



Teoria dell'Informazione e Applicazioni – a.a. 2014-2015

Esercizi su **Codifica** dei segnali (a ripetizione e a controllo di parità)

23-10-2014
Ing. P. Fazio

CODICI A BLOCCO (RIPETIZIONE)

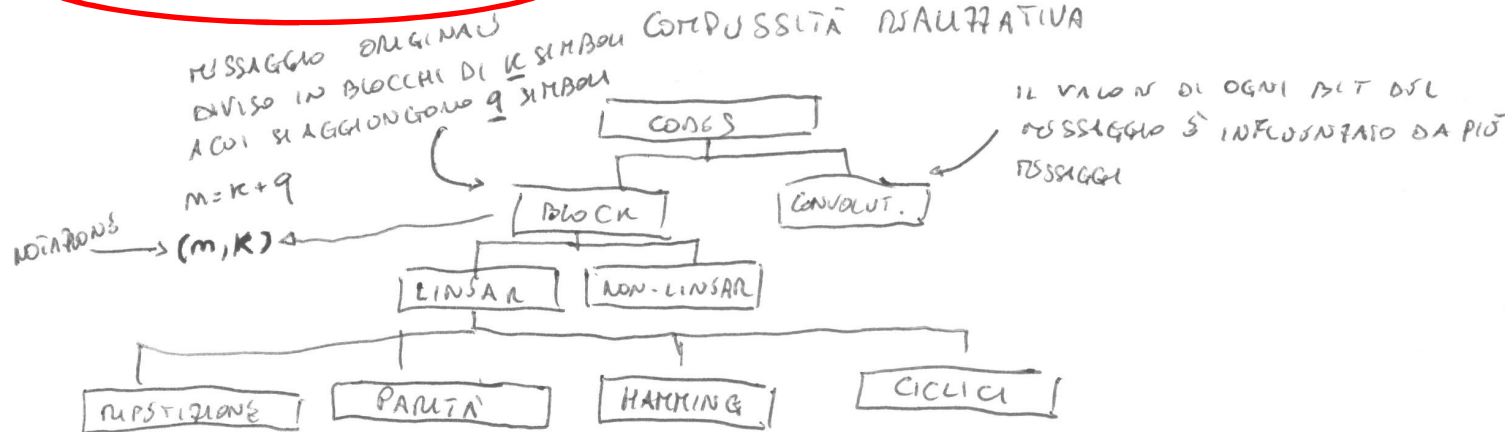
①

- PROBABILITÀ DI ERRORI SUL CANALE DI TRASMISSIONE;
- IN COSA CONSISTE LA CODIFICA;
- RIVELAZIONI E CORREZIONI;
- VANTAGGI E SVANTAGGI;
- RIDUZIONE P_e PER 1 BIT D'INFORMAZIONE (ESempi CONCRETI)
- AUTOMATIC REPEAT AND REQUEST (RITRASMISSIONI E CANALI DI FEEDBACK)
- FORWARD ERROR CORRECTION (RIVELAZIONI/CORREZIONI, UTILE QUANDO NON SI PUÒ RITR.)

② CAPACITÀ DI RIVELAZIONI

③ " DI CORREZIONE

PARAMETRI PER VALUTARE LE PRESTAZIONI DI UN CODICE, ASSIEME ALL'EFFICIENZA ($R_e = k/n$) E ALLA COMPLESSITÀ REALIZZATIVA



A) Codice a ripetizione: Dato un bit di informazioni, essi ripetono m volte il bit, sono quindi a blocchi $(m, 1)$ quindi, cioè $k=1$ $q=m-1$ //

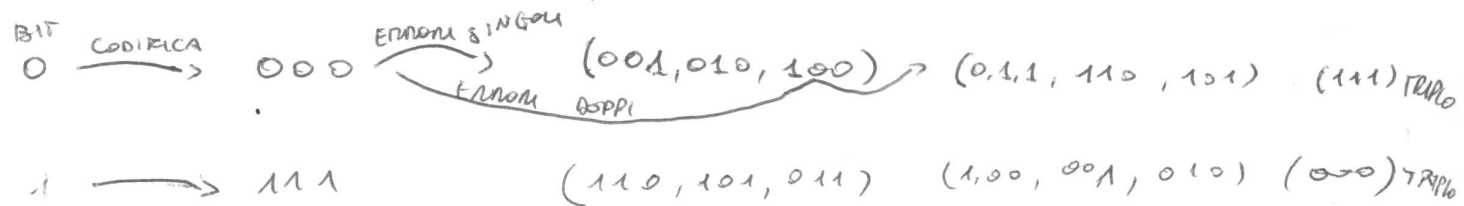
$$P_e(i, m) = \binom{m}{i} \alpha^i (1-\alpha)^{m-i} \approx \binom{m}{i} \alpha^i$$

m : lunghezza parola di codice
 i : num. di errori

α : Prob. canale e indipendente

SE $\alpha \ll 1$ LA CODIFICA A RIPETIZIONE È EFFICIENTE CON $P_e(i+1, m) < P_e(i, m)$

ES.: $R(3, 1) \Rightarrow m=3$ $k=1$ $q=2 = m-k$



L'ERRORE TRIPLO NON PUÒ ESSERE RIVELATO (PORTA AD UN CAMBIAMENTO DI PAROLA)

POICHÉ ERRORE TRIPLO NON POSSONO ESSERE RIVELATI, AVREMO CHE LA ⁽²⁾ PROBABILITÀ DI NON RIVELARE ERRORE IN UNA PAROLA DI CODICE INCERTA È:

$$P(3, 3) = \binom{3}{3} \alpha^3 = \alpha^3 \equiv P(3, 3) = \binom{3}{3} \alpha^3 (1-\alpha)^0 = \alpha^3$$

(CODI PERFETTA)

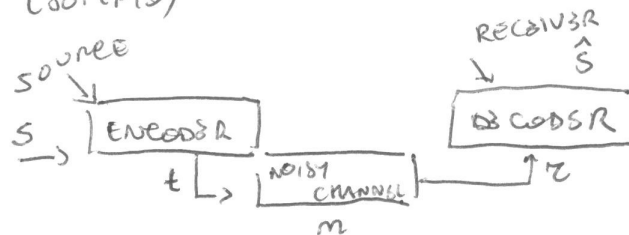
PER RISPONDERE ALL'ERRORE SI USA LA DECISIONE DI MAGGIORANZA: QUANDO UNA PAROLA NON APPARTIENE AL CODICE, LA SI TRASFORMA NELLA PAROLA DI CODICE AD ESSA PIÙ VICINA, ASSUMENDO CHE ALMENO $\frac{m+1}{2}$ BIT SIANO CORRETTI.

$$m - \frac{m+1}{2} = \frac{m-1}{2}$$

PER IL CODICE $R(3,1)$ LA PROBABILITÀ DI SPAGLIARE LA CORRUZIONE δ :

$$\begin{cases} P_e(2,3) + P_e(3,3) = \binom{3}{2} \alpha^2 + \binom{3}{3} \alpha^3 = \frac{3!}{2!1!} \alpha^2 + \alpha^3 = 3\alpha^2 + \alpha^3 \\ P_e(2,3) + P_e(3,3) = \binom{3}{2} \alpha^2 (1-\alpha) + \binom{3}{3} \alpha^3 (1-\alpha)^0 = 3\alpha^2 - 3\alpha^3 + \alpha^3 = 3\alpha^2 - 2\alpha^3 \end{cases}$$

ESEMPLO)



$$S = 0010110 \quad \alpha = 0.1$$

$$t = 00000111001111000$$

$$m = 0000010000010100000$$

$$r = 0000011110001011100$$

$$\hat{S} = 0010110$$

(PICCOLA PROBABILITÀ DI ERRORI DI CORRUZIONE (CON CODIFICA PIÙ ROBUSTA)
SI SPAGLIA DI MENO

$$R_3 = P_e(2,3) + P_e(3,3) = 3\alpha^2 - 2\alpha^3$$

$$\text{LOWER BOUND } \frac{n+1}{2} = \frac{3+1}{2} = 2 \text{ bit diversi per lettera}$$

$$R_5 \text{ lower bound } \frac{n+1}{2} = \frac{6}{2} = 3 \Rightarrow P_e(3,5) + P_e(4,5) + P_e(5,5) =$$

$$\begin{aligned} &= \binom{5}{3} \alpha^3 (1-\alpha)^2 + \binom{5}{4} \alpha^4 (1-\alpha) + \binom{5}{5} \alpha^5 = \frac{5!}{3!2!} \alpha^3 (1-\alpha)^2 + \frac{5!}{4!1!} \alpha^4 (1-\alpha) + \alpha^5 \\ &= \frac{5 \cdot 4 \cdot 3!}{3! \cdot 2} \alpha^3 (1-\alpha)^2 + \frac{5 \cdot 4!}{4!} \alpha^4 (1-\alpha) + \alpha^5 = 10\alpha^3 (1-\alpha)^2 + 5\alpha^4 (1-\alpha) + \alpha^5 \\ &= 10\alpha^3 (1-2\alpha + \alpha^2) + 5\alpha^4 - 5\alpha^5 + \alpha^5 = \underline{10\alpha^3} - \underline{20\alpha^4} + \underline{10\alpha^5} + \underline{5\alpha^4} - \underline{4\alpha^5} = \\ &= 6\alpha^3 - 15\alpha^4 + \underline{10\alpha^3} \text{ leading order!} \end{aligned}$$

$$R_7 \text{ lower bound } \frac{n+1}{2} = \frac{8}{2} = 4 \quad P_e(4,7) + P_e(5,7) + P_e(6,7) + P_e(7,7) =$$

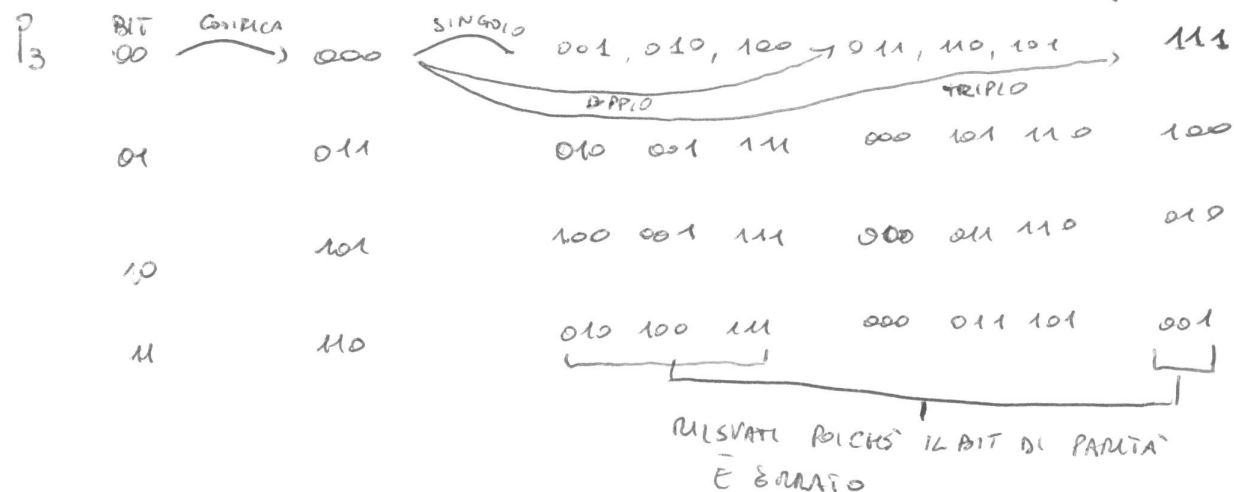
GENERALIZZANDO:

$$R_m \Rightarrow \text{Purpure-Longine} = \left(\frac{m}{m+1}\right) d^{\frac{m+1}{2}} (1-d)^{m-\frac{m+1}{2}} = \left(\frac{m}{m+1}\right) d^{\frac{m+1}{2}} (1-d)^{\frac{2m-m+1}{2}}$$

(3)

B) COME A CONTROLLO DI PARITÀ: SONO COME $(m, m-1)$ $K=m-1$ $q=1$

PERO' OGNI $m-1$ BIT DI INFORMAZIONI, SI AGGIUNGE UN BIT DI CONTROLLO, CHE VALS 0
SE CONTIENE UN NUMERO PAR (EVEN), 0 1 SE UN NUMERO DISPARI DI 1 (ODD)



NON SE RISULTA L'ERRORE, QUINDI, QUANDO I BIT E RAPPRESENTAZIONE SONO PAR:

$$P(\text{pari}) = \sum_{i=\text{pari}}^m P(i, m) \approx P(2, m) = \binom{m}{2} d^2 (1-d)^{m-2} \approx \frac{m(m-1)}{2} d^2$$

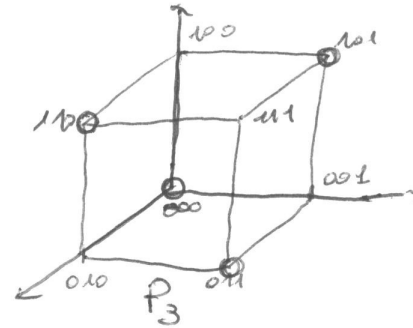
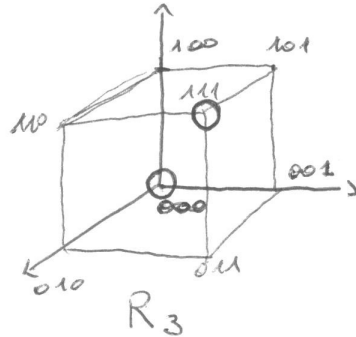
L'APPROSSIMAZIONE È VALIDA PER $d \ll 1$

I COME A CONTROLLO PARITÀ NON POSSONO CORRISPONDERE ERRORI!

ESSEMPIO)

$$m=10 \quad K=9 \quad q=1 \quad d=10^{-3} \\ P(\text{pari}) \approx \frac{m(m-1)}{2} d^2 = \frac{10 \cdot 9}{2} d^2 = 45 d^2 = 45 \cdot 10^{-6}$$

CONFRONTO NELLO SPAZIO DEI CODICI



SAPREMO CHE IN IL CASO DI R_3 LE PAROLE COMPLETATE SONO PIÙ DISTANTI, QUINDI SI POSSONO RILEVARE PIÙ ERRORI

IL CONCETTO DI SEPARAZIONE TRA PAROLE DI CODICI È BASATO SU: ④

- DISTANZA DI HAMMING $d(x, y)$ TRA DUE PAROLE DI CODICI

- DISTANZA MINIMA d_{\min}

CAPACITÀ RILEVATIVA

1) SE IL NUMERO DI ERRORI $\bar{e} < d_{\min}$ LA PAROLA USCITA NON È PRESENTA NELLE CODICI, QUINDI SI RILEVA L'ERRORI

$$\bar{e} \leq d_{\min} - 1$$

2) SE IL NUMERO DI ERRORI $\bar{e} \geq d_{\min}$ LA PAROLA USCITA POTREBBE APPARTENERE AL CODICI, QUINDI NON SI PUÒ RILEVARE

CAPACITÀ CORRETTIVA (t_{\max})

$$t \leq \frac{d_{\min} - 1}{2}$$

ESSEMIO :

R_3 (3,1) $X_1 = 000$ $X_2 = 111$ $d(X_1, X_2) = 3 = d_{\min}$

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

$$t_{\max} = 1$$

P_3 (3,2) $X_1 = 000$ $X_2 = 011$ $X_3 = 101$ $X_4 = 110$

$$d(X_i, X_j) = 2 \quad \forall i, j = 1, \dots, 4 \quad i \neq j \Rightarrow d_{\min} = 2$$

$$d_{\max} = 1$$

$$t_{\max} = 1/2 \Rightarrow \text{NO CONNECTION!}$$

ES. PER CASA:

$\alpha = 0,1$ $P_e \leq 10^{-15}$, QUANTE RIPETIZIONI SONO NCESSARIE?

5

- $S \rightarrow [R_m] \xrightarrow{\text{out}_1} [R_m] \xrightarrow{\text{out}_2} \text{CHANNELS} \rightarrow [DSC_{IN}] \rightarrow [DSC_{OUT}] \rightarrow S$
- \uparrow
OUTER
- \uparrow
INNER

$$\alpha = 0,1$$

$$P_2^1(3,5) = \binom{5}{3} \alpha^3 = \frac{5!}{3!2!} \alpha^3 = \frac{5 \cdot 4 \cdot 3!}{3! \cdot 2} \alpha^3 = 10 \alpha^3 = 10 \cdot (0,001) = 0,01 = 10^{-2}$$

COMPARISON

$$P_e(13, 25) = \binom{25}{13} \alpha^{13} = \frac{25!}{13! 12!} = \boxed{5,2 \cdot 10^{-7}}$$

поиск по формуле

VALORI R_2 CON R_3^2 O R_9 , EFFETTUARE IL CONFRONTO