PROBABILITA'

$p_x(a) = P(x = a)$

$DISTRIBUZIONE$: $F_x(a) = P(x \le a) = \sum_{x<a, x\in A_x} p_x(x) = \int_{-\infty}^{a} f_x(x)dx \;\rightarrow\; P(x \in [A,B]) = P(A \le x \le B) = P(x \le B) - P(x \le A) = F_x(B) - F_x(A) = \int_A^B f_x(x)dx$

$VALORE\ ATTESO$: $E[X] = m_x = \sum_{x\in A_x} x p_x(x) = \int_{-\infty}^{+\infty} x f_x(x)dx \qquad E[g(x)] = \sum_{x\in A_x} p_x(x)g(x) = \int_{-\infty}^{+\infty} f_x(x)g(x)dx \qquad E[K] = k$

$POTENZA$: $E[X^2] = M_x = \sum_{x\in A_x} x^2 p_x(x) = E[X]^2 + \sigma_X^2 = {m_x}^2 + \sigma_X^2 = \int_{-\infty}^{+\infty} f_x(x)x^2dx$

$VARIANZA$: $VAR[X] = \sigma_X^2 = E[(x-m_x)^2] = \sum_{x\in A_x}(x-m_x)^2 p_x(x) = E[X^2] - E[X]^2 = M_x - m_x \qquad DEVIAZIONE\ STANDARD$: $\sigma_X = \sqrt{VAR[X]}$

$CONDIZIONAMENTO\ BAYES$: $P(A|B) = \frac{P(AB)}{P(B)} = \frac{P(B|A)P(A)}{P(B)} \qquad PROB.TOT.(CON\ PARTIZIONE\ B1, B2, \dots Bn)$: $P(A) = \sum_{i\in B} P(A|B_i)P(B_i)$

LIMITE CENTRALE: Sia Xn una successione di v.a. indipendenti ed equidistribuite con media μ e var. σ_X^2 >0 Allora: $\frac{\sqrt{n}}{\sigma}\left(\frac{1}{n}\sum x_k - \mu\right) \xrightarrow{n\to\infty} \mathcal{N}(0,1)$

V.A. UNIFORME $X \sim \mathcal{U}([A,B])$

$f_x(a) = \begin{cases} \frac{1}{B-A} & con\ a \in [A,B] \\ 0\ altrimenti \end{cases}$

$F_x(a) = \int_{-\infty}^{+\infty} f_x(a)da = \begin{cases} 0 & a < A \\ \frac{a-A}{B-A} & con\ a \in [A,B] \\ 1 & a > B \end{cases}$

$E[X] = \frac{A+B}{2}$

$VAR[X] = \frac{(b-a)^2}{12}$

V.A. BERNULLI $X \sim \mathcal{B}(p)$

$P(x=1) = p \qquad P(x=0) = 1-p$

$E[X] = p \qquad Var[X] = p(1-p)$

V.A. GAUSSIANA $X \sim \mathcal{N}(\mu, \sigma^2)$

(standard con $\mu = 0, \sigma = 1$)

$E[\mathcal{N}] = \mu \qquad VAR[\mathcal{N}] = \sigma^2$

($se\ Z = X + Y$=gaussiana= $\mathcal{N}(\mu_x + \mu_y, \sigma_x^2 + \sigma_y^2)$)

$f_x(a) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{a-\mu}{\sigma}\right)^2}$

$P(x \le a) = F_x(a) = \Phi(a) = 1 - Q(a)$

$P(x > a) = 1 - P(x \le a) = 1 - F_x(a) = Q(a)$

Non standard $P(x > a) = P\left(z > \frac{a-\mu}{\sigma}\right) = Q\left(\frac{a-\mu}{\sigma}\right)$

$P(x \in [A,B]) = F_x(b) - F_x(a) = \Phi(b) - \Phi(a) = Q(a) - Q(b)$

$Q(-a) = 1 - Q(a)$

SEGNALI

GRADINO

$1(t) = \begin{cases} 1 & t > 0 \\ \frac{1}{2} & t = 0 \\ 0 & t < 0 \end{cases}$

TRIANGOLO

$1(t) = \begin{cases} 1-|t| & |t| < 1 \\ 0 & altrove \end{cases}$

IMPULSO DI DIRAC

$\delta(t) = \begin{cases} 0 & \forall t \ne 0 \\ +\infty & t = 0 \end{cases}$

RETTANGOLO

$1(t) = \begin{cases} 1 & |t| < 1/2 \\ \frac{1}{2} & t = 0 \\ 0 & altrove \end{cases}$

DECIBEL

$(A)_{dB} = 10log_{10}(A)$

$A = 10^{(A)_{dB}/10}$

Potenza da milli a unità

$(P)_{dBm} = 30 + (P)_{dB}$

ONDA SINUSOIDALE

$s(t) = Acos(2\pi f_o t + \varphi_o)$

TRASLAZIONE DEL SEGNALE

s(t) ------> s(t-T)

T > 0 traslazione a DX

T < 0 traslazione a SX

SCALAMENTO DEL TEMPO

s(t) ------> s(At)

|A| > 1 compressione

|A| < 1 dilatazione

A = -1 ribaltamento

SCALAMENTO DEL SEGNALE

s(t) ------> As(t)

|A| > 1 amplificazione

|A| < 1 attenuazione

CONVOLUZIONE TEMPO CONTINUO

$z(t) = x(t) * y(t) = \int_{-\infty}^{+\infty} x(\tau)y(t-\tau)d\tau$

$\int \delta(t)dt = 1$

$\int x(t)\delta(t)dt = x(0)$

$\delta(t) * x(t) = \int_{-\infty}^{+\infty} \delta(\tau)x(t-\tau)d\tau = x(t)$

CONVOLUZIONE TEMPO DISCRETO

$z(nT) = x(nT) * y(nT) = \sum_k x(kT)y((n-k)T)$

ENERGIA DI UN SEGNALE

$continuo\ E_x = \int_{-\infty}^{+\infty} x^2(t)dt$

$discreto\ E_x = \sum_{n=-\infty}^{+\infty} x^2(nT)$

y(t)=As(t) ---> $E_y = A^2E_s$

|A|>1 amplificazione

|A|<1 attenuazione (attenuazione e amplificazione in dB si riferiscono a rapporti di energia)

POTENZA MEDIA DI UN SEGNALE

$P_x = \frac{1}{T}\int_0^T x^2(t)dt$

ENERGIA DEL RETTANGOLO

$s(t) = Arett\left(\frac{t-t_0}{B}\right) \qquad E_{rett} = A^2B$

ENERGIA DEL TRIANGOLO

$s(t) = Atrian\left(\frac{t-t_0}{B/2}\right) \qquad E_{tr} = \frac{A^2B}{3}$

RAPPRESENTAZIONE DI SEGNALI COME VETTORI

PRODOTTO INTERNO

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

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

$\langle x(t), x(t)\rangle = 0 \Leftrightarrow x(t) = 0$

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

NORMA INDOTTA DAL PRODOTTO INTERNO

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

ORTOGONALITA'

x(t), y(t) ortogonali se $\langle x(t), y(t)\rangle = 0$

norma unitaria se $\langle x(t), x(t)\rangle = 1 = E_x$

ORTONORMALIZZAZIONE DI GRAM-SCHMIDT

N vettori $s_1(t) \dots s_n(t)$che generano un sottospazio, ottengo una base $\phi_1(t) \dots \phi_I(t)$ con:

1) $\phi_1(t) = \frac{s_1(t)}{\sqrt{E_{s1}}}$

2) $\phi_n'(t) = s_n(t) - \sum_{i=1}^{I}\langle s_n(t), \phi_i(t)\rangle\phi_i(t)$

3) $\phi_n(t) = \frac{\phi_n'(t)}{\sqrt{E_{\phi_n'}}}$

PROIEZIONE ORTOGONALE DI UN SEGNALE IN UN SOTTOSPAZIO DI SEGNALI

Dato un segnale s(t) e un sottospazio definito da una base ortonormale $\phi_1(t) \dots \phi_I(t)$, la proiezione di s(t) nel sottospazio è il segnale:

$s_{\underline{\phi}}(t) = \sum_{i=1}^{I}\langle s(t), \phi_i(t)\rangle\phi_i(t) \ne s(t)$

$s(t) = s_{\underline{\phi}}(t) + e(t) \quad \langle e(t), \phi_i(t)\rangle = 0 \quad e(t) = 0\ se\ s(t) \in sottospazio$

SEGNALI COME SPAZIO VETTORIALE, ISOMORFISMO, VETTORE EUCLIDEO

Dato un segnale s(t) appartenente ad uno spazio vettoriale di dim. I con base $\{\phi_1(t) \dots \phi_I(t)\}$, il corrispondente vettore euclideo è:

$\underline{s} = \{s_1 \dots s_I\} \quad con\ s_i = \langle s(t), \phi_i(t)\rangle$

PRODOTTO INTERNO, NORMA ED ENERGIA

$x(t) = \sum_{i=1}^{I} x_i\phi_i(t) \qquad y(t) = \sum_{j=1}^{I} y_j\phi_j(t)$

$\langle x(t), y(t)\rangle = \sum_{i=1}^{I} x_iy_i = \langle \underline{x}, \underline{y}\rangle \qquad ||x(t)|| = ||\underline{x}||$

$E_s = \langle s(t), s(t)\rangle = \langle \underline{s}, \underline{s}\rangle = E_{\underline{s}} = \sum_{i=1}^{I} s_i^2 \qquad s(t) \leftrightarrow \underline{s} = [s_1 \dots s_I]$

DISTANZA TRA DUE VETTORI

$d^2(x(t), y(t)) = ||x(t) - y(t)||^2 = \langle x(t)-y(t), x(t)-y(t)\rangle = \int (x(t)-y(t))^2dt$

$= E_x + E_y - 2\langle x(t), y(t)\rangle = \langle \underline{x}-\underline{y}, \underline{x}-\underline{y}\rangle = d^2(\underline{x}, \underline{y}) = \sum_{i=1}^{I}(x_i - y_i)^2$

CANALE AWGN

CANALE AWGN IDEALE

$r(t) = s_{tx}(t) + w(t) \;\leftrightarrow\; r = s_{tx} + w$

Potenza media del rumore (PSD)

$P_W = \frac{1}{T}\int_0^T w^2(t)dt = \sigma_W^2 = \frac{N_o}{2}$

Potenza media del segnale utile

$P_{s_{tx}} = \frac{1}{T}\int_0^T {s_{tx}}^2(t)dt = \frac{E_{s_{tx}}}{T}$

CANALE AWGN con AMPLIFICAZIONE/ATTENUAZIONE

$r(t) = As_{tx}(t) + w(t)$

Energia del segnale utile al ricevitore

$E_{As_{tx}} = E_{s_{rx}} = A^2E_{s_{tx}}$

CANALE DISPERSIVO O CON ECHI

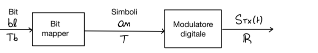
$r(t) = As_{tx}(t) + Bs_{tx}(t - t_0) + w(t)$

TRASMISSIONE DIGITALE

MODULAZIONE DIGITALE

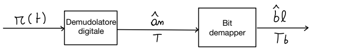
Bit mapper: raggruppa i bit in simboli

Modulatore digitale: associa a ciascun simbolo un segnale (forma d'onda) $a_0 \rightarrow s_{a_0}(t)$



DEMODULAZIONE DIGITALE

In generale se nel canale ho rumore o faccio errori in demodulazione ho $a_n \ne \hat{a}_n\ b_l \ne \hat{b}_l$



$trasmesso\ a_0 \rightarrow s_{a_0}(t)\ ricevo\ r(t) = s_{a_0}(t) + w(t)$

Nello spazio euclideo (nel sottospazio generato dalla base ortonormale per la segnalazione) $\underline{r} = \underline{s_{a_0}} + \underline{w}$

RICEVITORE DIGITALE → 2 operazioni di base:

Proiezione del segnale ricevuto sulla base ortonormale

Assegna a ciascun punto dello spazio un corrispondente indice n, per decidere quale segnale è stato trasmesso in base a quanto ricevuto→regione di decisione Rn

TEOREMA DELL'IRRILEVANZA (canale AWGN)

Base costruita su $s_1 \dots s_n = \{\phi_1 \dots \phi_I\}\ e\ aggiungiamo\ \phi_{I+1}$

$\underline{r} = [\underline{s}_{a_0}, 0] + [\underline{w}, \underline{w}_{I+1}] \rightarrow \quad \underline{r} = [\underline{r}_1 \dots \underline{r}_I, \underline{r}_{I+1}]$

$\rightarrow\ \underline{r}_{I+1}\ non\ dipende\ da\ n \rightarrow P_{\underline{r}_{I+1}}[\underline{r'}_{I+1}]\ non\ dipende\ da\ n$

$\hat{a}_0 = argmax_n\left(P_{\underline{r}|a_0}[\underline{r}'|n]P_{\underline{r}_{I+1}}[\underline{r}'_{I+1}]P[a_0 = n]\right)$

$= argmax_n(P_{\underline{r}|a_0}[\underline{r}'|n]P[a_0 = n])$

Se allargo la base la probabilità per la decisione non cambia ($\underline{w}_{I+1}$ è $componente\ \underline{w}_{\perp}\ ortogonale\ alla\ base \rightarrow irrilevante$)

PROBABILITA' DI DECISIONE CORRETTA

$P[C] = P[\hat{a}_0 = a_0] = 1 - P[E] = \sum_{n=1}^{N} P[\hat{a}_0 = a_0|a_0 = n]P[a_0 = n] = \sum_{n=1}^{N} P[\hat{a}_0 = n|a_0 = n]P[a_0 = n] = \sum_{n=1}^{N} P[\underline{r} \in R_n|a_0 = n]P[a_0 = n] = \sum_{n=1}^{N}\left(\int_{R_n} P_{\underline{r}|a_0}[\underline{r}'|n]d\underline{r}'\right)P[a_0 = n]$

$= \sum_{n=1}^{N}\int_{R_n} P[\underline{r}|a_{0=}n]d\underline{r}\,P[a_0 = n] = \sum_{n=1}^{N}\int_{R_n} \mu_n(\underline{r})P[\underline{r}|a_{0=}n]d\underline{r}\,P[a_0 = n] = \int_{R_n}\sum_{n=1}^{N} \mu_n(\underline{r})P[\underline{r}|a_{0=}n]P[a_0 = n]\,d\underline{r} = \int_{R_n}\sum_{n=1}^{N} \mu_n(\underline{r})D(\underline{r}, n)\,d\underline{r}$

$variabile\ indicatrice\ della\ regione\ R_n$: $\mu_n(\underline{r}) = \begin{cases} 1 & \underline{r} \in R_n \\ 0\ altrove \end{cases}$

$D(\underline{r}, n) = P[\underline{r}|a_{0=}n]P[a_0 = n]$

CRITERI DI DECISIONE DEL BIT RICEVUTO → massimizzare la probabilità di decisione corretta P[c]

$\hat{a}_0 = argmax_nD(\underline{r}, n)$

MAP: $\hat{a}_0 = argmax_n(P_{\underline{r}|a_0}[\underline{r}'|n]P[a_0 = n]) = argmax_n(P_{\underline{r}|a_0}[\underline{r}'|n]) = argmax_n(P_{a_0|\underline{r}}[n|\underline{r}']P_{\underline{r}}[\underline{r}']) = argmax_nP[a_0 = n|\underline{r}]$

ML: $simboli\ equiprobabili\ P(a_0 = n) = {}^1/_N \rightarrow \hat{a}_0 = argmax_n(P_{\underline{r}|a_0}[\underline{r}'|n]P[a_0 = n]) = argmax_nP_{\underline{r}|a_0}[\underline{r}'|n] = argmax_nP[\underline{r}|a_0 = n] \quad (P[a_0 = n]\ uguale\ per\ tutti, non\ influisce\ sull'argmax)$

MD: $canale\ AWGN\ con\ simboli\ equiprobabili \quad \hat{a}_0 = argmax_nP[\underline{r}|a_0 = n] = tutti\ gli\ elementi\ di\ \underline{r}\ sono\ indipendenti = argmax_n\prod_{i=1}^{I} P[\underline{r}_i|a_0 = n] = argmax_n\left(e^{-\frac{1}{2}\sum\left(\frac{r_i - s_{n,i}}{\sigma_W}\right)^2}\right) =$

$= argmin_n\sum\left(\frac{r_i - s_{n,i}}{\sigma_W}\right)^2 = argmin_n\sum(r_i - s_{n,i})^2 = argmin_n\langle\underline{r} - \underline{s}_n, \underline{r} - \underline{s}_n\rangle = argmin_nd^2(\underline{r}, \underline{s}_n)$

MD2: $\hat{a}_0 = argmin_n\sum(r_i - s_{n,i})^2 = argmin_n\sum(r_i^2 + s_{n,i}^2 - 2r_is_{n,i}) = r_i^2\ non\ dipende\ da\ m = argmin_n(\sum s_{n,i}^2 - 2\sum r_is_{n,i}) = cambio\ segno = argmax_n(2\sum r_is_{n,i} - E_{s_n}) =$

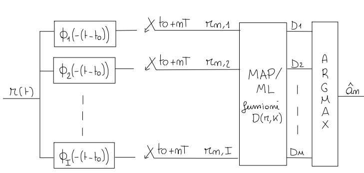
$= argmax_n\left(\sum r_is_{n,i} - \frac{E_{s_n}}{2}\right) = argmax_n\left(\langle\underline{r}, \underline{s}_n\rangle - \frac{E_{s_n}}{2}\right)$

IMPLEMENTAZIONE DEI RICEVITORI DIGITALI

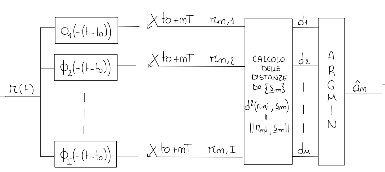
$r_i = \langle\phi_i(t), r(t)\rangle \quad con\ i = 1 \dots I \quad \rightarrow \quad r_i = \int_{-\infty}^{+\infty}\phi_i(-\tau)r(t-\tau)\,d\tau|_{t=0} = \int_{-\infty}^{+\infty}\phi_i(-(\tau - t_0))r(t-\tau)\,d\tau|_{t=t_0} = cambio\ di\ var = \int_{-\infty}^{+\infty}\phi_i(t)r(t)\,d\tau$

$r_i = \int_{-\infty}^{+\infty}\phi_i(-(\tau - t_0))r(t_0 - \tau)\,d\tau \rightarrow scelgo\ t_0\ in\ modo\ che\ sia\ il\ più\ piccolo\ valore\ che\ rende\ \phi_i(-(\tau - t_0))\ causale$

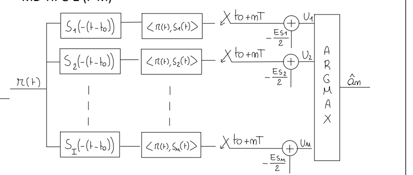
MAP



MD TIPO 1 (I<M)



MD TIPO 2 (I=M)



MODULAZIONE DIGITALE BINARIA

MODULAZIONE BINARIA (simboli equiprobabili e rumore AWGN)

$M = 2 \rightarrow s_1(t) \ne s_2(t) \qquad I \le 2 \rightarrow \phi_1(t)\ \phi_2(t)$

$\underline{s}_1 = [\langle s_1(t), \phi_1(t)\rangle, \langle s_1(t), \phi_2(t)\rangle]$

$\underline{s}_2 = [\langle s_2(t), \phi_1(t)\rangle, \langle s_2(t), \phi_2(t)\rangle]$

(caso I = 1 ho $s_1(t) = -s_2(t)$)

$distanza\ tra\ \underline{s}_1\ \underline{s}_2$: $d^2(\underline{s}_1, \underline{s}_2) = ||\underline{s}_1 - \underline{s}_2||^2 = \langle\underline{s}_1 - \underline{s}_2, \underline{s}_1 - \underline{s}_2\rangle = (s_{1,1}s_{2,1})^2 + (s_{1,2}s_{2,2})^2$

PROBABILITA' DI ERRORE

$P(E) = 1 - P(C) \rightarrow P(C) = P(\hat{a}_0 = a_0) = \frac{1}{2}P(\hat{a}_0 = 1|a_0 = 1) + \frac{1}{2}P(\hat{a}_0 = 2|a_0 = 2)$

$P(\hat{a}_0 = 1|a_0 = 1) = P\left(\langle\underline{w}, \underline{s}_2 - \underline{s}_1\rangle \le \frac{1}{2}d^2\right) \rightarrow \langle\underline{w}, \underline{s}_2 - \underline{s}_1\rangle \sim \mathcal{N}(0, \sigma_I{}^2d^2)$

$\rightarrow P(\hat{a}_0 = 1|a_0 = 1) = P(\hat{a}_0 = 2|a_0 = 2) = 1 - Q\left(\frac{d^2}{2\sigma_Id}\right) = 1 - Q\left(\frac{d}{2\sigma_I}\right)$

$P(C) = 1 - Q\left(\frac{d}{2\sigma_I}\right) \rightarrow \quad P(E) = Q\left(\frac{d}{2\sigma_I}\right)$

ENERGIA DEI SEGNALI

$E_{S1} = \langle s_1(t), s_1(t)\rangle = \langle\underline{s}_1, \underline{s}_1\rangle = \sum s_{1,i}^2\ \ distanza\ da\ O = \sqrt{E_{S1}}$

$E_{S2} = \langle\underline{s}_2, \underline{s}_2\rangle = \sum s_{2,i}^2\ \ distanza\ da\ O = \sqrt{E_{S2}}$

$ENERGIA\ MEDIA\ DELLA\ SEGNALAZIONE$ $E_S = \frac{1}{2}E_{S1} + \frac{1}{2}E_{S2}$

MODULAZIONE BINARIA

COEFFICIENTE DI CORRELAZIONE TRA DUE VETTORI

$\rho = \frac{\langle s_1(t), s_2(t)\rangle}{\sqrt{E_{S1}E_{S2}}} \quad |\rho| \le 1 \qquad \begin{matrix} se\ s_1(t) = -s_2(t) \rightarrow \rho = -1 \\ se\ s_1(t) = s_2(t) \rightarrow \rho = 1 \\ se\ s_1(t) \perp s_2(t) \rightarrow \rho = 0 \end{matrix}$

CASO $E_S = E_{S1} = E_{S2}$

$\underline{s}_1 = [\sqrt{E_S}, 0] \quad \underline{s}_2 = [\rho\sqrt{E_S}, \sqrt{E_S - \rho^2E_S}] = [\rho\sqrt{E_S}, \sqrt{E_S}\sqrt{1-\rho^2}]$

$d(s_1(t), s_2(t)) = \sqrt{2E_S(1-\rho)}$

$P(E) = Q\left(\frac{d}{2\sigma_I}\right) = Q\left(\frac{\sqrt{2E_S(1-\rho)}}{2\sigma_I}\right) = Q\left(\sqrt{\left(\frac{E_S}{\sigma_I{}^2}\right)\left(\frac{1-\rho}{2}\right)}\right)$

$con\ signal\ to\ noise\ ratio\ (SNR) = \left(\frac{E_S}{\sigma_I{}^2}\right)$

CASO SEGNALI ANTIPODALI → $s_1(t) = -s_2(t) \rightarrow \rho = -1$ → $P(E) = Q\left(\sqrt{\frac{E_S}{\sigma_I{}^2}}\right)$

CASO SEGNALI ORTOGONALI → $s_1(t) \perp s_2(t) \rightarrow \rho = 0$ → $P(E) = Q\left(\sqrt{\frac{E_S}{2\sigma_I{}^2}}\right)$

(si assume sempre $E_S = E_{S1} = E_{S2}$)

(si assume sempre $E_S = E_{S1} = E_{S2}$)

MODULAZIONE BPSK ANTIPODALE

(binary phase shift keying)

$s_1(t) = \begin{cases} Acos(2\pi f_0t) & con\ t \in [0,T] \\ 0 & altrove \end{cases}$

$s_2(t) = \begin{cases} -Acos(2\pi f_0t) & con\ t \in [0,T] \\ 0 & altrove \end{cases}$

$E_S = E_{S1} = E_{S2} = \frac{1}{2}A^2T \quad T \gg \frac{1}{f_0}$

(si assume sempre $E_S = E_{S1} = E_{S2}$)

MODULAZIONE BPSK ORTOGONALE

$s_1(t) = \begin{cases} cos(2\pi f_0t) & con\ t \in [0,T] \\ 0 & altrove \end{cases}$

$s_2(t) = \begin{cases} sen(2\pi f_0t) & con\ t \in [0,T] \\ 0 & altrove \end{cases}$

$E_S = E_{S1} = E_{S2} = \frac{1}{2}A^2T \quad T \gg \frac{1}{f_0}$

RICEVITORE A SINGOLO FILTRO PER MODULAZIONE BINARIA CON $E_S = E_{S1} = E_{S2}$

$\phi_1(t) = \frac{s_1(t) - s_2(t)}{\sqrt{2E_S(1-\rho)}} \qquad \phi_2(t) = \frac{s_1(t) + s_2(t)}{\sqrt{2E_S(1+\rho)}}$

I segnali s_1, s_2 sono alla stessa altezza nel piano generato dalla base $\phi_1(t), \phi_2(t)$

Il piano viene diviso da un threshold "verticale" $S = \frac{E_{S1} - E_{S2}}{2d} = \frac{E_{S1} - E_{S2}}{2\sqrt{2E_S(1-\rho)}}$

$\underline{r} = [r_1, r_2] \rightarrow\ r_2\ determina\ l'altezza, devo\ quindi\ basarmi\ solo\ su\ r1$

$\rightarrow \begin{matrix} se\ r_1 \ge S\ allora\ \hat{a}_0 = 1 \\ se\ r_1 < S\ allora\ \hat{a}_0 = 2 \end{matrix}$

MODULAZIONE DIGITALE M-ARIA (M>2)

MODULAZIONE M-ARIA $s_1(t) \dots s_M(t)\ M\ segnali \rightarrow log_2M = bit\ per\ simbolo$

Simboli equiprobabili canale AWGN: $P(a_0 = m) = \frac{1}{M}$

PROBABILITA' DI ERRORE

$P(E) = \sum_{m=1}^{M} P(\hat{a}_0 \ne m|a_0 = m)P(a_0 = m)$

$\rightarrow definisco\ \&_{n,m}\{evento\ statistico\ che\ \underline{r}\ sia\ più\ vicino\ a\ \underline{s}_n\ che\ a\ \underline{s}_m\} \rightarrow \{\hat{a}_0 \ne m|a_0 = m\} = \bigcup_{n\ne m}\&_{n,m}$

$P(E)_{precisa} = \sum_{m=1}^{M} P\left(\bigcup_{n\ne m}\&_{n,m}\right)P(a_0 = m) \le \sum_{m=1}^{M}\sum_{n\ne m} P(\&_{n,m})P(a_0 = m)$

$\rightarrow P(\&_{n,m}) = P\left(d(\underline{r}, \underline{s}_n) < d(\underline{r}, \underline{s}_m)\right) = Q\left(\frac{d_{n,m}}{2\sigma_I}\right)$

$P(E) \le \frac{1}{M}\sum_{m=1}^{M}\sum_{n\ne m} Q\left(\frac{d_{n,m}}{2\sigma_I}\right) \rightarrow servono\ \frac{M(M-1)}{2} distanze \rightarrow cerco\ upperbound\ migliore$

UPPER BOUND

$uso\ la\ distanza\ minima\ tra\ m\ e\ gli\ altri\ simboli$: $min_n(d_{n,m}) = d_{min,m} \quad (per\ M - 1\ punti)$

$P(E) \le \frac{1}{M}\sum_{m=1}^{M}\sum_{n\ne m} Q\left(\frac{d_{n,m}}{2\sigma_I}\right) \le \frac{M-1}{M}\sum_{m=1}^{M} Q\left(\frac{d_{min,m}}{2\sigma_I}\right) = UPPER\ BOUND\ 1$

$uso\ la\ distanza\ minima\ tra\ ogni\ coppia\ di\ simboli$: d_{min} (per M punti)

$P(E) \le \frac{M-1}{M}MQ\left(\frac{d_{min}}{2\sigma_I}\right) \le (M-1)Q\left(\frac{d_{min}}{2\sigma_I}\right) = UPPER\ BOUND\ 2\ (più\ lasco, uso\ 1\ distanza)$

LOWER BOUND

$P(E) \ge \frac{1}{M}\sum_{m=1}^{M} P(\&_{\bar{n},m}) \ge \frac{1}{M}\sum_{m=1}^{M} Q\left(\frac{d_{min,m}}{2\sigma_I}\right) = LOWER\ BOUND\ con\ \bar{n}\ più\ vicino\ a\ m$

MODULAZIONE ORTOGONALE (tutti i segnali della segnalazione sono ortogonali)

$s_1(t) \dots s_m(t) \quad s_m(t) \ne 0 \quad \langle s_i(t), s_j(t)\rangle = 0 \quad \forall i \ne j$

Per la base ortonormale prendo i segnali stessi (sono tutti ortogonali)

$I = M \quad \phi_i(t) = \frac{s_i(t)}{\sqrt{E_{s_i}}} \quad \rightarrow \quad \underline{s}_m = [0 \dots 0, \underbrace{\sqrt{E_{s_m}}}_{m-esimo}, 0 \dots 0]$

Simboli equiprobabili in canale AWGN con $E_{s_1} = E_{s_2} \dots = E_s = energia\ media$

$d_{min,m} = d_{min} = \sqrt{2E_s} \rightarrow BOUND\ \ Q\left(\frac{\sqrt{2E_s}}{2\sigma_I}\right) \le P(E) \le (M-1)Q\left(\frac{\sqrt{2E_s}}{2\sigma_I}\right)$

MODULAZIONE BIORTOGONALE (M PARI)

$M\ segnali\begin{cases} {}^M/_2\ sono\ ortogonali\ s_1(t), s_3(t) \dots s_{m-1}(t) \\ {}^M/_2\ sono\ antipodali \rightarrow s_2(t) = -s_1(t) \dots s_M(t) = -s_{m-1}(t) \end{cases}$

Ortogonali sono distanti $\sqrt{2E_s}$ antipodali sono distanti dal loro segnale$2\sqrt{E_s}$

BOUND $Q\left(\frac{\sqrt{2E_s}}{2\sigma_I}\right) \le P(E) \le (M-2)Q\left(\frac{\sqrt{2E_s}}{2\sigma_I}\right) + Q\left(\frac{2\sqrt{E_s}}{2\sigma_I}\right)$

PAM (PULSE AMPLITUDE MODULATION)

$s_m(t) = \alpha_mh_{TX}(t) \qquad \alpha_m = 2m - 1 - M \quad m = 1 \dots M\ (M\ pari) \qquad \underline{s}_m = [\alpha_m\sqrt{E_h}] \qquad base\ dimensione\ I = 1 \rightarrow h_{TX} \rightarrow \alpha_m$ è $uno\ scalamento\ di\ h_{TX}$

BASE $\phi_1(t) = \frac{h_{TX}}{\sqrt{E_h}} \qquad distanza\ tra\ punti\ sempre\ uguale = d_{min} = 2\sqrt{E_h} \qquad distanza\ tra\ un\ punto\ e\ il\ confine\ di\ regione = \sqrt{E_h}$

ENERGIA MEDIA PER SIMBOLI EQUIPROBABILI

$E_s = \frac{1}{M}\sum_{m=1}^{M} E_{s_m} = \frac{1}{M}\sum_{m=1}^{M}\alpha_m^2E_h = \frac{1}{M}\sum_{m=1}^{M}(2m - 1 - M)^2E_h = \frac{M^2 - 1}{3}E_h \qquad \rightarrow E_h = \frac{3E_s}{M^2 - 1}$

PROBABILITA' DI ERRORE

$P(E) = \sum_{m=1}^{M} P(E|a_0 = m)P(a_0 = m) = \frac{1}{M}\sum_{m=1}^{M} P(E|a_0 = m) \qquad \underline{r} = \underline{s}_n + \underline{w}_n \quad con\ \underline{w}_n \sim \mathcal{N}(0, \sigma_I{}^2)$

$P(E|simbolo\ interno) = P(\underline{r} > \underline{s}_{int} + \sqrt{E_h}\ \vee\ \underline{r} < \underline{s}_{int} - \sqrt{E_h}|a_0 = interno) = P(\underline{w} > \sqrt{E_h}\ \vee\ \underline{w} < -\sqrt{E_h}) = P(\underline{w} > \sqrt{E_h}) + P(\underline{w} < -\sqrt{E_h}) = 2Q\left(\frac{\sqrt{E_h}}{\sigma_I}\right)$

$P(E|simbolo\ esterno) = P(\underline{r} > \underline{s}_{ext} + \sqrt{E_h}|a_0 = esterno) = Q\left(\frac{d_{s1,s2}}{2\sigma_I}\right) = Q\left(\frac{2\sqrt{E_h}}{2\sigma_I}\right) = Q\left(\frac{\sqrt{E_h}}{\sigma_I}\right)$

$P(E)_{TOT} = \frac{1}{M}\left[2Q\left(\frac{\sqrt{E_h}}{\sigma_I}\right) + (M-2)2Q\left(\frac{\sqrt{E_h}}{\sigma_I}\right)\right] = 2\left(1 - \frac{1}{M}\right)Q\left(\frac{\sqrt{E_h}}{\sigma_I}\right) = 2\left(1 - \frac{1}{M}\right)Q\left(\sqrt{\frac{3E_s}{(M^2-1)\sigma_I{}^2}}\right)$

$PROBABILITA'\ DI\ ERRORE\ SUL\ BIT\ (con\ mappa\ di\ gray)$: $P_{bit} = \frac{P(E)}{log_2M}$

QAM (QUADRATURE AMPLITUDE MODULATION)

$\rightarrow s_m(t) = \alpha_{m,I} h_{TX}(t)\cos(2\pi f_0 t + \varphi_0) - \alpha_{m,Q} h_{TX}(t)\,\mathrm{sen}(2\pi f_0 t + \varphi_0) \qquad m = 1 \dots M. \qquad \alpha_{m,I}, \alpha_{m,Q} \in \{-(L-1), -(L-3) \dots -1, 1, 3 \dots (L-3), (L-1)\}$

$M = L^2 \qquad \alpha_{k,I} = (2k - \sqrt{M} - 1)$

BASE ($Ho\ sempre\ dimensione\ 2\ con\ \cos \perp \mathrm{sen}\ per\ f_0 \gg \frac{1}{T}$)

$\phi_1 = h_{TX}(t)\cos(2\pi f_0 t + \varphi_0)\sqrt{\frac{2}{E_h}} \qquad \phi_2 = -h_{TX}(t)\,\mathrm{sen}(2\pi f_0 t + \varphi_0)\sqrt{\frac{2}{E_h}} \qquad \underline{s}_m = \left[\sqrt{\frac{E_h}{2}}\alpha_{m,I}, \sqrt{\frac{E_h}{2}}\alpha_{m,Q}\right]$

ENERGIA MEDIA PER SIMBOLI EQUIPROBABILI

$E_s = \frac{1}{M}\sum_{m=1}^{M} E_{s_m} = \frac{1}{M}\sum_{m=1}^{M}\left[\left(\alpha_{m,I}\sqrt{\frac{E_h}{2}}\right)^2 + \left(\alpha_{m,Q}\sqrt{\frac{E_h}{2}}\right)^2\right] = \frac{E_h}{2M}\sum_{m=1}^{M}\left[(\alpha_{m,I})^2 + (\alpha_{m,Q})^2\right] = \frac{2E_h}{2M}\sum_{m=1}^{M}(\alpha_{m,I})^2 = \frac{2E_h}{2M}\sqrt{M}\sum_{k=1}^{\sqrt{M}}(2k - \sqrt{M} - 1)^2 = \frac{E_h(M-1)}{3}$

$\rightarrow E_h = \frac{3E_s}{M-1}$

PROBABILITA' DI ERRORE

$d_{min} = \sqrt{2E_h} \qquad d_{bordo} = \sqrt{\frac{E_h}{2}} \qquad \underline{r} = \underline{s}_n + \underline{w}_n \qquad M - QAM \begin{matrix} tipo\ A{:}4\ regioni \\ tipo\ B{:}4(L-2) regioni \\ tipo\ C{:}(L-2)^2\ regioni \end{matrix}$

REGIONE A (∟): $P(C|a_0 tipoA) = P\left(\underline{w}_1 > -\sqrt{\frac{E_h}{2}} \wedge \underline{w}_2 > -\sqrt{\frac{E_h}{2}} \middle| a_0 \in A\right) = \left[Q\left(-\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right]^2 = \left[1 - Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right]^2$

REGIONE B (⊔): $P(C|a_0 tipoB) = P\left(\underline{w}_1 \in \left\{-\sqrt{\frac{E_h}{2}}, \sqrt{\frac{E_h}{2}}\right\} \wedge \underline{w}_2 > -\sqrt{\frac{E_h}{2}} \middle| a_0 \in B\right) = \left[Q\left(-\sqrt{\frac{E_h}{2\sigma_I^2}}\right) - Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right]Q\left(-\sqrt{\frac{E_h}{2\sigma_I^2}}\right) = \left(1 - 2Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right)\left(1 - Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right)$

REGIONE C (☐): $P(C|a_0 tipoC) = P\left(\underline{w}_1 \in \left\{-\sqrt{\frac{E_h}{2}}, \sqrt{\frac{E_h}{2}}\right\} \wedge \underline{w}_2 \in \left\{-\sqrt{\frac{E_h}{2}}, \sqrt{\frac{E_h}{2}}\right\} \middle| a_0 \in C\right) = \left[1 - 2Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right]^2$

$P(E)_{TOT} = \frac{1}{M}\sum_{m=1}^{M}(1 - P(C|a_0 = m)) = \dots = 4\frac{L-1}{L}Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right) - \left(2\frac{L-1}{L}Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right)\right)^2 \approx 4\frac{L-1}{L}Q\left(\sqrt{\frac{E_h}{2\sigma_I^2}}\right) \approx 4\left(1 - \frac{1}{\sqrt{M}}\right)Q\left(\sqrt{\frac{3}{(M-1)}\frac{E_h}{2\sigma_I^2}}\right)$

$PROBABILITA'DI\ ERRORE\ SUL\ BIT\ (con\ mappa\ di\ gray){:}\ P_{bit} = \frac{P(E)}{log_2 M}$

SEGNALI A TEMPO DISCRETO $x(nT){:}\ T quanto\ temporale$

CONVOLUZIONE A TEMPO DISCRETO

$z(nT) = \sum x(kT)y((n-k)T)$

CAMPIONAMENTO $y(nT) = x(nT){:}\ x\ a\ tempo\ continuo$

INTERPOLAZIONE

$y(t) = \sum x(nT)h(t - nT)\ :\ h\ ripsosta\ impulsiva$

QUANTIZZAZIONE UNIFORME

$\Delta{:}\ passo\ di\ quantizzazione \qquad L{:}\ numero\ di\ livelli\ di\ quantizzazione$

$V_{sat}{:}\ valore\ di\ saturazione \qquad b{:}\ numero\ di\ bit\ per\ campione$

$0 < y < \Delta \rightarrow y^Q = \frac{\Delta}{2} \qquad \Delta < y < 2\Delta \rightarrow y^Q = \frac{3\Delta}{2} \quad \dots. \qquad V_{sat} = \frac{L}{2}\Delta \qquad L = 2^b$

$se\ |y_m| \le A \rightarrow V_{sat} = A \qquad se\ y_m \in \{A, B\} \rightarrow V_{sat} = \max\{|A|, |B|\} \qquad in\ generale{:}\ y_m \in [-V_{sat}, V_{sat}]$

PROBABILITA' DI SATURAZIONE ($\varepsilon{:}\ parametro\ di\ progetto$)

$y_m \sim \mathcal{N}(0, \sigma_I^2) \rightarrow P_{saturazione} = P(y_m \notin [-V_{sat}, V_{sat}]) \le \varepsilon \quad \rightarrow P_{sat} = 2Q\left(\frac{V_{sat}}{\sigma_I}\right) = \varepsilon \rightarrow V_{sat} = Q^{-1}\left(\frac{\varepsilon}{2}\right)\sigma_I$

ERRORE GRANULARE

$e_q = y_m - y_m^Q \rightarrow e_q \in \left[-\frac{\Delta}{2}, \frac{\Delta}{2}\right] \quad P_{y_m}(a) \approx P_{y_m}(y_m^Q) \quad P_{e_q}(a) = \frac{1}{\Delta} \quad E(e_q) = 0$

$E(e_q^2) = \int_{-\Delta/2}^{\Delta/2} P_{e_q}(a)a^2 da = \frac{\Delta^2}{12}$

RAPPORTO SEGNALE-RUMORE DI QAUNTIZZAZIONE

$\Lambda_q = \frac{E(y_m^2)}{E(e_{qm}^2)} = \frac{12L^2\sigma_I^2}{4V_{sat}^2} = \frac{3L^2\sigma_I^2}{V_{sat}^2} = \frac{3\ 2^{2b}\sigma_I^2}{V_{sat}^2} \qquad con\ E(y_m^2) = \sigma_I^2$

$(\Lambda_q)_{dB} = 10\log_2\Lambda_q = 20log\frac{\sigma_I}{V_{sat}} + 10log3 + b20log2 = 20log\frac{\sigma_I}{V_{sat}} + 4{,}77 + 6{,}02b$

SOMMATORIE UTILI

$\sum_{n=1}^{N} n = \frac{N(N+1)}{2}$

$\sum_{n=1}^{N} n^2 = \frac{N(N+1)(2N+1)}{6}$

$\sum_{n=1}^{N} n^3 = \left(\frac{N(N+1)}{2}\right)^2$

MAPPA di GRAY

M=2	M=4	M=8
0	00	000
1	<u>01</u>	001
	11	011
	10	<u>010</u>
		110
		111
		101
		100

CODIFICA DI CANALE

CODIFICA A BLOCCO

Un vettore di k bit viene codificato in un vettore di n bit $(n > k)$ che costituisce una parola di codice $\mathcal{C} = \{2^k parole\ di\ codice\ lunghe\ n\}$

Obbiettivo: rilevare e correggere errori introdotti dal canale di trasmissione

$\boxed{\underline{b}{:}\ bit\ trasmessi} \rightarrow \boxed{\underline{c}{:}\ vettore\ codificato \in \mathcal{C}} \rightarrow \boxed{\underline{\tilde{c}}{:}\ vettore\ ricevuto \notin \mathcal{C}} \rightarrow \boxed{\underline{\hat{b}}{:}\ bit\ decodificati} \rightarrow \boxed{\underline{\hat{c}}{:}\ parola\ di\ codice\ decodificata}$

$in\ generale\ (\underline{c} = [c_1 \dots c_n]) \neq (\underline{\tilde{c}} = [\tilde{c}_1 \dots \tilde{c}_n])\ cioè\ \underline{\tilde{c}}_i = (c_i + e_i)_2 \quad e_i \in \{0,1\}$

Obbiettivo: minimizzare la probabilità di errore nel processo di decodifica

PROBABILITA' DI DECISIONE CORRETTA

$P(C) = P(\underline{\hat{b}} = \underline{b}) = \sum_{c_0 \in \mathcal{C}} P(\underline{\hat{b}} = \underline{b}|\underline{c} = \underline{c}_0)P(\underline{c} = \underline{c}_0)$

$(quando\ ricevo\ \underline{\tilde{c}} = \underline{\beta}\ decido\ per\ la\ sequenza\ \underline{\hat{c}} = \underline{\alpha})$

MAP $\rightarrow \underline{\hat{c}} = argmax_{\underline{\alpha}\in\mathcal{C}} P(\underline{\tilde{c}} = \underline{\beta}|\underline{c} = \underline{\alpha})P(\underline{c} = \underline{\alpha})$ ML $\rightarrow P(\underline{c} = \underline{\alpha}) = \frac{1}{|\mathcal{C}|} = parole\ equiprobabili \rightarrow \underline{\hat{c}} = argmax_{\underline{\alpha}\in\mathcal{C}} P(\underline{\tilde{c}} = \underline{\beta}|\underline{c} = \underline{\alpha})$

CANALE BINARIO SIMMETRICO SENZA MEMORIA (L'errore introdotto dal canale è indipendente per ciascuno bit (senza memoria))

$P(\underline{\tilde{c}} = \underline{\beta}|\underline{c} = \underline{\alpha}) = P(\tilde{c}_1 = \beta_1 \dots \tilde{c}_n = \beta_n | c_1 = \alpha_1 \dots c_n = \alpha_n) = \prod_{i=1}^{N} P(\tilde{c}_i = \beta_i | c_i = \alpha_i)$

Simmetrico: $P(\tilde{c}_i = 1|c_i = 0) = P(\tilde{c}_i = 0|c_i = 1) = P_e \qquad \rightarrow P(\tilde{c}_i = \beta_i|c_i = \alpha_i) = \begin{cases} 1 - P_e & \beta_i = \alpha_i \\ P_e & \beta_i \neq \alpha_i \end{cases}$

DISTANZA DI HAMMING

$\underline{a} = [a_1 \dots a_n] \qquad \underline{b} = [b_1 \dots b_n] \qquad a_i, b_i \in \{0,1\}$

$d_H(\underline{a}, \underline{b}) = \#\ elementi\ in\ cui\ le\ due\ sequenze\ sono\ diverse, quanti\ bit\ sono\ diversi\ nella\ stessa\ posizione$

trasmissione in canale binario simmetrico senza memoria con parole equiprobabili: $P(\underline{\tilde{c}} = \underline{\beta}|\underline{c} = \underline{\alpha}) = P_e^{d_H(\underline{\alpha},\underline{\beta})}(1 - P_e)^{n - d_H(\underline{\alpha},\underline{\beta})}$

ML diventa: $\underline{\hat{c}} = argmax_{\underline{\alpha}\in\mathcal{C}} P_e^{d_H(\underline{\alpha},\underline{\beta})}(1 - P_e)^{n - d_H(\underline{\alpha},\underline{\beta})} = argmax_{\underline{\alpha}\in\mathcal{C}}\left(\frac{P_e}{1-P_e}\right)^{d_H(\underline{\alpha},\underline{\beta})}(1 - P_e)^n = argmax_{\underline{\alpha}\in\mathcal{C}}\left(\frac{P_e}{1-P_e}\right)^{d_H(\underline{\alpha},\underline{\beta})}$

$se\ P_e < \frac{1}{2}{:} \quad \left(\frac{P_e}{1-P_e}\right) < 1 \quad \rightarrow \quad \underline{\hat{c}} = argmin_{\underline{\alpha}\in\mathcal{C}} d_H(\underline{\alpha}, \underline{\beta}) = criterio\ MD$

$se\ P_e \ge \frac{1}{2}{:} \quad \begin{cases} P_e = \frac{1}{2} \quad ho\ prob.\ \frac{1}{2}\ di\ trovare\ giusto\ o\ sbagliato, come\ se\ uscita\ e\ entrata\ fossero\ indipendenti \\ P_e = 1 \quad cambia\ sempre\ il\ bit, \ \ basta\ invertirli\ tutti\ e\ recupero\ il\ segnale\ di\ ingresso\ corretto. \\ P_e > \frac{1}{2},\ P_e \neq 1 \quad cambio\ tutti\ i\ bit\ al\ ricevitore\ e\ applico\ MD \rightarrow mi\ riconduco\ al\ caso\ P_e < \frac{1}{2} \end{cases}$

BOUND DI HAMMING

$t{:}\ raggio\ di\ circonferenza\ attorno\ a\ \underline{c}, tutte\ le\ sequenze\ \underline{\tilde{c}}\ per\ cui\ d_H(\underline{\tilde{c}}, \underline{c}) \le t\ sono\ dentro\ la\ regione\ di\ decisione\ di\ \underline{c}$

$numero\ di\ sequenze\ \underline{\tilde{c}}\ con\ r\ errori = \binom{n}{r} \dashrightarrow numero\ di\ punti\ che\ cadono\ in\ tutti\ i\ cerchi = 2^k\sum_{r=0}^{t}\binom{n}{r} \le 2^n$

$\rightarrow \log_2 2^k + \log_2\left(\sum_{r=0}^{t}\binom{n}{r}\right) \le \log_2 2^n \rightarrow \frac{k}{n} \le 1 - \frac{1}{n}\log_2\left(\sum_{r=0}^{t}\binom{n}{r}\right) = BOUND\ DI\ HAMMING$

$RATE\ DEL\ CODICE = \frac{k}{n} = \frac{\#bit\ da\ codificare}{\#bit\ codificati}$

DISTANZA DI HAMMING MINIMA DI UN CODICE $d_{min} = \min d_H(\underline{\alpha}_i, \underline{\alpha}_j) \qquad con\ \underline{\alpha}_i, \underline{\alpha}_j \in \mathcal{C}, \underline{\alpha}_i \neq \underline{\alpha}_j \qquad t < \frac{d_{min}}{2}$

NUMERO MASSIMO DI ERRORI RILEVO SEMPRE= $d_{min} - 1$

NUMERO MASSIMO DI ERRORI CHE CORREGGO SEMPRE= $\left\lfloor\frac{d_{min}-1}{2}\right\rfloor = \begin{cases} \frac{d_{min}-1}{2} & se\ d_{min} dispari \\ \frac{d_{min}-2}{2} & se\ d_{min} pari \end{cases}$

CODICI LINEARI A BLOCCO

$\underline{a} = [a_1 \dots a_n] \qquad \underline{b} = [b_1 \dots b_n] \quad c = bit \quad a_i, b_i, c \in \{0,1\} \qquad$ CAMPO $\mathbb{F} = (\{0,1\}, +, \bullet) \quad --\!> \quad$ SAPZIO VETTORIALE $\mathbb{V} = \mathbb{F}^n$

SOMMA $\underline{a} + \underline{b} = [a_1 + b_1 \dots a_n + b_n]$ PRODOTTO $c\underline{a} = [ca_1 \dots ca_n] \quad ---> \quad c_1\underline{a} + c_2\underline{b} \in \mathbb{V} \qquad \underline{a} + \underline{a} = 0 \rightarrow \underline{a} = -\underline{a}$

PESO DI HAMMING (NORMA PER $\mathbb{V}$) $\|\underline{x}\|_H = numero\ di\ elementi\ (bit) del\ vettore\ diversi\ da\ zero$

$1)\ \|\underline{x}\|_H \ge 0 \quad 2)\ \|\underline{x}\|_H = 0 \Leftrightarrow \underline{x} = 0 = [0 \dots 0] \quad 3)\ \|\underline{x}_1 + \underline{x}_2\|_H \le \|\underline{x}_1\|_H + \|\underline{x}_2\|_H \quad 4)\ \|a\underline{x}\|_H = |a|\ \|\underline{x}\|_H$

DISTANZA DI HAMMING $d_H(\underline{x}_1, \underline{x}_2) = \|\underline{x}_1 - \underline{x}_2\|_H$

CODICE LINEARE A BLOCCO: $\mathcal{C}\ è\ un\ codice\ lineare\ a\ blocco\ se\ è\ un\ sottospazio\ vettoriale\ dello\ spazio\ \mathbb{F}^n \rightarrow \underline{a} + \underline{b} \in \mathcal{C},\ c_1\underline{a} + c_2\underline{b} \in \mathcal{C}$

Trucco di verifica: $\underline{a}_1 \in \mathcal{C} \rightarrow \underline{a}_1 + \underline{a}_1 = 0 \in \mathcal{C} \rightarrow se\ \underline{0} \notin \mathcal{C}\ il\ codice\ non\ è\ lineare \rightarrow ogni\ codice\ lineare\ include\ il\ vettore\ \underline{0}$

PESO DI HAMMING DI UN CODICE LINEARE A BLOCCO: $W_{min}(\mathcal{C}) = \min_{\underline{a}\neq 0 \in \mathcal{C}}\|\underline{a}\|_H = \min_{\underline{a}\neq\underline{b}} d_H(\underline{a}, \underline{b})$

$W_{min}(\mathcal{C}) = minimo\ peso\ tra\ tutti\ quelli\ delle\ parole\ di\ codice\ \neq \underline{0}, coincide\ con\ la\ distanza\ minima\ di\ Hamming\ del\ codice$

MATRICE GENERATRICE DI UN CODICE LINEARE

$k\ bit\ tasmessi\ con\ \underline{b} \quad - \quad n\ bit\ codificati\ in\ \underline{c}$

$\underline{c} = \underline{G}\,\underline{b} \quad \rightarrow \begin{bmatrix} c_1 \\ \dots \\ c_n \end{bmatrix} = n\left\{\overbrace{[\underline{G}]}^{k}\right. \begin{bmatrix} b_1 \\ \dots \\ b_k \end{bmatrix} \rightarrow \begin{cases} n\ righe, k\ colonne\ lin.\ indipendenti{:}\ n \times k\ bit\ necessari\ per\ rappresentare\ un\ codice\ lineare \\ (n \times 2^k\ bit\ per\ un\ codice\ non\ lineare) \\ basta\ prendere\ k\ parole\ di\ codice\ (di\ lunghezza\ n) lin.\ indipendenti\ e\ usarle\ come\ colonne \end{cases}$

CODICE LINEARE IN FORMA SISTEMATICA (È un codice lineare ottenuto da una matrice generatrice in forma sistematica)

$\underline{G} = \begin{bmatrix} \underline{I}_k \\ \underline{A} \end{bmatrix} \begin{matrix} \rightarrow matrice\ identica\ k \times k. \\ \rightarrow matrice\ di\ dimensione\ (n-k)k \end{matrix} \rightarrow \underline{c} = \underline{G}\,\underline{b} = \begin{bmatrix} \underline{I}_k \\ \underline{A} \end{bmatrix}\underline{b} = \begin{bmatrix} \underline{b} \\ \underline{Ab} \end{bmatrix} \begin{matrix} \rightarrow basta\ memorizzare\ la\ matrice\ \underline{A} \rightarrow servono\ solo\ (n-k)k\ bit \\ \rightarrow BIT\ DI\ PARITA' \end{matrix}$

È sempre possibile ottenere una matrice sistematica una matrice generatrice con combinazioni lineari delle colonne e permutazioni delle righe

Cosi facendo cambia il codice ma le prestazioni rimangono le stesse

Una matrice in froma sistematica garantisce la linearità del codice

BOUND DI SINGLETON

Per codici lineari a blocco (n,k) la distanza minima di Hamming del codice è limitata superiormente $d_{min} < n - k + 1$

DECODIFICA DI CODICI LINEARI

MATRICE DI CONTROLLO DI PARITA' $\underline{H}$ controlla che la somma dei bit trasmessi sia effettivamente quella che ci aspettiamo

-> deve soddisfare: $\underline{H}\,\underline{a} = \underline{0} \quad \Leftrightarrow \quad \underline{a} \in \mathcal{C}$

$\underline{H}\ è\ matrice\ di\ controllo\ di\ parità\ di\ un\ codice\ lineare\ \mathcal{C}\ con\ matrice\ generatrice\ \underline{G} \Leftrightarrow \underline{HG} = \underline{0}\ e\ RANGO(\underline{H}) = n - k$

RANGO = # di righe o colonne linearmente indipendenti

MATRICE DI CONTROLLO DI PARITA' PER CODICI IN FORMA SISTEMATICA: $\underline{G} = \begin{bmatrix} \underline{I}_k \\ \underline{A} \end{bmatrix} \quad \underline{H} = [\underline{A}, \underline{I}_{n-k}] \rightarrow Es.\ \underline{G} = \begin{bmatrix} 100 \\ 010 \\ \underline{001} \\ 111 \end{bmatrix} \quad \underline{H} = [111|1]$

DECODIFICA TRAMITE SINDROME

SINDROME di una sequenza di n bit relativa ad un codice lineare con matrice di parità $\underline{H}$:

$SINDROME\ \underline{\sigma} = \underline{Ha} \quad con\ \underline{a}\ seq.\ di\ bit \quad \underline{\sigma} = 0 \Leftrightarrow \underline{a} \in \mathcal{C}$

$COSET\ associato\ ad\ una\ SINDROME = insieme\ di\ sequenze\ \underline{a}\ tali\ che\ la\ loro\ sindrome\ è\ \underline{\sigma}{:}\ COSET(\underline{\sigma}) = \{\underline{a}{:}\ \underline{Ha} = \underline{\sigma}\} \quad |coset| = 2^k$

Data una seq. $\underline{a}$ con sindrome $\underline{\sigma}$, coset($\underline{\sigma}$)={sequenze $\underline{a} + \underline{\delta} \quad \forall\underline{\delta} \in \mathcal{C}$} $\quad infatti\ \underline{H}(\underline{a} + \underline{\delta}) = \underline{Ha} + \underline{H\delta} = \underline{Ha} + 0 = \underline{\sigma}$

DECODIFICA A MINIMA DISTANZA (CON SINDROME)

Cerchiamo la parola di codice $\underline{\delta} \in \mathcal{C}$ a minima distanza di Hamming da $\underline{a}$: con $\underline{\beta} = \underline{a} - \underline{\delta} \rightarrow \underline{\beta}\ è\ nel\ coset\ (\underline{\sigma}(\underline{a}))$

$\underline{\hat{\delta}} = argmin_{\underline{\delta}\in\mathcal{C}} d_H(\underline{a}, \underline{\delta}) = argmin\|\underline{a} - \underline{\delta}\|_H = \underline{a} + argmin\|\underline{\beta}\|_H = \underline{a} + \underline{\beta}_{min}(\underline{\sigma}(\underline{a}))$

$1)\ calcolo\ la\ sindrome\ \underline{\sigma}(\underline{a}) = \underline{H}\,\underline{a}$

$2)\ trovo\ nel\ coset\ (\underline{\sigma}(\underline{a}))\ una\ sequenza\ con\ peso_H\ minimo{:}\ \underline{\beta}_{min}(\underline{\sigma}(\underline{a})) \qquad 3)\ calcolo\ \underline{\hat{\delta}} = \underline{a} + \underline{\beta}_{min}(\underline{\sigma}(\underline{a}))$

CODICI DI HAMMING

È un codice lineare a blocco che ha matrice di parità che contiene nelle colonne tutte le parole non nulle di lunghezza (n-k)

$\underline{H} = \underbrace{[\bullet]}_{n}\}n - k \rightarrow \begin{matrix} (n-k) righe \\ n = 2^{n-k} - 1 = colonne = \#sequenze\ di\ (n-k) bit \neq \underline{0} \end{matrix}$

PRESTAZIONI DEI CODICI DI HAMMING $\quad d_{min}\ di\ un\ codice\ di\ Hamming \rightarrow d_{min} = 3$

I codici di Hamming soddisfano il Bound di Hamming come eguaglianza: $\frac{k}{n} = 1 - \frac{1}{n}\log_2\left(\sum_{r=0}^{t}\binom{n}{r}\right)$ #max di errori sempre corretti t=1

TEORIA DELL'INFORMAZIONE

INFROMAZIONE

$Spazio\ di\ eventi\ \Omega = \{A_1 \dots A_n\}\ con\ probabilità\ associata\ P(A_i)$

$Funzione\ informazione\ di\ un\ evento\ A{:}\ \ i(A) = g(P(A)) = -logP(A) = log\frac{1}{P(A)} \quad \rightarrow base\ 2{:}\ [bit]/base\ e{:}\ [neper]$

$1)\ i(A) \ge 0\ \forall A. \qquad 2)\ i(\Omega) = 0 \quad (\Omega = intero\ spazio\ degli\ eventi = evento\ certo) \rightarrow evento\ certo\ non\ mi\ porta\ informazione$

$3)\ P(A) \le P(B) \Rightarrow i(A) \ge i(B) \rightarrow eventi\ meno\ probabili\ mi\ portano\ più\ informazione, quelli\ che\ conosco\ già\ non\ mi\ danno\ informazioni$

$4)\ A\ e\ B \in \Omega\ indipendenti \Rightarrow informazione\ dell'avvenimento\ simultaneo\ dei\ due\ eventi\ i(A \cap B) = i(A) + i(B)$

FUNZIONE INFORMAZIONE DI UNA VAR. DISCRETA x

$x \in A_x = \{a_1 \dots a_n\} \quad p_x(a) = P(x = a) \rightarrow i_x(a) = i(x = a) = \log_2 1/P_x(a) \qquad \rightarrow P_x(a) = 2^{-i(a)}$

$se\ A = \{x \in \{a_1 \dots a_n\}\} \rightarrow i(A) = -logP(A) = -logP(x \in \{a_1 \dots a_n\}) = -\log[P_x(a_1) + \dots + P_x(a_n)]$

ENTROPIA DI UNA VARIABILE ALEATORIA x (valore medio dell'informazione): $H(x) = E_x(i_x(x)) = \sum_{a\in A_x} P_x(a)i_x(a) = \sum_{a\in A_x} P_x(a)\log_2\frac{1}{P_x(a)}$

$1) H(x) \ge 0 \qquad 2)\ H(x) = 0 \Leftrightarrow x\ è\ deterministica = assume\ un\ solo\ valore\ con\ probabilità\ 1 \rightarrow \sum_{a\in A_x} P_x(a)\log_2\frac{1}{P_x(a)} = 0 \Leftrightarrow P_x(a) = 0 \vee P_x(a) = 1$

$3)\ H(x) \le \log_2 M\ sempre\ con\ M = |A_x| cardinalità\ di\ A_x\ e\ i(x) è\ in\ base\ 2 \rightarrow se\ x\ è\ uniforme\ sull'alfabeto A_x \rightarrow H(x) = \log_2 M$

$\rightarrow 0 \le H(x) \le \log_2 M$

VETTORI ALEATORI

$\underline{x} = [x_1 \dots x_n]\ con\ x_i\ v.a. \in A_i\ (ogni\ v.a.\ ha\ il\ suo\ alfabeto) \rightarrow \underline{x} \in A_1 \times A_2 \times \dots \times A_n$

$DENSITA'\ DI\ PROBABILITA'\ CONGIUNTA\ DEL\ VETTORE\ \underline{x}{:}\ P_{\underline{x}}(\underline{a}) = P(x_1 = a_1, x_2 = a_2 \dots x_n = a_n) \qquad con\ \underline{a} = [a_1 \dots a_n]$

$FUNZIONE\ INFORMAZIONE{:}\ i_{\underline{x}}(\underline{a}) = \log_2 1/P_{\underline{x}}(\underline{a})$

$ENTROPIA\ DI\ UN\ VETTORE\ ALEATORIO{:}\ \ H(\underline{x}) = E(i_{\underline{x}}(\underline{x})) = \sum_{\underline{a}\in A_1\times\dots\times A_n} P_{\underline{x}}(\underline{a})\log_2 1/P_{\underline{x}}(\underline{a})$

DIPENDENZA TRA COPPIE DI V.A.

$funzione\ deterministica{:}\ dato\ un\ valore\ di\ x \rightarrow y\ assume\ un\ valore\ determinato{:}\ (x = a) \Rightarrow y = f(a) \rightarrow P(y = f(a)|x = a) = 1$

- $se\ y\ funzione\ deterministica\ di\ x \rightarrow H(x, y) = H(x) \qquad (H(x, y) = H(x) = H(y) \Leftrightarrow H(x) = H(y)\ in\ genere\ non\ vale)$
- $se\ y\ NON\ è\ funzione\ deterministica\ di\ x \rightarrow H(x, y) > H(x)$
- $se\ x, y\ sono\ indipendenti \rightarrow H(x, y) = H(x) + H(y)$
- $se\ x, y\ NON\ sono\ indipendenti \rightarrow H(x, y) < H(x) + H(y)$
- $se\ x \in A_x, y \in A_y\ con\ M_x = |A_x|, M_y = |A_y| \rightarrow vale\ sempre\ H(x, y) \le \log_2 M_x + \log_2 M_y$

$\rightarrow 0 \le \max\{H(x), H(y)\} \le H(x, y) \le H(x) + H(y) \le \log_2 M_x + \log_2 M_y$

V.A. CONDIZIONATE

$P_{x|y}(a|b) = P(x = a|y = b) \rightarrow i_{x|y}(a|b) = \log_2 1\ /\ P_{x|y}(a|b)$

$ENTROPIA\ CONDIZIONATA \qquad (P_{x,y}(a, b) = P_{x|y}(a|b)P_y(b) \rightarrow P_{x|y}(a|b) = P_{x,y}(a, b)/P_y(b))$

$H(x|y) = E_{x,y}(i_{x|y}(x|y)) = \sum_{a,b\in A_x\times A_y} P_{x,y}(a, b)i_{x|y}(a|b) = \sum P_{x,y}(a, b)\log_2 1/P_{x|y}(a|b) = \sum P_{x,y}(a, b)\log_2 P_y(b)/P_{x,y}(a, b)$

$= \sum P_{x,y}(a, b)\log_2 1/P_{x,y}(a, b) - \sum P_y(b)\log_2 1/P_y(b) = H(x, y) - H(y)$

$H(x, y) = H(x|y) + H(y) = H(y|x) + H(x)$

ENTROPIA MEDIA PER SIMBOLO DI UN VETTORE ALEATORIO $\underline{x} = [x_1 \dots x_N]$: $\quad H_{simbol}(\underline{x}) = \frac{1}{N}H(\underline{x}) \rightarrow H(\underline{x}) = NH_{simbol}(\underline{x})$

Se $[x_1 \dots x_N]$ sono indipendenti e hanno stessa entropia $H_s(\underline{x}) = H(x_i)$

SORGENTE SEMPRE ATTIVA-->VETTORE ALEATORIO DI LUNGHEZZA INFINITA $\underline{x} = [x_{-\infty} \dots x_0 \dots x_\infty], uniformemente\ distribuito$

ENTROPIA MEDIA PER SIMBOLO $su\ \underline{x}\ infinito{:}\ H_s(\underline{x}) = \lim_{N\to\infty}\left(\frac{1}{2N+1}\right)H([x_{-N} \dots x_0 \dots x_N]) = \lim_{N\to\infty}\left(\frac{1}{2N+1}\right)H(x_i)(2N + 1) = H(x_i)$

TASSO DI INFORMAZIONE DI UN MESSAGGIO (INFORMATION RATE) -->Sorgente genera simboli con periodo T: $R(\underline{x}) = \frac{1}{T}H_s(\underline{x}) = \left[\frac{bit}{sec}\right]$

TASSO DI INFORMAZIONE NOMINALE= $\frac{1}{T}\log_2 M$ (Simboli indipendenti presi uniformemente da un alfabeto di cardinalità M)

Vale sempre $R(\underline{x}) \le \frac{1}{T}\log_2 M$ TASSO DI SIMBOLO (symbol rate) -->$R(x) = \frac{1}{T}H_s(x) = fH_s(x)$

EFFICACIA DI UN MESSAGGIO: $\eta(\underline{x}) = \frac{R(\underline{x})}{Flog_2 M} = \frac{TR(\underline{x})}{\log_2 M} = \frac{H_s(\underline{x})}{\log_2 M}$

INFORMAZIONE MUTUA TRA DUE V.A.

$i(x, y) = H(x) + H(y) - H(x, y) = H(y) + H(x) - H(y, x) = i(y, x) \qquad se\ x, y\ v.a.\ indipendenti\ i(x, y) = 0$

$H(x, y) = H(x|y) + H(y) \rightarrow i(x, y) = H(x) - H(x|y) = H(y) + H(y|x) \qquad se\ y\ funz.\ deterministica\ di\ x\ i(x, y) = H(y)$

INFORMAZIONE MUTUA PER SIMBOLO TRA DUE VETTORI ALEATORI: $i_s(\underline{x}, \underline{y}) = H_s(\underline{x}) + H_s(\underline{y}) - H_s(\underline{x}, \underline{y})$

INFORMAZIONE MUTUA TRA DUE VETTORI ALEATORI FINITI: $i(\underline{x}, \underline{y}) = H(\underline{x}) + H(\underline{y}) - H(\underline{x}, \underline{y})$

VALORI DELL'INFORMAZIONE MUTUA E BOUND

$0 \le i(x, y) \le \min\{H(x), H(y)\} \le \min\{\log_2 M_x, \log_2 M_y\}$

CANALE NUMERICO M-ARIO SENZA MEMORIA g->CASO PARTICOLARE: CANALE BINARIO SENZA MEMORIA

Canale senza memoria: $P(y_n|x_n, x_{n-1} \dots) = P(y_n|x_n) \qquad x_n, y_n \in A\{a_1, a_2 \dots a_n\} \qquad |A| = M$

Se M=2 $\boxed{b{:}\ k\ bit\ ogni\ T_b} \rightarrow \boxed{COD} \rightarrow \boxed{c{:}\ n\ bit\ ogni\ T_c} \qquad kT_b = nT_c \rightarrow \frac{k}{n} = \frac{T_c}{T_b} \le 1 \rightarrow T_b \ge T_c$

TASSO DI INFORMAZIONE $R(g) = \frac{1}{T_c}i_s(\underline{x}, \underline{y}) = \frac{1}{T_c}\left(H_s(\underline{y}) - H_s(\underline{y}|\underline{x})\right) = \frac{1}{T_c}\left(H_s(\underline{x}) + H_s(\underline{y}) - H_s(\underline{x}, \underline{y})\right)$

$se\ non\ ci\ sono\ errori\ H_s(\underline{y}|\underline{x}) = 0 \rightarrow R(g) = H_s(\underline{y}) = H(\underline{x})$

CAPACITA' DEL CANALE: $C(g) = max_{\{P_{\underline{x}}\}}R(g)$ (max tasso di informazione del canale tra tutte le densità di probabilità dell'ingresso)

CAPACITA' per un canale AWGN: $C(g) = \frac{1}{T}\log_2\left(1 + \frac{\sigma_I^2}{\sigma_w^2}\right) = \frac{1}{T}\log_2\left(1 + \frac{E_s}{\sigma_w^2}\right) \qquad con\ densità\ di\ prob.\ di\ x \sim \mathcal{N}(0, \sigma_I^2)$

CANALE AWGN CON INGRESSO GAUSSIANO $C(g) = \frac{1}{2}\log_2\left(1 + \frac{\sigma_I^2}{\sigma_w^2}\right) = i(x, y) \quad nel\ caso\ y = x + w, x\ e\ w\ gauss.\ indipendenti$

EFFICIENZA SPETTRALE: $C_s(g) = max_{\{P_x\}}i_s(x, y) = CT_c \qquad [bit] = [bit/sec/Hz] \qquad C(g) = [bit/sec]$

TEOREMA DI SHANNON PER LA CODIFICA DI CANALE: canale m-ario numerico senza memoria con periodo di simbolo T_c e capacità C $\{b_l\}$ messaggio con tasso di informazione nominale $R = \frac{1}{T}\log_2 M$. Se $R < C$ allora $\forall\delta > 0\ e\ \forall n$ suff. grande $\exists$ un codice con $2^k = \lceil 2^{RnT_c}\rceil$ parole lunghe n con P_{errore} sulla parola $< \delta. \rightarrow k = nRT_c \rightarrow \frac{k}{n} = RT_c < CT_c$

TEOREMA CONVERSE: canale m-ario senza memoria con capacità C esiste $\delta > 0$ tale che per un qualsiasi codice e strategia di codifica, se $R \ge C$ allora P_{errore} sulla parola è sempre $> \delta$.

CANALE BINARIO E MESSAGGIO BINARIO: $R = \frac{1}{T_b}\log_2 M_b = \frac{1}{T_b} \rightarrow T_b = \frac{1}{R}\ C = \frac{1}{T_c}i_s(\underline{x}, \underline{y}) \rightarrow T_c = \frac{i_s(\underline{x},\underline{y})}{C}\ R < C \rightarrow \frac{k}{n} = \frac{T_c}{T_b} = \frac{R}{C}i_s < i_s$

CANALE BINARIO SIMMETRICO SENZA MEMORIA(BSCLM): $\quad b_l \rightarrow \boxed{BSCLM} \rightarrow \hat{b}_l$

$P(\hat{b} = 1|b = 0) = P(\hat{b} = 0|b = 1) = P_{bit} \qquad P(b = \hat{b}) = 1 - P_{bit} \qquad C = \frac{1}{T_b}\max_{\{P_b\}} i(b, \hat{b}) \qquad i(b, \hat{b}) = H(\hat{b}) - H(\hat{b}|b)$

$P_b(0) = q \qquad P_b(1) = 1 - q$

$P_{\hat{b}}(0) = P(\hat{b} = 1|b = 0)P_b(0) + P(\hat{b} = 0|b = 1)P_b(1) = P_{bit} - 2qP_{bit} + q \qquad P_{\hat{b}}(1) = 1 - P_{\hat{b}}(0) = (1 - q)(1 - P_{bit}) + qP_{bit}$

$H(\hat{b}) = -(P_{bit} + q - 2qP_{bit})\log_2(P_{bit} + q - 2qP_{bit}) - (1 - P_{bit} - q + 2qP_{bit})\log_2(1 - P_{bit} - q + 2qP_{bit}) \rightarrow \max H(\hat{b}) = 1$

$H(\hat{b}|b) = -P_{bit}\log_2 P_{bit} - (1 - P_{bit})\log_2(1 - P_{bit})$ per trovare C devo massimizzare $i(b, \hat{b})$: avviene per $q = \frac{1}{2} \rightarrow H(\hat{b}) = 1$

$C = \frac{1}{T_b}\max_{\{P_b\}} i(b, \hat{b}) = \frac{1}{T_b}[1 + P_{bit}\log_2 P_{bit} + (1 - P_{bit})\log_2(1 - P_{bit})] \rightarrow \begin{matrix} P_{bit} = \frac{1}{2} \rightarrow C = 0 \\ P_{bit} = 1, P_{bit} = 0 \rightarrow C = \frac{1}{T_b} \end{matrix}$

CANALE BINARIO SENZA MEMORIA CON CANCELLAZIONE: se sono a metà tra 1 e 0, sono indeciso, ho un valore erasure

$P_{y|x}(0|0) = P_{y|x}(1|1) = 1 - \alpha \qquad P_{y|x}(E|1) = P_{y|x}(E|0) = \alpha \qquad P_x(1) = q \qquad P_x(0) = 1 - q \qquad i(x, y) = H(y) - H(y|x)$

$P_y(0) = P_{y|x}(0|0)P_x(0) + P_{y|x}(0|1)P_x(1) = (1 - \alpha)(1 - q) \quad P_y(1) = (1 - \alpha)q \quad P_y(E) = P_{y|x}(E|0)P_x(0) + P_{y|x}(E|1)P_x(1) = \alpha$

$H(y) = -(1 - \alpha)(1 - q)\log_2[(1 - \alpha)(1 - q)] - (1 - \alpha)q\log_2[(1 - \alpha)q] - \alpha\log_2\alpha$

$H(y|x) = -\alpha\log_2\alpha - (1 - \alpha)\log_2(1 - \alpha)$

$i(x, y) = -(1 - \alpha)(1 - q)\log_2[(1 - \alpha)(1 - q)] - (1 - \alpha)q\log_2[(1 - \alpha)q] - \alpha\log_2\alpha + (1 - \alpha)\log_2(1 - \alpha) + \alpha\log_2\alpha$

Per trovare C devo massimizzare $i(x, y)$: avviene per $q = 1\ /\ 2 \rightarrow C = (1\ /\ T_b)(1 - \alpha)$

CODIFICA DI SORGENTE

Scopo: comprimere il segnale di ingresso. Se non ho perdite riesco sempre a ricondurmi al messaggio iniziale, con perdite no.

Il codificatore fa corrispondere a ciascuna parola del dizionario D_x di ingresso una sola parola di D_y di uscita $\rightarrow |D_x| = |D_y|$

Lunghezza della parola $\underline{b} \in D_y{:}\ L(\underline{b}) = \#lettere\ di\ \underline{b}$ $\rightarrow$ lunghezza media delle parole di $D_y{:}\ L_y = E(L(\underline{b})) = \sum_{\underline{b}\in D_y} L(\underline{b})P_{\underline{y}}(\underline{b})$

CODICE A PREFISSO: D_y tale per cui nessuna parola è prefisso di un'altra, riesco sempre a distinguerle leggendo lettera per lettera

TEOREMA DI KRAFT-MCMILLAN:

1) per ogni codice decodificabile deve valere $\sum_{\underline{b}\in D_y}\frac{1}{M_y^{L_y(\underline{b})}} \le 1\ \ con\ M_y = |A_y| = \#\ lettere\ disponibili$

2)per una sorgente con dizionario di cardinalità N se $l_1, l_2 \dots l_N$ sono interi tali che $\sum_{i=1}^{N} 1/M^{l_i} \le 1$ allora esiste un codice prefisso con alfabeto con cardinalità $M_y = M$ e parole di codice di lunghezza l_i per la sorgente

TEOREMA DI SHANNON PER LA CODIFICA DI SORGENTE

1) Per ogni codice decodificabile con alfabeto di cardinalità M_y la lunghezza media delle sue parole soddisfa $L_y \ge \frac{H(\underline{x})}{\log_2 M_y} \quad \underline{x} \in D_x \quad M_y = |A_y| \quad H(\underline{x}){:}\ entropia\ delle\ parole\ in\ ingresso\ al\ codificatore$

2) Esiste un codice prefisso con alfabeto di cardinalità M_y e lunghezza media delle parole $L_y < \frac{H(\underline{x})}{\log_2 M_y} + 1 \qquad \rightarrow \frac{H(\underline{x})}{\log_2 M_y} \le L_y < \frac{H(\underline{x})}{\log_2 M_y} + 1$

CODICE SHANNON-FANO: codice ottenuto dal teorema di Shannon, le lunghezze delle parole sono $l_i = \lceil\log_{1/M_y} P_x(a_i)\rceil = \lceil-\log_{M_y} P_x(a_i)\rceil$, in generale questo codice non è ottimo cioè non ha lunghezza media minima

CODICE SHANNON-FANO OTTIMO: quando $l_i = -\log_{M_y} P_x(a_i)$ è un numero intero $\forall\ a_i \in D_x \quad \rightarrow \quad L_y = E(l_i) = E(-\log_{M_y} P_x(a_i)) = \frac{H(\underline{x})}{\log_2 M_y} = lower\ bound\ dato\ da\ Shannon \rightarrow ottimo$

CODIFICA DI SORGENTE OTTIMA: In generale possono esserci più codici ottimi ma devono avere tutti la lunghezza media minima e rispettare le condizioni di ottimalità:

1) Per un codice ottimo parole a più bassa probabilità hanno lunghezza maggiore $P_x(a_1) > P_x(a_2) \rightarrow P_y(b_1) > P_y(b_2) \Rightarrow L(b_1) < L(b_2)$

2) Nel dizionario del codice ottimo a prefisso ci sono almeno due parole di codice $\underline{b}'\ e\ \underline{b}''$ che hanno lunghezza massima che differiscono solo nell'ultimo simbolo (bit in caso binario)

```
a2     a3     a4     a5     a1
0,45   0,25   0,16   0,09   0,05        a2->0
 |      |      |      |1___|0           a3->11
 |      |      |          |0,14         a4->100
 |      |      |0________|1             a5->1011
 |      |            |0,30              a1->1010
 |      |1_________ |0
 |            |0,55
 |0__________|1
        |start
```

PROCEDURA DI HUFFMAN PER TROVARE CODICE BINARIO OTTIMO A PREFISSO : Dato un dizionario di ingresso D_x con parole $a_1 \dots a_n$ e densità di probabilità $P_x(a_1) \dots P_x(a_n)$

1)Ordiniamo le parole in ingresso con probabilità decrescente $P_x(a_1) > P_x(a_2) > \dots > P_x(a_n)$ 2)Assegniamo le parole di uscita più lunghe a $a_n\ e\ a_{n-1}$: abbiamo deciso l'ultimo bit di queste due parole--> assegno 1 o 0 (arbitrariamente) a $a_n\ e\ a_{n-1}$

3)Consideriamo un nuovo dizionario di ingresso uguale a prima ma con $n - 1$ parole dove l'ultima ha probabilità $P(a_{n-1}) + P(a_n)$: accorpo le ultime due parole con probabilità minore 4)Ripeto 2 e 3.

CODIFICA ARITMETICA-CODICE DI ELIAS : n parole generate da una sorgente in ordine noto, l'intervallo unitario viene diviso in n sottointervalli, m_{a_n}: valore del punto medio del segmento relativo ad a_n. $(m_{a_n})_2 = 0{,}011 = 0{,}0 \cdot 2^{-1} + 1 \cdot 2^{-2} + 1 \cdot 2^{-3}(m_{a_n})_{10} = \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$

Da m_{a_n} scriviamo la sequenza di bit che troviamo dopo la virgola troncata a $\lceil i(a_n)\rceil + 1\ bit$. Più rara è una parola più alta è l'informazione, più lunga sarà la parola in bit.

1) Dalle probabilità di simbolo $P(a_n)$ scrivo $m_{a_n} = \sum_{i=1}^{n-1}P(a_i) + \frac{P(a_n)}{2}$ 2)converto m_{a_n} in binario $(m_{a_n})_2 = 0, \dots 1010$ 3)tronco la sequenza di bit dopo la virgola a $\lceil i(a_n)\rceil + 1\ bit$

Lunghezza media del codice di Elias: $L_{elias} = \sum_{n=1}^{N} l(a_n)P(a_n) = \sum(\lceil i(a_n)\rceil + 1)P(a_n) \ge \sum i(a_n)P(a_n) + \sum P(a_n) = H(x) + 1$

$EFFICINEZA\ DI\ UNA\ GENERICA\ SORGENTE\ CHE\ EMETTE\ PAROLE\ \underline{x}{:}\ \eta_x = \frac{R(x)}{flog_2 M} = \frac{H_s(\underline{x})}{\log_2 M_x}$ EFFICIENZA DI USCITA DI UN CODIFIFCATORE DI SORGENTE $\eta_y = \frac{H_s(\underline{y})}{\log_2 M_y} = \frac{H(\underline{y})}{L_y\log_2 M_y} = \frac{H(\underline{x})}{L_y\log_2 M_y}$ $\quad da\ Shannon{:}\ \eta_y > 1 - \frac{1}{L_y} \ge 1 - \frac{\log_2 M_y}{H(\underline{x})}$ TASSO NOMINALE PER CODIFICA DI SORGENTE $R = \frac{L_y}{T_{simbolo}}$