disgiunte è che
$2t_{max} < d_{min} \implies t_{max} < d_{min}/2$.
Altrimenti, se fosse $2t_{max} \geq d_{min}$ ci sarebbero almeno due parole $\mathbf{x}_1$ e $\mathbf{x}_2$ la cui distanza $d(\mathbf{x}_1, \mathbf{x}_2) = d_{min} \leq 2t_{max}$ e le due sfere di raggio t avrebbero almeno un punto in comune.



Capacità di correggere errori (*error correction*)

Consideriamo il codice $\mathcal{C}(k, n)$ che ha una certa d_{min} e t_{max} tale che $2t_{max} + 1 \leq d_{min}$. Sia $\mathbf{x} \in \mathcal{C}(k, n)$ la parola trasmessa, $\mathbf{y} = \mathbf{x} + \mathbf{e}$ la corrispondente sequenza di n bit ricevuta e $\mathbf{c} \in \mathcal{C}(k, n)$ un'altra generica parola di codice.
Grazie alla disuguaglianza triangolare si ha

$$d_H(\mathbf{x}, \mathbf{y}) + d_H(\mathbf{c}, \mathbf{y}) \geq d_H(\mathbf{x}, \mathbf{c}) \implies d_H(\mathbf{c}, \mathbf{y}) \geq d_H(\mathbf{x}, \mathbf{c}) - d_H(\mathbf{x}, \mathbf{y}) \tag{10}$$

Per ipotesi si ha anche

$$d_H(\mathbf{x}, \mathbf{c}) \geq d_{min} \geq 2t_{max} + 1 \tag{11}$$

Supponiamo che il canale introduca un certo numero di errori $t \leq t_{max}$, così da avere $d_H(\mathbf{x}, \mathbf{y}) = t$.

$$d_H(\mathbf{c}, \mathbf{y}) \geq 2t_{max} + 1 - t > t_{max} \geq t = d_H(\mathbf{x}, \mathbf{y}) \tag{12}$$

I codici di Hamming: definizione e proprietà

- I codici di Hamming sono definiti a partire a da un parametro $m \geq 2$

$$n = 2^m - 1, k = 2^m - m - 1 \tag{13}$$

- Poiché la matrice di controllo di parità $\mathbf{H}$ ha dimensione $(n-k) \times n$, per i codici di Hamming la matrice $\mathbf{H}$ ha dimensione $m \times (2^m - 1)$.
- Per un codice di Hamming sistematico, la matrice di parità $\mathbf{P}$ viene costruita così che le colonne di $\mathbf{H} = [\mathbf{P}^T, \mathbf{I}_{n-k}]$ siano tutte le possibili $2^m - 1$ combinazioni (escluso l'n-upla di tutti 0) di m bit.
- La distanza minima di un qualsiasi codice di Hamming $\mathcal{C}_H(m)$ è $d_{min}(\mathcal{C}_H(m)) = 3$. Dimostrazione.

I codici di Hamming: il codice $\mathcal{C}_H(2)$

- il codice a ripetizione $R = 1/3$ è il codice di Hamming con $m = 2$ con $n = 2^2 - 1 = 3$, e $k = 2^2 - 2 - 1 = 1$.
- La matrice di controllo di parità per il codice a ripetizione con $R = 1/3$ è

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \tag{14}$$

- Poiché la matrice $\mathbf{H}$ ha 2 righe e 3 colonne e rappresenta tutte le possibili combinazioni di 2 bit (esclusa la n-upla di tutti 0) $\implies$ $\mathbf{H}$ è la matrice di controllo di parità per il codice di Hamming $\mathcal{C}_H(2)$.

I codici di Hamming: il codice $\mathcal{C}_H(3)$

- Se $m = 3 \implies n = 7, k = 4$. La matrice di controllo di parità **H** per $\mathcal{C}_H(3)$ ha 3 righe e 7 colonne. In forma sistematica una possibile coppia **H** e **G** è

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

- Si fanno controlli di parità su combinazioni diverse di bit di ingresso.

$$p_1 = u_1 + u_2 + u_4$$
$$p_2 = u_1 + u_3 + u_4$$
$$p_3 = u_2 + u_3 + u_4$$