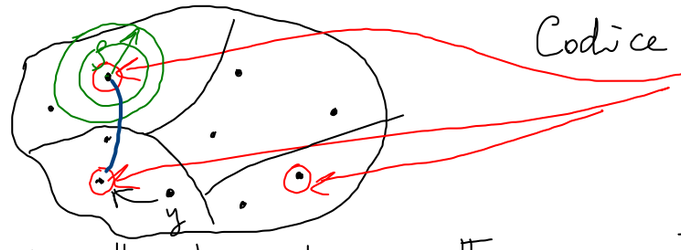
Spazio di Hamming



Codice $\mathcal{C} \subseteq \mathcal{A}^n$

$= \{x^{(1)}, x^{(2)}, \dots, x^{(T)}\}$

$|\mathcal{A}^n| = q^n$

$\mathcal{A}^n$ spazio vettoriale sul campo $\mathbb{F}_q$ $(GF(q))$

In generale, $\mathcal{A}^n \setminus \mathcal{C}$ non sarà vuoto

Sfera di Hamming: $S_\varrho(x)$

$\mathcal{A} = \{a_1, \dots, a_q\}$

$a \in \mathcal{A} = \mathbb{F}_q$

Metrica indotta dalla funzione distanza di Hamming:

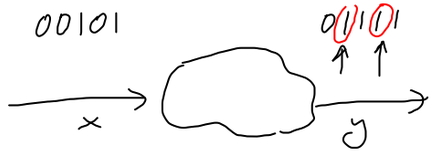
$d_H(x,y) = \#$ posizioni i tali che $x_i \neq y_i$

$d_H(x,z) \leq d_H(x,y) + d_H(y,z)$

$d_H(x,y) = d_H(y,x)$

$d_H(x,y) \geq 0$

$d_H(x,y) = 0 \iff x = y$



$e = y - x$

↑ parola di errore

$e = 01010$

Decodifica a massima verosimiglianza:

Data la y ricevuta, scegli la sequenza x che massimizza la prob. condizionata $p(y|x)$:

restituisci $\hat{x}_{MLE} = \underset{x^{(i)} \in \mathcal{C}}{\arg\max}\ p(y|x^{(i)})$

$p(y|\hat{x}) = \max_{i=1\dots T} p(y|x^{(i)})$

(Ipotesi : il canale è il canale binario simmetrico $BSC(\varepsilon)$, con $0 \le \varepsilon < 1/2$)

Prop. La decodifica a massima verosimiglianza equivale alla decodifica a distanza minima : dato y, scegli x che minimizza $d_H(x,y)$:

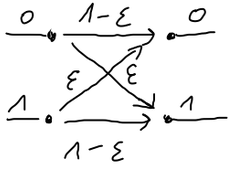
restituisci $\hat{x}_{dmin} = \underset{x^{(i)} \in \mathcal{C}}{\operatorname{argmin}} \; d_H(x^{(i)}, y)$.

Dim. Sia $e = y - x$ la configurazione di errore. ($\to y = x + e$)

Allora $p(y|x) = p(x+e|x) = p(e|x)$

$= p(e)$

$= \varepsilon^{wt(e)} (1-\varepsilon)^{n - wt(e)}$

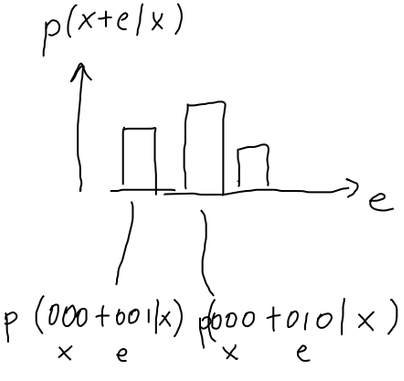


$p(e=0) = 1-\varepsilon$

$p(e=1) = \varepsilon$

$p(\text{conf. errore} = \underbrace{000\ldots0}_{n}) = (1-\varepsilon)^n$

$p(\text{conf. errore} = 111\ldots1) = \varepsilon^n$



dove $wt(e)$ è il numero di posizioni di e diverse da 0

$$p(y|x) = \varepsilon^{wt(e)} (1-\varepsilon)^{n-wt(e)}$$

$y - x = e$

$$= (1-\varepsilon)^n \varepsilon^{wt(e)} (1-\varepsilon)^{-wt(e)}$$

$x = y - e$

$$= \underbrace{(1-\varepsilon)^n}_{\text{non dipende dalla conf. di errore } e} \left(\frac{\varepsilon}{1-\varepsilon}\right)^{wt(e)}$$

Poiché $\varepsilon < 1/2$, ho $1-\varepsilon > 1/2$ e quindi $\frac{\varepsilon}{1-\varepsilon} < \frac{1/2}{1/2} = 1$.

Per massimizzare $p(y|x)$, devo minimizzare $wt(e)$.

Ma $wt(e) = wt(y-x) = d_H(x,y)$; quindi massimizzare $p(y|x)$ rispetto a x equivale a minimizzare $d_H(x,y)$ rispetto a x.

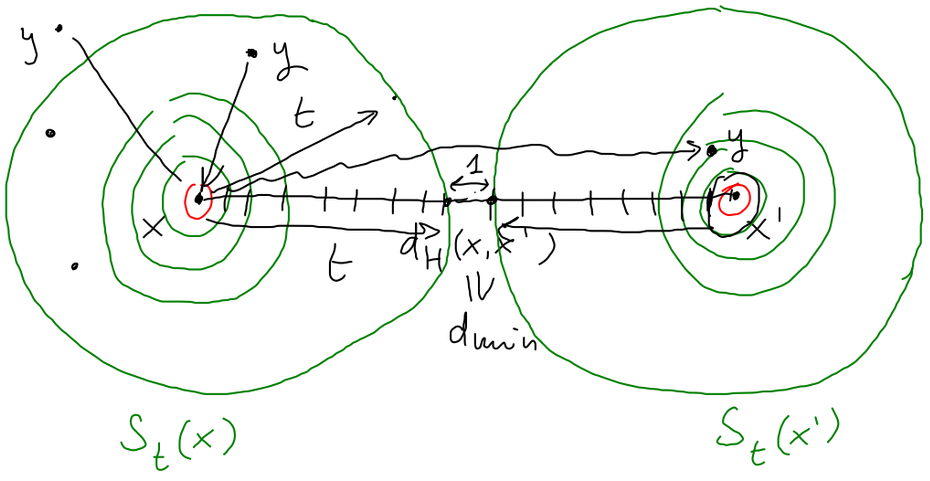
QED.

Def. Dato un codice C, si chiama distanza minima del codice la quantità

$$d_{min} \triangleq \min_{x,x' \in C,\, x \neq x'} d_H(x,x').$$

Sicuramente, per definizione, date 2 parole di codice $x, x' \in \mathcal{C}$,

$d_H(x, x') \geq d_{min}$



Quanto grande posso prendere $t \in \mathbb{N}$ tale che $S_t(x) \cap S_t(x') = \emptyset$?

Se $2t + 1 \leq d_{min}$, allora sicuramente

$S_t(x) \cap S_t(x') = \emptyset$

Il vincolo è soddisfatto se

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

Quindi un codice può correggere fino a $\left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$ errori (in qualsiasi configurazione)

e può rilevare fino a $d_{min} - 1$ errori (in qualsiasi configurazione)

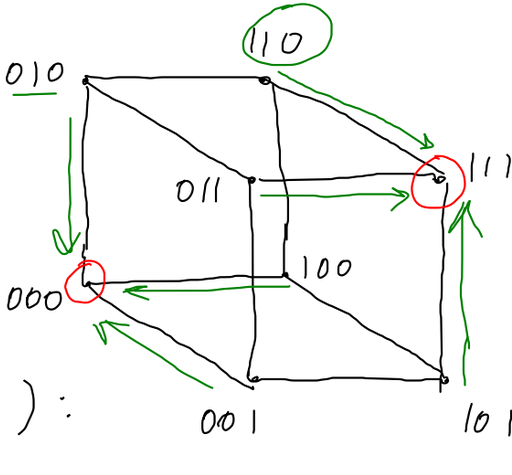
Capacità di correzione del codice : $\lambda = \frac{d_{min}}{n} \in [0,1]$

Esempio. Codice a ripetizione binario con $n = 3$.

$A = \{0,1\}$, $A^n = \{000, 001, 010, \dots, 110, 111\}$

$C = \{000, 111\}$ $\quad d_{min} = 3 \rightarrow \lambda = \frac{3}{3} = 1$

messaggio: 0 ↑ 1 ↑



Numero di errori che posso correggere (in qualunque config. di errore):

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

Numero di errori che posso rilevare (" " " ")

$d_{min} - 1 = 2$.

Quali sono le prob. di errore nel canale $BSC(\varepsilon)$ quando $\varepsilon = 0.1$?

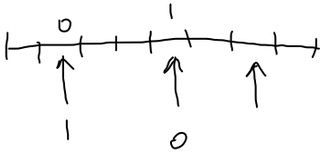
	e	$p(e)$		
$d_H(x,y)=0$	000	$(1-\varepsilon)^3$	0.729	prob. di corretta decodifica 0.972
$d_H(x,y)=1$	001	$(1-\varepsilon)^2\varepsilon$	0.081	
	010	$(1-\varepsilon)\varepsilon(1-\varepsilon)$	0.081	
	100	$\varepsilon(1-\varepsilon)^2$	0.081	
		$3\varepsilon(1-\varepsilon)^2$		
$d_H(x,y)=2$	110	$(1-\varepsilon)\varepsilon^2$	0.009	prob. di errore in decodifica $P_e = 0.028$
	101		0.009	
	011		0.009	
		$3\varepsilon^2(1-\varepsilon)$		
$d_H(x,y)=3$	111	ε^3	0.001	

In generale, per un codice a ripetizione,

$$P_e = Pr[wt(e) \geq t+1] = \sum_{i=t+1}^{n} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i}$$

$p(e)$ quando e ha peso $wt(e) = i$

$\binom{n}{i}$ → # di config. di errore di peso i



(binario)

In un codice a ripetizione $\mathcal{V}$ di lunghezza n, $d_{min} = n$

(solo 2 parole di codice : $\underbrace{000\ldots0}_{n}$, $\underbrace{111\ldots1}_{n}$) $\Rightarrow \lambda = \frac{n}{n} = 1$.

$0 \leftrightarrow k$ $\quad$ $1 \leftrightarrow k$

Tasso del codice $R = \frac{k}{n} = \frac{1}{n}$.