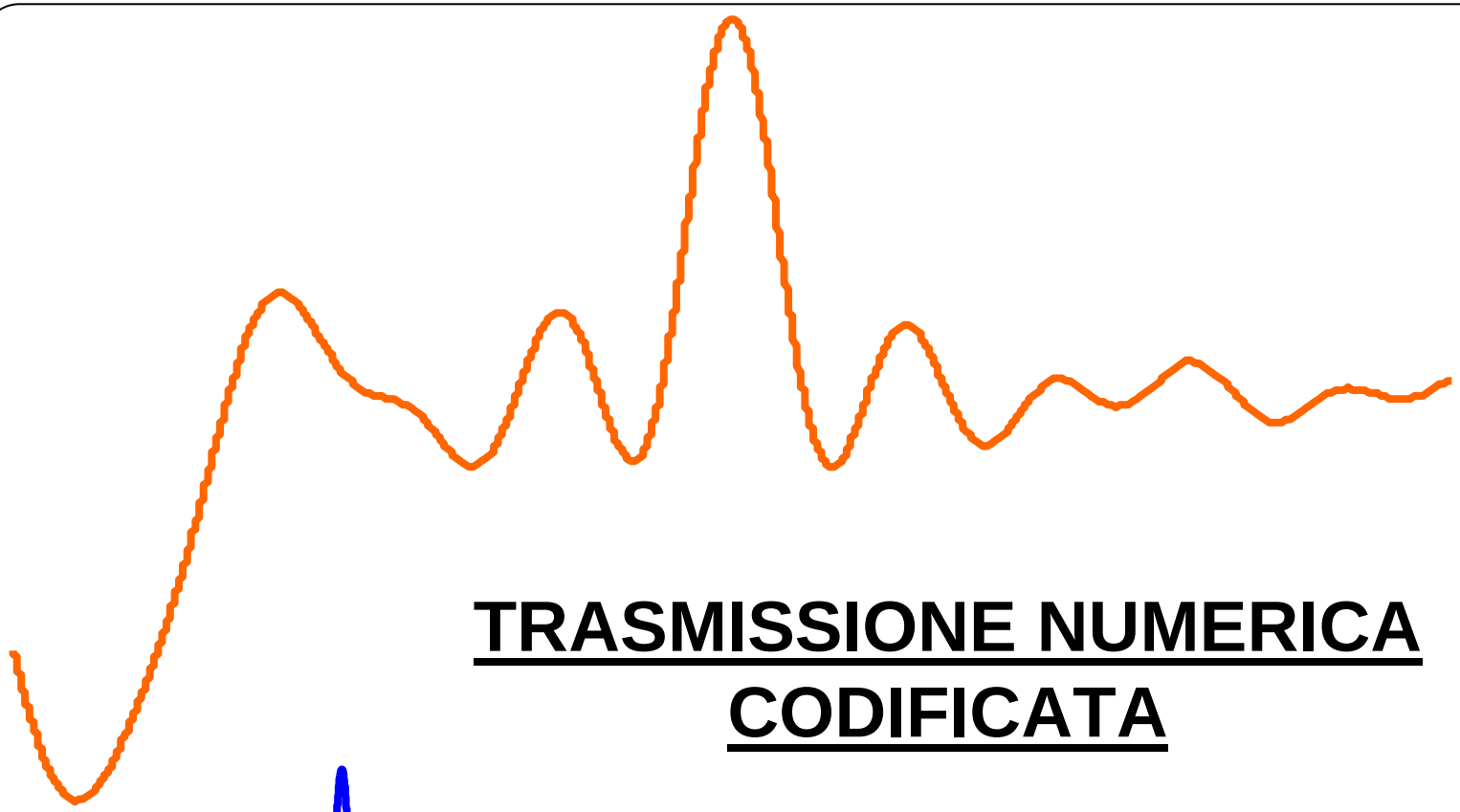
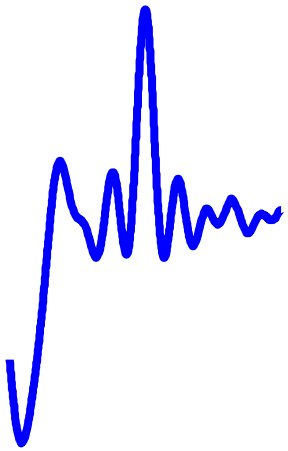
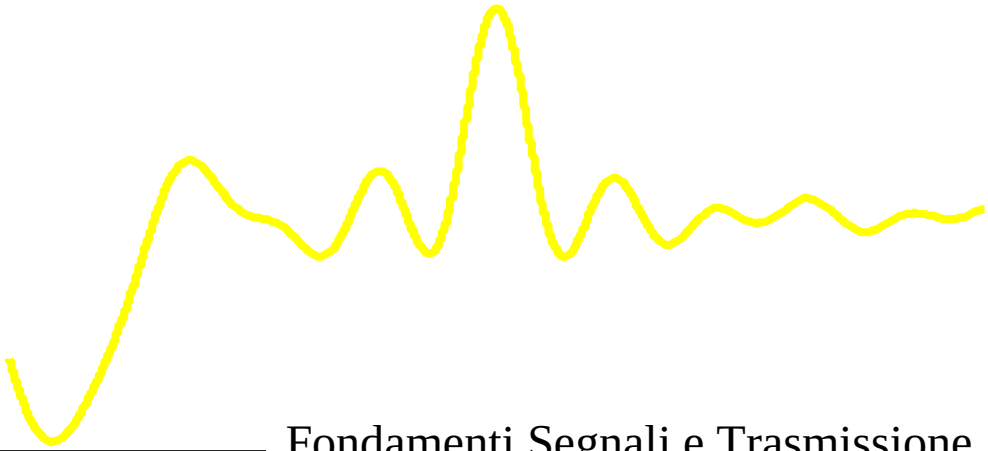


TRASMISSIONE NUMERICA CODIFICATA





Introduzione alla trasmissione numerica codificata

Esiste un metodo per ridurre la probabilità d'errore, ad un certo rapporto segnale/rumore assegnato: utilizzare un codice per la correzione degli errori, cioè trasmettere dei bit aggiuntivi di controllo che permettono al ricevitore di verificare la presenza di errori ed eventualmente di correggerli.

Esempio: dividiamo il flusso di bit da trasmettere in blocchi di K=4 bit (u_1,u_2,u_3 ,u_4) e per ogni quaterna, trasmettiamo tre bit di controllo in più (p_1,p_2,p_3), così calcolati:

$$p_1 = u_1 \oplus u_2 \oplus u_3, \quad p_2 = u_2 \oplus u_3 \oplus u_4, \quad p_3 = u_1 \oplus u_2 \oplus u_4$$

Anche in ricezione ogni blocchetto di N=7 bit deve quindi rispettare le N-K=3 "equazioni di parità":

$$s_1 = p_1 \oplus u_1 \oplus u_2 \oplus u_3 = 0$$
$$s_2 = p_2 \oplus u_2 \oplus u_3 \oplus u_4 = 0$$
$$s_3 = p_3 \oplus u_1 \oplus u_2 \oplus u_4 = 0$$

se è così, il ricevitore assume che non ci sono errori. Altrimenti il bit errato sarà:

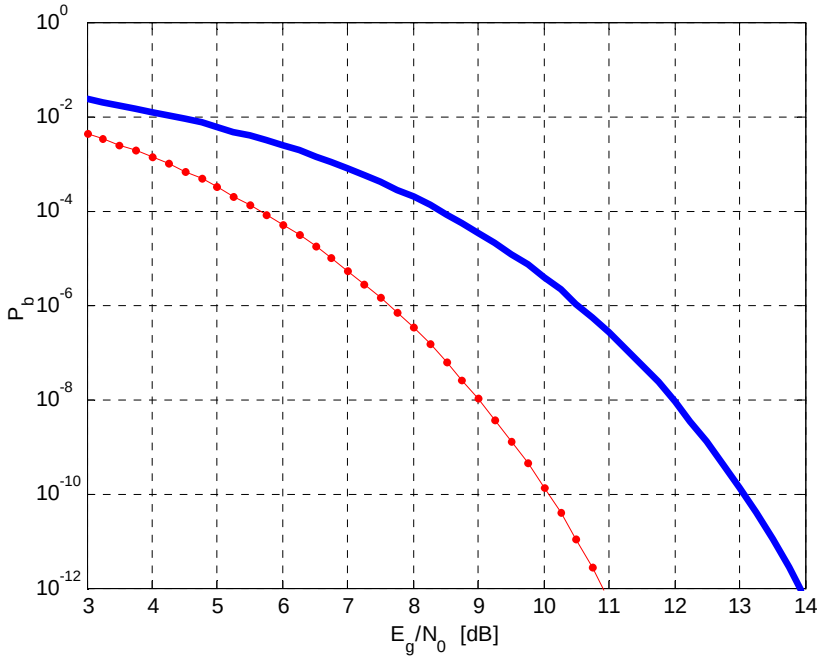
s_1,s_2,s_3	*1 0 0*	*0 1 0*	*0 0 1*	*1 0 1*	*1 1 1*	*1 1 0*	*0 1 1*
bit	p_1	p_2	p_3	u_1	u_2	u_3	u_4

Introduzione alla trasmissione numerica codificata (2)

Quali sono le prestazioni del sistema di trasmissione che abbiamo ideato?

Se la *parola* di N=7 bit contiene un solo errore, lo correggiamo; se ne contiene di più, alla peggio ne aggiungiamo un altro in correzione.

Il tasso d'errore globale diminuisce se il rapporto segnale-rumore è abbastanza alto da rendere improbabile che si presenti più di un errore nella parola

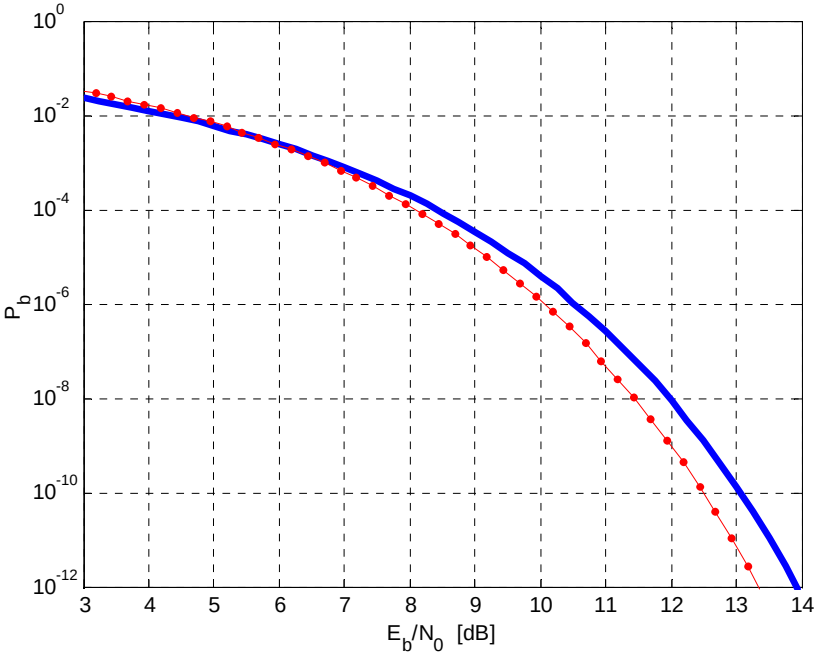


Introduzione alla trasmissione numerica codificata (3)

Questo vantaggio si paga in due modi:

1) in realtà l'energia totale che spendiamo aumenta di un fattore N/K a pari probabilità di errore singolo prima della "decodifica"

Possiamo operare il confronto a pari E_b energia spesa per ogni bit di informazione trasmesso. Poichè $7E_g$=$4E_b$, il confronto a pari E_b va fatto con 2.5 dB in meno di E_g per il sistema codificato.



2) a pari ritmo di trasmissione dell'informazione (R_b bit/s), il ritmo di trasmissione sul canale, e quindi la banda necessaria, aumentano di un fattore N/K

Vantaggio difficilmente "quantificabile" in termini di prestazioni. Si può formalizzare dicendo che il sistema 2PAM non codificato trasmette con *efficienza spettrale* di 1 bit/simbolo, mentre un sistema codificato trasmette solo K/N bit/simbolo.

Ci sono applicazioni nelle quali c'é disponibilità di banda, e ci si può permettere efficienze spettrali più basse. In caso contrario, potrebbe venire in mente di compensare l'espansione di banda con una modulazione multilivello.

Codici a blocco e decodifica algebrica (1)

• Si divide il flusso di informazione in blocchi di K simboli, e si aggiungono N-K simboli di parità, ottenendo parole di codice di lunghezza N simboli.

• Si chiama *rate* del codice il rapporto $R=K/N$. L'espansione di banda è pari a $1/R$

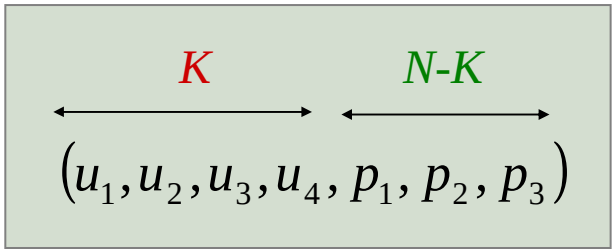
• Se i simboli sono bit, si chiamano codici binari, ma esistono anche codici non binari (operazioni elementari sui byte in algebra estesa dall'algebra binaria)

• Le regole di definizione del codice determinano la *distanza minima di Hamming* d ovvero il minimo numero di simboli in cui differiscono due parole di codice. Dal parametro d dipendono fortemente le prestazioni del codice.

Esempio iniziale:

codice binario

$(K,N,d)=(4,7,3)$, $R=4/7$



Codici a blocco e decodifica algebrica (2)

- Dato un codice di parametri (N,K,d), utilizzando un sottoinsieme K-a dei simboli di informazione, cioè ponendo a zero (e non trasmettendo) gli a rimanenti prima di calcolare le cifre di parità, si ottiene un *codice accorciato* $(N\text{-}a,K\text{-}a,d)$.
- In ricezione si può utilizzare il codice in due modi:

  1. come *correttore* di errori (FEC, Forward Error Correction): il decodificatore sceglie il pattern di errore più probabile (minimo numero di errori) compatibile con la sequenza ricevuta; sceglie la sequenza lecita a minima distanza di Hamming da quella ricevuta (*decodifica algebrica*).
  2. come *rivelatore* di errori: il decodificatore controlla solo la validità della sequenza ricevuta e segnala l'eventuale fallimento. Si usa per esempio, nel caso sia possibile chiedere la ritrasmissione della sequenza (ARQ, Automatic Repeat reQuest).

  Le due funzioni si possono combinare: si può decidere di correggere fino ad un certo numero di errori, e limitarsi a rivelare la presenza di errori oltre tale soglia (utile per ridurre la probabilità di richiesta di ritrasmissione).

Codici a blocco binari: il codificatore (1)

Generazione delle parole di codice: matrice generatrice

$$(u_1, u_2 \ldots u_K) \cdot \underline{\underline{G}}^{[K,N]} = (x_1, x_2 \ldots x_N)$$

Esempio iniziale:

$$(u_1, u_2, u_3, u_4) \cdot \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] = (u_1, u_2, u_3, u_4, p_1, p_2, p_3)$$

matrice identità K x K

matrice P K x (N-K)

Approccio comodo solo a scopo descrittivo. In realtà è più comune associare un polinomio (di grado N-1) nella variabile D alla parola di codice:

$$x(D) = x_1 D^{N-1} + x_2 D^{N-2} \ldots + x_{N-1} D + x_N$$

Codici a blocco binari: il codificatore (2)

Il codice può essere descritto tramite il suo *polinomio generatore g(D)*, di grado N-K

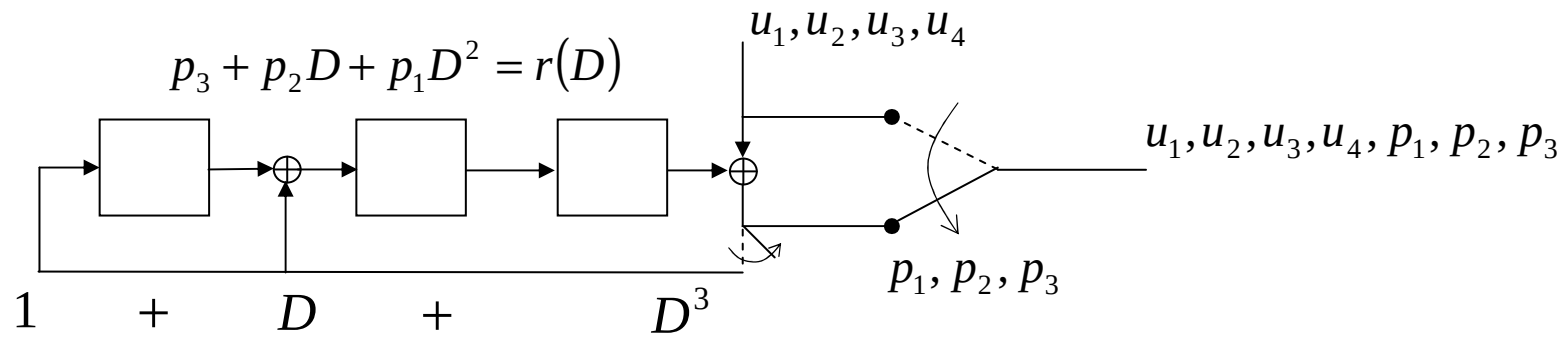
Appartengono al codice solo le N-ple con polinomio *x(D) divisibile* per *g(D)*

Il codificatore calcola il resto *r(D)* della divisione $\left(u_1 D^{N-1} + u_2 D^{N-2} + \ldots u_K D^{N-K}\right) / g(D)$

$x(D) = D^{N-K} u(D) + r(D)$ è divisibile per *g(D)* !

Esempio iniziale:

si può verificare che il codice (7,4) ammette come polinomio generatore $g(D) = D^3 + D + 1$



Codici a blocco: il decodificatore

Il controllo delle equazioni di parità tramite la matrice di parità $H^{[N,N-K]}$ rivela se la sequenza è di codice (rivelazione):

$$(x_1, x_2 \ldots x_N) \bullet \underline{\underline{H}} = (s_1, s_2 \ldots s_{N-K})$$

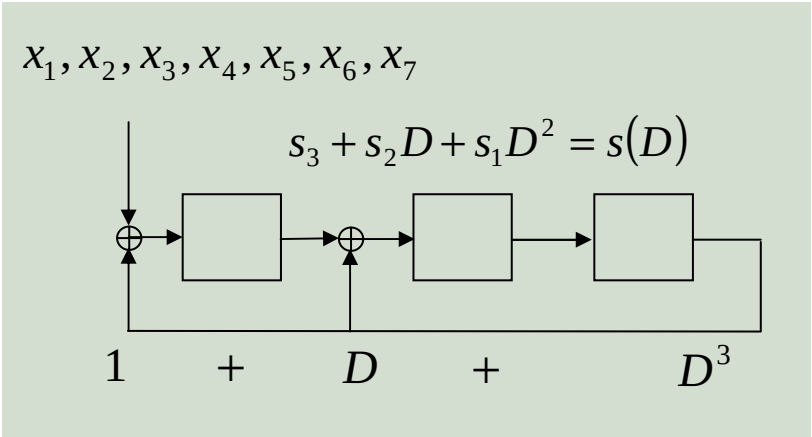
Oppure si calcola il resto *s(D)* della divisione tra *x(D)* e *g(D)* con lo stesso circuito usato in fase di codifica, ma entrando nella cella di grado zero. Nell'esempio iniziale questo permette di risalire anche alla posizione dell'errore (correzione).

Esempio iniziale:

$$(u_1, u_2, u_3, u_4, p_1, p_2, p_3) \bullet \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (s_1, s_2, s_3)$$

matrice P K x (N-K)

identità K x K



Per codici con potere correttore maggiore, tramite operazioni nell'algebra dei campi finiti è possibile risalire dalle *sindromi* alle posizioni degli errori, e correggerli.

Prestazioni del decodificatore (1)

Per la *distanza minima di Hamming* d, qualunque sia il codice vale la proprietà:

$$d \leq N - K + 1$$

Infatti, cambiando un solo simbolo di informazione di un parola di codice, se ne ottiene un'altra che non può differire dalla prima in un numero di simboli superiore agli N-K simboli di parità, oltre a quello di informazione. Inoltre i parametri *potere correttore* t e *potere rivelatore* r, sono legati a d nel seguente modo:

$$r = d - 1, \qquad t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

- qualunque pattern di e errori con $e<d$ dà sindromi non nulle e ne permette la rivelazione, mentre con $e=d$ si può ottenere una diversa parola di codice
- fino a $e=t$ errori sulla parola di codice trasmessa, non vi può essere un'altra parola a distanza di Hamming minore o uguale a e in quanto si troverebbe a distanza minore o uguale a $2e<d$ dalla trasmessa; questa condizione si può invece verificare per $e>t$.
- si può usare un codice per correggere t errori e rivelarne fino a r, a patto che $r+t<d$

Prestazioni del decodificatore (2)

Le prestazioni del codice usato in correzione dipendono dal potere correttore t. La probabilità di errata decodifica è la probabilità che nella parola si presentino più di t errori:

$$P_e = \sum_{i=t+1}^{N} \binom{N}{i} p^i (1-p)^{N-i} \cong \binom{N}{t+1} p^{t+1} (1-p)^{N-t-1} \cong \frac{N^{t+1}}{(t+1)!} p^{t+1}$$

La probabilità d'errore sul bit dipende da quanti bit si sbagliano in caso di errore di decodifica. Supponendo che agli i già presenti, il decodificatore non aggiunga errori:

$$P_b = \sum_{i=t+1}^{N} \binom{N}{i} \frac{i}{N} p^i (1-p)^{N-i} \cong \binom{N}{t+1} \frac{t+1}{N} p^{t+1} (1-p)^{N-t-1} \cong \frac{N^t}{t!} p^{t+1}$$

Dove p è la probabilità di ricevere un bit errato dal canale, quindi con modulazione 2PAM o 4QAM:

$$p = Q\left(\sqrt{\frac{2E_g}{N_0}}\right) = Q\left(\sqrt{\frac{2E_b}{N_0} R}\right)$$

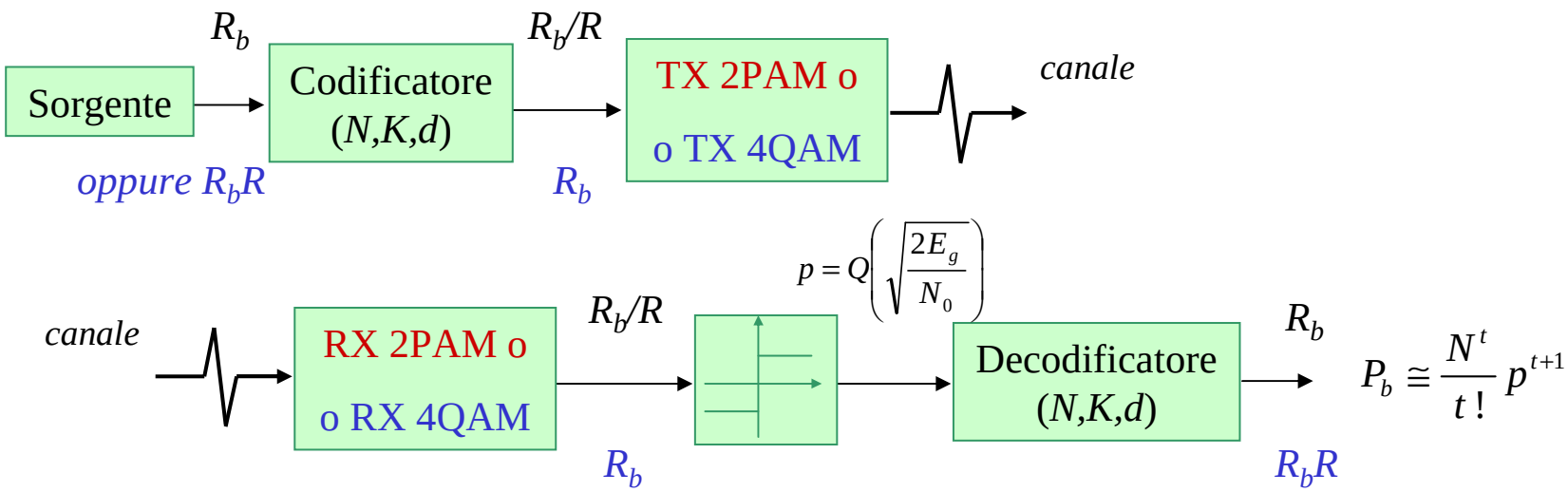
Trasmissione binaria codificata

Riassumendo quanto abbiamo visto:

• si possono migliorare le prestazioni di un sistema di trasmissione numerico binario utilizzando un codice (N,K,d) cioè trasmettendo dei simboli di parità aggiuntivi

• il ritmo con cui si inviano bit sul canale, e quindi la banda necessaria, aumentano di un fattore $1/R$ a pari ritmo di informazione, per trasmettere anche i simboli di parità (in tal caso E_g diminuisce di un fattore R a pari potenza trasmessa); in alternativa, a pari banda, il ritmo di trasmissione dei bit d'informazione va ridotto di un fattore R (in tal caso E_g rimane invariata a pari potenza trasmessa).

• in ricezione occorre svolgere le operazioni di decodifica che consentono di correggere fino a t errori o di rivelarne fino ad r (maggior complessità del ricevitore)



Codici di Hamming

Codici binari, le cui N-K equazioni di parità sono scelte in modo da individuare univocamente la posizione di un errore singolo (come il codice dell'esempio iniziale).

- N posizioni possibili, 2^{N-K} sindromi: $2^{N-K}=N+1$
- $N= 2^{N-K}$ -1, K di conseguenza: $(N,K) = (7,4), (15,11), (31,26), (63,57), (127,120)$...
- $d = 3$ ⇒ $t = 1$ oppure $r = 2$
- la matrice P contiene tutte le righe di N-K bit con due o più "uni", in tutto

$$2^{N-K} - 1 - (N-K) = K \quad \text{righe.}$$

tutti 0 — *un solo 1*

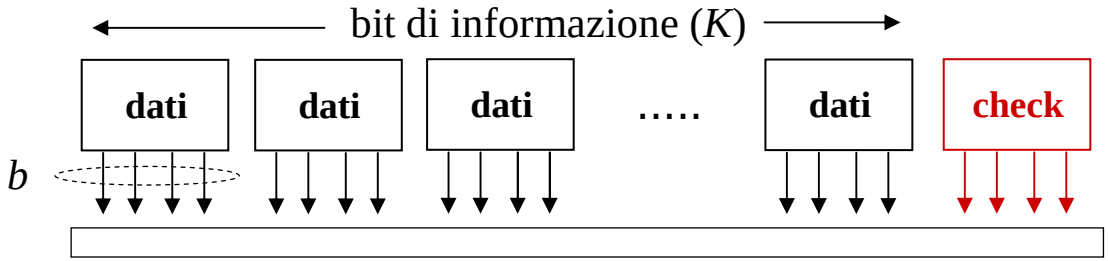
Codici di Hamming estesi

se alle parole di un codice di Hamming si aggiunge un bit di parità complessiva, si ottiene un *codice di Hamming esteso*, con $(N,K) = (8,4), (16,11), (32,26)$... e d=4.

Gli Hamming estesi possono correggere tutti gli errori singoli e rivelare tutti gli errori doppi, infatti t=1, ma $t+r = 1+2 = 3 < d = 4$.

Applicazione alle memorie ad alta velocità (b-bit per chip)

- codici di controllo e correzione: velocità di codifica e decodifica (reti combinatorie)
- basso numero di cifre di controllo per non sprecare memoria
- memorie organizzate in chip di *byte* da b bit



Gli Hamming estesi sono codici SEC/DED (Single Error Correcting, Double Error Detecting). Da loro versioni modificate e accorciate si ottengono codici SEC/DED/SbED (Single b-bit byte Error Detecting), con la capacità di rivelare anche più di due errori, se concentrati in un byte di b bit.

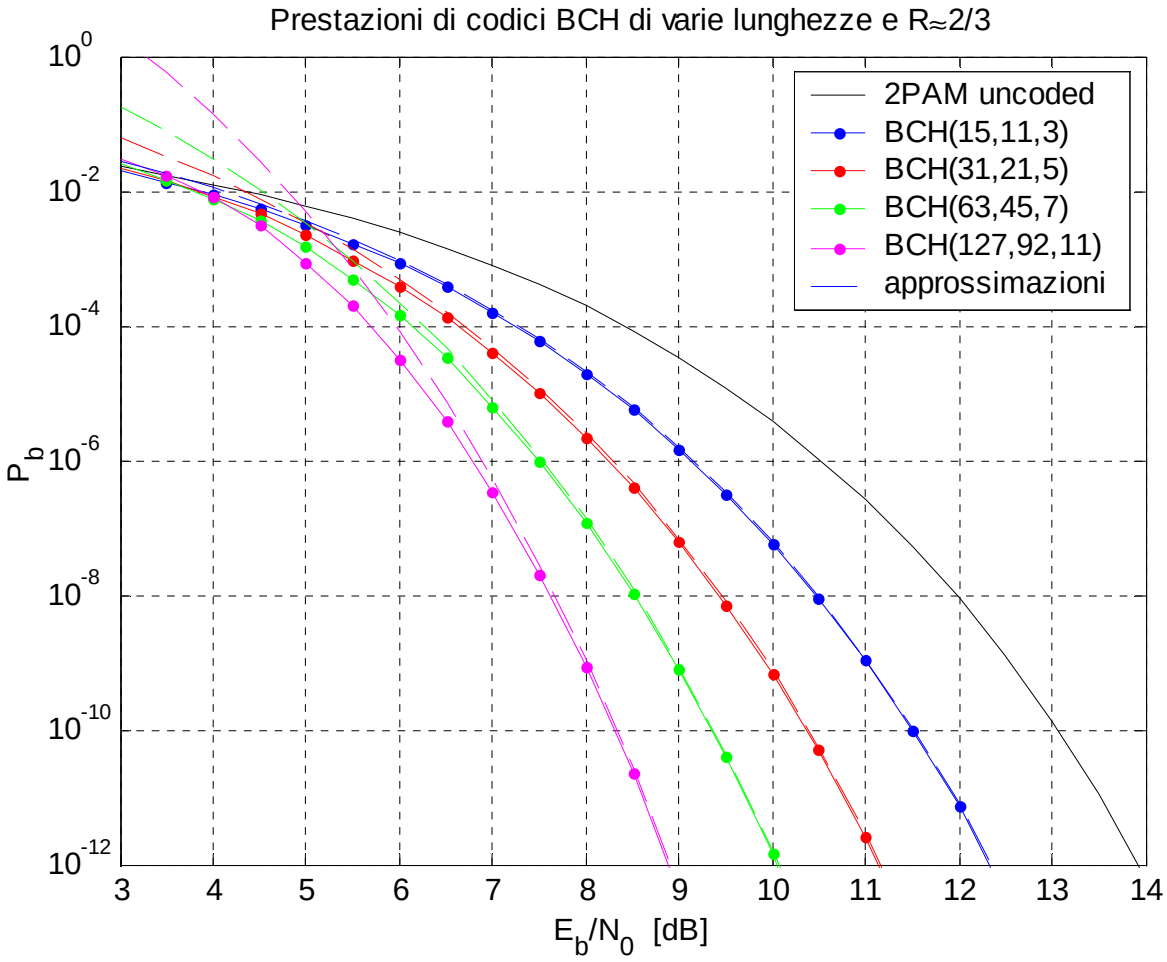
Esempio:
codici SEC/DED/SbED, b=4

bit (*K*)	32	64	128
N-K minimi	7	8	9

Codici BCH (Bose Ray-Chaudhuri, Hocquenghem)

Codici binari progettati con criteri basati sull'algebra dei campi finiti. Includono i codici di Hamming come caso particolare, ma ammettono diversi valori di K per ogni lunghezza del blocco ($N = 2^m-1$, $m \in N$). Anch'essi possono essere accorciati.

N	*K*	*d*	*t*	*N*	*K*	*d*	*t*
15	11	3	1	127	120	3	1
	7	5	2		113	5	2
	5	7	3		106	7	3
	1	15	7		99	9	4
31	26	3	1		92	11	5
	21	5	2		...		
	16	7	3	255	247	3	1
	11	11	5		239	5	2
	...				231	7	3
63	57	3	1		223	9	4
	51	5	2		215	11	5
	45	7	3		207	13	6
	39	9	4		199	15	7
	36 ...	11	5		191 ...	17	8



codici Reed-Solomon (RS)

Codici non binari, spesso utilizzati con byte di m=4 o m=8 bit. Tutti i parametri, N, K, d, t ed r si riferiscono quindi a byte e non a bit. Come i BCH sono progettati con criteri basati sull'algebra dei campi finiti ($GF(16)$ o $GF(256)$), e ammettono diversi valori di distanza minima, al variare del numero dei simboli di parità.

- lunghezza del blocco $N=2^m-1$, poi si accorciano ottenendo codici $(N\text{-}a, K\text{-}a, d)$
- $d=N-K+1$, $r=N-K$ oppure $t=(N-K)/2$

Per le prestazioni, valgono le espressioni viste, con probabilità di errore sui byte! Se p_b è la probabilità di bit errato (prob. indipendenti):

$$p_B = 1-(1-p_b)^m \quad \Rightarrow \quad P_B \cong \frac{N^t}{t!} p_B^{t+1}$$

Memorie ad alta velocità

I codici RS sono "per natura" codici di tipo bEC/ bED perchè si possono definire su byte di b bit. Per avere un RS che corregga singoli byte errati e riveli fino a due byte errati (SbEC/ DbED) occorre d=4 ($r+t<d$), e quindi bastano N-K=3 byte di parità.

Se b=8, 24 bit di parità bastano per ogni dimensione del blocco fino a bN=1020 bit.

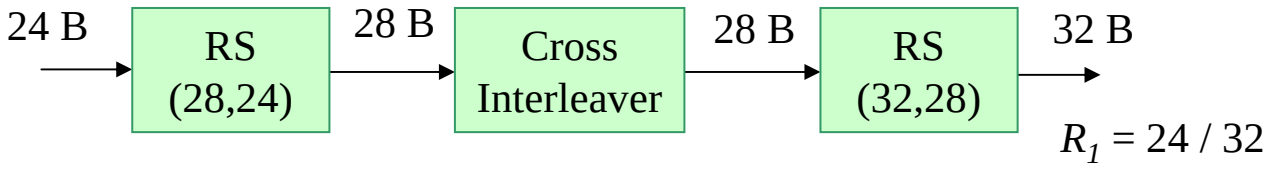
bit (bK)	32	64	128
b(N-K)	24	24	24

codici Reed-Solomon (RS)

Formato CD, codici CIRC (cross-interleaved RS codes)

Per garantire un livello di protezione adeguato nel formato CD-audio, si utilizza la concatenazione di due codici RS su $GF(256)$ a d=5: (N,K,d)= (255,251,5). Questi vengono accorciati a (28,24,5) e (32,28,5) rispettivamente, per un rate totale di:

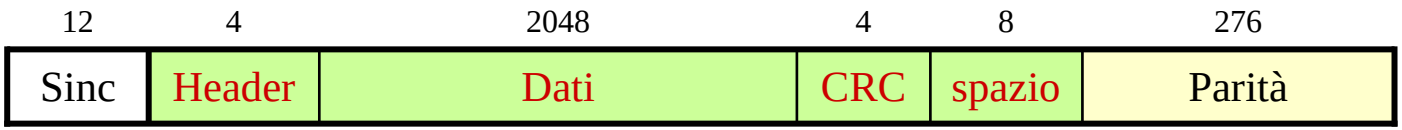
$$R_1 = \frac{24}{28} \cdot \frac{28}{32} = \frac{3}{4}$$



Quindi la capacità "vera" di un CD da 74' non è quella effettiva di

$$176.4\ 10^3\ B/s\ 4440\ s = 747.5\ MB, \quad \text{ma} \quad 747.5/R_1 = 996\ MB!$$

Per i dati, per cui è richiesto un livello di protezione superiore, si premette un ulteriore livello di codifica con un codice rivelatore (CRC) con 4 byte di parità, ed il "prodotto" di due RS su $GF(256)$ accorciati (26,24,3) e (45,43,3). Byte di sincronismo e header portano l'overhead a 304 byte su 2048, per un rate totale di R_2 = 2048/2352.



La capacità "dati" effettiva di un CD si riduce di un ulteriore fattore R_2 a 650 MB.

Capacità di canale (1)

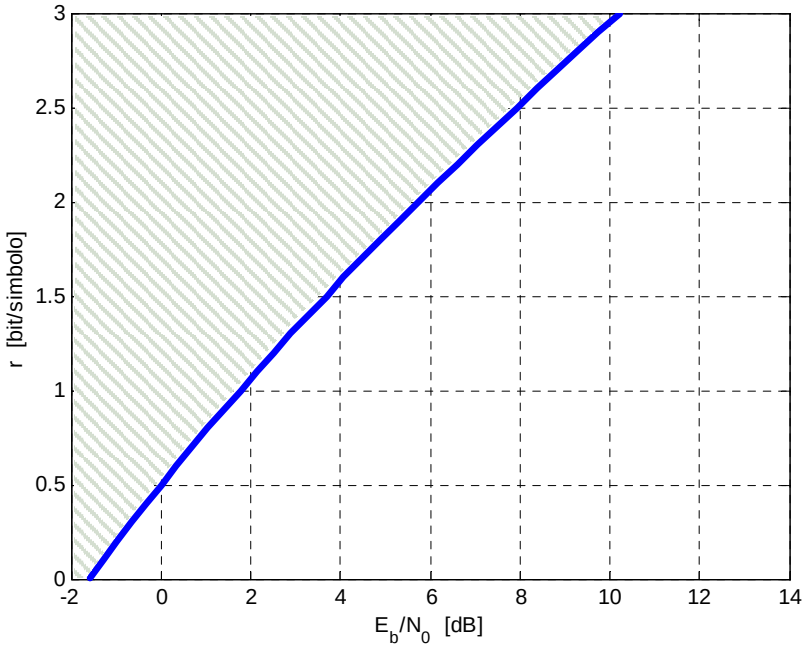
Due deduzioni dall'analisi dei codici visti:

- a pari N, più si abbassa il rate R e più le prestazioni migliorano
- a pari R, più si aumenta la lunghezza del blocco N e più le prestazioni migliorano

Ci si può chiedere se, assegnata una certa efficienza spettrale r in [*bit/simbolo*] (in banda base), esiste un limite alle prestazioni che un sistema di trasmissione può raggiungere all'aumentare della dimensione del blocco N. Esiste cioè una soglia di SNR oltre la quale posso ottenere un certo tasso d'errore a patto di scegliere un codice sufficientemente lungo?

Oppure, viceversa, assegnato un certo SNR, e fissato il tasso d'errore, esiste un'efficienza spettrale massima che mi posso permettere, di nuovo, a patto di scegliere N abbastanza grande?

$$r \le \frac{1}{2}\log_2\left(1+2r\frac{E_b}{N_0}\right), \qquad \frac{E_b}{N_0} \ge \frac{2^{2r}-1}{2r}$$



Capacità di canale (2)

Inoltre, assegnata una certa efficienza spettrale r in [*bit/simbolo*], il bit rate R_b è dato da r per il ritmo di simbolo $1/T$. Sostituendo anche la banda minima corrispondente si ottiene:

$$R_b = \frac{r}{T} = 2rB \quad \Rightarrow \quad 2r = \frac{R_b}{B} \qquad \Rightarrow \qquad R_b \le B \log_2\left(1 + \frac{R_b E_b}{B N_0}\right)$$

dove il prodotto $P = R_b E_b$ dà la potenza ricevuta. La quantità limite

$$C = B \log_2\left(1 + \frac{P}{B N_0}\right)$$

E' detta *capacità di canale* [bit/s] e rappresenta il massimo bit rate che si può trasmettere con tasso d'errore piccolo a piacere su un canale di banda limitata (B) corrotto da AWGN ($N_0/2$) con potenza P al ricevitore.

Capacità di canale (2)

Inoltre, assegnata una certa efficienza spettrale r in [*bit/simbolo*], il bit rate R_b è dato da r per il ritmo di simbolo $1/T$. Sostituendo anche la banda minima corrispondente si ottiene:

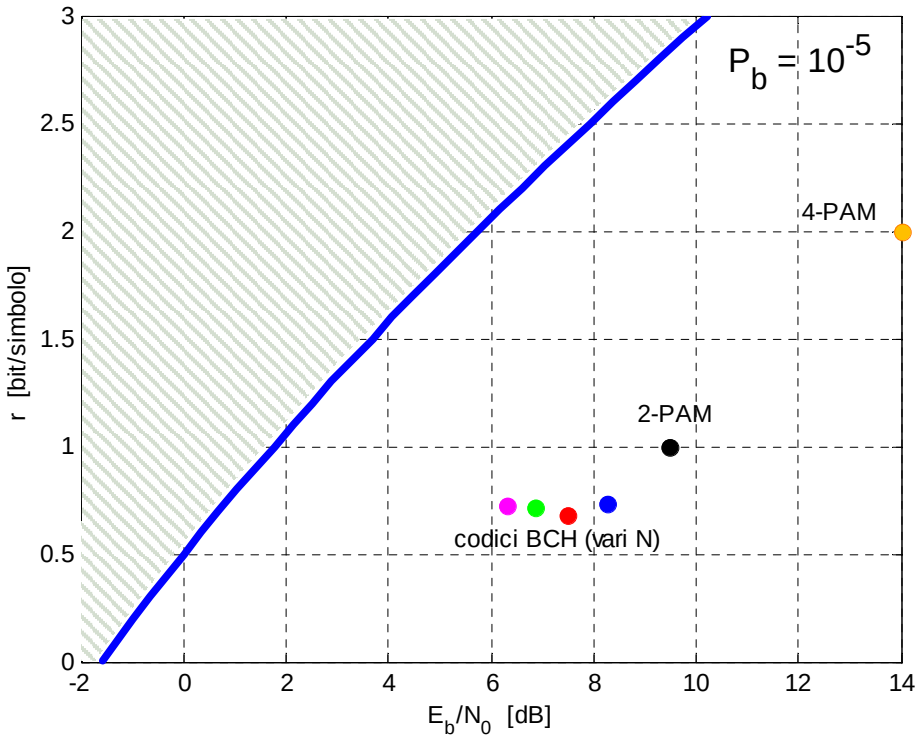
$$R_b = \frac{r}{T} = 2rB \quad \Rightarrow \quad 2r = \frac{R_b}{B} \qquad \Rightarrow \qquad R_b \le B \log_2\left(1+\frac{R_b E_b}{B N_0}\right)$$

dove il prodotto $P=R_bE_b$ dà la potenza ricevuta. La quantità limite

$$C = B \log_2\left(1+\frac{P}{B N_0}\right)$$

E' detta *capacità di canale* [bit/s] e rappresenta il massimo bit rate che si può trasmettere con tasso d'errore piccolo a piacere.

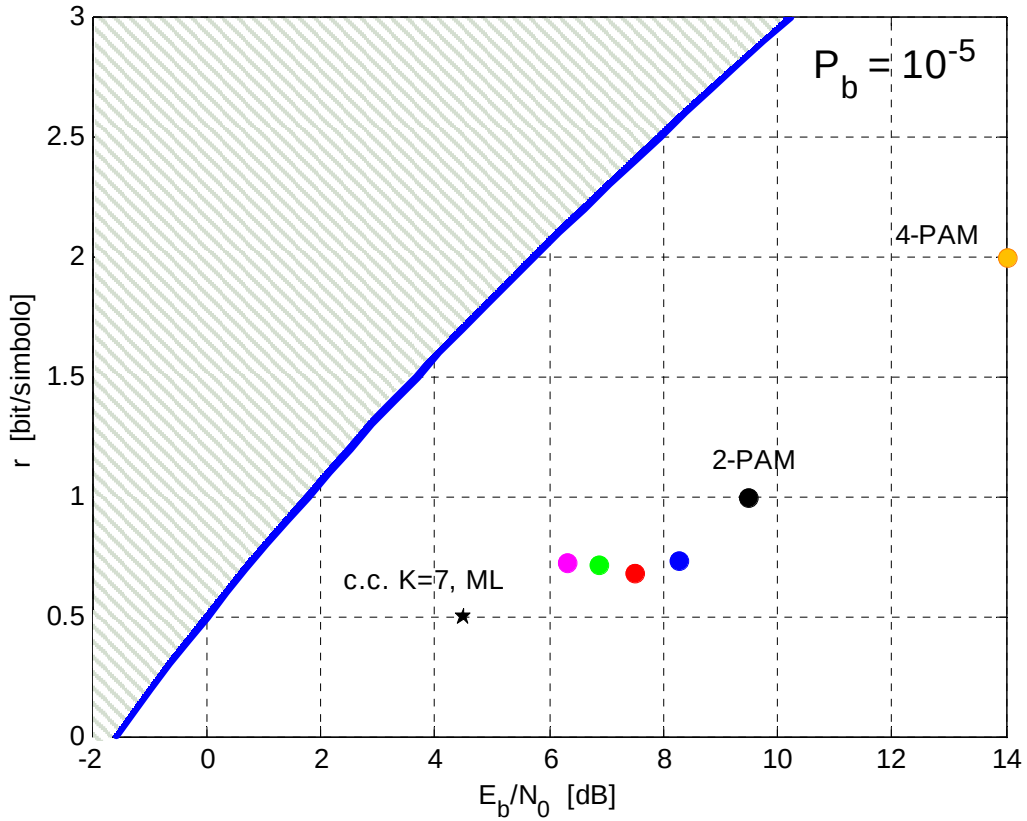
I codici che abbiamo visto offrono preziosi guadagni rispetto ai sistemi non codificati. Eppure si hanno ancora ampi margini di miglioramento, rispetto al limite teorico.



Approfondimenti: anni 60'-70'

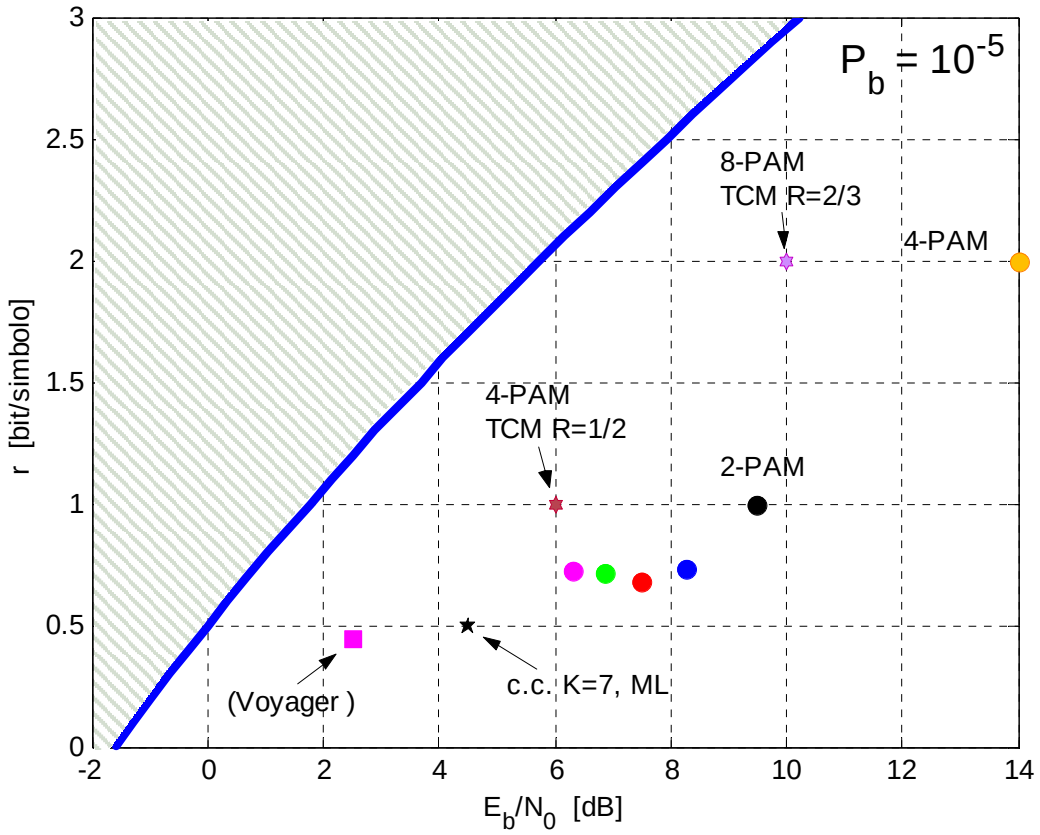
Decodifica a *massima verosimiglianza* (ML) anzichè a minima distanza di Hamming di segnali codificati: interpretazione geometrica dei segnali, maggior complessità, migliori prestazioni.

- codici convoluzionali (constrained length K, 2^{K-1} stati), algoritmo di Viterbi (ML)



Approfondimenti: anni ‘80

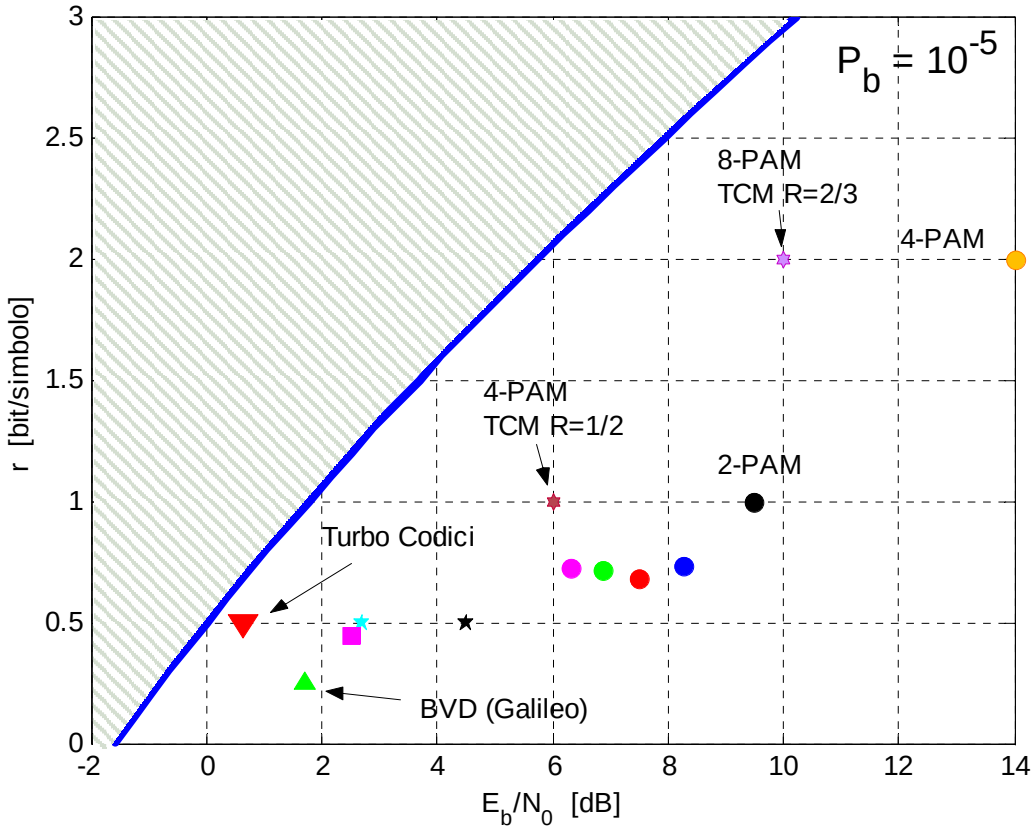
- Codici concatenati: Reed Solomon + Codice Convoluzionale
  - Voyager: RS (255,223,33) + codice conv. R=1/2, K=7
- Codifica e modulazioni multilivello: codici TCM (Trellis Coded Modulation)



Approfondimenti: anni ‘90

• Applicazioni spaziali, efficienze spettrali < 0.5, Big Viterbi Decoding (Galileo): codice convoluzionale, R=1/4, K=15, decodifica ML

•1993 - Turbo Codici: concatenazione di codici convoluzionali *recursivi*



- decodifica iterativa “quasi ML”, di codici con blocchi lunghissimi
- già adottati in molti standard (DVB-RCS, CCSDS, UMTS)