- Codifica di sorgente
  - Possibilità teoriche
  - Costruzioni di codici di sorgente
- Codifica di canale
  - Possibilità teoriche
  - Costruzioni di codici di canale

$p(x/y)$

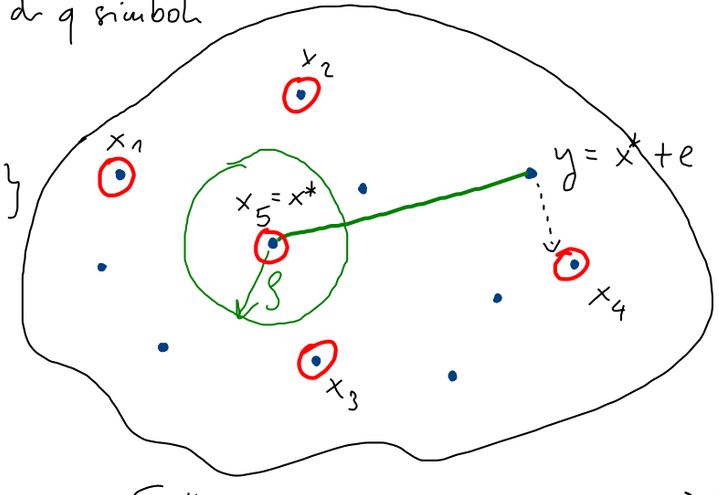
Lunghezza $n$
Alfabeto di $q$ simboli

$A^n$

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

$\vec{q}^{\,n}$

$|\vec{q}^{\,n}| = q^n$



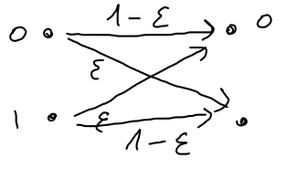

- Tutte le $n$-ple su $q$ simboli : $\vec{q}^{\,n}$
- Parole di codice : $\mathcal{C} \subseteq \vec{q}^{\,n}$

Distanza di Hamming $d_H(x, y)$

Sfera di Hamming $S_\varrho(x)$

$p(y/x)$

Canale binario simmetrico $BSC(\varepsilon)$




Criterio di massima verosimiglianza

($x^*$ trasmessa)
$y$ ricevuta $\longmapsto$ $\hat{x}$ ricostruzione (stima) di $x^*$

Scelgo $\hat{x} = x$ se $p(y|x) = \max_{1 \le i \le M} p(y|x_i)$

(Nel canale $BSC(\varepsilon)$, con $\varepsilon < 1/2$)

**Prop.** La decodifica secondo il criterio di massima verosimiglianza corrisponde alla decodifica a distanza minima

(→ fra tutte le $x_i$, scegli quella a distanza di Hamming minima da $y$).

**Dim.**

Scelgo $\hat{x} = x$ se $p(y|x) = \max_{1 \le i \le M} p(y|x_i)$

Ma (configurazione di errore (dipende da ciò che succede sul canale))

$$p(y|x) = p(x+e \mid x) = p(e|x) = p(e) =$$

(la config. di errore e non dipende da $x$)

$$\rightarrow p(e) = \varepsilon^{\overbrace{wt(e)}^{\#\text{ di '1' in } e}} (1-\varepsilon)^{\overbrace{n-wt(e)}^{\#\text{ di '0' in } e}} = \varepsilon^{d_H(x,y)} (1-\varepsilon)^{n-d_H(x,y)}$$

$y = x + e$

$\Rightarrow e = y - x$

| | |
|---|---|
| $x$ | 0010 |
| $y$ | 1011 |
| $e$ | 1001 |

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

$= \varepsilon^2 (1-\varepsilon)^2$

$\left( wt(e) = d_H(e, \underbrace{00\ldots0}_{n \text{ zeri}}) = d_H(y-x, 00\ldots0) = d_H(y, x) \right)$

$$p(y|x) = p(e) = \varepsilon^{d_H(x,y)} (1-\varepsilon)^{n-d_H(x,y)} = \varepsilon^{d_H(x,y)} \underbrace{(1-\varepsilon)^{-d_H(x,y)}}_{1/(1-\varepsilon)^{d_H(x,y)}} \cdot (1-\varepsilon)^n$$

$$= \underbrace{\left(\frac{\varepsilon}{1-\varepsilon}\right)^{d_H(x,y)}}_{\text{Voglio massimizzare questo termine}} \cdot \underbrace{(1-\varepsilon)^n}_{\text{Non dipende da } x}$$

Poiché $\varepsilon < 1/2$, $\frac{\varepsilon}{1-\varepsilon} < 1$

$\Leftrightarrow$ $\varepsilon < 1-\varepsilon$

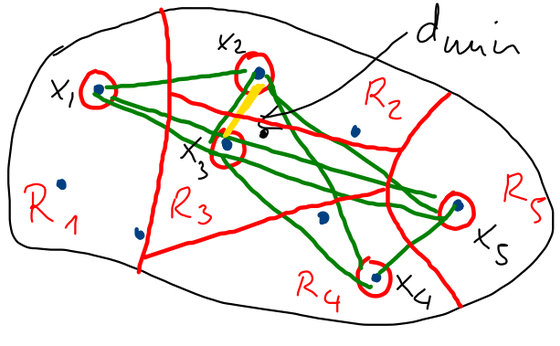
$\Leftrightarrow$ $2\varepsilon < 1$

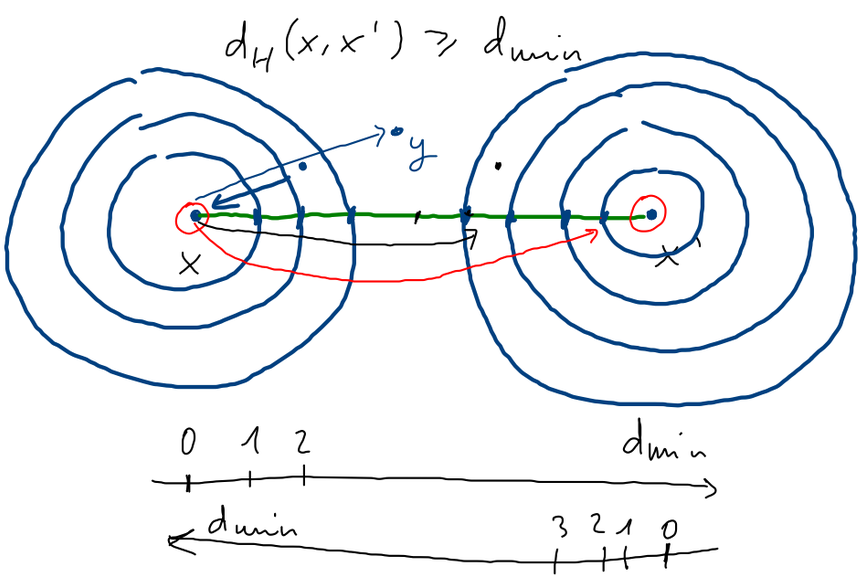
$\Leftrightarrow$ $\varepsilon < 1/2$

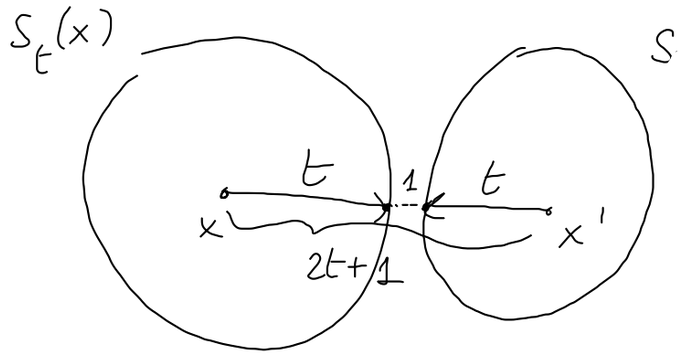
$\Rightarrow$ Voglio minimizzare $d_H(x,y)$ $\Rightarrow$ decodifica a distanza minima. QED

Def. Per un codice $\mathcal{C}$, la distanza minima del codice è:

$$d_{min} \triangleq \min_{\substack{x,y \in \mathcal{C} \\ x \neq y}} d_H(x,y)$$






$\lfloor x \rfloor \leq x$

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

Se $d_H(x,y) > \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ allora potrei decodificare non correttamente

Se $d_H(x,y) \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$, decodifico correttamente

$\Rightarrow$ Le sfere di Hamming di raggio $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ sono tutte disgiunte

$\Rightarrow$ Riusciamo a correggere fino a $t$ errori sul canale (in qualunque configurazione)
Riusciamo a rilevare fino a $d_{min}-1$ errori sul canale (in qualunque configurazione)

La Capacità di correzione del codice è : $\lambda \triangleq \frac{d_{min}}{n}$ $\quad (0 \le \lambda \le 1)$

Esempio: Codice a ripetizione con $n=3$, binario $(q=2)$ ; BSC($\varepsilon$) con $\varepsilon = 0.1$

$\mathcal{C} = \{000, 111\}$

$\mathcal{C} = \{\underbrace{000\ldots0}_{n}, \underbrace{11\ldots1}_{n}\}$

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

$0 \rightarrow 000$
$1 \rightarrow 111$

$R_{000} = \{000, 001, 010, 100\}$
$R_{111} = \{111, 110, 101, 011\}$

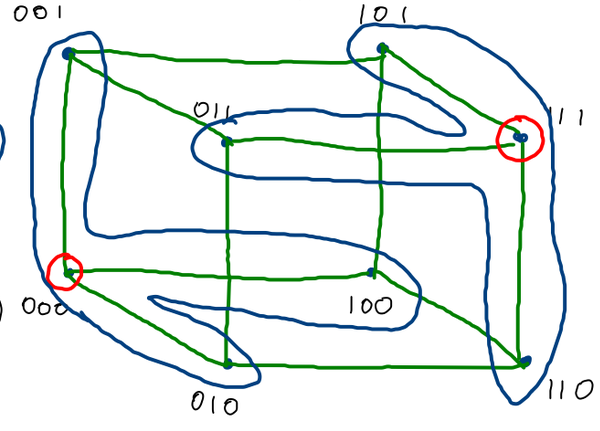
$\{00000, 11111\}$

$M = |\mathcal{C}| = 2$
$q = 2, n$

$R_{000} = S_1(000)$

$S_1(111) = R_{111}$

$n = 5$
$d_{min} = 5$
$\Rightarrow t = \left\lfloor \frac{5-1}{2} \right\rfloor = 2$




In generale per un codice a ripetizione

$$P_e = P_r[wt(e) \ge t+1] = \sum_{i=t+1}^{2t+1} \binom{n}{i} \varepsilon^i (1-\varepsilon)^{n-i}$$

Tasso $R = \frac{\log_q M}{n} = \frac{1}{n}$ ; Capacità di correzione $\lambda = {}^{n}/_{n} = 1$

Quali sono le prob. di errore nel BSC($\varepsilon$), con $\varepsilon = 0.1$

| | e | wt(e) | $P_e(x)$ | $P_e(x)$ con $\varepsilon = 0.1$ | |
|---|---|---|---|---|---|
| $\binom{n}{0} = 1$ | 000 | 0 | $(1-\varepsilon)^3$ | 0.729 | $P_{correttо} = 0.972$ |
| $\binom{n}{1}$ ✓ | 001 | 1 | $\varepsilon(1-\varepsilon)^2$ | 0.081 | |
| | 010 | | $\varepsilon(1-\varepsilon)^2$ | 0.081 | |
| | 100 | | $\varepsilon(1-\varepsilon)^2$ | 0.081 | |
| $\binom{n}{2}$ ✗ | 011 | 2 | $\varepsilon^2(1-\varepsilon)$ | 0.009 | $P_e = 0.028$ |
| | 101 | | $\varepsilon^2(1-\varepsilon)$ | 0.009 | |
| | 110 | | $\varepsilon^2(1-\varepsilon)$ | 0.009 | |
| $\binom{n}{3}$ | 111 | 3 | $\varepsilon^3$ | 0.001 | |