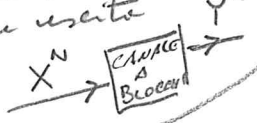
7.5.2 La disuguaglianza di Fano per il canale ~~esteso~~ a blocchi

blocchi di lunghezza e N all'ingresso e

Consideriamo ora il canale con ~~$n = m$ al cui ingresso sono applicate delle stringhe di simboli di lunghezza N~~. Nella associazione tipica ingresso-uscita la probabilità di errore è

blocchi di lunghezza N in uscita. Gli alfabeti siano gli stessi sia in ingresso che in uscita



$$Pr\{Y^N \neq X^N\} = P(e_N), \tag{7.53}$$

che denominiamo probabilità di *errore-per-parola* (*word-error probability*). Infatti l'evento errore e_N si verifica quando almeno uno (qualunque) degli N simboli della stringa in uscita è diverso da quelli dell'ingresso. La disuguaglianza di Fano diventa

$$\mathcal{H}(X^N|Y^N) \leq \mathcal{H}(P(e_N)) + P(e_N)\log_2(n^N - 1). \tag{7.54}$$

~~Nel caso particolare di usi indipendenti del~~

~~Avendo assunto gli usi del canale indipendenti, abbiamo che $\mathcal{I}(X^N;Y^N) \leq NC$.~~ [2] ~~Quindi $\mathcal{H}(X^N|Y^N) = \mathcal{H}(X^N) - \mathcal{I}(X^N;Y^N) > \mathcal{H}(X^N) - NC$. Pertanto la disuguaglianza di Fano fornisce~~

Quindi $H(X^N|Y^N) = H(X^N) - I(X^N;Y^N) > H(X^N) - C_N$

dove

$$C_N = \underset{\Pi_{X^N}}{\arg\max}\, I(X^N;Y^N)$$

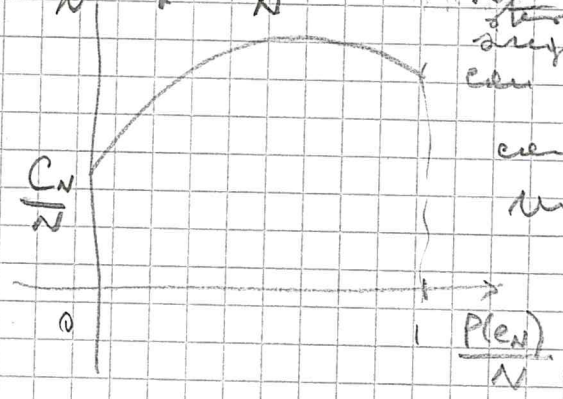
Quindi

$$H(X^N) \leq C_N + H(P(e_N)) + P(e_N)\log(n^N - 1)$$

che possiamo anche leggere

$$\frac{H(X^N)}{N} \leq \frac{C_N}{N} + \frac{H(P(e_N))}{N} + \frac{P(e_N)}{N}\log(n^N - 1)$$

stessa figura singolo uso, ma con riferimento a $\frac{C_N}{N}$ con caratteristiche mediate.



Se gli usi del canale sono indipendenti, $C_N = NC$ e

$$\frac{\mathcal{H}(X^N)}{N} \leq C + \frac{\mathcal{H}(P(e_N))}{N} + \frac{P(e_N)}{N}\log_2(n^N - 1), \tag{7.56}$$

che può essere riscritta come

$$\frac{\mathcal{H}(X^N)}{N} \leq C + \frac{1}{N}\mathcal{F}\left(P(e_N), n^N\right). \tag{7.57}$$

La relazione ottenuta sancisce per il canale esteso come la probabilità di errore-per-parola all'uscita del canale non può essere arbitrariamente piccola se l'informazione media per simbolo all'ingresso eccede la capacità di canale (teorema inverso).

[2] Il lettore noti che l'unica ipotesi necessaria per la maggiorazione $\mathcal{I}(X^N; Y^N) \leq NC$ è che gli usi del canale siano indipendenti. Se le componenti dell'ingresso fossero indipendenti all'interno di ogni stringa, avremmo anche $\mathcal{H}(X^N) = N\mathcal{H}(X)$ e $\mathcal{I}(X^N; Y^N) = N\mathcal{I}(X;Y)$. Tale ipotesi non è necessariamente verificata se la stringa X^N è l'uscita di un codificatore che distribuisce le probabilità in maniera non fattorizzabile sulle parole, ovvero

$$\pi_x^N \neq \underbrace{\pi_x \otimes \pi_x \otimes \ldots \otimes \pi_x}_{N}. \tag{7.55}$$

L'indipendenza sarebbe comunque garantita tra stringhe successive.

7.6 Codifica di canale

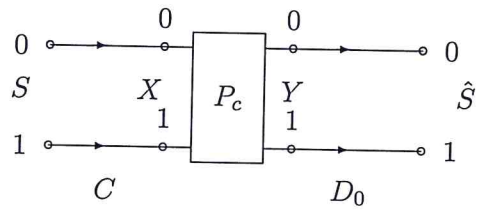
Nel modello di una catena di comunicazione, il cuore del sistema è sempre costituito da un canale rumoroso. Tale blocco di sistema può essere il risultato di molti stadi di elaborazione, codifica e decodifica e in genere fornisce un trasporto inaffidabile che potrebbe non essere migliorabile. Si pensi ai limiti di potenza imposti su canali trasmissivi elettromagnetici, magari su canali di comunicazione interplanetari, a sistemi cellulari o a reti di sensori. La questione è: possiamo comunicare comunque in maniera affidabile anche se il canale è inaffidabile? Al primo impatto la domanda sembrerebbe non avere senso. A pensarci bene però, se l'uscita del canale è in qualche modo statisticamente dipendente dall'ingresso, anche se magari debolmente dipendente, qualcosa sull'ingresso dovrebbe essere possibile ricostruire dall'osservazione dell'uscita. Allora il problema non è tanto se sia possibile fare una comunicazione affidabile, ma piuttosto quanta informazione è possibile trasportare. Evidentemente serve a una metodologia di riferimento per capire come quantificare e elaborare l'informazione da trasportare. La teoria dell'informazione e il sorprendente risultato del II teorema di Shannon, che presenteremo in seguito, forniscono la risposta definitiva: *è sempre possibile fare una comunicazione affidabile anche se il sistema interposto introduce incertezze.* In altre parole è sempre possibile ottenere una affidabilità arbitraria del trasporto, a patto che si "regoli" opportunamente l'informazione all'ingresso del canale e la si elabori in uscita.

Abbiamo visto come sia possibile in ricezione elaborare l'informazione in maniera ottima progettando un decisore che, implementando la regola MAP, dalla conoscenza delle caratteristiche probabilistiche di sorgente e canale, ci garantisce la minima probabilità di errore. Ma se la capacità di trasporto del canale è limitata, come predetto dalla capacità di canale, come fare a organizzare il sistema per un trasporto affidabile? Si intuisce come sia necessario "regolare," o "modulare", o "adattare" l'informazione all'ingresso del canale in modo tale da consentire al decodificatore di risalire in maniera sperabilmente univoca al messaggio trasmesso, anche se esso è stato ricevuto attraverso un sistema inaffidabile.

Le considerazioni appena esposte puntano chiaramente nella direzione di un sistema che preveda uno stadio di *codifica* tra la sorgente e il canale e un decodificatore in ricezione. Il *codificatore* dovrà essere opportunamente progettato per realizzare un adattamento dell'informazione alle caratteristice inaffidabili di trasporto del canale, tenendo conto che il ricevitore ne conosce la struttura e che è in grado di "inferire" sui possibili simboli trasmessi.

Prima di presentare la teoria generale, presentiamo degli esempi.

Esempio 7.5 Codice a ripetizione Consideriamo un canale binario simmetrico con probablità di errore $p = 0.1$ e simboli di ingresso e di uscita rispettivamente $\mathcal{X} = \{0,1\}$ e $\mathcal{Y} = \{0,1\}$. Il canale deve trasportare simboli provenienti da una sorgente S avente alfabeto $\mathcal{S} = \{0,1\}$ con simboli equiprobabili, $\Pi_S = \{0.5, 0.5\}$. La soluzione più immediata è collegare direttamente la sorgente al canale mediante lo schema complessivo riportato nella seguente figura.



Un codificatore tra S e X non potrebbe fare molto. Ricordiamo che un codificatore è un blocco deterministico che potrebbe quindi solo invertire i due simboli senza alcun evidente vantaggio. Il codificatore scelto è pertanto semplicemente $C = I_2$. Per il decodificatore la regola MAP equivale ad una regola ML in quanto i simboli in ingresso sono equiprobabili. Dalla matrice di canale

$$P_c = \begin{pmatrix} (1-p) & p \\ p & (1-p) \end{pmatrix} = \begin{pmatrix} 0.9 & 0.1 \\ 0.1 & 0.9 \end{pmatrix} \tag{7.58}$$

si evince immediatamente che il decisore ottimo è banalmente

$$D_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2. \tag{7.59}$$

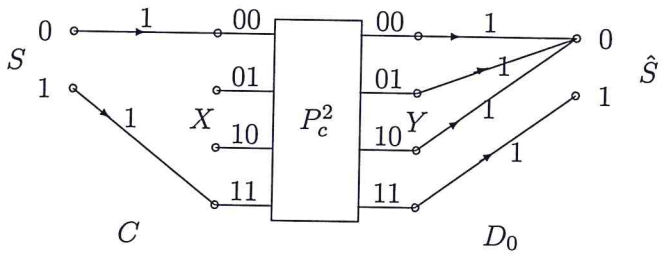
La matrice di canale complessiva è $P_t = P_c$ e la probabilità di errore complessiva $P(e) = p = 0.1$. Un segmento di una realizzazione delle sequenze di sorgente, uscita del codificatore, uscita del canale e del decodificatore sono qui riportate.

$$\begin{array}{lccccccc} \{s[k]\} & \ldots & 0 & 1 & 0 & 0 & 1 & 0 \ldots \\ \{x[k]\} & \ldots & 0 & 1 & 0 & 0 & 1 & 0 \ldots \\ \{y[k]\} & \ldots & 1 & 1 & 0 & 0 & 0 & 0 \ldots \\ \{\hat{s}[k]\} & \ldots & 1 & 1 & 0 & 0 & 0 & 0 \ldots \end{array} \tag{7.60}$$

Il canale ha introdotto due errori che si ripercuotono su due errori sull'uscita.

La questione è ora: come fare a migliorare le prestazioni se la probabilità di errore non è soddisfacente e il canale non può essere migliorato? Il canale potrebbe essere il sistema equivalente di stadi di modulazione su cui non è possibile intervenire. E' possibile ottenere una comunicazione più affidabile su tale canale? La risposta è affermativa e una possibile strada potrebbe essere quella di "rallentare" la sorgente riducendo l'entità di informazione presentata all'ingresso del canale. Lo schema più immediato è ripetere due volte il simbolo emesso (codice a ripetizione). Ovvero, quando la sorgente emette un bit, diciamo 0, il canale viene usato due volte con i simboli 0 e poi 0 di nuovo. Analogamente per il simbolo 1. Questa persistenza dovrebbe consentire al decodificatore una migliore inferenza sul simbolo di sorgente ogni due simboli osservati. Vediamo.

Lo cascata di codificatore, canale e decodificatore è rappresentato in figura.



Il codificatore utilizza solo due dei quattro simboli disponibili all'ingresso del canale esteso. La matrice del codificatore è

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{7.61}$$

La cascata di codificatore e canale ha matrice equivalente

$$CP_c^2 = \begin{pmatrix} (1-p)^2 & (1-p)p & p(1-p) & p^2 \\ p^2 & p(1-p) & (1-p)p & (1-p)^2 \end{pmatrix} = \begin{pmatrix} 0.8100 & 0.0900 & 0.0900 & 0.0100 \\ 0.0100 & 0.0900 & 0.0900 & 0.8100 \end{pmatrix}. \tag{7.62}$$

Poiché l'ingresso è a distribuzione uniforme la regola MAP per il ricevitore coincide con la regola MV. Guardando alle colonne di CP_c^2 scegliamo il ricevitore con matrice

$$D_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{7.63}$$

Si noti che in caso di ricezione dei simboli 01 e 10 la decisione per 0 o 1 ai fini della probabilità di errore media è equivalente per entrambi i casi. Si è scelto

pertanto di assegnare entrambi i simboli a 0. La matrice equivalente di tutta la cascata è

$$P_t = CP_c^2D_0 = \begin{pmatrix} (1-p)^2+(1-p)p+p(1-p) & p^2 \\ p^2+p(1-p)+(1-p)p & (1-p)^2 \end{pmatrix} \quad (7.64)$$

$$= \begin{pmatrix} 1-p^2 & p^2 \\ 2p-p^2 & (1-p)^2 \end{pmatrix} = \begin{pmatrix} 0.9900 & 0.0100 \\ 0.1900 & 0.8100 \end{pmatrix}. \quad (7.65)$$

La scelta del ricevitore asimmetrico ha prodotto un canale binario equivalente non simmetrico in cui il simbolo 0 è evidentemente più protetto avendo probabilità di errore condizionata $p^2 = 0.01$. Viceversa il simbolo 1 è meno protetto con probabilità di errore condizionata $2p - p^2 = 0.19$, addirittura peggiore del caso non codificato. La probabilità di errore media è

$$P(e) = 1 - P(c) = 1 - (1-p^2)\frac{1}{2} - (1-p)^2\frac{1}{2} = 1 - p = 0.1. \quad (7.66)$$

Il codice a ripetizione per $N = 2$ non ha prodotto alcun miglioramento in termini di probabilità di errore media. La ridondanza introdotta non consente una migliore inferenza sull'ingresso da parte del decodificatore. Un segmento possibile per le sequenze è

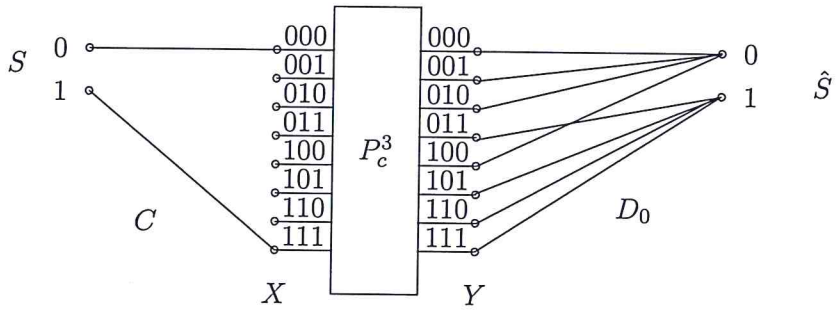
$$\begin{array}{lccccccccccccccc} \{s[k]\} & . & . & . & 0 & & 1 & & 0 & & 0 & & 1 & & 0 & & . & . & . \\ \{x[k]\} & . & . & . & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & . & . & . \\ \{y[k]\} & . & . & . & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & . & . & . \\ \{\hat{s}[k]\} & . & . & . & & 0 & & 0 & & 0 & & 0 & & 1 & & 0 & . & . & . \end{array} \quad (7.67)$$

Si notino i due errori sul canale e un errore sulla sequenza decodificata. Il lettore potrà facilmente vericare che anche la scelta del decisore

$$D_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad (7.68)$$

avrebbe portato alla stessa probabilità di errore media.

Non diamoci per vinti e proviamo ad aumentare l'ordine dell'estensione a $N = 3$. La seguente figura mostra lo schema equivalente del codice a ripetizione che per ogni bit d'ingresso, associa tre bit uguali a tre usi successsivi del canale.



La matrice del codificatore a monte del canale esteso di ordine tre è

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{7.69}$$

La cascata di codificatore e canale ha matrice equivalente

$$\begin{aligned} CP_c^3 &= \begin{pmatrix} (1-p)^3 & (1-p)^2p & p(1-p)^2 & (1-p)p^2 & p(1-p)^2 & p^2(1-p) & p^2(1-p) & p^3 \\ p^3 & p^2(1-p) & p^2(1-p) & p(1-p)^2 & (1-p)p^2 & (1-p)^2p & (1-p)^2p & (1-p)^3 \end{pmatrix} \\ &= \begin{pmatrix} 0.7290 & 0.0810 & 0.0810 & 0.0090 & 0.0810 & 0.0090 & 0.0090 & 0.0010 \\ 0.0010 & 0.0090 & 0.0090 & 0.0810 & 0.0090 & 0.0810 & 0.0810 & 0.7290 \end{pmatrix} \end{aligned} \tag{7.70}$$

Anche qui il ricevitore MAP coincide con il ricevitore ML e dall'esame delle colonne della matrice CP_c^3 è

$$D_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}. \tag{7.71}$$

E' interessante guardare alla natura della regola ML: il ricevitore sceglie il bit maggiormente presente nella terna binaria (regola a maggioranza). Si tratta della strategia più intuitiva - che è anche quella ottima. La matrice equivalente di tutta la cascata è

$$\begin{aligned} P_t &= CP_c^3D_0 = \begin{pmatrix} (1-p)^3 + 3p(1-p)^2 & p^3 + 3p^2(1-p) \\ p^3 + 3p^2(1-p) & (1-p)^3 + 3p(1-p)^2 \end{pmatrix} \\ &= \begin{pmatrix} 2p^3 - 3p^2 + 1 & -2p^3 + 3p^2 \\ -2p^3 + 3p^2 & 2p^3 - 3p^2 + 1 \end{pmatrix} = \begin{pmatrix} 0.9720 & 0.0280 \\ 0.0280 & 0.9720 \end{pmatrix}. \end{aligned} \tag{7.72}$$

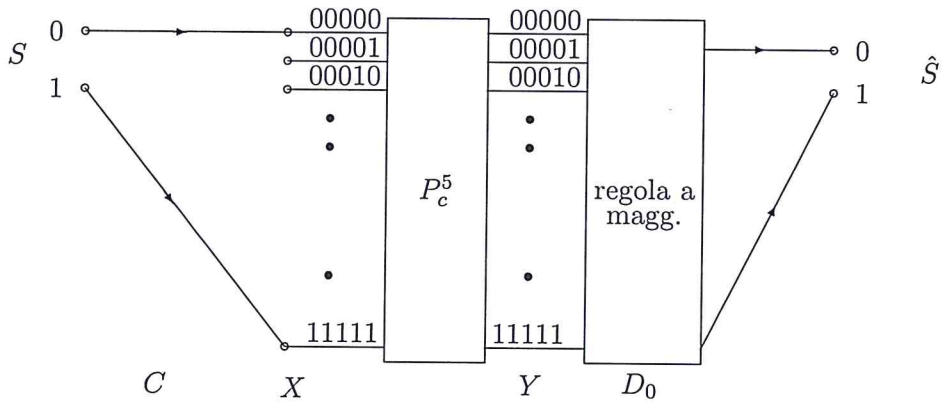
Il canale equivalente è un BSC e la cascata esibisce una probabilità di errore pari pari a $P(e) = -2p^3 + 3p^2 = 0.0280$, certamente inferiore al caso non codificato. Il

decodificatore corregge sempre quando c'è un errore sulla stringa. Un segmento possibile per le sequenze è

$$
\begin{array}{lccccccccccccccccccccc}
\{s[k]\} & . & . & . & 0 & & & 1 & & & 0 & & & 0 & & & 1 & & & 0 & & & . & . & . \\
\{x[k]\} & . & . & . & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & . & . & . \\
\{y[k]\} & . & . & . & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & . & . & . \\
\{\hat{s}[k]\} & . & . & . & & & 0 & & & 1 & & & 0 & & & 0 & & & 0 & & & 0 & . & . & .
\end{array}
\tag{7.73}
$$

Si notino i cinque errori sul canale e il singolo errore sulla sequenza decodificata (il numero degli errori è stato un pò esagerato in quanto solo un bit su 10 all'incirca dovrebbe essere errato).

Per migliorare ulteriormente le prestazioni si potrebbe considerare il codice per $N = 4$. La simmetria della parole binaria porta a concludere facilmente che le prestazioni non migliorerebbero rispetto al caso per $N = 3$. Il lettore attento verichi di persona una tale conclusione. Consideriamo per brevità direttamente $N = 5, 7, ...$ La figura seguente mostra la cascata di codificatore, canale e decodificatore per $N = 5$.



La descrizione esplicita matriciale già per $N = 5$ è un pò onerosa, anche se numericamente le matrici possono essere manipolate facilmente fino a N dell'ordine di qualche decina. Cerchiamo una descrizione diretta visto che sia il codificatore che il canale hanno un struttura molto semplice. Notiamo prima di tutto, così come nei casi precedenti che l'ingresso alla cascata codificatore-canale esteso è uniforme e pertanto la regola di decisione ottima è quella a massima verosimiglianza. Le funzioni di verosimiglianza per le 2^N possibili parole ricevute $\mathcal{Y}^N = \{y_1^N, y_2^N, ..., y_{2^N}^N\}$ dipendono solo dal numero di 0 o di 1 presenti nella stringa. Ovvero le probabilità condizionate possono essere scritte come

$$Pr\{y_i^N|00...0\} \;=\; Pr\{\#\ di\ 1\ in\ y_i^N|00...0\},$$

$$Pr\{y_i^N|11...1\} = Pr\{\#\ di\ 1\ in\ y_i^N|11...1\}. \tag{7.74}$$

Ma il numero di 1 in y_i^N dato 00...0 è pari al numero di errori che il canale ha introdotto. Analogamente il numero di 1 in y_i^N dato 11...1 è pari al numero di corretti trasporti che il canale ha realizzato, quindi denotando con

$$W(y_i^N) = \#\ di\ 1\ in\ y_i^N\ \ (peso\ di\ y_i^N), \tag{7.75}$$

abbiamo

$$\begin{aligned} Pr\{y_i^N|00...0\} &= p^{W(y_i^N)}(1-p)^{N-W(y_i^N)}, \\ Pr\{y_i^N|11...1\} &= (1-p)^{W(y_i^N)}p^{N-W(y_i^N)}. \end{aligned} \tag{7.76}$$

Il ricevitore deve decidere per 0 o 1 a seconda che la maggiore sia rispettivamente la prima o la seconda verosimiglianza. Ovvero

$$\begin{aligned} \hat{S} &= 0 \quad se \quad p^{W(y_i^N)}(1-p)^{N-W(y_i^N)} > (1-p)^{W(y_i^N)}p^{N-W(y_i^N)}, \\ \hat{S} &= 1 \quad se \quad p^{W(y_i^N)}(1-p)^{N-W(y_i^N)} < (1-p)^{W(y_i^N)}p^{N-W(y_i^N)}. \end{aligned} \tag{7.77}$$

La condizione può essere riscritta come

$$\begin{aligned} \hat{S} &= 0 \quad se \quad \left(\frac{p}{1-p}\right)^{2W(y_i^N)} > \left(\frac{p}{1-p}\right)^{N}, \\ \hat{S} &= 1 \quad se \quad \left(\frac{p}{1-p}\right)^{2W(y_i^N)} < \left(\frac{p}{1-p}\right)^{N}. \end{aligned} \tag{7.78}$$

Poiché $p/(1-p) < 1$, ovvero $p < 1/2$, [3] abbiamo la regola

$$\begin{aligned} \hat{S} &= 0 \quad se \quad W(y_i^N) < \frac{N}{2}, \\ \hat{S} &= 1 \quad se \quad W(y_i^N) > \frac{N}{2}. \end{aligned} \tag{7.79}$$

La regola ottenuta è anche una regola a maggioranza. Ad esempio per $N = 5$ se la stringa ricevuta contiene zero, uno o due 1, $\hat{S} = 0$, viceversa se contiene tre, quattro o cinque 1, $\hat{S} = 1$. La situazione di parità non può verificarsi poiché N è dispari. Anche il canale binario equivalente è facilmente calcolabile. Data la regola a maggioranza e la struttura simmetrica del BSC

$$\begin{aligned} Pr\{\hat{S} = 1|S = 0\} &= Pr\{\text{almeno } \frac{N+1}{2}\ bit\ in\ \ y_i^N\ pari\ a\ 1|S = 0\} \\ Pr\{\hat{S} = 0|S = 1\} &= Pr\{\text{almeno } \frac{N+1}{2}\ bit\ in\ y_i^N\ pari\ a\ 0|S = 1\} \end{aligned} \tag{7.80}$$

[3] E' ragionevole assumere che un canale binario abbia probabilità di errore $< 1/2$, poichè altrimenti la matrice di canale potrebbe essere ridefinita con i simboli invertiti.

Il canale binario equivalente è un BSC con

$$p_e = Pr\{\hat{S} = 1|S = 0\} = Pr\{\hat{S} = 0|S = 1\} = \sum_{i=\frac{N+1}{2}}^{N} \binom{N}{i} p^i (1-p)^{N-i}. \quad (7.81)$$

Il calcolo esplicito per $N = 1, 3, 5, 7$ fornisce i seguenti polinomi

$$\begin{array}{ll} N = 1 & p_e = p \\ N = 3 & p_e = p^2 - 2p^3 \\ N = 5 & p_e = 10p^3 - 15\ p^4 + 6p^5 \\ N = 7 & p_e = 35\ p^4 - 84\ p^5 + 154\ p^6 - 20\ p^7 \end{array} \quad (7.82)$$

In particolare nell'esempio $p = 0.1$ abbiamo $p_e = \{0.1, 0.0280, 0.0086, 0.0028\}$. Il miglioramento delle prestazioni è stato ottenuto grazie alla introduzione di *ridondanza*: per ogni simbolo di sorgente il canale viene usato N volte, con un *tasso di codifica* è pari a $R_c = \frac{1}{N}$. Il canale teoricamente ha una capacità di trasporto di NC bit, che nel caso di $p = 0.1$ vale $0.5310\ N$. La sorgente all'ingresso del codificatore ha una entropia pari a un bit, pertanto già per $N = 2$ il flusso all'ingresso ha un tasso di informazione inferiore alla capacità di canale. La figura 7.8 mostra l'andamento delle probabilità di errore al crescere di N, ovvero al decrescere del tasso. L'andamento in scala logaritmica è lineare, ma è molto distante dal limite teorico previsto dalla teoria dell'informazione che sancisce l'esistenza di un codificatore che genera una probabilità di errore praticamente nulla per flussi informativi al di sotto della capacità di canale (II teorema di Shannon, che sarà presentato in seguito). Quindi il codice a ripetizione non è molto efficiente e saranno necessarie delle strutture di codifica migliori per arrivare a probabilità di errore virtualmente nulle quando si è di poco al di sopra della capacità di canale.

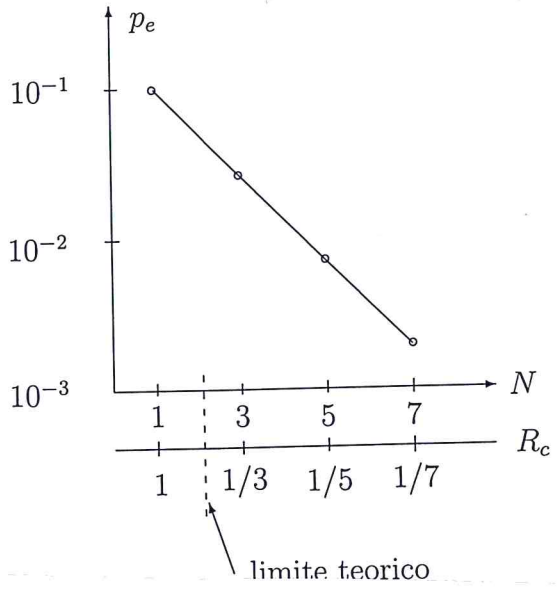


Figura 7.8: Le prestazioni del codice a ripetizione per il BSC con $p = 0.1$.

7.7 Schema generale

27

Lo schema generale di un sistema sorgente, codificatore, canale e decodificatore è mostrato in figura 7.9. Ad ogni intervallo T_s, la sorgente emette un simbolo $S[k]$ prelevandolo da un alfabeto $\mathcal{A} = \{a_1, ..., a_d\}$ con probabilità $\Pi_S = \{p_1, ..., p_d\}$. I simboli vengono organizzati in una stringa di lunghezza K per il codificatore. In generale la sorgente potrebbe emettere i simboli direttamente a blocchi e quindi in maniera non necessariamente indipendente come nella sorgente estesa di ordine K.

Il codificatore associa ad ogni stringa di K simboli di sorgente una stringa di N simboli prelevati da un alfabeto di codice $\mathcal{X} = \{x_1, ..., x_n\}$ che viene presentata al canale.

Assumiamo un tempo di riferimento per ogni simbolo x di T_c secondi.

~~I simboli $X[\ell]$ sono presentati all'ingresso del canale a intervalli di tempo T_c. Il canale, assunto qui senza memoria, associa ad ogni simbolo d'ingresso un simbolo d'uscita $Y[\ell]$ appartenente all'alfabeto $\mathcal{Y} = \{y_1, ..., y_m\}$.~~

Il canale in generale opera blocco per blocco trasformando la stringa di lunghezza N in una stringa di lunghezza M di simboli appartenenti all'alfabeto $\mathcal{Y} = \{y_1, ..., y_m\}$.
Il tempo di riferimento per i simboli di uscita al canale sia T_u.
Se il canale è assunto senza memoria $N = M$ e $T_c = T_u$, e ogni simbolo $x \in \mathcal{X}$ viene trattato singolarmente dal canale e trasformato in un simbolo $y \in \mathcal{Y}$.
In generale il canale però opera blocco per blocco e può avere un alfabeto di uscita diverso da $\mathcal{X}$ (si pensi ai canali con cancellazione).
Alla fine della catena la stringa di M simboli appartenenti a $\mathcal{Y}$ vengono "decodificati" in

una stringa di K simboli appartenenti allo stesso alfabeto $\mathcal{A}$ utilizzato dalla sorgente. L'obiettivo è evidentemente ottenere delle stringhe in uscita che siano una replica fedele delle stringhe di sorgente.

La sorgente emette un simbolo ogni T_s secondi e gruppi di K simboli vengono trasformati in stringhe di N simboli inviati sul canale ogni NT_c secondi. Deve pertanto essere verificata la relazione di continuità temporale

$$KT_s = NT_c. \tag{7.83}$$

Analogamente ai capi del canale bisogna avere $NT_c = MT_u$, anche se il caso tipico è $N = M$ e $T_c = T_u$.

Si definisce inoltre *rapporto di codifica* (o *coding rate*), il rapporto tra le frequenze di cifra all'ingresso e all'uscita del codificatore

$$R_c = \frac{\text{bit} - \text{rate all'ingresso del codificatore}}{\text{bit} - \text{rate all'uscita del codificatore}} = \frac{\log_2 d \,/T_s}{log_2 n/T_c} = \frac{\log_2 d}{log_2 n}\,\frac{T_c}{T_s}. \tag{7.84}$$

Usando la relazione di continuità temporale

$$R_c = \frac{\log_2 d}{log_2 n}\,\frac{K}{N}. \tag{7.85}$$

Nel caso tipico di alfabeti binari ($d = n = 2$) $R_c = \frac{K}{N}$.

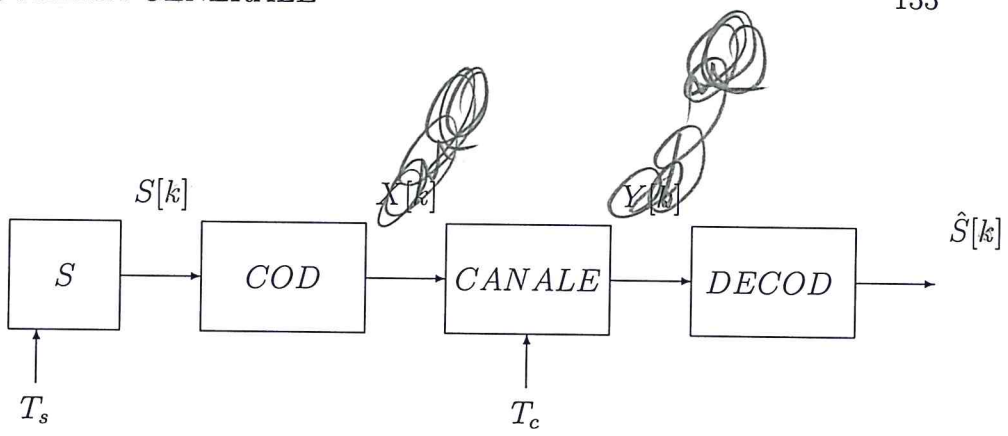


Figura 7.9: Lo schema generale di comunicazione con sorgente, codificatore, canale e decodificatore

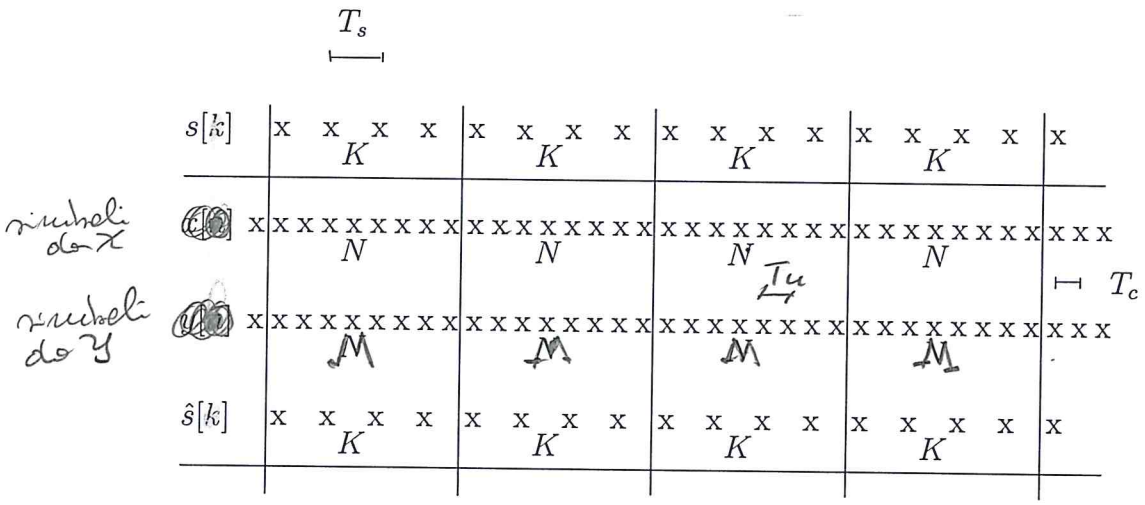


Figura 7.10: Il diagramma temporale dei simboli nella catena di comunicazione

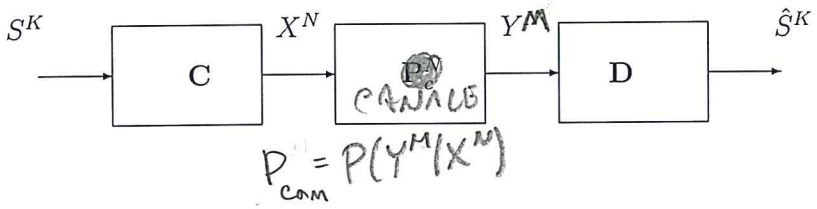


Figura 7.11: Lo schema equivalente della catena di comunicazione con riferimento ai ~~simboli estesi~~ blocchi di simboli.

La figura 7.11 mostra la catena di comunicazione con riferimento alle stringhe appartenenti agli alfabeti estesi, ovvero

$$S^K \in \mathcal{A}^K; \quad X^K \in \mathcal{X}^N; \quad Y^M \in \mathcal{Y}^M; \quad \hat{S}^K \in \mathcal{A}^K. \tag{7.86}$$

La matrice di canale P_{can} ha dimensioni $M^N \times m^M$ e contiene tutte le probabilità con cui le n^N stringhe X^N si trasformano nelle m^M stringhe Y^M.

Nel caso tipico in cui $M=N$ e il canale è senza memoria, ad ognuno indipendente corrisponde una matrice P_c di dimensioni $n \times m$ e P_{can} è il prodotto di Kronecker $P_{can} = \underbrace{P_c \otimes P_c \otimes \cdots \otimes P_c}_{N}$.

Il canale è assunto senza memoria e ha matrice di canale $\mathbf{P}_c^N$ di dimensioni $n^N \times m^N$ ottenuta dal prodotto di Kronecker di $\mathbf{P}_c$ con se stessa N volte. Il codificatore è una matrice $\mathbf{C}$ di dimensioni $d^K \times n^N$ e il decodificatore è una matrice $\mathbf{D}$ di dimensioni $m^M \times d^K$. Il canale equivalente tra S^K e $\hat{S}^K$ è la matrice $d^K \times d^K$

$$\mathbf{P}_t = \mathbf{C}\mathbf{P}_c^N\mathbf{D}. \tag{7.87}$$

Ogni volta che qualche simbolo (almeno uno) della parola $\hat{S}^K$ è diverso da S^K, si è verificato un errore di parola (*word-error*). La probabilità di errore a livello di parola (*word-error probability*) è quindi

$$P(e_w) = Pr\{S^K \neq \hat{S}^K\}. \tag{7.88}$$