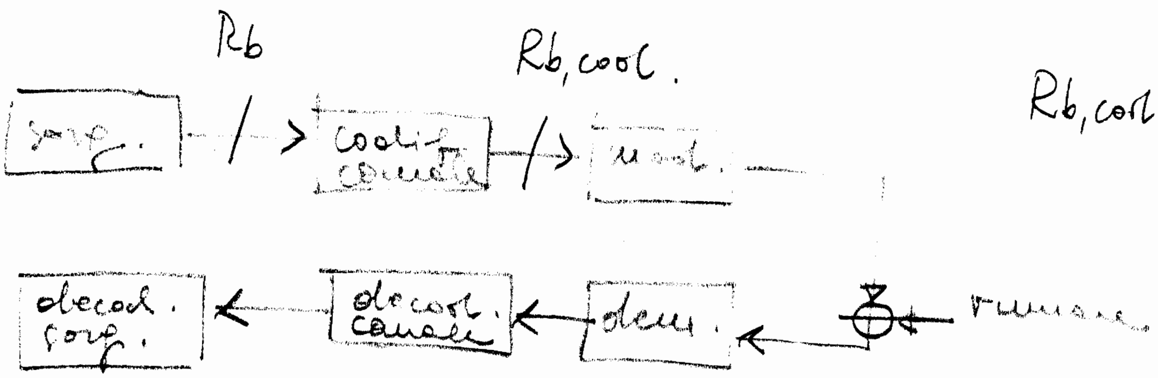
CODIFICA DI CANALE (NOTE)

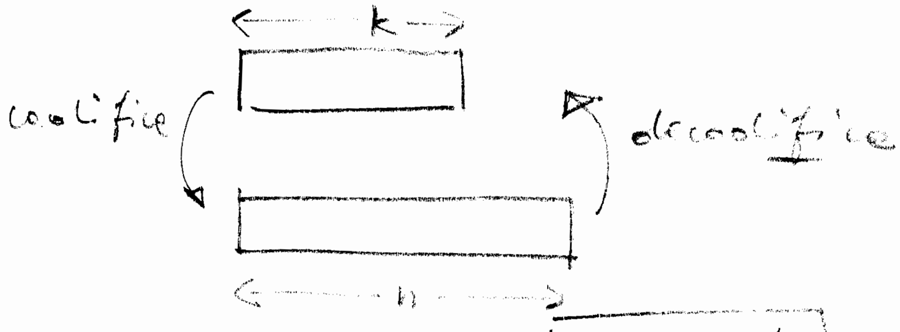


$R_{b,cod} > R_b$

<u>modulazione</u>: mapping simboli/forme d'onda

<u>codif. canale</u>: mapping sequenze binarie con $R_{b,cod} > R_b$.

Codifica binaria a blocco (codici a blocco).



Rate del codice $\boxed{R = k/n} \le 1$

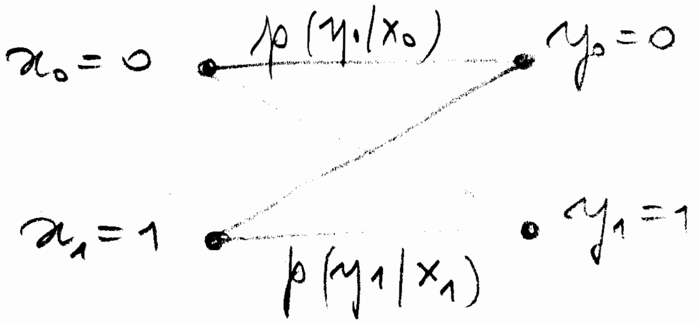
k bit $\rightarrow$ 2^k stati possibili (config. msg inform.)

n bit $\rightarrow$ 2^n stati possibili (config. parole codif.)

$\rightarrow$ tuttavia solo 2^k stati dei complessivi 2^n sono ammissibili, i rimanenti sono possibili ma identificano condizioni di errore.

$$R_{b,cod} = R_b / R$$

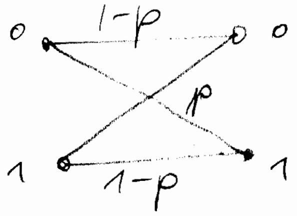
Rappresentazione canale binario :



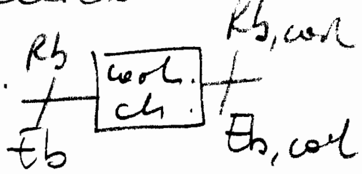
prob. errore:

$p(E) = p(y_0|x_1)\,p(x_1) + p(y_1|x_0)\,p(x_0)$.

<u>BSC</u> : $p(y_0|x_1) = p(y_1|x_0) = p$



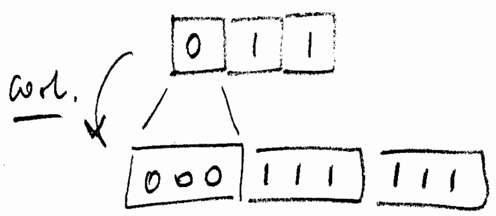
Nota che il dimensionamento e valutazione delle codifiche di canale segue i criteri validi per il sistema in assenza di codifica definendo le quantità $E_{b,cod}$ e $R_{b,cod}$.



<u>Codice a ripetizione</u> $R = 1/n$

$n = 2m+1$ (dispari)

$R = 1/3$



R_b

$R_{b,cod} = 3R_b$

Condizioni di errore

×			1 errore (può essere corretto) $p(1-p)^2$
	×		
		×	
×	×		2 errori (corretto uno con errore) $p^2(1-p)$
×		×	
	×	×	
×	×	×	3 errori (p^3

condizioni di errore (non può essere corretto!)

<u>Generale</u>: codice ripetizione corregge m errori su $2m+1$.

Calcolo prob. di errore
(decodifica hard o decodifica bit-a-bit)

$p(i,n) \triangleq$ prob. di avere i-errori in una parola di codice di lungh. n

$$p(i,n) = \underbrace{\binom{n}{i}}_{\text{n. di combinazioni distinte di i-errori su n posizioni possibili}} \times p^i \times (1-p)^{n-i}$$

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$$

per un codice a ripetizione la condiz. di errore si ha quando $i \geq m+1$ da cui si ha:

$$p_b(E) = \sum_{i=m+1}^{n} p(i,n) = \sum_{i=m+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}$$

$$\simeq \sum_{i=m+1}^{n} \binom{n}{i} p^i \simeq \binom{n}{m+1} p^{m+1}$$

$(p \ll 1)$

$p(i+1,n) \ll p(i,n)$
(errori multipli hanno minore prob.).

R	1	1/3	1/5	1/7	… $R \to 0$
$P_b(E)$	10^{-2}	3×10^{-4}	10^{-6}	4×10^{-7}	$P_b(E) \to 0$.

quindi riducendo il rate (R) la $P_b(E) \to 0$!

<u>Codice a parità</u> (codice blocco $(3,2) = (n=3, k=2)$)

info		parità
0	0	0
0	1	1
1	0	1
1	1	0

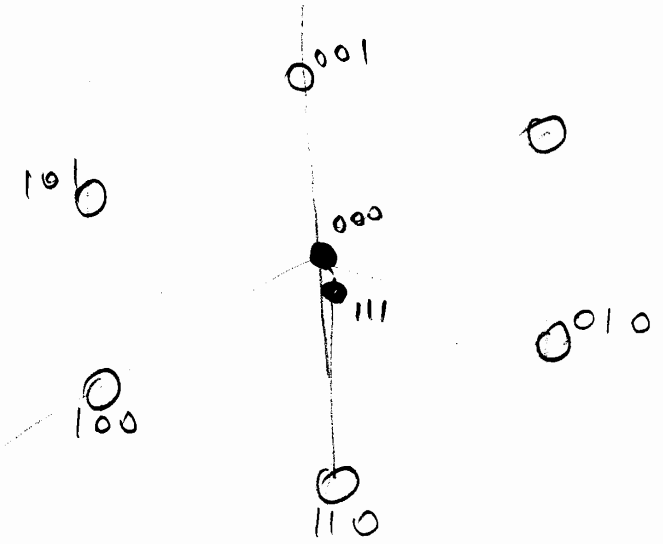
parole codice 3 bit

→ 4 parole codice (consecutive)

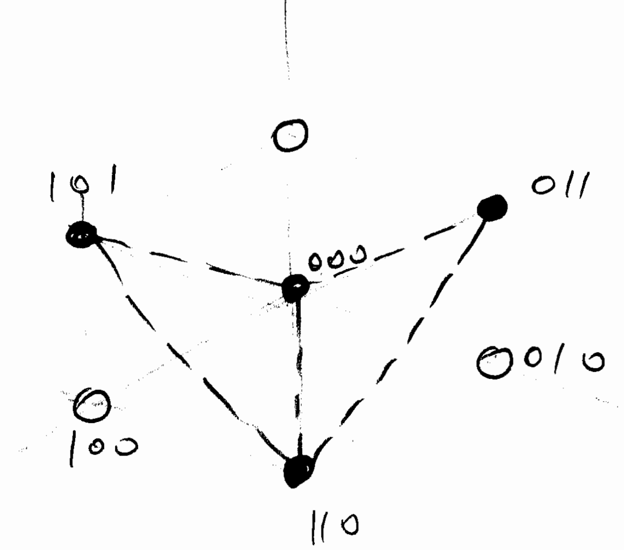
→ Δ. 4 parole codice (indice di errore)

<u>Rappresentazione geometrica</u> (spazio $n=3$)

Codice ripetizione (3,1)



Codice parità (3,2)



$d_H(000, 111) = 3$

$d_H(101, 110) = \cdots = 2$

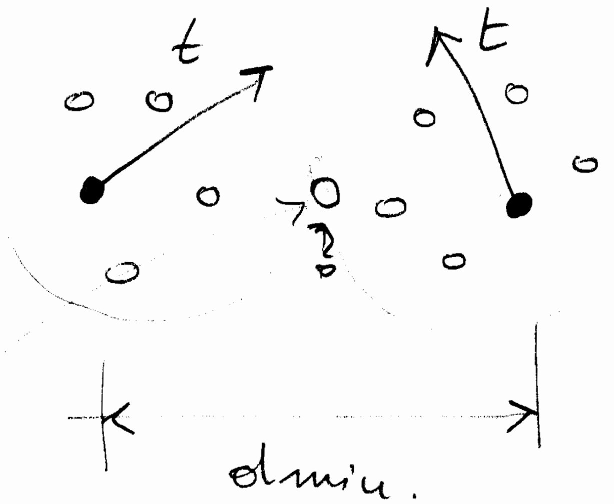
$d_H(c_i, c_j)$ distanza di Hamming è pari al numero di valori differenti tra le due parole di codice c_i e c_j

$d_{min} = \min_{c_i \neq c_j} d(c_i, c_j)$: <u>min. distanza</u>

Errori rilevabili / correggibili

Se un codice ha distanza minima dmin allora:

- Se il numero di errori $\boxed{l \leq d_{min} - 1}$ allora è possibile rilevare l'inammissibilità di una parola di codice con errori.

- 

k bit

2^k parole ammissibili

$2^n >> 2^k$

dmin − 1 per evitare che un punto possa essere ambiguo

$$\boxed{t \leq \frac{d_{min} - 1}{2}}$$ se dmin è dispari

$$\boxed{t \leq \frac{d_{min}}{2} - 1}$$ se dmin è pari

n. errori che possono essere corretti dal codice (pari a metà di quelli rilevabili)

EX

$d_{min} = 3$

$l \leq 3-1 = 2$ errori rilevabili

$t \leq \frac{3-1}{2} = 1$ errori corregg.

EX

$d_{min} = 7$

$l \leq 6$

$t \leq 3$ (correzione errori singoli/doppi/tripli)

Notazioni

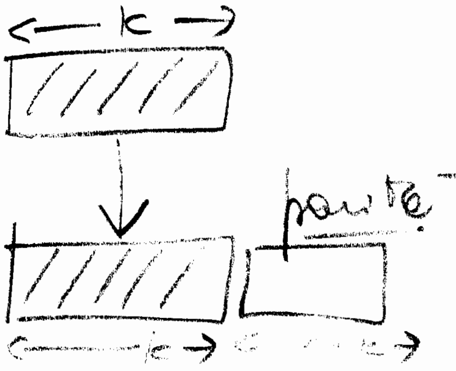
Codici blocco (n,k) mapping k bit $\rightarrow$ n bit.

Codici convoluzionali: convoluzione (t. discreta) tra sequenze bit ingresso e uscita a seguito di operazioni binarie ex-or $\oplus$ e and $\cdot$

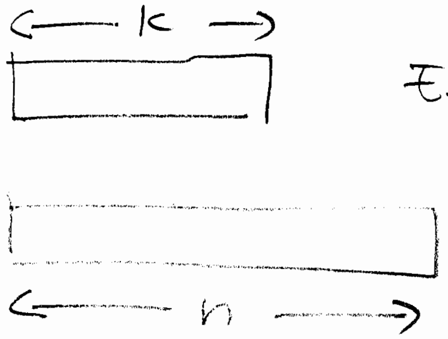
FEC (forward error correction) strategie controllo errori

ARQ (auto repeat request) strategie di ritrasmissione.

Codici a blocco sistematici: codici a blocchi in cui si preserva copia del msg

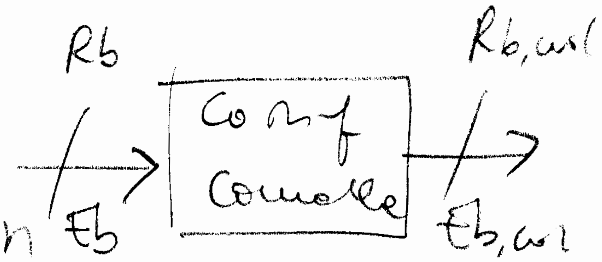


Nozioni di dimensionamento FEC (n, k) Cod 7



$$E_{TOT} = E_b \times k$$

$$E_{TOT} = E_{b,cod} \times n$$



Conserv. energie $E_b \times k = E_{b,cod} \times n$

$$\boxed{E_{b,cod} = E_b \times \frac{k}{n} = E_b \times R}$$

Assumendo di avere canale AWGN con modulazione BPSK allora:

$$p = Q\left(\sqrt{\frac{2E_{b,cod}}{N_0}}\right) = Q\left(\sqrt{\frac{2E_b}{N_0} \cdot R}\right)$$

riduzione SNR

Decodifica Hard (bit-a-bit)

$$P(E) = \sum_{i=t+1}^{n} p(i,n) \simeq p(t+1,n) \simeq \binom{n}{t+1} p^{t+1}$$

Questa è la prob. che sul blocco codif. di lungh. n ci siano errori non correggibili. Globalmente ci sono $t+1$ errori su n e quindi:

$$P_{b,cod}(E) \simeq \frac{t+1}{n} \cdot \binom{n}{t+1} p^{t+1}$$

Cod8

$$P_{b,cod}(t) \simeq \frac{t+1}{n} \cdot \binom{n}{t+1} p^{t+1} =$$

$$= \underbrace{\frac{t+1}{n} \cdot \frac{n!}{(t+1)!\,(n-t-1)!}}_{} p^{t+1} = \binom{n-1}{t} p^{t+1}$$

$$\frac{t+1}{n} \cdot \frac{n\,(n-1)!}{(t+1)\,t!\,(n-1-t)!} = \binom{n-1}{t}$$

Sapendo che $Q(x) \simeq e^{-x^2/2} \leftarrow (*)$

$$P_{b,cod}(t) \simeq \binom{n-1}{t} p^{t+1} = \binom{n-1}{t} \cdot Q\left(\sqrt{\frac{2E_b}{N_0} R}\right)^{t+1} \simeq$$

$$\underset{(*)}{\simeq} \binom{n-1}{t} \left(e^{-\frac{1}{2}\left(\frac{2E_b}{N_0} R\right)} \right)^{t+1} =$$

$$= \binom{n-1}{t} e^{-\frac{1}{2}\left(\frac{2E_b}{N_0} \cdot R(t+1)\right)} \simeq$$

$$\underset{(*)}{\simeq} \binom{n-1}{t} Q\left(\sqrt{\frac{2E_b}{N_0} \cdot R(t+1)} \right)$$

guadagno $\boxed{G_{Hard} \simeq R(t+1)}$

Decodifica soft
(estende ai sistemi codif.
le nozioni di distanza
tra segnale codificato
e segnale ricevuto)

- è ottimale
- è molto complessa (vedi corsi teoria codici)
- prestazioni (estensione union bound)

$$P_{b,cod}(E) \underset{(SOFT)}{\le} \underbrace{\frac{d_{min}}{n}}_{\substack{\#\text{ bit errati}\\ \text{sul blocco}}} \times \underbrace{N_{conc.}}_{\substack{\#\text{ concorrenti}\\ \text{a distanza}\\ d_{min}}} \times Q\left(\sqrt{\frac{2E_b \cdot R \cdot d_{min}}{N_0}}\right)$$

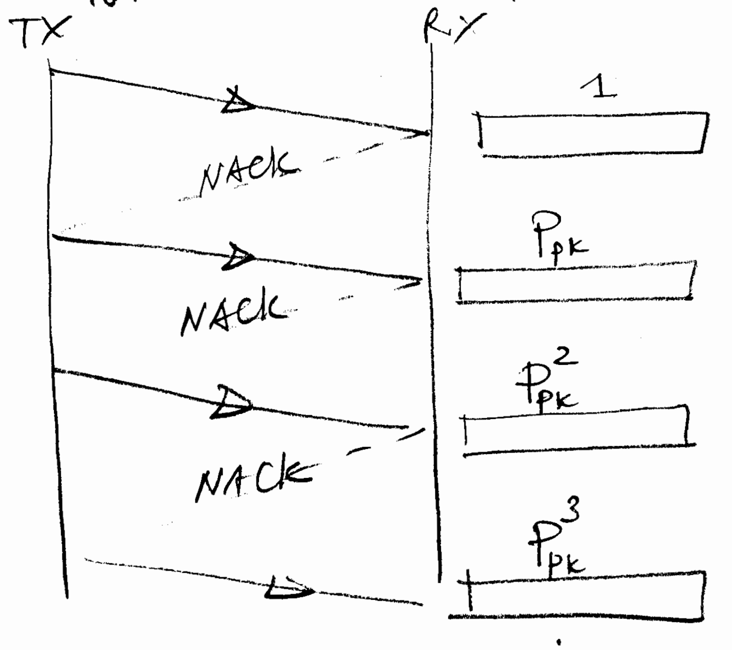
guadagno:

$$\boxed{G_{SOFT} \simeq R \times d_{min}}$$

notare che $\dfrac{G_{SOFT}}{G_{HARD}} \simeq \dfrac{d_{min}}{t+1} \simeq \begin{cases} \dfrac{2 d_{min}}{1+d_{min}} \\ \sim 2 \end{cases}$

quindi ho
un guadagno
di circa +3 dB.

Dimens. sist. ritrasmissione (ARQ) Cod 10



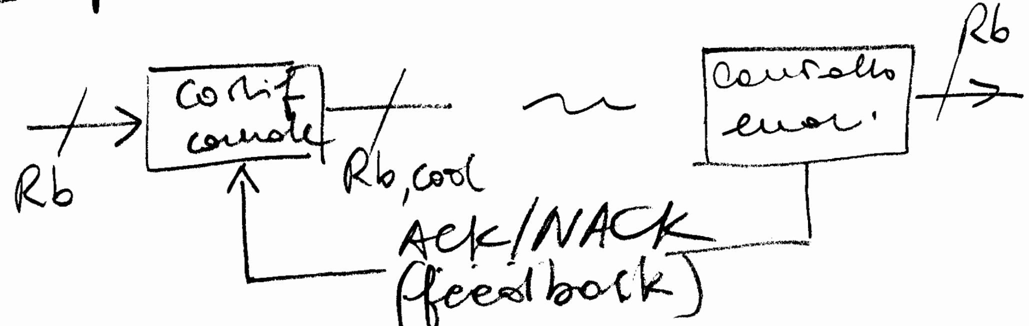
prob. trasm. pacchetto $= 1$

prob. 1ª ritrasm. $= P_{pk}$

prob. 2ª ritrasm. $= P_{pk}^2$

prob 3ª ritrasm. $= P_{pk}^3$

$\boxed{P_{pk}}$ prob errore del singolo pacchetto.



opz.1 controllo errori (senza FEC): $P_{pk} = 1-(1-p)^n$

opz.2 controllo errori con FEC (prima controlla errori e corregge fino dove possibile)

$$P_{pk} = \sum_{i=t+1}^{\ell} p(i,n) \sim p(t+1,n)$$

$$R_{b,cod\,TOT} = R_{b,cod} + \underbrace{R_{b,cod} \times P_{pk}}_{\substack{\text{ritmo (medio)} \\ 1^a\ \text{ritrasm.}}} + \underbrace{R_{b,cod} \times P_{pk}^2}_{\substack{\text{ritmo (medio)} \\ 2^a\ \text{ritrasm.}}} + \dots =$$

$$= R_{b,cod} \times \sum_{i=0}^{\infty} P_{pk}^i = \frac{R_{b,cod}}{1-P_{pk}}$$

$$\boxed{R_{b,TOT} = \frac{R_{b,cod} \times R}{1-P_{pk}}}$$

il ritmo di trasm. è ridotto da $1/1-P_{pk}$ (ritrasmissioni).

Cod 11

Esempi codici (n, k, d) ← distanza min.

(Vedi altri corsi Teoria codici)

Hamming (correzione $t=1$ errore)
rispettano il vincolo (a seguito delle propr. di correzione del codice): $\boxed{n = 2^{n-k} - 1}$

EX: $(n,k) = (3,1)$
$(7,4)$
$(15,11)$
$\vdots$

BCH (Bose, Ray-Chaudhuri, Hocquenghem, 1960)
sono progettati per garantire d_{min}

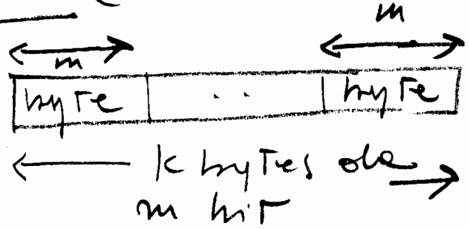
n	k	d	
15	11	3	$\rightarrow R = 0{,}733$
15	7	5	
15	5	7	
15	1	15	
31	26	3	$\rightarrow R = 0.839$
31	21	5	
⋮			
255	247	3	$\rightarrow R = 0.969$
255	239	5	

nota che per $d = 3 = \text{cost}$, se $n \to \infty$ allora $R \to 1$ ma il decodif. diventa molto complesso (si ricordi che 2^n sono le combinaz. ricev.)!

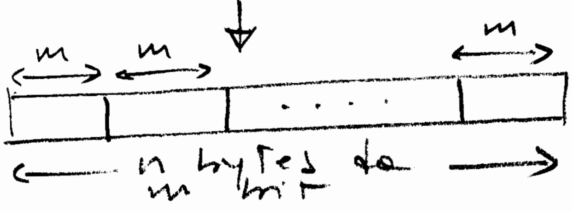
RS (Reed-Solomon)

$$\boxed{\begin{array}{l} n = 2^m - 1 \\ n - k = 2t \end{array}}$$

nota che l'errore è sul simbolo da m bit



(k simboli non-binari)



EX RS(255, 239)
$(m = 8) \rightarrow t = \frac{17-1}{2} = 8$

potere correttore 8 byte questi da 8 bit ciascuno.

$$R = \frac{239 \times 8}{255 \times 8} = 239/255.$$

Analisi comparata prestazioni
(a parità di E_b/N_0 per bit di inform.)

$$p = Q\left(\sqrt{\frac{2E_b}{N_0}\cdot\frac{k}{n}}\right)$$

Se $R=1 \Rightarrow p$ è il sistema non-codif.

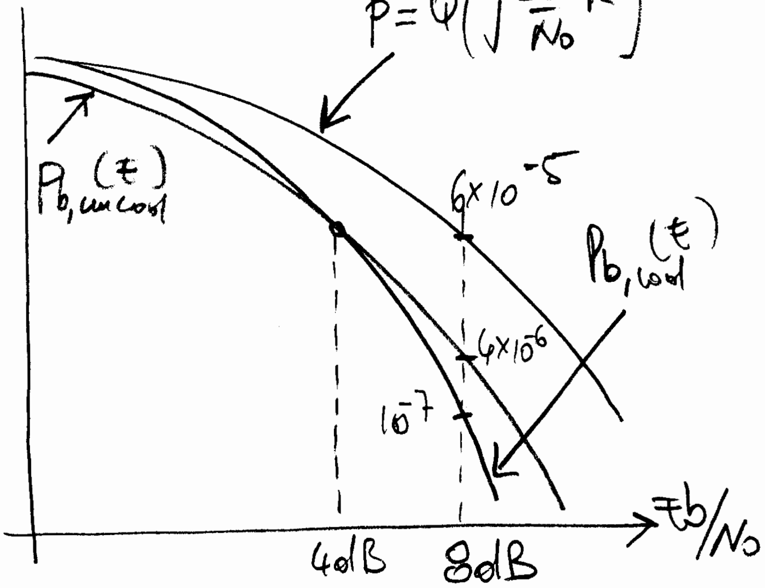
$$P_{b,cod}(\varepsilon) \cong \binom{n-1}{t}\underbrace{\left[Q\left(\sqrt{\frac{2E_b}{N_0}\cdot R}\right)\right]}_{}^{t+1}$$

l'introduzione delle codifica riduce l'energia usata per ogni bit di informazione con riduz. del rapporto $\frac{E_b}{N_0}$ e aumento prob. di errore

<u>Esempio</u> BCH(15, 11, 3) $\rightarrow t = 1$
$E_b/N_0 = 8$ dB, $R = 11/15$ (aumento banda)

$$p = \underbrace{Q\left(\sqrt{\frac{2E_b}{N_0}\cdot\frac{11}{15}}\right)}_{\substack{\text{per } E_b/N_0 = 8\text{ dB} \\ p \simeq 6\times 10^{-5}}} > \underbrace{Q\left(\sqrt{\frac{2E_b}{N_0}}\right)}_{\substack{E_b/N_0 = 8\text{ dB} \\ \sim 4\times 10^{-6}}} = P_{b,uncod}(\varepsilon)$$

$$P_{b,cod}(\varepsilon) \simeq \binom{14}{1} p^2 = 14p^2 \simeq 10^{-7}$$



<u>osservazioni</u>

1) $E_b/N_0 < 4$dB: non si guadagna dalle codifica

2) nonostante $p > P_{b,uncod}(\varepsilon)$ la codif. guadagna per la capacità di correz. di <u>pochi</u> errori <u>isolati</u>