

# Fondamenti di Telecomunicazioni

## Cheat Sheet

PROBABILITÀ densità di probabilità  $p_x(s)$   V.A. uniforme  $f_x(s) = \frac{1}{B-A}$  per  $s \in [A, B]$   valore atteso  $E(x) = \int f_x(s) \cdot s \, ds$

$$E(X+bY) = E(X)+bE(Y) \quad | \text{ potenz } E(X^2) = M_2 \quad | \quad V_{2x}(X) = E((X-m_x)^2) = \sigma^2 \quad | \quad \frac{N_0}{2} = \sigma^2 \quad | \quad p(x|y) = \frac{p(x,y)}{p(y)} \quad | \quad X, Y \sim N(Z=N_0 + Y - N_1(m_x+m_y, \sigma_x^2 + \sigma_y^2))$$

$$P(X, A) = Q\left(\frac{A - m_x}{\sigma_x}\right) \quad | \quad f_u(z) = \frac{1}{\sigma_x \sqrt{2\pi}} e^{-\frac{(z - m_x)^2}{2\sigma_x^2}}$$

$$\text{SEGNALI} \quad P_s([-T, T]) = E_s([-T, T]) \frac{1}{2T} \quad |E_{sin} = \frac{A^2 T}{2} \text{ se } f_0 > \frac{1}{T} \quad |E_{rect} = A^2 T \cdot t \text{ tring} \left( \frac{t-t_0}{T} \right) \quad |E = A^2 \frac{2B}{3} \text{ amplificazione di } 20 \text{ dB } r(t) = A_s(t) \quad |F_s = F_r = A^2 F_r \quad - \frac{(E_s)}{(E_s)} + (A^2)_{dB} = 20 \text{ dB}$$

$$\int \cos^2(x) dx = \frac{1}{2}(x + \sin x \cos x) + C \quad \left| \int_a^b f(x) g(x) dx = \left[ f(x)g(x) \right]_a^b - \int_a^b f'(x)g(x) dx \right.$$

$$\text{CANALI} \quad \text{RAME} \quad \left( \tilde{\alpha}_{Ch}(f_i) \right)_{dp} = \left( \tilde{\alpha}_{Ch}(f_i) \right)_{dP_{km}} \cdot (d)_{km} \sqrt{\frac{f}{f_i}}$$

$$\text{RADIO } (z_{ch})_{dB} = 32.4 + 20 \log_{10}(d)_{km} + 20 \log_{10}(f)_{MHz} - \left( g_{Ant, Tr} \right)_{dB} - \left( g_{Ant, Rx} \right)_{dB} \quad g_{Ant, Tx} = \frac{\pi r^2 A_{ant}}{c^2} f_0^2 \eta_{ant} \quad g_{Ant, Rx} = A_{ant, Rx}$$

$$\text{MAP} \quad \hat{s}_o = \arg \max \left( p(\text{simbolo}) \cdot p(u | s - \sqrt{E_s}) \right) \quad \text{densità di prob. del rumore}$$

ML (simboli equiprobabili)  $\hat{\Sigma}_0 = \arg \max_{\Sigma} \left( \text{pr}(\Sigma - \sqrt{E_S}) \right)$

MD (simboli equiprobabili + AWGN)  $\hat{x}_0 = \arg \min \|x - s_n\|^2$

## SCHEMA A

### BLOCCHI

The diagram illustrates the TD II structure. It shows the forward pass through layers  $\text{MLP}_1$ ,  $\text{MLP}_2$ , and  $\text{MLP}_3$  (represented by gray rectangles) receiving inputs  $x_{n+1}, \dots, x_m$ . The backward pass is shown using error terms  $E_{\theta_1}, E_{\theta_2}, E_{\theta_3}$  and weights  $s_{(t-KT)}$  to calculate gradients  $\frac{\partial L}{\partial \theta_i}$  for  $i=1, 2, 3$ .

$$P_{\text{bit}} = P(E) = Q\left(\frac{d}{2\sigma_w}\right)$$

$$\text{EQUIENERGETICHE} \quad \underline{\xi}_1 = [\sqrt{E_s}, 0] \quad \underline{\xi}_2 = [\rho \sqrt{E_s}, \pm \sqrt{E_s(1-\rho^2)}] \quad d^2 = 2 E_s(1-\rho) \quad P(E) = Q \left( \frac{\sqrt{E_s(1-\rho)}}{2d^2} \right)$$

$$\text{BPSK} \quad \left( s_i = A \cos(2\pi f_{\text{RF}} t_i), \quad s_{-i} = -A \cos(2\pi f_{\text{RF}} t_i) \quad s_{\text{RF}} \in [0, T] \right) \quad p_{-i} = 1 \quad E_s = \frac{A^2}{2} T \quad P(E) = Q\left(\sqrt{\frac{E_s}{\sigma_n^2}}\right)$$

$$\text{MOD. BIL. ORTOGONALE} \quad (s_x = A \cos(2\pi f_0 t), \quad s_y = A \sin(2\pi f_0 t)) \quad s_x, s_y \in [0, T] \quad p=0 \quad E_s = \frac{A^2}{2} T \quad P(E) = Q \left( \frac{E_s}{20 \cdot 3} \right)$$

$$\text{MODULAZIONI M-ARIE} \quad \frac{N_{\min}}{M} Q\left(\frac{d_{\min}}{2\sigma_w}\right) \leq \sum_{m=1}^M (n-1) Q\left(\frac{d_{m,n,m}}{2\sigma_w}\right) \leq P(E) \leq \frac{1}{M} \sum_{m=1}^M \sum_{n=1}^M Q\left(\frac{d_{m,n,m}}{2\sigma_w}\right) \leq \frac{1}{M} \sum_{m=1}^M (n-1) Q\left(\frac{d_{m,n,m}}{2\sigma_w}\right) \leq (n-1) Q\left(\frac{d_{\min}}{2\sigma_w}\right)$$

$$\text{ORTOGONALI} \quad (m \text{ segnali ortogonali}) \quad Q\left(\frac{E_s}{12\sigma^2}\right) \leq P(E) \leq (M-1)Q\left(\frac{E_s}{2\sigma^2}\right)$$

$$\text{BIORTOGONALI } \left( \frac{M}{2} \text{ segnali ortogonali, } \frac{M}{2} \text{ antipodali} \right) \quad Q\left(\frac{|E_S|}{2\sigma^2}\right) \leq P(E) \leq (M-2)Q\left(\frac{|E_S|}{2\sigma^2}\right) + Q\left(\frac{|E_S|}{\sigma^2}\right)$$

$$SE \text{ IN MAPPATURA DI GRAY} \quad P_{bit} = \frac{P(E)}{\log_2 M}$$

$$4\text{-PHASE SHIFT KEYING} \quad \left( s_m(t) = \cos(2\pi f_0 t + \varphi_m) \quad \varphi_m = \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\} \right) \quad \phi_1(t) = \cos(2\pi f_0 t) \quad \phi_2(t) = \sin(2\pi f_0 t)$$

$$\text{PULSE AMPLITUDE MOD. } \left( S_m = \alpha_m h_{T_p}(t) \quad \alpha_m = 2m-1-M \right) \quad E_{S_{\text{modulated}}} = \frac{M^2-1}{2} E_h \quad P(E) = 2 \left( 1 - \frac{1}{M} \right) Q \sqrt{\frac{E_s \cdot 3}{\sigma^2 (M^2-1)}}$$

$$\text{QUADRATURE AMPLITUDE MOD. } s_q(t) = A_m \cos(2\pi f_m t) - A_s \sin(2\pi f_s t) \quad |E_{q-1} = \frac{M-1}{2} E_s| \quad P_{q-1} = \frac{M-1}{2} E_s$$

$$\phi'(t) = -1(t) \cos(-\omega_0 t), \quad \phi(t) = 1(t) \sin(-\omega_0 t)$$

**QUANTIZZATORE**  $\Delta_q = \frac{E(x)}{E(e)} = \frac{\sigma_x}{\frac{\sigma_e}{\sqrt{2}\pi} \cdot 20} = 20 \log_{10} \frac{\sigma_x}{\sigma_e \sqrt{2\pi}} + 4.77 + 6.02 b$  |  $\Delta = \frac{2^b}{2b}$

**CODICE DI CANALE A BLOCCI**  $K \times n$  bit | errori rilevati  $d_{\min} - 1$  | errori corretti  $\frac{d_{\min}}{2} - 1$  (o  $\frac{d_{\min}-1}{2}$ ) |  $R = \frac{K}{n} \leq 1 - \frac{1}{n} \log_2 \sum_{i=1}^n p_i^{-1}$  bound di Hamming

**CODICE DI CANALE A BLOCCI LINEARE**  $\subseteq \mathbb{C}^k$ ,  $Hx = 0 \Leftrightarrow x \in \mathcal{E}$  |  $\mathcal{E} = \begin{bmatrix} I_n \\ A \end{bmatrix}$  |  $H = [A]_{n \times k}$  |  $d_{\min} \leq n-k+1$  bound di Singleton

$$d_{\min} = w_h(e) = \min_{\text{secl } \mathcal{E}} \|\mathbf{c}\|_h \leftarrow H \begin{pmatrix} \mathbf{c} \\ \mathbf{0} \end{pmatrix} = 0? , H \begin{pmatrix} \mathbf{0} \\ \mathbf{c} \end{pmatrix} = 0? , \dots$$

sono una base di  $\mathcal{E}$ , posso scambiare con combinazioni lineari ( $c_j = c_i + c_k$ )

$G = \begin{bmatrix} \mathbf{I}_n \\ A \end{bmatrix}$  scambiando le righe cambia il codice  $\Leftrightarrow$  scambiare le righe qui non le prestazioni  $\Leftrightarrow$  è equivalente a scambiare colonne di  $H$

**COSET**  $\mathcal{E} = Hy$ , il coset è  $\{\xi\}$  dove  $\xi_i = y_i + c_i$ . Il coset leader  $\mathcal{E}_{\text{min}}(y) = \text{zermf}(\|\xi\|_h)$

**CODICE DI HAMMING** le colonne di  $H$  sono tutte le sequenze di  $(n-k)$  bit non nulli  $H = \begin{bmatrix} \mathbf{I}_{n-k} & \mathbf{0}_{k \times k} \end{bmatrix}$   $\Leftrightarrow n = 2^{k-k} - 1$

il codice di Hamming soddisfa all'ugualanza il bound di Hamming  $d_{\min} = 3 \Leftrightarrow k=4$

**TEORIA DELL' INF.**  $i_x(z) = -\log_z p_x(z)$  |  $H(x) = E(i_x(z)) = \sum_{z \in \mathcal{X}} p_x(z) \cdot i_x(z)$  |  $0 \leq H(x) \leq \log_2 M$  ( $M$  cardinalità di  $\mathcal{X}$ )

$\max \{H(x), H(y)\} \leq H(x,y) \leq H(x) + H(y)$  |  $H(X|Y) = H(X,Y) - H(Y)$   
= se  $x$  e  $y$  indipendenti.  
due variabili è funzione deterministica dell'altra

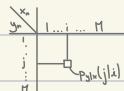
$$H(x,y) = \sum_{a \in A, b \in B} p_{xy}(a,b) i_{x,y}(a,b)$$

$$H(X|Y) = E_y(H(X|Y=y)) = \sum_{b \in B} p_y(b) \sum_{a \in A} p_{xy}(a|b) \log_a p_{xy}(a|b)$$

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) - H(Y) - H(X,Y)$$

In generale se  $x_n \rightarrow y_n$

**CAPACITÀ** tasso di informazione  $R(x) = \frac{H_s(x)}{T}$  |  $c = \max_{\{p_{ab}\}} \frac{I_a(x; y)}{T} = \max_{\{p_{ab}\}} R(f)$  (capacità o efficienza spettrale)



$$\text{canale binario senza memoria: } c = \frac{1}{T} \left[ -p_{00} \log_2 \frac{1}{p_{00}} - (1-p_{00}) \log_2 \frac{1}{1-p_{00}} \right]$$

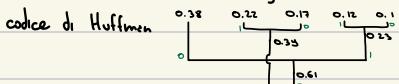
$$\text{canale AWGN: } c = \frac{1}{2T} \log_2 \left( 1 + \frac{E(s)}{E(w)} \right)$$

$$\text{canale con cancellazione: } c = \frac{1}{T} (1-a)$$



**CODIFICA DI SORGENTE**  $L_y = E_y(L(y)) = \sum_{b \in B} \frac{1}{M_y} \leq 1$  (= è ottimo) esiste un codice t.c.  $\frac{H(x)}{\log_2 M_y} \leq L_y \leq \frac{H(x)}{\log_2 M_y} + 1$

codice di Shannon  $L_i = \lceil \log_2 p_x(c_i) \rceil$  ottimo  $\Leftrightarrow p_x(c_i)$  potenze di 2



codice di Elias 1.  $L_i = \lceil \log_2 p_x(c_i) \rceil + 1$

2. Rappresento  $m_i$  in forma binaria  $m_i = 0.010011\dots$

3. Le parole associate è la parte dopo la virgola  $L_i = 010011$

**EFFICIENZA DI CODICE**  $0 \leq h = \frac{H(x)}{L_y \log_2 M_y} \leq 1 \Rightarrow h \geq \frac{H(x)}{H(x) + \log_2 M_y}$  ( $h$  aumenta al diminuire di  $M_y$ , ecco perché  $M_y=2$ )

$$= \frac{H(x)}{\log_2 M_y}$$



$$\text{Se } x \sim N(0, \sigma^2) \quad P(x > A) = Q\left(\frac{A - \mu}{\sigma}\right)$$

$y$	$Q(y)$	$y$	$Q(y)$	$y$	$Q(y)$
0.00	$5.000 \cdot 10^{-1}$	2.0	$2.275 \cdot 10^{-2}$	6.0	$9.866 \cdot 10^{-10}$
0.05	$4.801 \cdot 10^{-1}$	2.1	$1.786 \cdot 10^{-2}$	6.2	$2.823 \cdot 10^{-10}$
0.10	$4.602 \cdot 10^{-1}$	2.2	$1.390 \cdot 10^{-2}$	6.4	$7.769 \cdot 10^{-11}$
0.15	$4.404 \cdot 10^{-1}$	2.3	$1.072 \cdot 10^{-2}$	6.6	$2.056 \cdot 10^{-11}$
0.20	$4.207 \cdot 10^{-1}$	2.4	$8.198 \cdot 10^{-3}$	6.8	$5.231 \cdot 10^{-12}$
0.25	$4.013 \cdot 10^{-1}$	2.5	$6.210 \cdot 10^{-3}$	7.0	$1.280 \cdot 10^{-12}$
0.30	$3.821 \cdot 10^{-1}$	2.6	$4.661 \cdot 10^{-3}$	7.2	$3.011 \cdot 10^{-13}$
0.35	$3.632 \cdot 10^{-1}$	2.7	$3.467 \cdot 10^{-3}$	7.4	$6.809 \cdot 10^{-14}$
0.40	$3.446 \cdot 10^{-1}$	2.8	$2.555 \cdot 10^{-3}$	7.6	$1.481 \cdot 10^{-14}$
0.45	$3.264 \cdot 10^{-1}$	2.9	$1.866 \cdot 10^{-3}$	7.8	$3.095 \cdot 10^{-15}$
0.50	$3.085 \cdot 10^{-1}$	3.0	$1.350 \cdot 10^{-3}$	8.0	$6.221 \cdot 10^{-16}$
0.55	$2.912 \cdot 10^{-1}$	3.1	$9.676 \cdot 10^{-4}$	8.2	$1.202 \cdot 10^{-16}$
0.60	$2.743 \cdot 10^{-1}$	3.2	$6.871 \cdot 10^{-4}$	8.4	$2.232 \cdot 10^{-17}$
0.65	$2.578 \cdot 10^{-1}$	3.3	$4.834 \cdot 10^{-4}$	8.6	$3.986 \cdot 10^{-18}$
0.70	$2.420 \cdot 10^{-1}$	3.4	$3.369 \cdot 10^{-4}$	8.8	$6.841 \cdot 10^{-19}$
0.75	$2.266 \cdot 10^{-1}$	3.5	$2.326 \cdot 10^{-4}$	9.0	$1.129 \cdot 10^{-19}$
0.80	$2.119 \cdot 10^{-1}$	3.6	$1.591 \cdot 10^{-4}$	9.2	$1.790 \cdot 10^{-20}$
0.85	$1.977 \cdot 10^{-1}$	3.7	$1.078 \cdot 10^{-4}$	9.4	$2.728 \cdot 10^{-21}$
0.90	$1.841 \cdot 10^{-1}$	3.8	$7.235 \cdot 10^{-5}$	9.6	$3.997 \cdot 10^{-22}$
0.95	$1.711 \cdot 10^{-1}$	3.9	$4.810 \cdot 10^{-5}$	9.8	$5.629 \cdot 10^{-23}$
1.00	$1.587 \cdot 10^{-1}$	4.0	$3.167 \cdot 10^{-5}$	10	$7.620 \cdot 10^{-24}$
1.05	$1.469 \cdot 10^{-1}$	4.1	$2.066 \cdot 10^{-5}$	11	$1.911 \cdot 10^{-28}$
1.10	$1.357 \cdot 10^{-1}$	4.2	$1.335 \cdot 10^{-5}$	12	$1.776 \cdot 10^{-33}$
1.15	$1.251 \cdot 10^{-1}$	4.3	$8.540 \cdot 10^{-6}$	13	$6.117 \cdot 10^{-39}$
1.20	$1.151 \cdot 10^{-1}$	4.4	$5.413 \cdot 10^{-6}$	14	$7.794 \cdot 10^{-45}$
1.25	$1.056 \cdot 10^{-1}$	4.5	$3.398 \cdot 10^{-6}$	15	$3.671 \cdot 10^{-51}$
1.30	$9.680 \cdot 10^{-2}$	4.6	$2.112 \cdot 10^{-6}$	16	$6.389 \cdot 10^{-58}$
1.35	$8.851 \cdot 10^{-2}$	4.7	$1.301 \cdot 10^{-6}$	17	$4.106 \cdot 10^{-65}$
1.40	$8.076 \cdot 10^{-2}$	4.8	$7.933 \cdot 10^{-7}$	18	$9.741 \cdot 10^{-73}$
1.45	$7.353 \cdot 10^{-2}$	4.9	$4.792 \cdot 10^{-7}$	19	$8.527 \cdot 10^{-81}$
1.50	$6.681 \cdot 10^{-2}$	5.0	$2.867 \cdot 10^{-7}$	20	$2.754 \cdot 10^{-89}$
1.55	$6.057 \cdot 10^{-2}$	5.1	$1.698 \cdot 10^{-7}$	21	$3.279 \cdot 10^{-98}$
1.60	$5.480 \cdot 10^{-2}$	5.2	$9.964 \cdot 10^{-8}$	22	$1.440 \cdot 10^{-107}$
1.65	$4.947 \cdot 10^{-2}$	5.3	$5.790 \cdot 10^{-8}$	23	$2.331 \cdot 10^{-117}$
1.70	$4.457 \cdot 10^{-2}$	5.4	$3.332 \cdot 10^{-8}$	24	$1.390 \cdot 10^{-127}$
1.75	$4.006 \cdot 10^{-2}$	5.5	$1.899 \cdot 10^{-8}$	25	$3.057 \cdot 10^{-138}$
1.80	$3.593 \cdot 10^{-2}$	5.6	$1.072 \cdot 10^{-8}$	26	$2.476 \cdot 10^{-149}$
1.85	$3.216 \cdot 10^{-2}$	5.7	$5.990 \cdot 10^{-9}$	27	$7.389 \cdot 10^{-151}$
1.90	$2.872 \cdot 10^{-2}$	5.8	$3.316 \cdot 10^{-9}$	28	$8.124 \cdot 10^{-173}$
1.95	$2.559 \cdot 10^{-2}$	5.9	$1.818 \cdot 10^{-9}$	29	$3.290 \cdot 10^{-185}$
2.00	$2.275 \cdot 10^{-2}$	6.0	$9.866 \cdot 10^{-10}$	30	$4.907 \cdot 10^{-198}$

## 0. Prerequisiti - Probabilità

**Def** Dato un esperimento casuale (es. lancio di una moneta) possiamo definire lo spazio degli eventi, ovvero l'insieme dei possibili risultati.

Indichiamo questo insieme con  $S \subset \Omega$ .

**ES** Nell'esempio del lancio di una moneta  $\Omega = \{\text{testa, croce}\}$

**Def** Ogni risultato dell'esperimento (che diremo evento)  $X \in \Omega$  ha una certa probabilità di verificarsi  $P(X) \in [0,1]$

**PROP** -  $P(X \wedge Y) = \text{probabilità che } X \text{ e } Y \text{ si verifichino contemporaneamente}$

-  $P(X \vee Y) = \text{probabilità che o } X \text{ o } Y \text{ o entrambi si verifichino} = P(X) + P(Y) - P(X \wedge Y)$

-  $P(\emptyset) = 0$

### 0.1 Variabili Aleatorie

Spesso non siamo interessati alle probabilità che un evento dello spazio campionario si avveri, vogliamo cercare le probabilità secondo delle altre interrogazioni.

**ES** Lanciando due dadi qual è la probabilità che la loro somma sia 7?

**Def** Una variabile aleatoria è una funzione definita in uno spazio campionario  $\rightarrow$  valori reali  $X: \Omega \rightarrow \mathbb{R}$

Essa ha proprio il compito di mappare risultati di un'esperimento casuale in  $\mathbb{R}$ .

**ES** Lanciando due dadi qual è la loro somma?

$$(1,1) \xrightarrow{x} 2, (1,2) \xrightarrow{x} 3, \dots, (5,2) \xrightarrow{x} 7, \dots, (6,6) \xrightarrow{x} 12$$

**Def** Si dice alfabeto ( $A_X$ ) di una variabile aleatoria  $X$  la sua immagine (es.  $1, \dots, 12$ )

**Def**  $X$  si dice discreta se l'Im( $X$ ) è finito o numerabile. Altrimenti si dice continua.

(infiniti numerabili e non numerabili  $\rightarrow$  Hilbert Hotel  $\mathcal{O}$ )

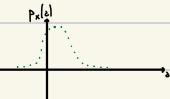
#### 0.1.1 Densità di Probabilità

**Def** La densità di probabilità di una variabile aleatoria è una funzione che associa ad ogni valore dell'alfabeto una probabilità:

$$p_X(z): A_X \rightarrow [0,1] \quad t.c. \quad p_X(z) = P(X=z)$$

**PROP** -  $P(X \neq z) = 1 - P(X=z)$

$$-\sum_{z \in A_X} p_X(z) = P\left(\bigcup_{z \in A_X} \{z\}\right) = 1$$



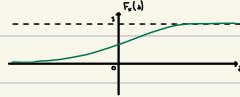
SOLO CONTINUE

**Def** Si dice funzione di distribuzione (cumulativa) di probabilità

$$F_X(z) = P(X \leq z)$$

**PROP** -  $\lim_{z \rightarrow -\infty} F_X(z) = 0, \lim_{z \rightarrow +\infty} F_X(z) = 1$

$$- P(X \in [A, B]) = P(X > A \wedge X < B) = F_X(B) - F_X(A)$$



**Def** Si dice densità di probabilità:

$$f_x(z) = \frac{dF_x(z)}{dz}$$

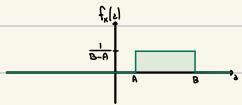
**PROP** -  $f_x(z) \geq 0 \quad \forall z \quad (f_x(z) \in [0, +\infty])$

$$- P(X \in [A, B]) = \int_A^B f_x(z) dz = F_x(B) - F_x(A)$$

$$- P(X \geq C) = \int_C^{+\infty} f_x(z) dz$$



**Def** Una variabile aleatoria  $X \in [A, B]$  si dice uniforme se  $f_x(z) = \frac{1}{B-A} \quad \forall z \in [A, B]$



### 0.1.2 Valore Atteso

**Def** Il valore atteso di una variabile aleatoria  $X$  è la media pesata di  $X$ .

$$E(X) = \sum_{z \in A_x} p_x(z) \cdot z = m_x \quad \text{se discreto}$$

$$E(X) = \int_{-\infty}^{+\infty} f_x(z) \cdot z dz \quad \text{se continuo}$$

**PROP** -  $E(zX+bY) = zE(X) + bE(Y)$ ,  $E$  è lineare

- Se  $g(X)$  una variabile aleatoria ( $Y$ )

$$E(g(X)) = \sum_{z \in A_x} p_x(z) \cdot g(z) = m_g \quad / E(g(X)) = \int_{-\infty}^{+\infty} f_x(z) g(z) dz = m_g$$

**Def** La potenza di una variabile aleatoria è  $E(X^2) = \sum_{z \in A_x} p_x(z) z^2 = M_x$  /  $E(X^2) = \int_{-\infty}^{+\infty} f_x(z) z^2 dz = M_x$

**Def** La varianza di una variabile aleatoria è  $E((X-m_x)^2) = \sigma_x^2$

dove  $\sigma_x$  è la deviazione standard (o varianza)

**OSS**  $E((X-m_x)^2) = E(X^2 - m_x^2 - 2m_x X) = E(X^2) + E(m_x^2) - 2m_x E(X) = M_x + m_x^2 - 2m_x^2 = M_x - m_x^2$

$$\Rightarrow M_x = m_x^2 + \sigma_x^2$$

**Def** Due variabili aleatorie  $X$  e  $Y$  si dicono indipendenti se:

$$p_{xy}(z, b) = P(X=z \text{ e } Y=b) = P(X=z) \cdot P(Y=b) \Rightarrow E(X \cdot Y) = E(X) \cdot E(Y) \quad \forall (z, b) \in A_x \times A_y$$

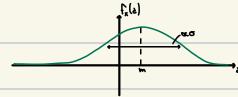
**Def** Date due variabili aleatorie  $X, Y$  legate tra loro, si dice probabilità condizionata

$$P(X=z | Y=b) = \frac{P(X=z, Y=b)}{P(Y=b)} \quad \begin{array}{l} \text{densità} \\ \text{probabilità} \end{array} \quad \begin{array}{l} z=x \text{ e } y=b \text{ avvengono} \\ \text{congiunti} \quad \text{contemporaneamente} \end{array}$$

### 0.2 Variabili Aleatorie Gaussiane

**Def** Diciamo che  $X \sim N(m_x, \sigma_x^2)$  se  $f_x(z) = \frac{1}{\sqrt{2\pi}\sigma_x} e^{-\frac{1}{2}(\frac{z-m_x}{\sigma_x})^2}$

dove  $m_x$  media e  $\sigma_x$  deviazione standard



**PROP** - Somma di variabili aleatorie gaussiane

Siano  $X \sim N(m_x, \sigma_x^2)$  e  $Y \sim N(m_y, \sigma_y^2)$

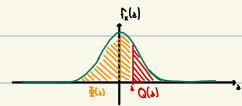
$$Z = X+Y \sim N(m_x+m_y, \sigma_x^2 + \sigma_y^2)$$

$$E(Z) = E(X+Y) = E(X) + E(Y)$$

$$\begin{aligned} \text{DIM } E(X+Y) &= \int_{-\infty}^{+\infty} (z+b) f_x(z) f_y(b) dz db \\ &= \int_{-\infty}^{+\infty} z f_x(z) f_y(b) dz db + \int_{-\infty}^{+\infty} b f_x(z) f_y(b) dz db \\ &= \left[ \int_{-\infty}^{+\infty} z f_x(z) dz \right] f_y(b) + \left[ \int_{-\infty}^{+\infty} b f_y(b) db \right] f_x(z) \\ &= m_x + m_y \end{aligned}$$

**Def** Una variabile aleatoria gaussiana si dice standard (o normale) se ha  $m_x=0$  e  $\sigma_x=1$

Calcolare i valori di  $P(X \leq z) = \Phi(z)$  e  $P(X \geq z) = Q(z)$  è difficile. Esistono delle tabelle.



**oss** Quindi  $P(X \in [A, B]) = Q(A) - Q(B) = \Phi(B) - \Phi(A)$

**oss** È possibile usare queste tabelle anche per variabili aleatorie gaussiane non standard  $X \sim N(m_x, \sigma_x^2)$

$$P(X \geq z) = \int_z^{+\infty} f_x(z) dz = \int_z^{+\infty} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}(\frac{z-m_x}{\sigma})^2} dz = \int_{\frac{z-m_x}{\sigma}}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}b^2} db = \Phi\left(\frac{m_x-z}{\sigma}\right)$$

pongo  $b = \frac{z-m_x}{\sigma}$   
 $f_x(z) dz = \sigma db$

## O. Prerequisiti - Segnali

I segnali sono funzioni del tempo, discrete o continue, a valori in  $\mathbb{C}$ .

$x: I \rightarrow \mathbb{C}$  dove  $I \subseteq \mathbb{R}$  un intervallo di tempo finito o infinito



TEMPO	
ANALOGICO	
T. CONTINUO	V. CONTINUI
V. CONTINUI	
DIGITALE	V. DISCRETI
	T. DISCRETO
	V. CONTINUI
	T. CONTINUO
	V. DISCRETI

VALORI:

**Def** Il supporto di un segnale è l'insieme di istanti nel tempo in cui il segnale è non nullo.  $|t: s(t) \neq 0|$



**Def** Un segnale si dice causale se ha supporto in  $[0, +\infty)$

**Def** Diciamo energia di un segnale

$$E_s = \int_{-\infty}^{+\infty} s^2(t) dt \quad \text{tempo continuo} \quad [E_s] = V^2 s \quad (\text{ipotizzando } [s(t)] = V)$$

$$E_s = \sum_{n=-\infty}^{+\infty} s^2(nT) \quad \text{tempo discreto}$$

**Def** Definiamo la potenza media del segnale  $s(t)$  nell'intervallo di tempo  $[-T, T]$

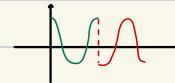
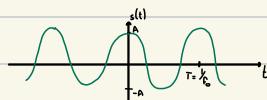
$$P_s([-T, T]) = \int_{-T}^T s^2(t) dt \cdot \frac{1}{2T} \quad [P_s] = V^2$$

SINUSOIDI

$$s(t) = A \cos(2\pi f t + \varphi) \quad \begin{matrix} \text{frequenza} \\ \text{Amplitude} \\ \text{Phase} \end{matrix}$$

$$E_{\text{sinusoida}} = \frac{A^2 T}{2}$$

es Trasmissione di bit tramite inversione di ampiezza



## RETTOANGOLO

$$\text{rect}(t) = \begin{cases} 1 & t \in [-\frac{T}{2}, \frac{T}{2}] \\ 0 & \text{altrimenti} \end{cases}$$

ritardo  
Ampiezza  
lunghezza

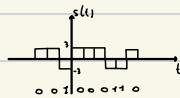


$$E_{\text{rect}} = A^2 T$$

es Trasmissione di bit tramite inversione di ampiezze

$$s(t) = 3 \text{rect}\left(\frac{t - \frac{T_2}{2}}{T}\right) + 3 \text{rect}\left(\frac{t - \left(\frac{T_2}{2} + \frac{T_1}{2}\right)}{T}\right) + 3 \text{rect}\left(\frac{t - \left(2T + \frac{T_1}{2}\right)}{T}\right) - 3 \text{rect}\left(\frac{t - \left(3T + \frac{T_1}{2}\right)}{T}\right)$$

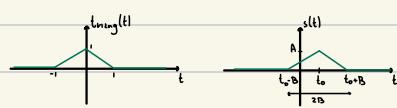
$$= \sum_{n=-\infty}^{+\infty} 3 \delta_n \text{rect}\left(\frac{t - \left(nT + \frac{T_1}{2}\right)}{T}\right) \quad \delta_n \in \{-1, +1\}$$



## TRIANGOLARE

$$\text{triang}(t) = \begin{cases} \frac{t_0}{t-t_0} & t \in [0, t_0] \\ \frac{t_0 - t}{t_0 - t_1} & t \in [t_1, t_0] \\ 0 & \text{altrimenti} \end{cases}$$

ritardo  
Ampiezza  
Base  $\frac{t_0 - t_1}{2}$



$$E_{\text{triang}} = A^2 \frac{2B}{3}$$

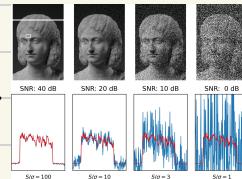
## 0.1 Il Decibel

Il Decibel (dB) è un modo per esprimere una quantità adimensionale, lo useremo per esprimere rapporti di energia o potenza

Dati due segnali  $s(t)$  e  $w(t)$  con energie  $E_s$  e  $E_w$

$$\left(\frac{E_s}{E_w}\right)_{\text{dB}} = 10 \log_{10} \left(\frac{E_s}{E_w}\right) = 10 \log_{10} (E_s) - 10 \log_{10} (E_w)$$

$$\left(\frac{P_s}{P_w}\right)_{\text{dB}} = 10 \log_{10} \left(\frac{P_s}{P_w}\right) = 10 \log_{10} (P_s) - 10 \log_{10} (P_w)$$



Permette di confrontare due segnali, siamo in particolare interessati al SNR (signal to noise ratio), esprime quanta energia sto usando per andare sopra il rumore di fondo.

ES

Il segnale  $x(t)$  viene amplificato/attenuato di 20dB

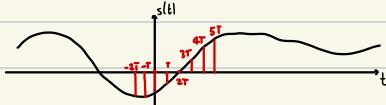
$$s_r(t) = Ax(t) \quad s_i(t) = \frac{1}{A}x(t)$$

$$E_s = \int_{-\infty}^{+\infty} A^2 x^2(t) dt = A^2 E_x \Rightarrow E_s = A^2 E_x \Rightarrow \left(\frac{E_s}{E_x}\right)_{\text{dB}} = \left(\frac{A^2}{1}\right)_{\text{dB}} = 10 \log_{10} A^2 = 20 \log_{10} A = 20 \text{ dB} \Rightarrow A = 10$$

## 0.2 Campionamento

Dato un segnale a tempo continuo  $s(t)$ , la sua versione campionata, con periodo (o quanto) di campionamento  $T$ .

è il segnale a tempo discreto (ma sempre a valori continui).



### 0.3 Interpolazione

L'operazione inversa del campionamento, dato un segnale a tempo discreto  $x(nT)$  l'interpolazione fornisce il segnale a tempo continuo.

$$s(t) = \sum_{n=-\infty}^{\infty} x(nT) h(t-nT)$$

dove  $h(t)$  è un segnale a tempo continuo detto risposta impulsiva dell'interpolatore

#### 0.3.1 Interpolatore a Tenuita

$$\text{Utilizzo } h(t) = \text{rect}\left(\frac{t-\frac{T}{2}}{\frac{T}{2}}\right)$$

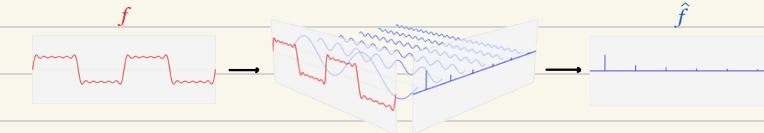


È semplice perché in ogni istante ho un solo segnale nella sommatoria



### 0.4 La trasformata di Fourier

La trasformata di Fourier trasforma i segnali dal dominio del tempo al dominio delle frequenze, in particolare, le frequenze e ampiezze delle sinusoidi che permettono di ricostruire il segnale.



Per segnali a tempo continuo la trasformata di un segnale  $s(t)$  è:

$$S: \mathbb{R} \rightarrow \mathbb{C} \quad S(f) = \int_{-\infty}^{+\infty} s(t) e^{-2\pi f t} dt \quad (f \text{ è la frequenza})$$

$$\text{L'intertrasformata di } S(f) \text{ è } s(t) = \int_{-\infty}^{+\infty} S(f) e^{2\pi f t} df$$



**Def** Diciamo ampiezze di bande le lunghezze dell'intervallo di frequenze in cui c'è il segnale.

**oss** Siamo interessati a segnali con ampiezze di bande finite. Questo perché trasmettendo la trasformata del segnale e campionando a frequenze doppie di quelle massime di trasmissione riusciamo a recuperare tutta l'informazione (garantito dal teorema di Nyquist-Shannon)

### 0.5 Spazio Vettoriale di Segnali a Energia Finita

L'insieme dei segnali  $\{s(t) : E_s < \infty\}$  è uno spazio vettoriale

**SOMMA**

La somma di due segnali  $x_1(t)$  e  $x_2(t)$  è  $y(t) = x_1(t) + x_2(t)$   $\forall t$ .

$x_1(t)$  e  $x_2(t)$  hanno energia finita allora  $y(t)$  ha energia finita

## PRONOTTO SCALARE - VETTORE

Se  $x(t)$  ha energia finita  $y(t) = \alpha x(t)$

$$\text{dim } E_y = \int_{-\infty}^{\infty} x^2(t) dt = \alpha^2 \int_{-\infty}^{\infty} x^2(t) dt = \alpha^2 E_x < \infty$$

## PRODOTTO INTERNO

$$\langle x(t), y(t) \rangle = \int_{-\infty}^{\infty} x(t) y(t) dt$$

### PROP

- $\langle x(t), x(t) \rangle = \int_{-\infty}^{\infty} x^2(t) dt = E_x < \infty$

- $\langle x(t), x(t) \rangle = 0 \iff x(t) = 0$

- $\langle \alpha x(t) + \beta y(t), z(t) \rangle = \alpha \langle x(t), z(t) \rangle + \beta \langle y(t), z(t) \rangle$

## ES



$$\langle x(t), y(t) \rangle = \int_{-\infty}^{\infty} x(t) y(t) dt = \int_0^{\infty} 1 \cdot 1 dt = 0$$

I due vettori sono ortogonali.

**Def** La norma di un segnale  $x(t)$  è

$$\|x(t)\| = \sqrt{\langle x(t), x(t) \rangle} = \sqrt{E_x}$$

## 0.5.1 Base Ortonormale dello Spazio

Ovvero un insieme di segnali  $\{x_i(t)\}$

tali che: -  $\langle x_i(t), x_j(t) \rangle = 0 \quad \forall i \neq j$

- $\|x_i(t)\| = 1$  (energia unitaria)



## 0.5.2 Sottospazio Generato da M Segnali

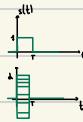
Dati  $M$  segnali  $s_1(t), \dots, s_M(t)$  (di energia finita) allora

$$V = \{s(t) : s(t) = \sum_{m=1}^M a_m s_m(t), \forall a_m \in \mathbb{R}\}$$

è un sottospazio vettoriale dello spazio dei segnali ad energia finita di dimensione  $\leq M$ .

## ES

$$s_1(t) = \text{rect}\left(\frac{t-T}{T}\right)$$



$$\|s(t)\| = 2 \|s_1(t)\|$$

## 0.5.3 Base del Sottospazio Generato da M Segnali

Dato un sottospazio vettoriale  $V$  generato da  $M$  vettori.

Sì dice base di  $V$  un insieme di vettori  $\{\phi_1(t), \dots, \phi_I(t)\}$  dove  $\phi_i(t) \in V$

$$V = \{s(t) : s(t) = \sum_{i=1}^I s_i \phi_i(t) \longleftrightarrow (s_1, \dots, s_I) \text{ vettore euclideo}$$

Allora  $\dim(V) = I \leq M$

OSS

Esiste un'isomorfismo (un rapporto 1:1) tra il sottospazio dei segnali  $V$  e lo spazio euclideo di dimensione  $I$

PROP  $E_x = \|x(t)\|^2 = \|\underline{x}\|^2$  vettore euclideo corrispondente a  $x(t)$ )

$$\text{DIM } \|x(t)\|^2 = \int_{-\infty}^{+\infty} x^2(t) dt = \left[ \left( \sum_{i=1}^I x_i \phi_i(t) \right)^2 \right] dt = \int_{-\infty}^{+\infty} \sum_{i=1}^I x_i^2 \phi_i^2(t) dt = \sum_{i=1}^I x_i^2 = \|\underline{x}\|^2$$

questo perché tutte le somme miste sono nulle

$$\int_{-\infty}^{+\infty} x_i x_j \phi_i(t) \phi_j(t) dt = 0 \text{ se } i \neq j$$

sono ortogonali

OSS - calcolo dei coefficienti  $x_1, \dots, x_I$  de  $x(t)$

$x_i = \langle x(t), \phi_i(t) \rangle$  ovvero la proiezione di  $x(t)$  su  $\phi_i(t)$

PROP

La distanza è lo stesso nello spazio dei segnali e in quello euclideo corrispondente.

$$d(x, y) = \|x - y\| = d(x(t), y(t)) = \|x(t) - y(t)\|$$

#### 0.5.4 Ortonormalizzazione di Gram-Schmidt

Per il sottospazio vettoriale generato dai segnali  $s_1(t), \dots, s_n(t)$  possiamo calcolare

una base ortonormale  $\phi_1(t), \dots, \phi_n(t)$

$$1) \text{ se } s_1(t) \neq 0 \quad \phi_1(t) = \frac{s_1(t)}{\sqrt{E_{s_1}}} \quad (\|\phi_1(t)\| = 1)$$

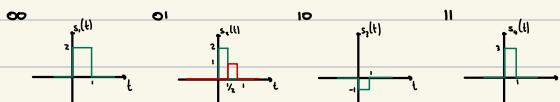
$$2) \phi_2(t) = s_2(t) - \langle \phi_1(t), s_2(t) \rangle \phi_1(t)$$

$$\text{se } \phi_2(t) \neq 0 \quad \phi_2(t) = \frac{\phi_2(t)}{\sqrt{E_{\phi_2}}}$$

$$n) \phi_n(t) = s_n(t) - \sum_{i=1}^{n-1} \langle \phi_i(t), s_n(t) \rangle \phi_i(t)$$

$$\text{se } \phi_n(t) \neq 0 \quad \phi_n(t) = \frac{\phi_n(t)}{\sqrt{E_{\phi_n}}}$$

ES - ortonormalizzazione di gram-schmidt



$$s_1(t) = 2 \operatorname{rect}(t - \frac{1}{2})$$

$$s_2(t) = 2 \operatorname{rect}\left(\frac{t - \frac{1}{2}}{\frac{1}{2}}\right) + \operatorname{rect}\left(\frac{t - \frac{3}{2}}{\frac{1}{2}}\right) = \operatorname{rect}(t - \frac{1}{2}) + \operatorname{rect}(\frac{t - \frac{3}{2}}{\frac{1}{2}})$$

$$s_3(t) = -\operatorname{rect}(t - \frac{1}{2})$$

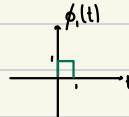
$$s_4(t) = 3 \operatorname{rect}(t - \frac{1}{2})$$

Costruisco una base ortonormale con il procedimento di Gram-Schmidt

$$1) E_{s_1} = \int s_1^2(t) dt = 4 \quad \left( \begin{array}{c} \text{red} \\ \text{white} \end{array} \right)$$

$$\phi_1(t) = \frac{s_1(t)}{\sqrt{E_{s_1}}} = \text{rect}(t - \frac{1}{2})$$

$$E_{\phi_1} = \int \text{rect}^2(t - \frac{1}{2}) dt = 1 \quad \left( \begin{array}{c} \text{white} \\ \text{red} \end{array} \right)$$



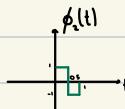
$$2) \langle s_2(t), \phi_1(t) \rangle = \int s_2(t) \phi_1(t) dt = 2,5 \leftarrow \text{errore di } s_2$$

$$\phi_2'(t) = s_2(t) - \langle s_2(t), \phi_1(t) \rangle \phi_1(t)$$

$$= \text{rect}(t - \frac{1}{2}) + \text{rect}\left(\frac{t - \frac{1}{2}}{\frac{1}{2}}\right) - 1.5 \text{rect}(t - \frac{1}{2}) \\ = -0.5 \text{rect}(t - \frac{1}{2}) + \text{rect}\left(\frac{t - \frac{1}{2}}{\frac{1}{2}}\right)$$

$$\left( \begin{array}{c} \text{red} \\ 0.5 \\ \text{white} \end{array} \right) + \left( \begin{array}{c} \text{white} \\ 1 \\ \text{red} \end{array} \right) = \left( \begin{array}{c} \text{red} \\ 0.5 \\ \text{white} \\ -0.5 \\ \text{red} \end{array} \right) \rightarrow \left( \begin{array}{c} \text{red} \\ 0.5 \\ \text{white} \\ -0.5 \\ \text{red} \\ \text{white} \end{array} \right) \quad E_{\phi_2'} = 0.25 = \frac{1}{4}$$

$$\phi_2(t) = \frac{\phi_2'(t)}{\sqrt{E_{\phi_2'}}} = -\text{rect}(t - \frac{1}{2}) + 2 \text{rect}\left(\frac{t - \frac{1}{2}}{\frac{1}{2}}\right)$$



$$3) \langle s_3(t), \phi_2(t) \rangle = \int s_3(t) \phi_2(t) dt = 0$$

$$\langle s_3(t), \phi_1(t) \rangle = \int s_3(t) \phi_1(t) dt = -1$$

$$\phi_3'(t) = s_3(t) - \langle s_3(t), \phi_1(t) \rangle \phi_1(t) - \langle s_3(t), \phi_2(t) \rangle \phi_2(t) \\ = -\text{rect}(t - \frac{1}{2}) + \text{rect}(t - \frac{1}{2}) = 0$$

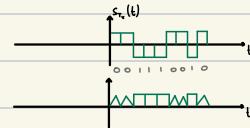
$$4) s_q(t) = 3\phi_1(t) + 0 \cdot \phi_2(t)$$

Quindi  $\{\phi_1(t), \phi_2(t)\}$  base ortonormale

## 1. Modulazione Digitale

Operazione di trasmissione di un segnale digitale (una sequenza di bit)

su un canale analogico. Con l'obiettivo di recuperare il messaggio al ricevitore.



### 1.1 Introduzione

Nel corso tratteremo la trasmissione di informazioni attraverso dei canali.



Questo schema rappresenta ogni trasmissione di informazione (radio, CPU-RAM). Vogliamo idealmente  $m = \hat{m}$

$$r(t) = A s_m(t - t_0) + w(t)$$

- A: scalamento dell'ampiezza.

L'antenna ricevente riceve una piccola parte dell'energia dell'antenna trasmettente.

-  $t_0$ : ritardo di propagazione ( $t_0 = \frac{d}{c}$ , c=velocità della luce, d=distanza)

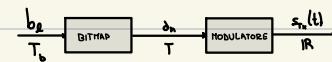


-  $w(t)$ : disturbo, rumore

Visto che è ignoto ne dà una descrizione statistica:  $w(t) \sim N(0, \sigma_w^2)$  Vt ( $w(t_1)$  e  $w(t_2)$  v.r. indipendenti Vt, t<sub>1</sub>, t<sub>2</sub>)

Viene detto Additive white gaussian noise (AWGN) perché contiene tutte le frequenze.

### 1.1.1 Trasmettitore



$b_n$ : sequenza di bit (il periodo di  $T_b$ ),  $b_n \in \{0, 1\}$

$s_m$ : sequenza di simboli appartenenti ad un alfabeto  $s_m \in \{1, 2, \dots, M\} = A$  (l'alfabeto) (il periodo di  $T$ ),  $|A| = M$

**Def** Lo bitmap converte un certo numero di bit in un elemento di un'alfabeto.

**OSS** - Ogni simbolo rappresenta  $\log_2 M$  bit

- Tra  $T$ ,  $T_b$  ed  $M$  vale la relazione:  $T = T_b \log_2 M$

- Se  $M=2$  parliamo di modulazione binaria, altrimenti è detta modulazione M-aria.

**Def** Il modulator converte gli elementi dell'alfabeto in segnali:

$$s_{tx}(t) = \sum_{n=-\infty}^{\infty} s_{m_n}(t-nT)$$

**OSS** Idealmente vogliamo segnali che non si sovrappongono, quindi di sostegno  $T$

### 1.1.2 Canale Tramssessivo

Esistono vari modelli del canale:

- IDEALE

$$r(t) = s_{m_n}(t) \quad \text{ricevuto = trasmesso}$$

- CANALE RUMOROSO (AWGN)

$$r(t) = s_{m_n}(t) + w(t)$$

$w(t) \sim N(0, \sigma_w^2)$  indipendente per ogni  $t$



- CANALE CON ATTENUAZIONE E RUMORE

$$r(t) = A s_{m_n}(t) + w(t)$$

- CANALE DISPERSIVO O MULTI-CAMMINO

$$r(t) = \sum_{n=1}^N A_n s_{m_n}(t-T_n) + w(t)$$

Il segnale viene ripetuto più volte in tempi diversi (come l'eco della voce in montagna)

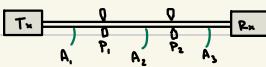
ES

$$r(t) = 1 s_{m_1}(t) + 0.5 s_{m_2}(t-3) + 2 s_{m_3}(t-9)$$



Di seguito alcune modellizzazioni di canali reali:

## TRASMISSIONE SU CAVO DI RAME



$$P_{R_x} = \frac{1}{A_1} P_{T_x} \Rightarrow P_{R_x} = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} P_{T_x} = \frac{1}{2^3} P_{T_x} = \frac{1}{A_1^3} P_{T_x}$$

$$\left( \frac{P_{T_x}}{P_{R_x}} \right)_{dB} = (A)^{dB} = 10 \log_{10} A^3 = 3 \cdot 10 \log_{10} A_1 = 3 \cdot (A_1)^{dB} = (\epsilon_{ch}(f))^{dB}_{km}$$

attenuazione per unità di cavo ( $\epsilon_{ch}(f)$ )<sub>dB/km</sub>  
di unità ( $A$ )<sub>km</sub>

$$\text{In generale } (\epsilon_{ch}(f))_{dB} = (\epsilon_{ch}(f))_{dB_{km}} (d) = (\epsilon_{ch}(f_i))_{dB_{km}} (d)_{km} \sqrt{\frac{F}{F_i}}$$

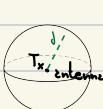
dove  $f$ : frequenza portante

$f_i$ : frequenza di riferimento

Per il rame  $(\epsilon_{ch}(f))_{dB_{km}} \approx (1,2) \text{ dB/km}$

Per la fibra ottica  $(\epsilon_{ch}(f))_{dB_{km}} \approx 0.2 \text{ dB/km}$

## COLLEGAMENTO RADIO



Ipotizziamo un'antenna isotropica, che irradia potenza in tutte le direzioni.

$$\text{La densità di potenza è } \Phi_0(d) = \frac{P_{T_x}}{4\pi d^2} \quad [\text{W/m}^2]$$

Se al posto di un'antenna isotropica ne avessi una direzionale (ipotizzando che il ricevitore sia nel cono di trasmissione)

$$\Phi(d) = \Phi_0(d) \cdot g_{Ant,T_x}$$

intensità di trasmissione



Integrando sull'area dell'intensità ricevuta otengo la potenza al ricevitore

$$P_{R_x} = \Phi_0(d) g_{Ant,T_x} g_{Ant,R_x} \quad \text{dove} \quad g_{Ant,T_x} = \frac{4\pi A_{Ant}}{c^2} f_0^2 \eta_{Ant} \quad g_{Ant,R_x} = A_{Ant,R_x}$$

$$\text{quindi } \epsilon_{ch} = \frac{P_{T_x}}{P_{R_x}} = \frac{\left(\frac{4\pi d}{c}\right)^2}{g_{Ant,T_x} \cdot g_{Ant,R_x}} \Rightarrow (\epsilon_{ch})_{dB} = 32.4 + 20 \log_{10} (d)_{km} + 20 \log_{10} (f_0)_{MHz} - (g_{Ant,T_x})_{dB} - (g_{Ant,R_x})_{dB}$$

### 1.1.3 Ricevitore



Vorremmo  $s_n = a_n \Rightarrow b_n = b_a$ . Cercare un buon demodulatore è quindi importante, su questo si concentrerà il capitolo.

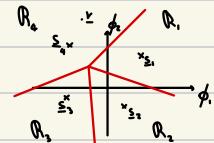
- Proietto il segnale ricevuto  $r(t)$  in una base ortonormale  $(\phi_1(t), \dots, \phi_I(t))$  del sottospazio dei segnali utilizzati in trasmissione  $(s_1(t), \dots, s_M(t))$ .

$$r(t) = \sum_{i=1}^I r_i \phi_i(t) + \sum_{i=I+1}^M r_i \phi_i(t) \quad \text{errore nella proiezione (1.3)}$$

- Otengo così il vettore nello spazio euclideo corrispondente ad  $r(t)$

$$\underline{r} = (r_1, \dots, r_I) \quad \text{dove } r_i = \langle r(t), \phi_i(t) \rangle$$

- Divido quindi lo spazio euclideo in regioni che utilizzo per scegliere quale segnale è stato trasmesso, anche se è stato modificato dal rumore.

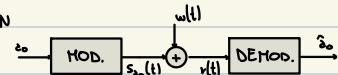


Le regioni sono una partizione dello spazio euclideo  $(\bigcup R_i = \mathbb{R}^I \quad R_i \cap R_j = \emptyset \quad \forall i \neq j)$

### 1.2 Trasmissione su canale AWGN

Studio il caso in cui un singolo segnale viene inviato attraverso un canale AWGN

$$r(t) = s_{a_0}(t) + w(t)$$



- Proiettiamo il segnale nello spazio euclideo di base  $\{\phi_i(t)\}_{i=1, \dots, I}$ .

Si assume che questa base sia completa per le  $M$  sequenze  $\{s_{a_n}(t)\}_{n=1, \dots, M}$ .

$$\langle r(t), \phi_i(t) \rangle = \langle s_{a_0}(t) + w(t), \phi_i(t) \rangle = \langle s_{a_0}(t), \phi_i(t) \rangle + \langle w(t), \phi_i(t) \rangle \quad \text{linearietà} \Rightarrow \begin{bmatrix} r_1 \\ \vdots \\ r_I \end{bmatrix} = \begin{bmatrix} s_{a_0,1} \\ \vdots \\ s_{a_0,I} \end{bmatrix} + \begin{bmatrix} w_1 \\ \vdots \\ w_I \end{bmatrix}$$

**oss** La base  $I$  può non essere una rappresentazione completa di  $w(t)$

$$w(t) = \sum_{i=1}^I w_i \phi_i(t) + \sum_{i=I+1}^M w_i \phi_i(t) \quad \text{teo. dell'irrilevanza (1.3)}$$

Caratterizziamo ora  $w_i$  sapendo  $w(t)$

$$w_i = \langle w(t), \phi_i(t) \rangle = \int w(t) \phi_i(t) dt = \text{combinazione di V.A. gaussiane}$$

media  $w_i: E(w_i) = E \int w(t) \phi_i(t) dt = \int E(w(t)) \phi_i(t) dt = 0$

$$\text{varianza } w_i: E(w_i^2) = E(w_i \cdot w_i) = \sigma_w^2 \quad \text{linearietà}$$

quindi  $w_i \sim N(0, \sigma_w^2)$

\* CORRELAZIONE TRA  $w_i$  e  $w_j: E(w_i \cdot w_j)$

$$E(\langle w(t), \phi_i(t) \rangle \cdot \langle w(t), \phi_j(t) \rangle) = E \left( \int w(t) \phi_i(t) dt \int w(t) \phi_j(t) dt \right) = \int \int \phi_i^2(t) \phi_j^2(t) dt = \sigma_w^2 \quad \text{se } i=j$$

$$= \int \int \phi_i^2(t) \phi_j^2(t) E(w(t), w(t)) dt, dt = 0 \quad \text{se } i \neq j$$

se  $t_1 \neq t_2 \rightarrow w(t_1), w(t_2)$  sono indipendenti,  $E(w(t_1) \cdot w(t_2)) = 0$

3. Vogliamo progettare delle regioni ottime, ovvero che massimizzino le probabilità di decisione corretto  $P(C) = P(\hat{s}_0 = s_0)$ .

$$\{R_{n, \text{opt}}\} = \underset{\{R_n\}}{\text{argmax}} P(C) = \underset{\{R_n\}}{\text{argmin}} P(E)$$

$\text{argmax}$  indica i/i valori per cui ho il massimo

$$P(C) = \sum_{m=1}^M P(\hat{s}_0 = s_0 | s_0 = m) P(s_0 = m) = \sum_{m=1}^M P(x \in R_{s_0} | s_0 = m) p_{s_0}(m) = \max_{\{R_n\}} \sum_{m=1}^M \int_{R_m} p_{s_0}(m) p_{x|s_0}(x|m) dx$$

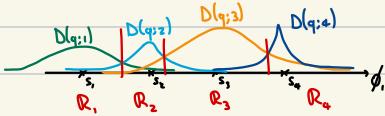
probabilità che il segnale ricevuto abbia coordinate  $x$  e separato da  $\epsilon$  stato inviato il simbolo  $m$

nelle pratiche è la densità di probabilità dell'interferenza centrate in  $m$

Dove suppongo di conoscere  $p_{x|s_0}$  e  $p_{s_0}$ .

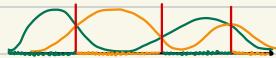
ES

$$I=1 \quad M=4 \quad D(q;m) = p_{s_0}(m) p_{x|s_0}(q|m)$$



OSS

Le regioni possono essere non contigue



### 1.2.1 Criteri di Decisione

#### MASSIMO A POSTERIORI (MAP)

$$\begin{aligned} \hat{s}_0 &= \underset{m}{\operatorname{argmax}} D(x; m) \\ &= \underset{m}{\operatorname{argmax}} p_{x|s_0}(x|m) p_{s_0}(m) \quad P(A|B)P(B) = P(A \cap B) = P(B|A)P(A) \\ &= \underset{m}{\operatorname{argmax}} p_{x|s_0}(m|x) \cancel{p(x)} \quad \text{non dipende da } x \\ &= \underset{m}{\operatorname{argmax}} p_{x|s_0}(m|x) \end{aligned}$$

#### MAXIMUM LIKELIHOOD (ML)

Quando i simboli sono equiprobabili  $p_{s_0}(m) = \frac{1}{M}$

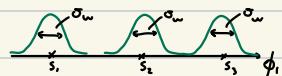
$$\begin{aligned} \hat{s}_0 &= \underset{m}{\operatorname{argmax}} p_{x|s_0}(x|m) p_{s_0}(m) \\ &= \underset{m}{\operatorname{argmax}} p_{x|s_0}(x|m) \end{aligned}$$

OSS Le regioni di decisione sono delimitate da  $D(x|s_i) = D(x|s_i)$

#### MINIMA DISTANZA (MD)

Quando i simboli sono equiprobabili e il canale è AWGN

$$r(t) = s_{s_0}(t) + w(t) \iff x = s_{s_0} + w \quad \left( \begin{array}{l} \text{per un dato } m_0 \text{ è costante} \\ r_i = s_{s_i} + w_i \\ w_i \sim N(0, \sigma_w^2) \text{ indipendenti} \end{array} \right)$$



criterio ML

$$\hat{s}_m = \arg \max_m p_{\text{ML}}(s_m | m) = \arg \max_m p_{\text{ML}}(r_1, \dots, r_I | m)$$

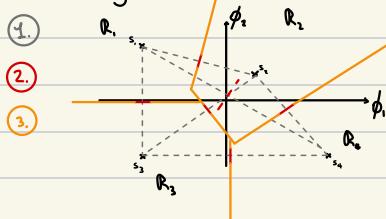
$$= \arg \max_m \prod_{i=1}^I p_{\text{ML}}(r_i | m) = \arg \max_m \prod_{i=1}^I \frac{1}{\sqrt{2\pi} \sigma_w} e^{-\frac{1}{2} \left( \frac{r_i - s_{mi}}{\sigma_w} \right)^2} = \arg \max_m \frac{1}{(\sqrt{2\pi} \sigma_w)^I} e^{-\frac{1}{2} \sum_{i=1}^I \left( \frac{r_i - s_{mi}}{\sigma_w} \right)^2}$$

$\sim N(s_{mi}, \sigma_w^2)$

$$= \arg \min_m \sum_{i=1}^I \left( \frac{r_i - s_{mi}}{\sigma_w} \right)^2 = \arg \min_m \sum_{i=1}^I (r_i - s_{mi})^2 = \arg \min_m \|r - s_m\|^2$$

ovvero m t.c. la distanza di  $r$  da  $s_m$  sia minima

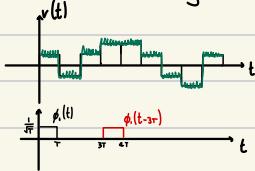
### OSS - procedure grafica



### 1.2.2 Demodulazione del Segnale i-esimo

Suppongo che il supporto dei segnali  $(s_1(t), \dots, s_n(t))$  sia lo stesso intervallo, di lunghezza  $T$ .

Usando  $\phi_i(t-nT)$  (il segnale di base traslato di  $n$  periodi) posso ottenere  $r$ , d. e.



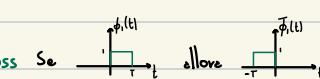
### 1.2.3 Implementazioni

#### CRITERI MAP/ML

$r_{ki}$  viene usato in ogni criterio di decisione, proviziono quindi, per quanto possibile, ed ottimizzarlo

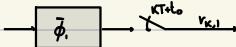
$$r_{ki} = \int_{-\infty}^{+\infty} r(t) \phi_k(t-kT) dt = \int_{-\infty}^{+\infty} r(t) \phi_k(-(kT-t)) dt = \int_{-\infty}^{+\infty} r(t) \phi_k(z-t) dt = \int_{-\infty}^{+\infty} r(t) \phi_k(z-t) dt$$

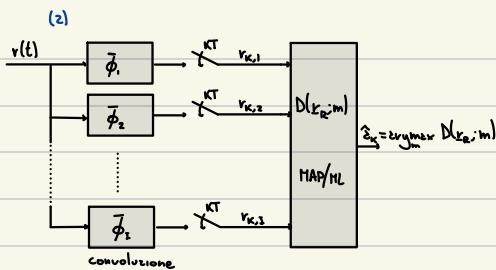
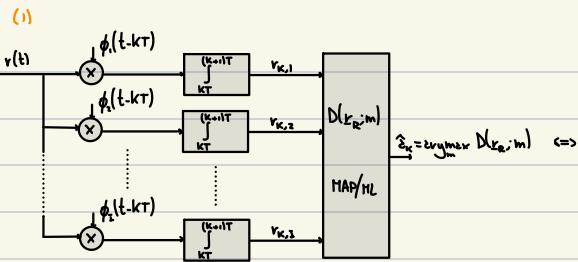
convoluzione



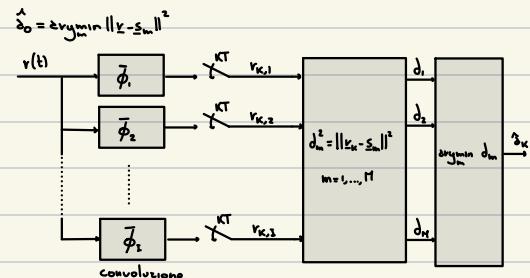
OSS Se allora

Per rendere il segnale causale devo trasferirlo verso destra





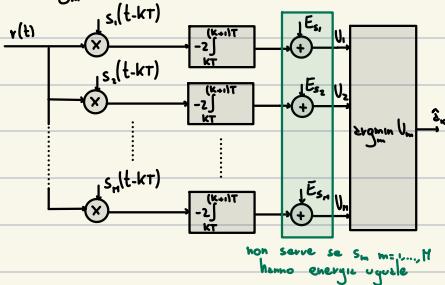
**CRITERIO MD**



È possibile ridurre il numero di operazioni:

$$\hat{s}_o = \arg\min_m \|v_o - s_m\|^2 = \arg\min_m \sum_{i=1}^I (v_i - s_{m,i})^2 = \arg\min_m \sum_{i=1}^I v_i^2 + s_{m,i}^2 - 2v_i s_{m,i} = \arg\min_m \left( \sum_{i=1}^I s_{m,i}^2 - 2 \sum_{i=1}^I v_i s_{m,i} \right) =$$

$$= \arg\min_m (E_{s_m} - 2 \langle v(t), s_m(t) \rangle)$$



**OSS** Se  $I < M$  si preferisce la prima, se  $I = M$  si preferisce la seconda.

### 1.3 Teorema dell'Irrilevanza

criterio MAP:  $\hat{s}_o = \arg\max_m P_{\text{MAP}}(v|m) p_{s|m}$

uso una base di dimensione  $I' \geq I$ . (per  $I' \rightarrow \infty$  ottengo una perfetta descrizione)

$$\hat{s}_o = \arg\max_m P_{\text{MAP}}([v_1, \dots, v_{I'}, v_{I'+1}, \dots, v_{I'}]|m) p_{s|m}$$

Ma  $v_1, \dots, v_{I'}$  contengono già tutte l'informazione su  $s_o$  ( $I'$  segnali  $t_{\text{int}}$  hanno base di dimensione  $I$ )

Nel caso AWGN  $v_{I'+1}, \dots, v_{I'}$  sono indipendenti da  $v_1, \dots, v_{I'}$ .

$$\text{Allora } \hat{s}_o = \arg\max_m P_{\text{MAP}}([v_1, \dots, v_{I'}]|m) p_{s|m}$$

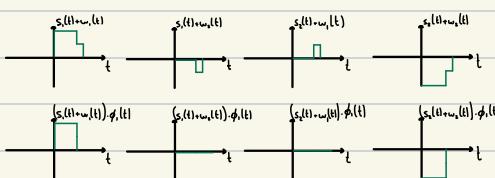
non dipende da  $I'$

## ESERCIZIO NOTEVOLE

Siano  $s_1(t), s_2(t)$

$$\phi_1(t) = \frac{s_1(t)}{\sqrt{\frac{2}{3}T}} = \frac{s_1(t)}{\sqrt{2}E_s}$$

Siano  $w_1(t), w_2(t)$



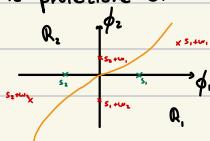
Non riesco a distinguere  $\langle s_1, w_2, \phi_1 \rangle$  da  $\langle s_2, w_1, \phi_1 \rangle$  anche se ci riesco "ad occhio".

Allora devo guardare su  $[2T/3, T]$ , lì posso campionare il rumore e utilizzarlo per distinguere i segnali.

Utilizzo:

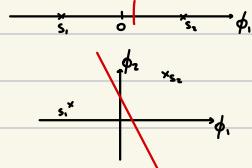
$$\langle v(t), \phi_2(t) \rangle = \begin{cases} A\frac{T}{3} & \text{se } w=w_1 \\ -A\frac{T}{3} & \text{se } w=w_2 \end{cases}$$

Ora la proiezione è:



## 1.4 Modulazioni Binarie

Sono modulazioni su 2 simboli ( $M=2$ ), ogni simbolo porta un solo bit.



### 1.4.1 Probabilità di Errore

Le probabilità di errore sul simbolo è, in questo caso, la stessa sul bit  $P(E) = P_{bit} = 1 - P(C)$ .

Se utilizzo un demodulatore a minima distanza:

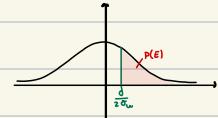
$$\hat{s}_0 = \operatorname{argmin}_{m \in \{1,2\}} \|r - s_m\|^2 \quad \text{e} \quad r = s_{20} + w, \quad w \sim N(0, \sigma_w^2)$$

$$P(C) = P(\hat{s}_0 = 1 | s_0 = 1) p_{s0}(1) + P(\hat{s}_0 = 2 | s_0 = 2) p_{s0}(2)$$

$$P(\hat{s}_0 = 1 | s_0 = 1) = P(\|r - s_1\|^2 < \|r - s_2\|^2 | s_0 = 1) = P(\|r - s_1 + w - s_1\|^2 < \|r - s_2 + w - s_1\|^2) =$$

$$\begin{aligned}
 &= P\left[\sum_{j=1}^L w_j^2 < \sum_{i=1}^L (s_{1,i} + w_i - s_{2,i})^2\right] = P\left[\sum_{j=1}^L w_j^2 < \sum_{i=1}^L (s_{1,i} - s_{2,i})^2 + \cancel{w_i^2} + 2w_i(s_{1,i} - s_{2,i})\right] = \\
 &= P\left[-2\sum_{j=1}^L w_j(s_{1,j} - s_{2,j}) < \sum_{i=1}^L (s_{1,i} - s_{2,i})^2\right] = P\left[-2\langle w, s_1 - s_2 \rangle < \|s_1 - s_2\|^2\right] = 1 - Q\left[\frac{\|w\|}{2\sigma_w}\right] = 1 - Q\left[\frac{d}{2\sigma_w}\right]
 \end{aligned}$$

igno. N.d.  
e medie 0



$$\begin{aligned}
 \text{quindi } P(C) &= \left(1 - Q\left[\frac{d}{2\sigma_w}\right]\right)p_{s_0}(1) + \left(1 - Q\left[\frac{d}{2\sigma_w}\right]\right)p_{s_0}(2) = \left(1 - Q\left[\frac{d}{2\sigma_w}\right]\right)(p_{s_0}(1) + p_{s_0}(2)) = 1 - Q\left[\frac{d}{2\sigma_w}\right] \\
 \text{quindi } P(E) &= Q\left[\frac{d}{2\sigma_w}\right]
 \end{aligned}$$

OSS  $d$  e  $P(E)$  sono direttamente proporzionali,  $\sigma_w$  e  $P(E)$  inversamente.

OSS  $d = d_2$ , quindi  $P(E)$  è uguale nelle segnalazioni, ma l'energia è diversa.  
Preferiamo segnalazioni a bassa energia

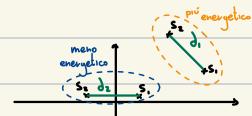
#### 1.4.2 Energia Media per Simbolo

Dato che il canale non modifica il segnale trasmesso ( $r(t) = s_o(t) + u(t)$ ) posso calcolare l'energia a partire dei segnali al ricevitore.

$$E_s = E(E_{s_{\phi_1}}) = \frac{1}{2}E_{s_1} + \frac{1}{2}E_{s_2}$$

veloce atteso

OSS  $E_{s_{\phi_i}} = \int_{-\infty}^{\infty} s_i^2(t) dt = \|s_i\|^2$  ovvero la distanza dall'origine al quadrato



ESEMPI



ORTOGONALI  $s_1 \perp s_2$

ANTIPODALI  $s_1 = -s_2$

Le due segnalazioni hanno la stessa energia media

Ma l'antipodale ha d maggiore, quindi la P(E) è inferiore.

#### 1.4.3 Coefficiente di correlazione

$$\rho = \frac{\langle s_1(t), s_2(t) \rangle}{\sqrt{E_{s_1} E_{s_2}}} \quad |\rho| \leq 1$$

ESEMPI

$$s_1 \perp s_2 \Rightarrow \langle s_1, s_2 \rangle = 0 \Rightarrow \rho = 0$$

$$s_1 = -s_2 \Rightarrow E_{s_1} = E_{s_2} \Rightarrow \frac{-\langle s_1(t), s_1(t) \rangle}{E_{s_1}} = -\frac{E_{s_1}}{E_{s_1}} = -1$$

$$s_1 = s_2 \Rightarrow \rho = 1$$

#### 1.4.4 Modulazioni Binarie Equienergetiche

Ovvero il caso  $E_{s_1} = E_{s_2} = E_s$   $\phi_1(t) = \frac{s_1(t)}{\sqrt{E_s}}$ ,  $\rho = \frac{\langle s_1, s_2 \rangle}{E_s}$

$$s_1 = [\sqrt{E_s}, 0] \quad s_2 = [\langle s_1(t), \phi_1(t) \rangle, \langle s_2(t), \phi_1(t) \rangle] = \left[ \frac{\langle s_1(t), s_1(t) \rangle}{\sqrt{E_s}}, \pm \sqrt{E_s(1-\rho^2)} \right] \Rightarrow s_2 = [\rho \sqrt{E_s}, \pm \sqrt{E_s(1-\rho^2)}]$$

\* questo si ricava perché  $E_s = \|s_2\|^2 = s_{2,1}^2 + s_{2,2}^2 = \rho^2 E_s + s_{2,2}^2 \Rightarrow s_{2,2} = \pm \sqrt{E_s - \rho^2 E_s} = \pm \sqrt{E_s(1-\rho^2)}$

Le distanze tra  $s_1$  e  $s_2$  è  $d^2 = 2E_s(1-\rho)$

$$P(E) = Q\left(\frac{\sqrt{2E_s(1-\rho)}}{2\sigma_w}\right) = Q\left(\sqrt{\frac{E_s(1-\rho)}{2\sigma_w^2}}\right)$$

dove  $\frac{E_s}{\sigma_w^2}$  è il signal-to-noise ratio  $\left[\frac{E_s}{\sigma_w^2}\right] = \text{dB}$

OSS

$P(E)$  si riduce se uso più energia o se riduco  $\sigma_w$  (i rapporti non sono lineari)

#### 1.4.5 Implementazioni

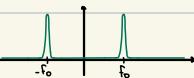
##### MODULAZIONE BINARY PHASE SHIFT KEYING (BPSK)

$$s_1(t) = \begin{cases} A \cos(2\pi f_0 t) & t \in [0, T] \\ 0 & \text{altrimenti} \end{cases}$$

$$s_2(t) = \begin{cases} -A \cos(2\pi f_0 t) = A \cos(2\pi f_0 t + \pi) & t \in [0, T] \\ 0 & \text{altrimenti} \end{cases}$$

dove  $f_0$  è la frequenza della portante

Ovvero la trasformata di Fourier ha un picco in  $f_0$



$$\rho = \frac{\langle s_1(t), s_2(t) \rangle}{\sqrt{E_s} \sqrt{E_s}} = \frac{-\int A^2 \cos^2(2\pi f_0 t) dt}{\sqrt{\int A^2 \cos^2(2\pi f_0 t) dt}} = -1 \quad (\text{antipodale})$$

$$E_{s_1} = E_{s_2} = \frac{A^2}{2} T \quad (\text{ipotizzando } f_0 \gg \frac{1}{T})$$

$$P(E) = Q\left(\sqrt{\frac{E_s}{\sigma_w^2}}\right) \quad (\rho = -1)$$



##### MODULAZIONE BINARIA ORTOGONALE

$$s_1(t) = \begin{cases} A \cos(2\pi f_0 t) & t \in [0, T] \\ 0 & \text{altrimenti} \end{cases}$$

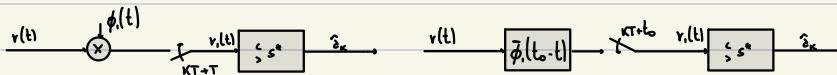
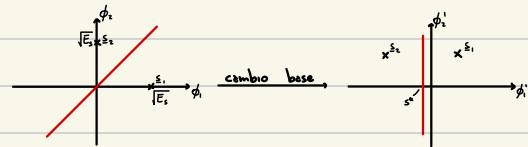
$$s_2(t) = \begin{cases} A \sin(2\pi f_0 t) & t \in [0, T] \\ 0 & \text{altrimenti} \end{cases}$$

$$E_{s_1} = E_{s_2} = \frac{A^2}{2} T, \quad \text{i segnali sono ortogonali} \Rightarrow \rho = 0$$

$$P(E) = Q\left(\frac{E_s}{2\sigma_w}\right)$$

oss. aumento rispetto all'antipode

oss. Possiamo cambiare la base a  $\{\phi_1', \phi_2'\}$ , la quale è più comoda in quanto  $s_1$  e  $s_2$  sono elle stesse altezza, ci basta confrontare le coordinate di  $\phi_1'$  per decidere la regione.



## 1.5 Modulazioni M-arie

$M=2$ , ogni simbolo rappresenta più di un bit. Dobbiamo quindi distinguere  $P(E)$  (probabilità di errore sul simbolo) e  $P_{bit}$  (probabilità di errore sul bit).

Mentre nelle modulazioni binarie le regioni di decisione sono semplici, delimitate da una retta, nelle modulazioni con  $M > 2$  questo non è più vero, rendendo  $P(E)$  complesso da calcolare.

$$P(E) = \sum_{m=1}^M P(\xi_{0:t_0} | z_0=m) \cdot \frac{1}{M} = \sum_{m=1}^M P(r_i(t_0) | z_0=m) \cdot \frac{1}{M} = \frac{1}{M} \sum_{m=1}^M \int_{R_m} P(r_i | z_0=m) dm$$

formula generale utilizzata dai calcolatori, troppo difficile e meno

Calcoleremo dei bound del valore effettivo.

### UPPER-BOUND

$$P(r_i \notin R_m | z_0=m) = P(r_i \text{ è più vicino a } s_1 \text{ che non a } s_n | z_0=m)$$

oppure

criterio FID

$$P(r_i \text{ è più vicino a } s_2 \text{ che non a } s_n | z_0=m)$$

diciamo  $\xi_{n,m} = r_i \text{ è più vicino a } s_n \text{ rispetto a } s_m | z_0=m$

$$= \frac{1}{M} \sum_{m=1}^M P(\bigcup_{\substack{n=1 \\ n \neq m}} \xi_{n,m}) \leq \frac{1}{M} \sum_{m=1}^M \sum_{n \neq m} P(\xi_{n,m} | z_0=m) = \frac{1}{M} \sum_{m=1}^M \sum_{n \neq m} Q\left(\frac{d_{min,m}}{2\sigma_w}\right) \leq \frac{1}{M} \sum_{m=1}^M (n-1) Q\left(\frac{d_{min,m}}{2\sigma_w}\right) \leq (n-1) Q\left(\frac{d_{min,m}}{2\sigma_w}\right)$$

gli eventi  $\xi$  non sono disgiunti

le loro somme ci fornisce un upper-bound

$P(\xi_{n,m})$  è uguale alla  $P(E)$

$d_{min,m} = \min_{n \neq m} d_{n,m}$ , la coppia di simboli a distanza minima.

### LOWER-BOUND

$$P(E) \geq \frac{1}{M} \sum_{m=1}^M (n-1) Q\left(\frac{d_{min,m}}{2\sigma_w}\right) \geq \frac{1}{M} Q\left(\frac{d_{min}}{2\sigma_w}\right)$$

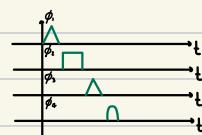
$\left( \frac{N_{min}}{M} Q\left(\frac{d_{min}}{2\sigma_w}\right)$  è una migliore approssimazione.  
 $N_{min} = \# \text{ di punti con un altro punto a distanza minima} \right)$



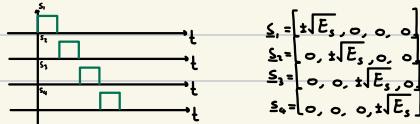
### 1.5.1 Modulazioni Ortogonali

Modulazione in cui tutte le coppie di segnali della modulazione sono a coppie ortogonalili.

$$\langle s_m, s_n \rangle = 0 \quad \forall n \neq m$$



### ESEMPIO - PULSE POSITION MODULATION



$$d_{n,m} = \|S_n - S_m\| = \left\| [0, \dots, 0, \sqrt{E_s}, 0, \dots, 0] - [0, \dots, 0, \sqrt{E_s}, 0, \dots, 0] \right\| = \sqrt{2E_s} \quad (= d_{\min})$$

$$Q\left(\frac{\sqrt{E_s}}{2\sigma_z}\right) \leq P(E) \leq (M-1)Q\left(\frac{\sqrt{E_s}}{2\sigma_z}\right)$$

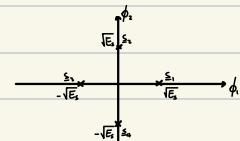
### 1.5.2 Modulazioni Biortogonali

Una segnalazione si dice biortogonale se  $\frac{M}{2}$  segnali della segnalazione sono ortogonali, mentre gli altri sono antipodali rispetto ai primi. (ipotizzo  $M$  pari)

$$s_{\frac{M}{2}+1}(t) = -s_1(t) \dots s_M(t) = s_{\frac{M}{2}}(t)$$

oss Per ogni segnale c'è un segnale a distanza  $\sqrt{2E_s}$  e  $(M-2)$  segnali a distanza  $\sqrt{2E_s}$

$$Q\left(\frac{\sqrt{E_s}}{2\sigma_z}\right) \leq P(E) \leq (M-2)Q\left(\frac{\sqrt{E_s}}{2\sigma_z}\right) + Q\left(\frac{\sqrt{E_s}}{\sigma_z}\right)$$



### 1.5.3 Mappatura di Gray

Vogliamo ora mitigare i risultati di un errore di segnale. Consideriamo il fatto che nella maggior parte dei casi la regione scelta sarà adiacente a quella corretta.



Utilizzando questa mappatura un piccolo errore di segnale si traduce in un errore grosso di BIT.

Utilizzando la mappatura di Gray sbagliano solo 1 bit quando scegliamo una regione adiacente a quella corretta.

$M=2$	0	$M=4$	0 0
	1		0 1
		1 1	1 0

Inoltre

$M=8$	0 0 0
	0 0 1
	0 1 1
	0 1 0
	1 1 0
	1 1 1
	1 0 1
	1 0 0

Utilizzando queste mappature possiamo scrivere le probabilità di errore sul bit come:

$$P_{\text{err}} \approx P(E) \frac{1}{\log_2 M}$$

considero che l'errore mi possa solo portare alla regione adiacente

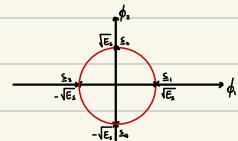
#### 1.5.4 Implementazioni

##### 4-PSK (PHASE SHIFT KEYING)

$$s_1(t) = \cos(2\pi f_0 t + \phi_1) \quad \phi_1 = 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$$

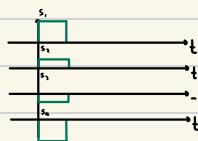
$$\phi_1(t) = \cos(2\pi f_0 t)$$

$$\phi_2(t) = \sin(2\pi f_0 t)$$



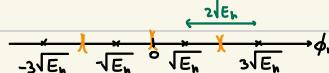
##### PULSE AMPLITUDE MODIFICATION

L'informazione è portata dall'ampiezza di un impulso prototipo  $\left( h_p(t), \phi(t) = \frac{h_p(t)}{\sqrt{E_h}} \right)$



In generale  $s_m = a_m h_p(t)$  dove  $a_m = 2m-1-M \quad m=1, \dots, M$  ( $M$  pari)

$$ES-M=4, \quad a_1=-3, \quad a_2=-1, \quad a_3=1, \quad a_4=3$$



OSS Si formano regioni tutte uguali (a meno di una traslazione), tranne le 2 regioni esterne.

L'energia media di una modulazione PAM è

$$E_s = \frac{1}{M} \sum_{m=1}^M a_m^2 E_h = \frac{1}{M} \sum_{m=1}^M (2m-1-M)^2 E_h = \frac{1}{M} \sum_{m=1}^M (2m-1-M)^2 E_h = \frac{1}{M} \sum_{m=1}^M [4m^2 + (1+M)^2 - 4m(1+M)] E_h = \frac{M^2-1}{3} E_h$$

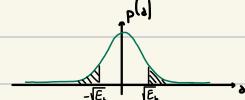
$$\sum_{m=1}^M m = \frac{M(M+1)}{2} \quad \sum_{m=1}^M m^2 = \frac{M(M+1)(2M+1)}{6}$$

Le probabilità di errore vengono calcolate separatamente per simboli interni ed esterni.

$$P(E) = \frac{1}{M} \sum_{m=1}^M P(s_m = d_m | d_m = m) \cdot P(d_m = m) = *$$

per simboli interni (sono  $M-2$ )

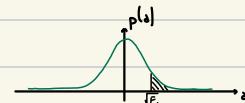
$$* = P(r \notin R_m | d_m = m) = P(s_m + w \notin [s_m - \sqrt{E_h}, s_m + \sqrt{E_h}] | d_m = m) = P(|w| > \sqrt{E_h}) = 2Q\left(\frac{\sqrt{E_h}}{\sigma_w^2}\right)$$



per simboli esterni (sono 2)

$$* = Q\left(\sqrt{\frac{E_h}{\sigma_w^2}}\right)$$

metà di quelli interni, posso sbagliare solo da un lato



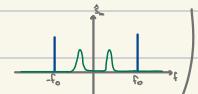
$$* = \frac{1}{M} [(M-2) \cdot 2Q\left(\sqrt{\frac{E_h}{\sigma_w^2}}\right) + 2 \cdot Q\left(\sqrt{\frac{E_h}{\sigma_w^2}}\right)] = \frac{1}{M} (2M-4+2) Q\left(\sqrt{\frac{E_h}{\sigma_w^2}}\right) = 2\left(1 - \frac{1}{M}\right) Q\left(\sqrt{\frac{E_s - 3}{\sigma_w^2 (M^2 - 1)}}\right)$$

## QUADRATURE AMPLITUDE MODULATION

$$s_m(t) = a_{m,1} h_{T_R}(t) \cos(2\pi f_0 t) - a_{m,2} h_{T_R}(t) \sin(2\pi f_0 t) \quad m=1, \dots, M \quad (\text{ipotizzo } \sqrt{M} \in \mathbb{N})$$

dove  $a_{m,1}, a_{m,2} \in \{2L-L-1, L=1, \dots, L=\sqrt{M}\}$

(ipotizzando  $h_{T_R}(t)$  abbia trasformata di Fourier in  $[-\frac{B}{2}, \frac{B}{2}]$  con Bcfo. In questo modo, per il teorema di Nyquist-Shannon è sufficiente campionare il segnale a  $2f_0$ )



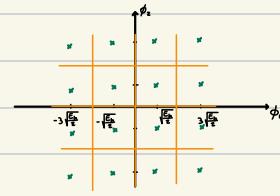
Sì dimostra che  $h_{T_R}(t) \cos(2\pi f_0 t)$  e  $h_{T_R}(t) \sin(2\pi f_0 t)$  sono ortogonali

$$\text{Useremo } \phi_1(t) = h_{T_R} \cos(2\pi f_0 t) \quad \phi_1(t) = \frac{\phi_1(t)}{\sqrt{E_{\phi_1}}}$$

$$\phi_2(t) = h_{T_R} \sin(2\pi f_0 t) \quad \phi_2(t) = \frac{\phi_2(t)}{\sqrt{E_{\phi_2}}}$$

$$\text{oss } E_{\phi_1} = E_{\phi_2} = \int_{-\infty}^{\infty} \cos^2(2\pi f_0 t) |h_{T_R}|^2 dt = \frac{1}{2} E_{h_R} \Rightarrow \sqrt{E_{\phi_1}} = \sqrt{E_{\phi_2}} = \sqrt{\frac{E_h}{2}}$$

$\phi_1, \phi_2$  sono una base della segnalazione  $s_m(t) = a_{m,1} \phi_1(t) \sqrt{E_{\phi_1}} + a_{m,2} \phi_2(t) \sqrt{E_{\phi_2}} \Rightarrow s_m = \left[ a_{m,1} \sqrt{\frac{E_h}{2}}, a_{m,2} \sqrt{\frac{E_h}{2}} \right]$



$$E_s = \frac{1}{M} \sum_{m=1}^M \|s_m\|^2 = \frac{1}{M} \sum_{m=1}^M \left[ \left( a_{m,1} \sqrt{\frac{E_h}{2}} \right)^2 + \left( a_{m,2} \sqrt{\frac{E_h}{2}} \right)^2 \right] = \frac{M-1}{3} E_h$$

$$P(E) = \frac{1}{M} \sum_{m=1}^M P(s_0 \neq s_m | z_0=m) = \frac{1}{M} \sum_{m=1}^M P(z \notin R_m | z_0=m) \quad \text{dove } z = [z_1, z_2] = [s_{m,1}, s_{m,2}] + [w_1, w_2]$$

Ci sono 3 tipi di regione da studiare



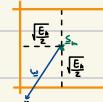
### TIPO A

$$\begin{aligned} P(s_0 + w \notin R_A | z_0=m) &= P(w_1 < -\sqrt{\frac{E_h}{2}} \text{ OPPURE } w_2 < -\sqrt{\frac{E_h}{2}}) = \\ &= 1 - P(s_0 + w \in R_A | z_0=m) = 1 - P(w_1 > -\sqrt{\frac{E_h}{2}} \text{ E } w_2 > -\sqrt{\frac{E_h}{2}}) = \\ &= 1 - Q^2\left(\frac{-\sqrt{\frac{E_h}{2}}}{\sigma_z}\right) = 1 - \left[1 - Q\left(\frac{\sqrt{\frac{E_h}{2}}}{\sigma_z}\right)\right]^2 \end{aligned}$$



### TIPO B

$$P(z \notin R_B | z=z_0) = 1 - P(w_1 > -\sqrt{\frac{E_h}{2}} \text{ E } w_2 \in [-\sqrt{\frac{E_h}{2}}, \sqrt{\frac{E_h}{2}}]) = 1 - \left[1 - Q\left(\frac{\sqrt{\frac{E_h}{2}}}{\sigma_z}\right)\right] \left[1 - 2Q\left(\frac{\sqrt{\frac{E_h}{2}}}{\sigma_z}\right)\right]$$



### TIPO C

$$P(z \notin R_B | z=z_0) = 1 - P(w_1 \in [-\sqrt{\frac{E_h}{2}}, \sqrt{\frac{E_h}{2}}] \text{ E } w_2 \in [-\sqrt{\frac{E_h}{2}}, \sqrt{\frac{E_h}{2}}]) = 1 - \left[1 - 2Q\left(\frac{\sqrt{\frac{E_h}{2}}}{\sigma_z}\right)\right]^2$$



La probabilità totale è la media pesata delle probabilità per le probabilità che il simbolo venga inviato.

$$P(E) = 4 \left(1 - \frac{1}{M}\right) Q\left(\frac{\sqrt{\frac{3}{2}}}{\sigma_z}\right) - 16 \left(\frac{M-1}{M}\right)^2 Q^2\left(\frac{\sqrt{\frac{3}{2}}}{\sigma_z}\right)$$

se  $\frac{E_h}{\sigma_z^2}$  è grande allora  $\sigma_z^2 \ll E_h$

Vediamo la mappatura dei bit per mitigare l'errore nei bit quando c'è un errore di segnale.



## 1.6 Quantizzatore

Il quantizzatore assieme al campionamento ci permette di spostarci dal mondo dei segnali analogici a quello digitale.

La quantizzazione è un'operazione istantanea che fornisce un segnale a valori discreti a partire da un segnale a valori continui.

$$x_q = Q[x] \text{ dove } x \in \mathbb{R} \text{ e } x_q \in A = \{a_1, \dots, a_n\}$$

OSS Se il segnale  $x(t)$  è continuo la sua quantizzazione sarà continua, se  $x(t)$  è discreto sarà discreto.

OSS La quantizzazione fa, per definizione, perdere delle informazioni (lossy conversion)

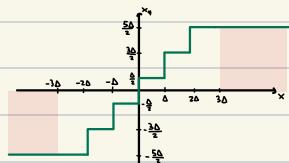
### 1.6.1 Quantizzatore uniforme

La funzione caratteristica è del tipo:

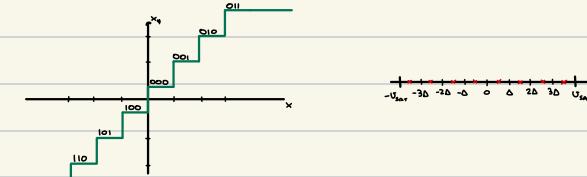
dove  $\Delta$  è il passo di quantizzazione.

$\Delta$  è il numero di livelli di quantizzazione (in questo caso  $L=6$ )

L'area in rosso è la zona di saturazione (l'errore diventa in modo incontrollato)



### ALTRI RAPPRESENTAZIONI



### 1.6.2 Errore di Quantizzazione

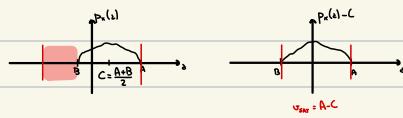
$$e = x - x_q = x - Q(x)$$

se  $x \in [-U_{\text{SAT}}, U_{\text{SAT}}]$   $\Rightarrow e \in [-\frac{\Delta}{2}, \frac{\Delta}{2}]$

se  $x \notin [-U_{\text{SAT}}, U_{\text{SAT}}]$   $\Rightarrow |e| > \frac{\Delta}{2}$  (errore di saturazione)

Vogliamo costruire il quantizzatore per evitare l'errore di saturazione:

$$\text{se } x \in [-A, A] \text{ con } A < +\infty \Rightarrow U_{\text{SAT}} = A$$

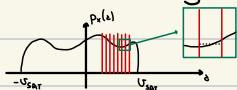


se  $x \in \mathbb{R}$  non posso trovare un quantizzatore che non abbia errore di saturazione.

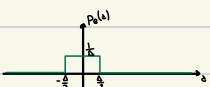
Quindi impongo una probabilità di saturazione  $P(|x| > u_{\text{sat}}) = \epsilon$  e trovo  $u_{\text{sat}}$  di conseguenza.

### 1.6.3 Errore Granulare

Ipotizzo un numero grande di livelli di quantizzazione



Allora  $x$  all'interno di ogni intervallo è una V.A. uniforme e quindi il suo errore è una V.A. uniforme



$$E(e) = 0, E(e^2) = \int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} \frac{1}{\Delta} \cdot \Delta dx = \frac{\Delta^2}{12}$$

### 1.6.4 Rapporto Segnale-Rumore di Quantizzazione

$$\Delta_q = \frac{E(x)}{E(e^2)} = \frac{\sigma_x^2}{\frac{\Delta^2}{12}}$$

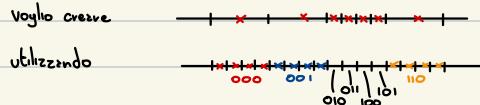
oss Una quantizzazione ha  $L = 2^b$  livelli tra  $-u_{\text{satur}}$  e  $u_{\text{satur}}$ , ognuno di larghezza  $\Delta$ . Quindi  $\frac{2u_{\text{satur}}}{2^b} = \Delta$

$$(\Delta_q)_{\text{dB}} = 20 \log_{10} \left( \frac{\sigma_x}{u_{\text{satur}}} \right) + 4.77 + 6.02 b$$

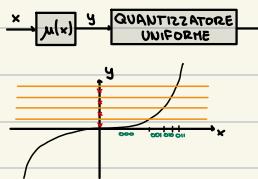
### 1.6.5 Quantizzatore non uniforme

Nei punti con densità di probabilità maggiore vogliamo un  $\Delta$  minore che nei punti a densità minore  
I quantizzatori sono implementati in hardware, quindi non è semplice implementare questo tipo di quantizzatori, di seguito alcune soluzioni modulari:

1. Utilizzo un quantizzatore uniforme preciso (con  $\Delta$  piccolo). Poi aggiungo alcuni intervalli meno usati.



2. Utilizzo una funzione di compressione (e poi decompressione)



## 2. Codifica di Canale

Disciplina che si occupa della riduzione degli errori in una trasmissione, in particolare punta a minimizzare l'errore del canale AWGN. Vengono utilizzate varie tecniche per ottenere ciò:

### 1. RITRASMISSIONE

Ovvero il messaggio viene reinviato dal trasmettitore se il ricevitore rileva un errore.

Per implementare questo è necessario:

↳ Canale di ritorno: il canale deve permettere al ricevitore di comunicare con il trasmettitore.

particularmente difficile nel caso  $T \leftarrow \begin{matrix} R_1 \\ R_2 \end{matrix}$

↳ Mecanismo di rilevamento dell'errore

### 2. CODIFICA DEL MESSAGGIO

Aggiungiamo dei bit di parità che permettono di riconoscere e correggere gli errori.

Questo viene detto forward error correction o FEC

### 3. SOLUZIONI MISTE

Quando i bit di parità mi segnalano un errore chiedo la ripetizione del segnale



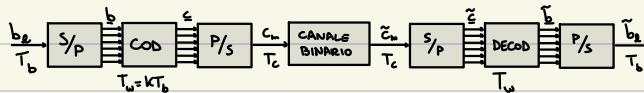
Def Si dice canale simmetrico un canale dove i bit "1" e i bit "0" vengono modificati con le stesse probabilità statistiche.

$$P(c_1 \neq \tilde{c}_1 | c_1 = 0) = P(c_1 \neq \tilde{c}_1 | c_1 = 1)$$

Def Si dice canale senza memoria un canale dove gli errori sono eventi indipendenti per ogni bit

Esistono vari modi per effettuare la codifica di canale, noi ci concentreremo solo sulla codifica a blocco

### 2.1 Codici di Canale a Blocco



Ricogliamo più bit e li trattiamo come un'unica blocco per la codifica di canale.  $b$  e  $c$  devono essere in lunghezza fissa.

$$\mathbf{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \quad \mathbf{c} = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \quad \text{dove } n \geq K \quad (\text{altrimenti ci sarebbe perdita di informazione})$$

Utilizziamo solo  $2^k$  tra le  $2^n$  sequenze di  $c$  in quanto il codificatore deve essere deterministico

**Def** Indichiamo con  $C = \{c_1, \dots, c_{2^m}\}$  l'insieme delle parole di codice.

**Def** Diciamo il tasso di codifica  $R = \frac{K}{n}$  ( $K \leq n \Rightarrow R \leq 1$ )

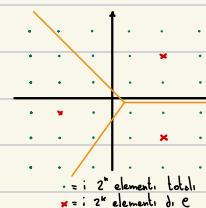
ES

00	010010
01	111000
10	100001
11	100101
b	c

### 2.1.1 Criteri di Decodifica

Se, a seguito della demodulazione ottengo un  $\hat{s}$  che non appartiene all'insieme delle parole di codice devo usare un criterio di decisione per approssimare. (se avviene un errore che mi porta ad una parola di codice non lo posso correggere)

Questo problema è simile a quello affrontato nella demodulazione digitale, applicheremo  
una soluzione simile.



Se il valore alle decodifiche cade in un pallino verde so che c'è un errore, posso correggerlo grazie a delle regole di decisione.

Definiamo le distanze in questo spazio:

## DISTANZA DI HAMMING

Siano  $s_1$  e  $s_2$  due sequenze di bit di lunghezza  $n$ :  $s_1 = [s_{1,1}, \dots, s_{1,n}]$      $s_2 = [s_{2,1}, \dots, s_{2,n}]$

Allora la loro distanza di Hamming è il numero di bit di differenza tra le due sequenze.

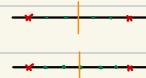
$$d_H(s_1, s_2) = \sum_{i=1}^n |s_{1,i} - s_{2,i}|$$

$$B = 10111001$$

**Def**  $d_{\min}$  è la distanza minima di Hamming tra ogni coppia di parole di codice.

$$d_{\min} = \min_{\substack{\beta, \beta' \in \mathcal{C} \\ \beta \neq \beta'}} d_H(\beta, \beta')$$

PROP Il numero di errori che possono essere sempre corretti è  $\frac{d_{\text{MIN}} - 1}{2}$  se  $d_{\text{MIN}}$  è pari  
 $\frac{d_{\text{MIN}} - 1}{2}$  se  $d_{\text{MIN}}$  è dispari



**PROP** Il numero di errori che possono essere sempre rilevati è  $d_{\min} - 1$ .

## criterio MAP

$$\hat{z}(B) = \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} P(\underline{z} = B | \underline{s} = \underline{s}) P(\underline{s} = \underline{s})$$

dove  $B$ : sequenza ricevuta

$\hat{z}$ : sequenza decisa

$P(\underline{s} = \underline{s})$ : probabilità che venga inviata  $\underline{s}$

$P(\underline{z} = B | \underline{s} = \underline{s})$ : probabilità che  $\underline{s}$  venga trasletta fino a  $B$

## criterio ML

Se le parole del codice sono equiprobabili

$$\hat{z}(B) = \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} P(\underline{z} = B | \underline{s} = \underline{s})$$

## criterio MD

Se le parole sono equiprobabili e il canale è un canale binario simmetrico senza memoria

Allora è possibile applicare il criterio di minima distanza di Hamming

$$\hat{z}(B) = \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmin}} d_H(\underline{z}, B)$$

DIM

Parto dal criterio ML e uso le proprietà del canale binario simmetrico senza memoria

$$\begin{aligned} \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} P(\underline{z} = B | \underline{s} = \underline{s}) &= \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} P(\underline{z}_1 = B_1, \dots, \underline{z}_n = B_n | c_1 = s_1, \dots, c_n = s_n) \\ &= \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} \prod_{i=1}^n P(\underline{z}_i = B_i | c_i = s_i) = \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} P_{\text{BIT}}^{d_H(\underline{z}, B)} (1 - P_{\text{BIT}})^{n - d_H(\underline{z}, B)} = \\ &= \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmax}} \left(1 - P_{\text{BIT}}\right)^n \left(\frac{P_{\text{BIT}}}{1 - P_{\text{BIT}}}\right)^{d_H(\underline{z}, B)} = \underset{\underline{z} \in \mathcal{C}}{\operatorname{argmin}} d_H(\underline{z}, B) \end{aligned}$$

Sono indipendenti per assenza di memoria.

il canale è simmetrico  
 $P(\underline{z}_i \neq c_i | c_i = 0) = P(\underline{z}_i \neq c_i | c_i = 1) = P_{\text{BIT}}$   
 $P(\underline{z}_i = c_i | c_i = 0) = P(\underline{z}_i = c_i | c_i = 1) = 1 - P_{\text{BIT}}$

non dipende da  $s$   
 se  $P_{\text{BIT}} = \frac{1}{2} \Rightarrow \underline{z} \sim \frac{P_{\text{BIT}}}{1 - P_{\text{BIT}}} = 1$

oss. Ipotizzando  $P_{\text{BIT}} < \frac{1}{2}$  non perdo generalità, se  $P_{\text{BIT}} > \frac{1}{2}$  è conveniente invertire tutti i bit ricevuti, quindi  $P'_{\text{BIT}} = 1 - P_{\text{BIT}} < \frac{1}{2}$

ES			
00	010010	$d_H = 6$	
01	111000	$d_H = 3$	
10	100001	$d_H = 2$	
11	100101	$d_H = 1$	
b	$\underline{z}$		

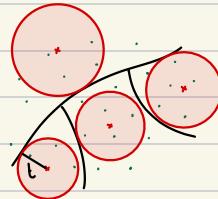
Scalo  $\underline{z} = 100101 \rightarrow \hat{b} = 11$

## 2.1.2 Bound di Hamming

Def Il bound di Hamming dato il numero massimo di errori che posso sempre correggere,  $t$ , ed il numero di bit codificati,  $n$ , ci fornisce un upper bound per il tasso di codice (upper bound) per il numero di bit decodificati,  $k$ )

$$R = \frac{k}{n} \leq 1 - \frac{t}{n} \log_2 \sum_{i=1}^t \binom{n}{i}$$

Siano i cerchi rossi delle approssimazione delle regioni di decisione e sia  $t$  il raggio del cerchio di raggio minore.



Il numero di sequenze contenute in un cerchio di raggio  $t$  centrato in  $c$  è la somma delle sequenze a distanza  $1, \dots, t$  da  $c$ .

Il numero di sequenze alla generica distanza  $r$  è  $\binom{n}{r}$  (tutti i possibili  $r$  errori su  $n$  bit)

Quindi in un cerchio di raggio  $t$  ci sono  $\sum_{r=1}^t \binom{n}{r}$

Il totale delle sequenze nei cerchi di raggio  $t$  centrati attorno a ciascuna parola è  $2^n \sum_{r=1}^t \binom{n}{r}$

Il totale delle sequenze che posso ricevere è  $2^n$ , le regioni coprono un'area minore o uguale al totale.

$$2^n \geq 2^k \sum_{r=1}^t \binom{n}{r} \Rightarrow \log_2 2^n \geq \log_2 2^k \sum_{r=1}^t \binom{n}{r} \Rightarrow n \geq k + \log_2 \sum_{r=1}^t \binom{n}{r} \Rightarrow \frac{k}{n} \leq 1 - \frac{1}{n} \log_2 \sum_{r=1}^t \binom{n}{r}$$

## 2.2 Codici di Canale a Blocco Lineari

### 2.2.1 Spazio Vettoriale dei Vettori Binari

I vettori binari di lunghezza  $n$  formano uno spazio vettoriale.

Siano  $x = [x_1, \dots, x_n]$   $y = [y_1, \dots, y_n]$  dove  $x_i, y_i \in \{0, 1\}$

#### SOMMA

$$\underline{x} = x + y = [x_1 \oplus y_1, \dots, x_n \oplus y_n]$$

dove  $\oplus$  è l'operazione di somma senza ripporto

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

OSS  $\underline{x} + \underline{x} = \underline{0}$

#### PRODOTTO SCALARE

Uso come insieme di scalari  $\{0, 1\}$

$$\alpha \underline{x} = [\alpha x_1, \dots, \alpha x_n]$$

Se  $\alpha = 0$   $\alpha \underline{x} = [0, \dots, 0]$

Se  $\alpha = 1$   $\alpha \underline{x} = \underline{x}$

#### NORMA DI HAMMING

$\|\underline{x}\|_H$ : numero di "1" nelle sequenze

#### PROP

$$\|\underline{x}\| \geq 0$$

$$\|\underline{x}\| = 0 \iff \underline{x} = [0, \dots, 0]$$

$$\|ax\| = a\|x\|$$

$$\|x+y\| \leq \|x\| + \|y\| \quad (\text{questo perché } 1 \otimes 1 = 0)$$

### DISTANZA DI HAMMING

$$d_H(x, y) = \|x-y\| = \|x+y\| = \# \text{ di elementi in cui } x \text{ e } y \text{ differiscono}$$

$y = -y$  (perché  $y$  è il vettore che dava somma a  $-y$  per ottenere  $[0, \dots, 0]$ )

### 2.2.2 Definizione

**Def** Un codice a blocco è detto lineare se il suo insieme di parole di codice  $C$  costituisce un sottospazio vettoriale dello spazio delle sequenze binarie di lunghezza  $n$ .

Ovvero se  $x, y \in C$ ,  $x+y \in C$  e  $\alpha x \in C$ .

**Oss** dim  $C = k$  in quanto vogliamo un isomorfismo con lo spazio di  $b$  che ha  $2^k$  parole.

**Def** Il peso di Hamming del codice è la minima norma di Hamming tra tutte le parole di codice tranne quelle nulle

$$w_H(C) = \min_{\substack{\mathbf{c} \in C \setminus \{0\}}} \|\mathbf{c}\|_H$$

### TEO

In un codice lineare a blocco il peso di Hamming del codice è uguale alla distanza minima del codice

$$d_{\min} = \min_{\substack{\mathbf{c}_i, \mathbf{c}_j \in C \\ \mathbf{c}_i \neq \mathbf{c}_j}} d_H(\mathbf{c}_i, \mathbf{c}_j) = \min_{\substack{\mathbf{c}_i, \mathbf{c}_j \in C \\ \mathbf{c}_i \neq \mathbf{c}_j}} \|\mathbf{c}_i - \mathbf{c}_j\| = \min_{\substack{\mathbf{c} \in C \setminus \{0\} \\ \text{perché } C \text{ è lineare}}} \|\mathbf{c}\|_H = w_H(C)$$

### 2.2.3 Matrice Generatrice

**Def** La matrice generatrice di un codice lineare a blocco è una matrice  $G$  tale che

$$G \cdot b$$

dove  $b$  è un vettore binario di  $K$  bit

$c$  è un vettore binario di  $n$  bit

$G$  è una matrice binaria  $n \times K$  con colonne linearmente indipendenti.

**Oss** Le colonne di  $G$  sono parole di codice linearmente indipendenti che formano una base di  $C$

- Posso costruire la matrice con  $K$  parole di codice linearmente indipendenti

### ES

$$n=4 \quad k=3 \quad G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \begin{aligned} c_1 &= b_1 \\ c_2 &= b_2 \\ c_3 &= b_3 \\ c_4 &= b_1 \oplus b_2 \oplus b_3 \end{aligned} \quad C = \{0000, 1001, 0101, 0011, 1100, 1010, 0110\}$$

$$c = G \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+0+0 \\ 0+0+0 \\ 0+0+1 \\ 1+0+1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

**oss** Posso sostituire colonne di  $\mathcal{G}$  con combinazioni lineari delle colonne e ottenere ancora una matrice generatrice dello stesso codice.

**oss** Posso permutare righe di  $\mathcal{G}$  e ottenere un insieme diverso di parole di codice, ma le prestazioni non cambiano

$$\begin{array}{l} c_1 = b_1 \\ c_1 = b_1 + b_2 \\ c_2 = b_1 + b_2 \end{array} \rightarrow \begin{array}{l} c_1 = b_1 + b_2 \\ c_2 = b_1 \end{array}$$

$$\left[ \begin{array}{c|c} c_1 & c_2 \\ \hline c_1 & c_2 \\ \vdots & \vdots \end{array} \right] = \boxed{\quad} \quad \boxed{b}$$

**Def** Diciamo  $\mathcal{G}$  in forma sistematica  $\mathcal{G} = \begin{bmatrix} I_k \\ A \end{bmatrix}$  dove  $A \in (n-k) \times k$

**oss** È sempre possibile, mediante permutazioni di righe e combinazioni lineari delle colonne, ottenere una matrice generatrice in forma sistematica a partire da una matrice generatrice qualsiasi.

**oss**  $c = \mathcal{G}b = \begin{bmatrix} b \\ Ab \end{bmatrix}$ , è sufficiente memorizzare  $A$

### 2.2.3 Bound di Singleton

Per codici lineari a blocco la distanza minima del codice è limitata superiormente

$$d_{\min} \leq n-k+1$$

DIM

Consideriamo  $\mathcal{G}$  in forma sistematica di un codice lineare  $\mathcal{G} = \begin{bmatrix} I_k \\ A \end{bmatrix}$

$w_H(\mathcal{G}) \leq 1+(n-k)$   
colonne  $k$ -esime di  $\mathcal{G}$  ipotessi che  $A$  abbia tutti "1"

$$\text{quindi } d_{\min} = w_H(\mathcal{C}) \leq 1+(n-k)$$

### 2.2.4 Decodifica di Codici di Canale a Blocco Lineari

#### MATRICE CONTROLLO PARITÀ

**Def** La matrice  $H: l \times n$  è di controllo di parità per il codice lineare a blocco  $\mathcal{C}$  se soddisfa

$$H\mathcal{C} = 0 \iff \mathcal{C} \subseteq \mathcal{E}$$

TEO

$H$  è una matrice di controllo di parità di un codice con matrice generatrice  $\mathcal{G}$  se e solo se

$$\underbrace{H}_{\text{dim } \mathcal{L} \text{ rank } l \times k} \mathcal{G} = 0 \quad \text{e} \quad \text{rang}(H) = n-k$$

DIM

$$H\mathcal{C} = H\mathcal{G}b = 0 \Rightarrow Hx = 0$$

Le parole di codice sono nel Kernel di  $H$  (ovvero  $H$  le parole in  $\mathcal{E}$ ), quindi  $\dim \text{Ker}(H) = K = \text{null}(H)$

$$n = \text{null}(H) + \text{rang}(H) \Rightarrow \text{rang}(H) = n-k$$

**oss** Poiché  $\text{rang}(H) = n-k$  ci devono essere  $n-k$  righe linearmente indipendenti  $\Rightarrow l \geq n-k$  (noi cercheremo  $l = n-k$ )

**PROP** Se  $G = \begin{bmatrix} I_K \\ A \end{bmatrix}$  allora  $H = [A | I_{n-K}]$

**DIM** 1.  $\text{rang}(H) = n - K$  perché c'è  $I_{n-K}$

$$2. H G = [A | I_{n-K}] \cdot \begin{bmatrix} I_K \\ A \end{bmatrix} = A I_K + I_{n-K} A = A + A = 0$$

$$A = A$$

**OSS** - È possibile permutare le colonne di  $H$  e ottenere un codice con le stesse prestazioni.

- È possibile sostituire una riga di  $H$  con una combinazione lineare delle altre righe ottenendo una matrice di parità dello stesso codice.

**OSS** Permutare le colonne  $i$  e  $j$  di  $H$  equivale a permutare le righe  $i$  e  $j$  di  $G$ .

**OSS** Sostituire colonne di  $G$  con combinazioni lineari non modifica  $H$ , sostituire righe di  $H$  con combinazioni lineari non modifica  $G$

**ES**

$$\text{Sia } A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

$$x = (1, 0, 0, 0, 1, 1) \in \mathcal{C} \quad Hx = (1+1+0+0+0+0, 1+0+1+1+0+0, 0+1+0+0+0+1) = (0, 0, 0) \quad \checkmark$$

### DECODIFICA CON SINDROME

La matrice di controllo parità permette un migliore algoritmo per applicare il criterio MD.

Sia  $y$  la parola ricevuta,  $y = c + \epsilon$  dove  $c$  è la parola trasmessa e  $\epsilon$  l'errore.

**Def** Il vettore di sindrome è definito come  $s = Hy$  ed ha lunghezza  $n - k$

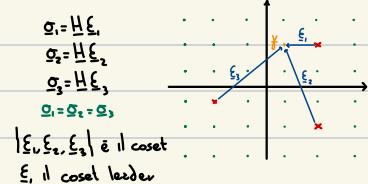
$$s = Hy = H(c + \epsilon) = Hc + H\epsilon = H\epsilon$$

**PROP**  $s = 0 \iff y \in \mathcal{C} (\epsilon = 0)$

**OSS** Se  $s \neq 0$  sicuramente c'è un errore. Il coset rende possibile anche la correzione degli errori.

**OSS** La corrispondenza tra  $\epsilon$  e  $s$  non è 1:1. Ci sono  $2^k$   $\epsilon$  e  $2^{n-k}$   $s$ .

In particolare il coset è lo stesso per ogni errore che porta una qualsiasi parola di  $\epsilon \in \mathcal{E}$



**Def** Sia  $s$  una sindrome, il suo coset è l'insieme delle sequenze  $\epsilon$  che hanno  $s$  come sindrome.

**OSS** Dato  $\tilde{\epsilon}$  t.c.  $H\tilde{\epsilon} = s$  tutti gli altri elementi del coset  $\tilde{\epsilon}_i$  sono  $\tilde{\epsilon}_i + \epsilon_i \forall \epsilon_i \in \mathcal{C}$

**Def** Una delle sequenze a peso di Hamming minimo nel coset  $s$  si chiama coset leader

$$E_{\min}(s) = \min_{\epsilon \in \text{coset di } s} \| \epsilon \|_H$$

**OSS** Se ci sono più sequenze a peso minimo ne scelgo una a caso. (sono nel caso

Vediamo come questo modifica il criterio di minima distanza.

$$\hat{\mathbf{e}} = \mathbf{y} + \underset{\mathbf{e} \in \mathcal{E}}{\operatorname{argmin}} \|\mathbf{y} - \mathbf{e}\|_H = \mathbf{y} + \underset{\mathbf{e} \in \mathcal{E}}{\operatorname{argmin}} \|\mathbf{E}(\mathbf{e})\|_H \Rightarrow \hat{\mathbf{e}} = \mathbf{y} + \mathbf{e}_{\min}(\mathbf{s})$$

$\mathbf{E}(\mathbf{e})$  è l'errore che devo sommare a  $\mathbf{s}$  per trovare  $\mathbf{y}$

Per migliorare le prestazioni è possibile memorizzare la tabella che associa ogni sindrome al suo coset leader

$$\mathbf{s} = \mathbf{H}\mathbf{e} \rightarrow \underline{\mathbf{s} | \mathbf{e}_{\min}} \rightarrow \hat{\mathbf{e}} = \mathbf{y} + \mathbf{e}_{\min}$$

ES

$$\text{Sic } \mathcal{C} = \{0000, 1010, 0101, 1111\} \quad G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

coset	$\mathbf{e}_{\min}$	$\mathbf{s}$
e	0000	00
{0000, 1110, 0001, 1011}	0001	01
{0000, 0010, 1101, 0111}	0010	10
{0001, 0011, 1100, 0110}	0011	11

$$\mathbf{s} = \begin{pmatrix} 1010 \\ 0101 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (2tc, b+d)$$

Sic  $\mathbf{y} = 1000$ ,  $\mathbf{s} = \mathbf{H}\mathbf{y} = [0, 1]$ , il coset leader è 0010

$\mathbf{y} + 0010 = 1010 \leftarrow$  parola decodificata

## 2.3 Implementazione - Codici di Hamming

Un codice di Hamming ha le colonne della matrice di parità che sono tutte e sole le sequenze di  $(n-k)$  bit non nulli. Il codice esiste se e solo se  $n=2^{k-h}-1$ .

ES  $n=7$ ,  $k=4$ ,  $n-k=3$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{\text{forma sistematica}} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad I_{n-k}$$

$d_{\min}$

per il codice di Hamming  $d_{\min}=3$

quindi rileva fino a 2 errori e corregge 1 errore

DIM

1) Non esistono parole di codice con  $w_H=1$

$$\mathbf{H} \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \mathbf{h}_1 \neq 0 \quad \text{perché le colonne di } \mathbf{H} \text{ sono non nulli}$$

colonna i-esima di  $\mathbf{H}$

2) Non esistono parole di codice con  $w_H=2$

$$\mathbf{H} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 \quad \text{infatti } \mathbf{h}_1 + \mathbf{h}_2, \text{ le colonne di } \mathbf{H} \text{ sono tutte diverse}$$

3) Esiste almeno una parola di codice con  $w_H=3$

$$\mathbf{H} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 \quad \text{se } \mathbf{h}_1 = \mathbf{h}_2 + \mathbf{h}_3 \neq 0 \quad \text{allora } \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3 = 0 \quad \text{e } \mathbf{h}_1 \in \mathbb{H}$$

Quindi  $d_{\min} = w_H(\mathcal{C}) = 3$

## BOUND DI HAMMING

Il codice di Hamming è ottimo perché soddisfa il bound di Hamming  $\left(\frac{k}{n} \leq 1 - \frac{1}{n} \log_2 \left[ \sum_{r=0}^t \binom{n}{r} \right]\right)$  all'ugualanza.

DIM

$$d_{\text{min}} = 3 \Rightarrow t = 1$$

$$1 - \frac{1}{n} \log_2 \left[ \binom{n}{1} + \binom{n}{0} \right] = 1 - \frac{1}{n} \log_2 (1+n) = 1 - \frac{1}{n} \log_2 (1+2^{n-k}) = 1 - \frac{1}{n} (n-k) = \frac{n-k}{n} = \frac{k}{n}$$

## 4. Teoria dell'Informazione

Ogni evento porta con sé una certa informazione, è la realizzazione di qualcosa di inaspettato.

L'evento "un uomo mangia un pollo" porta meno informazione di "un pollo mangia un uomo" perché quest'ultimo avviene con una probabilità minore.

Dato uno spazio degli eventi  $\Omega = \{A_1, \dots, A_n\}$  e una probabilità  $P(A)$

Vogliamo misurare l'informazione portata da un evento, diremo queste quantità  $i(A)$ .

### 4.1 Assiomi dell'Informazione

Dell'intuizione di informazione cerchiamo una funzione  $i: \Omega \rightarrow \mathbb{R}$  tale che:

$$1. i(A) \geq 0 \quad \forall A$$

$$2. P(A) \leq P(B) \Rightarrow i(A) \geq i(B)$$

$$3. i(\Omega) = 0$$

$$4. A \text{ e } B \text{ indipendenti} \Rightarrow i(A \cap B) = i(A) + i(B)$$

Def  $i(A) = -\log_2 P(A)$ , b1, soddisfa gli assiomi

$$\text{se } b=2 \quad [i(A)] = \text{bit}$$

$$b=e \quad [i(A)] = \text{neper}$$

### 4.2 Informazione di una V.A. Discreta

Sia  $x \in A_x = \{z_1, \dots, z_n\}$ ,  $p_x(z) = P(x=z)$

Def La funzione di informazione della variabile aleatoria discreta  $x$  è:

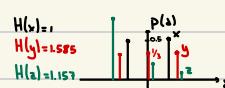
$$i_x(z) = i(x=z) = -\log_2 p_x(z)$$

Def Una variabile  $x$  si dice deterministica se  $i_x(z)=0 \quad \forall z$ , ovvero se  $p_x(z)=1$  oppure  $p_x(z)=0 \quad \forall z \in A_x$

### 4.3 Entropia di una V.A. Discreta

Def L'entropia di una variabile aleatoria discreta  $x$  è una misura dell'informazione media portata da una V.A.

$$H(x) = E(i_x(z)) = \sum_{z \in A_x} i_x(z) p_x(z) = \sum_{z \in A_x} -\log_2 p_x(z) \cdot p_x(z)$$



## PROP

1.  $H(x) \geq 0$
2.  $H(x) = 0 \Leftrightarrow x \text{ è deterministico}$
3.  $H(x) = \log_2 M$  dove  $M = |A_x|$
4.  $H(x) = \log_2 M \Leftrightarrow x \text{ è uniforme sull'alfabeto } (p_x(a) = \frac{1}{M} \forall a)$

## DIM

1.  $i_x(z) \geq 0, p_x(z) \geq 0 \Rightarrow H(x) \text{ è una somma di elementi positivi.}$

2.  $H(x) = \sum_{a \in A} i_x(a) \cdot p_x(a) = 0$

4.  $H(x) = E(i_x(x)) = E(-\log_2 p_x(x)) = E(\log_2 \frac{1}{p_x(x)}) < \log_2 E(\frac{1}{p_x(x)}) = \log_2 M$

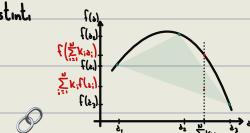
$\log$  è convesso  
disegnabilità di Jensen

OSS  $p_x(a)$  è un numero  $p_x(x)$  è una V.A. (applico  $p_x \mapsto x$  e mi ritorno ancora una V.A.)

## DISUGUAGLIANZA DI JENSEN

**Def** Una funzione  $f(x)$  è strettamente concava se dati  $K_1, \dots, K_n \in [0, 1]$  t.c.  $\sum_{i=1}^n K_i = 1$  e dati  $a_1, \dots, a_n$  distinti

vale che:  $\sum_{i=1}^n K_i f(a_i) < f\left(\sum_{i=1}^n K_i a_i\right)$



$\sum_{i=1}^n K_i a_i \leq \sum_{i=1}^n K_i a_n \leq a_n$  Viscoltà di  $K_1, \dots, K_n$

Il punto  $\left[\sum_{i=1}^n K_i a_i, \sum_{i=1}^n K_i f(a_i)\right]$  si trova sempre nell'area verde, trovata varendo i  $K$ .

Il punto  $\left[\sum_{i=1}^n K_i a_i, f\left(\sum_{i=1}^n K_i a_i\right)\right]$  si trova sul sostegno di  $f$ .

**PROP** - diseguaglianza di Jensen

Sia  $f$  una funzione strettamente concava e  $X$  una variabile casuale.

Allora:  $E(f(x)) < f(E(x)) \Rightarrow \sum_{a \in A_x} p_x(a) f(a) < f\left(\sum_{a \in A_x} p_x(a) a\right) \quad (p_x(a) \mapsto K_i \text{ e } a \mapsto a_i)$

### 4.3.1 Entropia Congiunta

L'entropia congiunta è l'entropia di un insieme di variabili

$$H(x,y) = \sum_{a \in A, b \in B} p_{x,y}(a,b) i_{x,y}(a,b)$$

**PROP** L'entropia congiunta di v.a. indipendenti è  $H(X,Y) = H(x) + H(y)$

$$\begin{aligned} \text{DIM } H(x,y) &= \sum_{a \in A, b \in B} p_{x,y}(a,b) i_{x,y}(a,b) = \sum_{a \in A} p_x(a) \sum_{b \in B} p_y(b) [i_{x,y}(a) + i_{y,y}(b)] = \sum_{a \in A} p_x(a) \sum_{b \in B} p_y(b) i_{y,y}(b) + \sum_{a \in A} p_x(a) i_{x,x}(a) = H(x) + H(y) \\ i_{y,y}(b) &= i_y(b) + i_y(b) \end{aligned}$$

**PROP** L'entropie congiunte di v.a. non indipendenti né funzioni deterministiche l'una dell'altra è  $H(x,y) < H(x) + H(y)$

$$\begin{aligned} \text{DIM } H(x,y) - H(x) - H(y) &< 0 \Rightarrow E_{x,y} \left( \log_2 \frac{1}{p_{x,y}(x,y)} - \log_2 \frac{1}{p_x(x)} - \log_2 \frac{1}{p_y(y)} \right) = E_{x,y} \left( \log_2 \frac{p_x(x)p_y(y)}{p_{x,y}(x,y)} \right) < \log_2 E_{x,y} \left( \frac{p_x(x)p_y(y)}{p_{x,y}(x,y)} \right) = \\ &= \log_2 \left( \sum_{a \in A, b \in B} p_{x,y}(a,b) \frac{p_x(a)p_y(b)}{p_{x,y}(a,b)} \right) = \log_2(1) = 0 \end{aligned}$$

L'entropia congiunta di due V.A. dove  $y$  non è una funzione deterministica di  $x$ , allora  $H(x,y) > H(x)$

DIM Esiste una coppia di valori  $\bar{a} \in X$  e  $\bar{b} \in Y$  per cui

$$p_{x,y}(\bar{a},\bar{b}) < p_x(\bar{a}) \Rightarrow \log_2 \frac{1}{p_{x,y}(\bar{a},\bar{b})} > \log_2 \frac{1}{p_x(\bar{a})} \Rightarrow \log_2 \frac{1}{p_{x,y}(\bar{a},\bar{b})} \geq \log_2 \frac{1}{p_y(\bar{b})} \quad \forall a,b$$

il denominatore diventa >

$$\text{quindi } H(x,y) = \sum_{a,b} p_{x,y}(a,b) \log_2 \frac{1}{p_{x,y}(a,b)} > \sum_{a,b} p_{x,y}(a,b) \log_2 \frac{1}{p_y(b)} = H(y)$$

L'entropia congiunta di due V.A. è, in generale:  $\max\{H(x), H(y)\} \leq H(x,y) \leq H(x) + H(y)$

= se una delle due variabili è funzione deterministica dell'altra
= se  $x$  e  $y$  indipendenti.

#### 4.3.2 Entropia Condizionata

Sia  $X$  una V.A. che condiziona ad un'altra V.A.  $Y$ , allora:

- la densità di probabilità condizionata è  $p_{x|y}(a|b) = P(x=a|y=b)$

- la funzione di informazione condizionata è  $i_{x|y}(a|b) = \log_2 \frac{1}{p_{x|y}(a|b)}$

- l'entropia condizionata ad un certo valore di  $Y$  è  $H(x|Y=b) = E_x(i_{x|y}(a|b))$

OSS Se  $x$  e  $y$  sono indipendenti:  $H(x|Y=b) = H(x)$

PROP l'entropia condizionata è  $H(x|Y) = E_y(H(x|Y=y)) = \sum_{b \in B} p_y(b) H(x|Y=b) = \sum_{b \in B} p_y(b) \sum_{a \in A} p_{x|y}(a|b) \log_2 \frac{1}{p_{x|y}(a|b)} =$

$$= \sum_{a \in A, b \in B} p_{x|y}(a|b) p_y(b) \log_2 \frac{p_y(b)}{p_{x|y}(a|b) p_y(b)} = \sum_{a \in A, b \in B} p_{x|y}(a|b) \log_2 \frac{p_y(b)}{p_{x|y}(a|b)} = \sum_{a \in A, b \in B} p_{x|y}(a|b) \left( \log_2 \frac{1}{p_{x|y}(a|b)} - \log_2 \frac{1}{p_y(b)} \right)$$

$$= H(x,y)$$

quindi  $H(x|Y) = H(X,Y) - H(Y) \Rightarrow H(X,Y) = H(x|Y) + H(Y)$

#### 4.3 Vettori Aleatori

Sono vettori del tipo  $\mathbf{x} = [x_1, \dots, x_N] \in A, x_i \in A_i$ , dove  $x_i, i=1, \dots, N$  è una V.A.

La densità di probabilità di  $\mathbf{x}$  è  $p_{\mathbf{x}}(\mathbf{z}) = P(\mathbf{x}=\mathbf{z}) = P(x_1=z_1, \dots, x_N=z_N)$

La funzione di informazione di  $\mathbf{x}$  è  $i_{\mathbf{x}}(\mathbf{z}) = \log_2 \left( \frac{1}{P_{\mathbf{x}}(\mathbf{z})} \right)$

L'entropia di  $\mathbf{x}$  è  $H(\mathbf{x}) = E(i_{\mathbf{x}}(\mathbf{z})) = \sum_{\mathbf{z} \in \Omega} p_{\mathbf{x}}(\mathbf{z}) \log_2 \frac{1}{p_{\mathbf{x}}(\mathbf{z})}$

#### 4.4 Informazione Mutua tra due V.A.

Diciamo informazione mutua la quantità di informazione in comune tra  $X$  e  $Y$

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = H(X) + H(Y) - H(X|Y) - H(Y|X) = H(X) - H(X|Y)$$

PROP  $I(X;Y) = I(Y;X)$ , I gode di proprietà commutativa

DIM  $I(X;Y) = H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$

**Oss** So che  $I(x;y) \geq 0$  perché  $H(x,y) \leq H(x) + H(y)$

**Oss**  $I(x;y) \leq \min\{H(x), H(y)\}$  perché  $I(x;y) = H(x) - H(x|y) \stackrel{>0}{=} I(x;y) \Rightarrow I(x;y) \leq H(x)$   
 $I(x;y) = H(y) - H(y|x) \stackrel{>0}{=} I(x;y) \Rightarrow I(x;y) \leq H(y)$

**Oss** Se  $X$  e  $Y$  sono indipendenti  $I(x;y) = H(x) - H(x|y) = 0$

**Oss** Se  $X=Y$   $I(x;y) = H(x) - H(x|y) = H(x) = H(y)$   
se conosco  $y$  non ho incertezza su  $x$

## 4.5 Sorgente di Simboli

Diciamo sorgente di simboli un dispositivo che emette dei simboli presi da un alfabeto discreto ad intervalli regolari (che diremo periodo di simbolo,  $T$ )



Siamo interessati all'informazione trasmessa, quindi voglio trovare l'entropia di un vettore contenente tutti i simboli trasmessi.

$$\underline{x} = [x_1, x_2, \dots, x_{N+1}, \dots, x_N]$$

simbolo emesso al tempo  $N$

### 4.5.1 Entropia per Simbolo

Sia  $\underline{x}$  un vettore di lunghezza  $2N+1$   $[x_1, \dots, x_N]$

$$H(\underline{x}) = (2N+1)H(x_n)$$

se i simboli sono equiprobabili  
e identicamente distribuiti

quindi l'entropia di un simbolo è  $H_s(\underline{x}) = \frac{1}{2N+1}H(\underline{x})$

Tornando al caso con  $\underline{x}$  di lunghezza infinita

$$H_s(\underline{x}) = \lim_{N \rightarrow +\infty} \frac{H(x_1, \dots, x_N)}{2N+1}$$

**Prop**  $0 \leq H_s(\underline{x}) \leq \log M$

**Def** Il tasso di informazione di un messaggio è

$$R(\underline{x}) = \frac{H_s(\underline{x})}{T} \quad [\text{bit/s}]$$

**Oss** uno schermo fisso o in loop ha tasso di informazione 0 ( $H_s(\underline{x})=0$ )

**Def** L'informazione mutua per simbolo tra due sorgenti è:

$$I_s(x;y) = H_s(x) + H_s(y) - H_s(x,y)$$

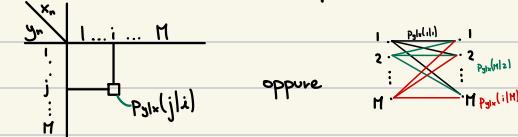
## 4.6 Canale M-ario Senza Memoria

Un canale dove i segnali in ingresso ed in uscita sono presi da un alfabeto di cardinalità  $M$ .

L'uscita del canale al tempo  $n$  dipende solo dall'ingresso al tempo  $n$

### 4.6.1 Matrice di Transizione

La matrice di transizione ci permette di trovare le probabilità di ogni uscita dato l'ingresso.



### 4.6.2 Tasso di Informazione

Sia il canale M-ario  $f$ , allora il suo tasso di informazione è:

$$R(f) = \frac{I_S(x; y)}{T} = \frac{H_S(x) + H_S(y) - H_S(x, y)}{T} \quad [\text{bit/s}]$$

ES nel canale  $y=x$   $R(f) = \frac{H_S(x) + H_S(x) - H_S(x, x)}{T} = R(x)$

ES nel canale  $y=[0, \dots, 0]$   $R(f) = 0 \text{ bit/s}$

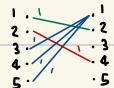
quindi  $R(f) \leq R(x)$

## 4.7 Capacità

La capacità di un canale è il tasso di informazione del canale massimo al variare delle densità di probabilità dell'ingresso  $\{p_x(\cdot)\}$  (ovvero ipotizzando di essere nelle migliori condizioni di sorgente)

$$C = \max_{\{p_x(\cdot)\}} R(f) = \max_{\{p_x(\cdot)\}} \frac{I_S(x; y)}{T} \quad [C] = \frac{\text{bit}}{\text{s}}$$

### 4.7.1 Capacità del Canale M-Ario senza Memoria



Posso ottenere una capacità migliore ponendo  $p_x(3)=p_x(4)=p_x(5)=0$

così ottengo un canale binario con  $y=x$  ( $1 \rightarrow 2$ )

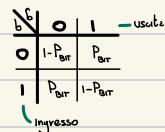
quindi  $R(f) = R(x) = \log_2 2 = 1 \text{ bit/s}$

Oppure posso utilizzare i dei 3 segnali che partono in 1. Quindi  $p_x(4)=p_x(5)=0$

Il canale è sempre con  $y=x$  ( $2 \rightarrow 4$ ) e  $R(f) = R(x) = \log_2 3 > \log_2 2$

Ottengo così una capacità migliore.

#### 4.7.2 Capacità del Canale Binario senza Memoria



il canale è senza memoria  
posso studiare il singolo bit

$$C = \max_{\{P_B\}} \frac{I_b(b; \hat{b})}{T} = \max_{\{P_B, P_B(0), P_B(1)\}} \frac{I(b; \hat{b})}{T} = \max_{\{P_B\}} \frac{I(b; \hat{b})}{T}$$

$P_B(i) = 1 - P_B(\bar{i})$

dove  $I(b; \hat{b}) = H(\hat{b}) - H(\hat{b}|b)$

dove  $H(\hat{b}; b) = E_b[H(\hat{b}|b=i)] = P_b(0)H(\hat{b}|b=0) + P_b(1)H(\hat{b}|b=1)$

dove  $H(\hat{b}|b=0) = \sum_{i=0} P_B(i|0) \log_2 \frac{1}{P_B(i|0)} = P_B(0|0) \log_2 \frac{1}{P_B(0|0)} + P_B(1|0) \log_2 \frac{1}{P_B(1|0)} = P_{Bit} \log_2 \frac{1}{P_{Bit}} + (1 - P_{Bit}) \log_2 \frac{1}{1 - P_{Bit}}$

e  $H(\hat{b}|b=1) = \sum_{i=1} P_B(i|1) \log_2 \frac{1}{P_B(i|1)} = P_B(0|1) \log_2 \frac{1}{P_B(0|1)} + P_B(1|1) \log_2 \frac{1}{P_B(1|1)} = (1 - P_{Bit}) \log_2 \frac{1}{1 - P_{Bit}} + P_{Bit} \log_2 \frac{1}{P_{Bit}}$

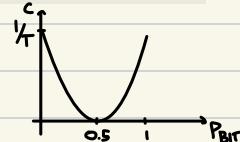
quindi  $H(\hat{b}|b=0) = H(\hat{b}|b=1)$

quindi  $H(\hat{b}; b) = P_{Bit} \log_2 \frac{1}{P_{Bit}} + (1 - P_{Bit}) \log_2 \frac{1}{1 - P_{Bit}}$

quindi  $I(b; \hat{b}) = H(\hat{b}) - [P_{Bit} \log_2 \frac{1}{P_{Bit}} + (1 - P_{Bit}) \log_2 \frac{1}{1 - P_{Bit}}]$  non dipende dall'ingresso  $b$

per massimizzare  $I(b; \hat{b})$  devo massimizzare  $H(\hat{b}) \Rightarrow P_B(0) = P_B(1) = \frac{1}{2} \Rightarrow P_B(0) = P_B(1) = \frac{1}{2}$

$$C = \frac{1}{T} \left[ -P_{Bit} \log_2 \frac{1}{P_{Bit}} - (1 - P_{Bit}) \log_2 \frac{1}{1 - P_{Bit}} \right]$$



#### 4.7.3 Capacità di un Canale AWGN

Ottenerò un canale dove  $r_n = s_n + w_n$

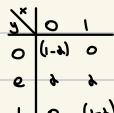
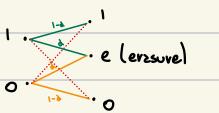
$$C = \frac{1}{2T} \log_2 \left( 1 + \frac{E(s^2)}{E(w^2)} \right)$$

perdita di simbolo

Per ottenere  $C$ , ottenerò la capacità ideale, servirebbe un numero infinito di segnali distribuiti secondo una gaussiana.

con densità di probabilità di  $s_n \sim N(0, E(s^2))$

#### 4.7.4 Capacità di un Canale con Ingresso Binario e Cancellazione



Quando finiamo su "e" non sappiamo se è stato trasmesso "0" o "1". Questo è un modo per indicare al decodificatore quanto è incerto la demodulazione.

ES si ottiene un dispositivo che fa interferenza, ottengo tutti e, decido di rinunciare alla decodifica.

$$p_y(0) = p_{y|x=0}(0|0)p_x(0) + p_{y|x=0}(0|1)p_x(1) = (1-\alpha)p_x(0)$$

$$p_y(1) = p_{y|x=1}(1|0)p_x(0) + p_{y|x=1}(1|1)p_x(1) = \alpha p_x(1)$$

$$p_y(e) = p_{y|x=0}(e|0)p_x(0) + p_{y|x=0}(e|1)p_x(1) = \alpha p_x(1) + (1-\alpha)p_x(0) = \alpha$$

il canale è senza memoria

$$c = \frac{1}{T} \max_{I_p} I_p(x:y) = \frac{1}{T} \max_{I_p} I(x:y)$$

$$\text{dove } I(x:y) = H(y) - H(y|x)$$

$$\text{dove } H(y) = E\left(\log_2 \frac{1}{p_y(y)}\right) = (1-\alpha)p_x(0) \log_2 \frac{1}{p_y(0)} + (1-\alpha)p_x(1) \log_2 \frac{1}{p_y(1)} + \alpha \log_2 \frac{1}{\alpha}$$

$$\text{e } H(y|x) = \sum_z p_x(z) H(y|x=z) = p_x(0)H(y|x=0) + p_x(1)H(y|x=1)$$

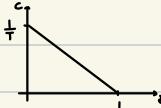
$$\text{dove } H(y|x=0) = \sum_b p_{y|x=0}(b|0) \log_2 \frac{1}{p_{y|x=0}(b|0)} = \alpha \log_2 \frac{1}{\alpha} + (1-\alpha) \log_2 \frac{1}{1-\alpha}$$

$$\text{e } H(y|x=1) = \alpha \log_2 \frac{1}{\alpha} + (1-\alpha) \log_2 \frac{1}{1-\alpha}$$

$$\text{quindi } H(y|x) = \alpha \log_2 \frac{1}{\alpha} + (1-\alpha) \log_2 \frac{1}{1-\alpha}$$

$$\begin{aligned} \text{quindi } I(x:y) &= (1-\alpha)p_x(0) \log_2 \frac{1}{p_y(0)} + (1-\alpha)p_x(1) \log_2 \frac{1}{p_y(1)} + \alpha \log_2 \frac{1}{\alpha} - \alpha \log_2 \frac{1}{\alpha} - (1-\alpha) \log_2 \frac{1}{1-\alpha} \\ &= (1-\alpha)p_x(0) \left( \log_2 \frac{1}{p_y(0)} + \log_2 \frac{1}{p_x(0)} \right) + (1-\alpha)p_x(1) \left( \log_2 \frac{1}{p_y(1)} + \log_2 \frac{1}{p_x(1)} \right) - (1-\alpha) \log_2 \frac{1}{1-\alpha} \\ &= (1-\alpha) \left[ p_x(0) \log_2 \frac{1}{p_y(0)} + p_x(1) \log_2 \frac{1}{p_y(1)} \right] = 1-a \\ &\quad = H(x|z=1) \end{aligned}$$

$$c = \frac{1}{T} (1-\alpha)$$



#### 4.8 Teorema di Shannon per la Codifica di Canale

Considerando un canale *mario* senza memoria con periodo di simbolo  $T$  e capacità  $c$ . Sia  $|b_2|$  una sorgente di simboli con cardinalità dell'alfabeto dei simboli  $M$  e tasso di informazione nominale del messaggio  $R = \frac{\log M}{Tb}$  (l'upper-bound, ovvero un segnale che non può essere compresso)

- se  $R < C$   $\forall n > 0$ , e ogni  $n$  sufficientemente grande esistono:

1. Un codificatore di canale che restituisce parole di lunghezza  $n$  e lettere prese dall'alfabeto  $M$ -ario con un numero di parole possibili  $\geq 2^{nR}$  ( $\geq 2^{\frac{nR}{Tb}}$ ) (che è lo stesso numero di parole in ingresso).  
(ci indica il numero di parole che vengono prese in input dal codificatore)
2. Un decodificatore con probabilità di errore sulla parola di codice inferiore  $> \delta$

- se  $R > C$  esiste un  $S_{\min} > L_C$  ogni codice è corretto per queste sorgente e questo canale mi fornisce una probabilità di errore sulla parola di codice  $\geq S_{\min}$ .



### INTERPRETAZIONE

Se  $R < C$  allora posso ottenere una probabilità di errore piccola e piccava.

Se  $R > C$  non posso mai scendere al di sotto di una certa probabilità di errore.

Es se  $M=2 \Rightarrow R=\frac{1}{T_b}$

il teorema a dice  $2^K = 2^{nRT} \Rightarrow K = nRT \Rightarrow \frac{K}{n} = RT = \frac{T}{T_b}$

dato che  $R < C \Rightarrow \frac{K}{n} \cdot \frac{1}{T} < C \Rightarrow \frac{K}{n} < CT = \max_{\{p(x)\}} I_S(x; y) \leq 1 \quad (\Rightarrow \frac{K}{n} \leq 1 \Rightarrow K \leq n)$

## 5. Codifica di Sorgente



La codifica di sorgente ha il compito di comprimere i dati inviati dalla sorgente. Ovvero ha il compito di aumentare l'entropia dei dati inviati dalla sorgente.

Esistono due tipologie:

1. con perdite (es. immagine più sgretolata) (non lo studieremo nel corso)
2. senza perdite, i bit vengono recuperati al 100%



Def  $D_x$  è il dizionario delle parole  $x_m$  a lunghezza variabile (es.  $x_1=[11]$ ,  $x_2=[VETTORE]$ )

$D_y$  è il dizionario delle parole  $y_m$

Il codificatore codifica indipendentemente ogni parola in ingresso è quindi una funzione:

$$j_m: D_x \rightarrow D_y, \quad y_m = j_m(x_m) \quad (\text{trasformazione istantanea})$$

Le prestazioni sono valutate osservando la lunghezza media delle parole  $y_m$  (più breve è migliore sono le prestazioni)

**Def** Sia  $D_x$  un dizionario di parole in ingresso al codificatore e sia  $p_x(z) = P(x_m=z)$   $\forall z \in D_x$  la densità di probabilità di tali parole.

Sia  $\mu_y : z \rightarrow y$ ,  $z \in D_x, y \in D_y$

Allora la lunghezza media delle parole in uscita del codificatore è:

$$L_y = E_y(L(y)) = \sum_{z \in D_x} p_x(z) L(\mu_y(z))$$

**oss** Questo assume parole indipendenti tra loro.

**ES**

$D_x : A \ B \ C \ D$

$D_y : 01 \ 101 \ 1111 \ 0101$

ACDBAAC  $\rightarrow$  01, 1111, 0101, 101, 01, 01, 1111  $\rightarrow$  ACAABAAC

L<sub>y</sub> decodifica risultate incorrette poiché il codice non è prefisso.

#### 5.0.1 Codici a Prefisso

In un codice di sorgente a prefisso nessuna parola del dizionario  $D_x$  è la prima parte (prefisso) di un'altra parola di codice.

È un codice senza perdite, quindi è necessaria una corrispondenza biunivoca tra  $D_x$  e  $D_y$ .

### 5.1 Teorema di Kraft-McMillan

1. Per ogni codificatore di sorgente senza perdite deve valere:

$$\sum_{y \in D_y} \frac{1}{M_y} \leq 1 \quad \text{dove } M_y \text{ è la cardinalità dell'alfabeto delle parole di uscita}$$

**oss** se  $M_y$  è grande è più facile soddisfare la disequazione, ma l'obiettivo è usare parole più piccole possibili.

2. Per una sorgente con dizionario  $D_x$  di cardinalità  $N$  (la stessa cardinalità di  $D_y$ ) se  $l_1, \dots, l_N$  sono interi t.c.  $\sum_{i=1}^N \frac{1}{M_{\mu_y(i)}} \leq 1$  dove  $M_y$  intero.

Allora esiste un codice a prefisso per la sorgente con alfabeto di cardinalità  $M_y$  e parole lunghe  $l_1, \dots, l_N$ .

#### INTERPRETAZIONE

$\sum_{y \in D_y} \frac{1}{M_y}$  è una misura dell'efficienza del codice:

se = 1 il codice può essere a prefisso e di lunghezza media minima.

se < 1 il codice non può essere a prefisso.

se > 1 il codice può essere a prefisso, anche se non ottimo.

## 5.2 Teorema di Shannon per la Codifica di Sorgente

1. Per ogni codice di sorgente con alfabeto di uscita di cardinalità  $M_y$ ,

e lunghezza media delle parole di codice deve soddisfare:

$$L_y \geq \frac{H(x)}{\log_2 M_y}$$

2. Esiste un codice a prefisso con alfabeto di cardinalità  $M_y$

e lunghezza media delle parole di codice:

$$L_y < \frac{H(x)}{\log_2 M_y} + 1$$

dove  $H(x)$  è l'entropia delle parole in ingresso al codificatore.

1+2.  $\Rightarrow$  è possibile trovare un codice di sorgente t.c.:

$$\frac{H(x)}{\log_2 M_y} \leq L_y < \frac{H(x)}{\log_2 M_y} + 1$$

**DIM**

1. Dal punto 1. del teorema di Kraft-McMillan

$$1 \geq \sum_{b \in D_y} \frac{1}{M_y^{|U(y)|}} = \sum_{b \in D_y} p_y(b) \frac{1}{M_y^{|U(y)|}} = E_y \left[ \frac{1}{M_y^{|U(y)|}} \right]$$

$$\Rightarrow 1 \geq E_y \left[ \frac{1}{M_y^{|U(y)|}} \right] \Rightarrow \log_2 1 \geq \log_2 E_y \left[ \frac{1}{M_y^{|U(y)|}} \right] \geq E_y \left[ \log_2 \frac{1}{M_y^{|U(y)|}} \right] = E_y \left[ \log_2 \frac{1}{M_y^{|U(y)|}} + \log_2 \frac{1}{p_y(y)} \right] = E_y \left[ U(y) \log_2 \frac{1}{M_y} \right] + H(x)$$

$$\Rightarrow L_y \log_2 \frac{1}{M_y} + H(x) \leq 0 \Rightarrow L_y \geq \frac{H(x)}{\log_2 M_y}$$

$x=y$ : le densità di prob. di  $x$  e  $y$   
sono uguali perché è una mappatura 1:1

2. Consideriamo come lunghezza delle parole di codice  $l_i = \log_{M_y} p_x(\varepsilon_i)$   $\forall \varepsilon_i \in D_x$

Verifichiamo di soddisfare il punto 2. del teorema di Kraft-McMillan

$$\sum_{i=1}^n \frac{1}{M_y^{l_i}} \leq 1 \Rightarrow \sum_{i=1}^n \left( \frac{1}{M_y} \right)^{\log_{M_y} p_x(\varepsilon_i)} \leq \sum_{i=1}^n \left( \frac{1}{M_y} \right) \log_{M_y} p_x(\varepsilon_i) = \sum_{i=1}^n p_x(\varepsilon_i) = 1 \quad \checkmark$$

so quindi che esiste un codice a prefisso per la sorgente con alfabeto di cardinalità  $M_y$  e parole lunghe  $l_i$

$$\text{Inoltre } L_y = E \left[ \log_{M_y} p_x(\varepsilon_i) \right] < E \left[ \log_{M_y} p_x(\varepsilon_i) + 1 \right] = 1 + E \left[ \frac{\log p_x(\varepsilon_i)}{\log_2 M_y} \right] = 1 + \frac{H(x)}{\log_2 M_y}$$

Il codice con lunghezze  $l_i$  si chiama codice di Shannon.

### 5.2.1 Codice di Shannon

$$l_i = \log_{M_y} p_x(\varepsilon_i) \quad \varepsilon_i \in D_x$$

$$L_y = E \left[ \log_{M_y} p_x(\varepsilon_i) \right] = \frac{H(x)}{\log_2 M_y}$$

Il codice è ottimo solo se  $p_x(\varepsilon_i)$  sono potenze intere di  $\frac{1}{M_y}$  (ovvero  $p_x(\varepsilon_i) = \left(\frac{1}{M_y}\right)^{k_i}, k_i \in \mathbb{Z}\right)$ . In questo caso  $l_i = k_i$ .

ES  $p_x(z_1) = \frac{1}{2}$   $p_x(z_2) = \frac{1}{4}$   $p_x(z_3) = \frac{1}{8}$   $p_x(z_4) = \frac{1}{8}$ ,  $M_y = z$  (output binario)

$$l_1 = \log_{\frac{1}{2}} \frac{1}{2} = 1 \quad l_2 = \log_{\frac{1}{4}} \frac{1}{4} = 2 \quad l_3 = l_4 = \log_{\frac{1}{8}} \frac{1}{8} = 3$$

$$L_y = 1 \cdot l_1 + 2 \cdot l_2 + 3 \cdot l_3 = 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 = 1 + 4 + 9 = 14$$

$\begin{array}{l} z_1 \rightarrow 0 \\ z_2 \rightarrow 10 \\ z_3 \rightarrow 110 \\ z_4 \rightarrow 111 \end{array}$

oss questo codice assegna ai simboli più usati una codifica più breve.

## 5.2.2 Teoremi Caratterizzazione della Codifica di Sorgente Ottima

TEO

Per un codice a prefisso ottimo, le parole di codice a più basse probabilità hanno lunghezza maggiore

DIM

Per assurdo, sia un codice ottimo in cui  $p(x_i) < p(x_j)$  e  $L(y_i) < L(y_j)$

Costruisco un nuovo codice in cui scambio  $y_i$  con  $y_j$ . La lunghezza media è inferiore a quella originale.

TEO

Nel dizionario di un codice a prefisso ottimo ci sono almeno due parole di codice  $b^i$  e  $b^j$  che hanno lunghezze massime e differiscono solo nell'ultimo simbolo.

DIM

- Se ci fosse una sola parola di lunghezza massima

~~1110~~ togliendo i bit finali la lunghezza  $\Rightarrow$  il codice iniziale non era ottimo  $\Rightarrow$  assurdo  
media si riduce

- Similmente, ipotizzando di avere due parole di lunghezza massima diverse fino ad un certo punto

~~1110~~ ~~1100~~ togliendo i bit finali la lunghezza  $\Rightarrow$  il codice iniziale non era ottimo  $\Rightarrow$  assurdo  
media si riduce

- L'unico caso che rende il codice ottimo è:

~~1110~~ due parole di lunghezza massima che differiscono di un solo bit

## 5.2.3 Procedura di Huffman

La procedura di Huffman permette di costruire un codice a prefisso ottimo.

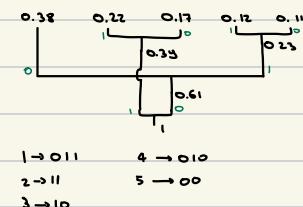
Dato lo distribuzione di ingresso  $p_x(z_i)$ ,  $z_i \in D_x$

1. Ordino le probabilità in ordine decrescente

2. Raccolgo le due probabilità più basse in un'unica parola di codice con probabilità la somma delle due probabilità.

3. Ripeto dal punto 1.

$$p_x(1) = 0.12 \quad p_x(2) = 0.22 \quad p_x(3) = 0.17 \quad p_x(4) = 0.11 \quad p_x(5) = 0.38$$



## 5.3 Codice di Elias

Il codice di Elias (o codice aritmetico) è un codice non ottimo.

### 5.3.1 Costruzione

Siano  $z_1, \dots, z_n \in D_x$  le parole in ingresso ordinate.



Rappresento  $m_i$  in forma binaria:  $m_i = 0.010011\dots$

La parola associata è la parte dopo la virgola:  $l_i = 010011\dots$

### 5.3.2 Proprietà

$$L_y = \lceil \log_2 p_x(z_i) \rceil + 1$$

Viene utilizzato, anche se non è ottimo perché permette di aggiornare dinamicamente codificatore e decodificatore.

Inizialmente assumo parole equiprobabili al codificatore e decodificatore, poi ad ogni invio (per il trasmettitore) e ricevimento (per il ricevitore) viene aumentata la probabilità di quel simbolo.

## 5.4 Efficienza di un Codice di Sorgente

$$0 \leq h = \frac{H(z)}{\log_2 M_y} = \frac{H(z)}{\log_2 \log_2 M_y} \leq 1$$

$$h=1 \text{ se } L_y = \frac{H(z)}{\log_2 M_y} \quad (\text{codice ottimo secondo TEO di Shannon})$$

Dal punto 2. del teorema di Shannon

$$L_y \leq \frac{H(z)}{\log_2 M_y} + 1 \quad \Rightarrow \quad \eta > \frac{H(z)}{H(z) + \log_2 M_y} \quad (\eta \text{ aumenta al diminuire di } M_y, \text{ ecco perche } M_y = z)$$