ES: Sia X binaria con $p_X(x) = \{\frac{1}{5}; \frac{4}{5}\}$ e $X = \{0,1\}$

Vogliamo fare un codice che codifica i numeri di questa sorgente

1) Calcolare $H(X)$
2) Codificare con Gilbert-Moore e Huffman con $L=2$
3) Ripetere con $L=3$

1) $H(X) = \sum_i p_X(x_i) \cdot \log\left(\frac{1}{p_X(x_i)}\right)$

$= \frac{1}{5}\log(5) + \frac{4}{5}\log\left(\frac{5}{4}\right) = 0.722$

2) Con Gilbert: dove $n(x_i) = \left\lceil \log\left(\frac{1}{p_X(x_i)}\right) \right\rceil$

x_k	x_{k+1}	$p_{x_k x_{k+1}}(x_i, x_j)$	$n(x_i)$	$C(x_i)$
0	0	1/25	5	11111
0	1	4/25	3	001
1	0	4/25	3	010
1	1	16/25	1	0

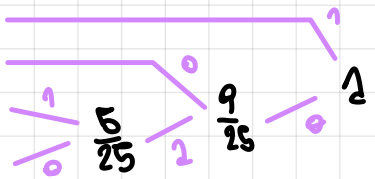
$\sum p_{x_k x_{k+1}}(x_i, x_j) = 1$

$\bar{n}_{C_2} = \frac{1}{25}\cdot 5 + 2\cdot\frac{4}{25}\cdot 3 + \frac{16}{25} = 1.8$ bit (codifica $L=2$)

$\bar{n}_C = \frac{\bar{n}_{C_2}}{2} = 0.9$ bit/simbolo $> H(x) = 0,722$

Huffman:

x_k	x_{k+1}	p congiunta	$C(x_i)$	$n(x_i)$
1	1	16/25	1	1
1	0	4/25	00	2
0	1	4/25	011	3
0	0	1/25	010	3



$\bar{n}_{C_2} = \frac{16}{25} + 2\cdot\frac{4}{25} + 3\cdot\frac{4}{25} + 3\cdot\frac{1}{25} = 1,56$ bit

$\bar{n}_C = \frac{\bar{n}_{C_2}}{2} = 0,78$ bit $> H(x) = 0.722$ bit

3) Gilbert

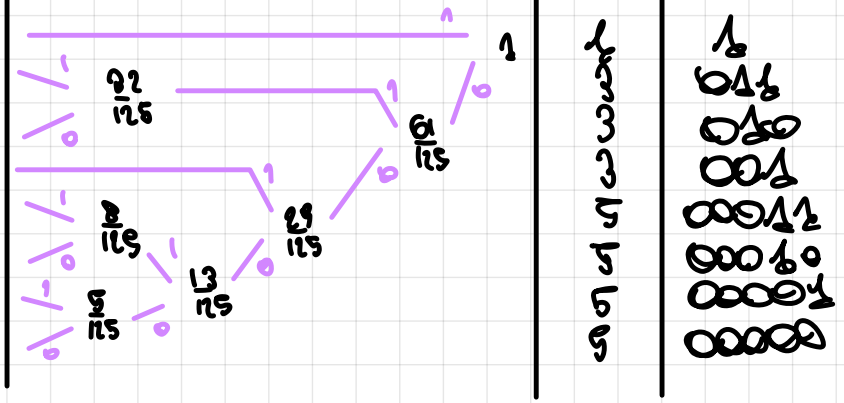
x_k	x_{k+1}	x_{k+2}	$p(x_k, x_{k+1}, x_{k+2})$	$n(x_i)$	$C(x_i)$
0	0	0	1/125	7	1111111
0	0	1	4/125	5	10111
0	1	0	4/125	5	11111
0	1	1	16/125	3	100
1	0	0	4/125	5	00001
1	0	1	16/125	3	010
1	1	0	16/125	3	001
1	1	1	64/125	1	0

$\mathcal{E} = 1$

$\bar{n}_{C_3} = 2.2 \Rightarrow \bar{n}_C = \frac{\bar{n}_{C_3}}{3} = 0,733 > H(x)$

Huffman

x_n x_{n+1} x_{n+2}	$p_{cong.}$	$n(x_i)$	$C(x_i)$
1 1 1	$64/125$	1	1
1 1 0	$16/125$	3	011
1 0 1	$16/125$	3	010
0 1 1	$16/125$	3	001
1 0 0	$8/125$	5	00011
0 1 0	$8/125$	5	00010
0 0 1	$8/125$	5	00001
0 0 0	$1/125$	5	00000



$n\bar{C}_3 = 2{,}184 \Rightarrow \bar{nC} = \frac{n\bar{C}_3}{3} = 0{,}728 > H(x)$

Esempio: $p_X(x) = \{1/2, 1/2\}$ X lin.

x_n x_{n+1}	$p_{congiunta}$	$h(x_i)$
0 0	1/4	2
0 1	1/4	2
1 0	1/4	2
1 1	1/4	2

$n\bar{C}_2 = 4 \cdot (1/4 \cdot 2) = 2$ bit

$\bar{nC} = 1$ bit

$H(x) = 1$ bit

Con $p_X(x) = \{1/5, 4/5\}$

$n\bar{C}_2 = 1.8$ bit

$\bar{nC} = 0{,}9$ bit

$H(x) = 0{,}722$ bit

Esame: 09/07/08

$X = \{0,1\}$ $p_X = \{1/5, 4/5\}$

$\underline{x} = 11\ldots1$ $|\underline{x}| = u$ $C(\underline{x}) = 1$ $p = (4/5)^u$

$\underline{x} \neq 11\ldots1$ $C(\underline{x}) = 0\underline{x}$ $p = 1 - (4/5)^u$

minimizzare u:

$$n\bar{C}_u = (4/5)^u \cdot (1) + (1 - (4/5)^u) \cdot (u+1)$$
$$= (4/5)^u + u + 1 - u(4/5)^u - (4/5)^u$$
$$= (u+1) - u(4/5)^u$$
$$\bar{nC} = 1 + \frac{1}{u} - (4/5)^u$$

Per tentativi:

u	$\bar{nC}$	
2	$1 + 0{,}5 - 0{,}64 = 0{,}86$	
3	$1 + 0{,}8 - 0{,}512 = 0{,}82$	$\Rightarrow$ u ottimo
4	$1 + 0{,}25 - 0{,}410 = 0{,}84$	min $\bar{nC}$

$p = (4/5)^u = (4/5)^3 = 0{,}512$

$p = 1 - (4/5)^u = 0{,}488$

Analogo un bit di infor. su 2 eventi equiprobabili

Esempio: codifica Lempel-Ziv

sequenza: 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0

Sottosequenza $S_n = (f_n, b_n)$ dove f_n: puntatore sottosequenza vista
b_n: bit nuovo

n	0	1	2	3	4	5	6	7
S_n	•	1	0	11	01	010	00	10
(f_n, b_n)		(-,1)	(0,0)	(1,1)	(2,1)	(4,0)	(2,0)	(1,0)
(f_n, b_n) binario		(0,1)	(0,0)	(01,1)	(10,1)	(100,0)	(010,0)	(001,0)
	$\lceil \log_2 n \rceil$ puntatore	$2^x = 1$ 0 bit	$2^x = 2$ 1 bit	$2^x = 3$ 2 bit	$2^x = 4$ 2 bit	$2^x = 5$ 3 bit	$2^x = 6$ 3 bit	$2^x = 7$ 3 bit

la sequenza codificata risulta: $\bigcup_i p_i b_i$ "concatenazione"

1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0

Decodifica:

mi devo ricordare che $\lceil \log_2 n \rceil + 1$ (bit nuovo)

n	0	1	2	3	4	5	6	7
binario (f_n, b_n)	•	(0,1)	(0,0)	(01,1)	(10,1)	(100,0)	(010,0)	(001,0)
decimale (p_n, b_n)		(·,1)	(0,0)	(1,1)	(2,1)	(4,0)	(2,0)	(1,0)
S_n		1	0	11	01	010	00	10

decodifica: 1 0 1 1 0 1 0 1 0 0 0 1 0

$$H(Y) = \sum_i P_Y(s_i) \cdot \log\left(\frac{1}{P_Y(s_i)}\right) =$$
$$= 2 \cdot \frac{p}{2} \log \frac{2}{p} + 2 \cdot \frac{1-p}{2} \log\left(\frac{1}{1-p}\right)$$
$$= p \log \frac{1}{p} + (1-p) \log\left(\frac{1}{1-p}\right) =$$
$$= p\left(\log 2 + \log \frac{1}{p}\right) + (1-p)\left(\log 2 + \log \frac{1}{1-p}\right)$$
$$= p + p \log \frac{1}{p} + 1 - p + (1-p) \log\left(\frac{1}{1-p}\right)$$
$$= 1 + H_2(p)$$

$$H(Y|x_i) = H(Y|0) = \sum_i P(y|0) \cdot \log \frac{1}{P(y|0)}$$
$$= P(r|0) \cdot \log\left(\frac{1}{P(r|0)}\right) + P(s|0) \cdot \log\left(\frac{1}{P(s|0)}\right)$$
$$= \tfrac{1}{2} \log 2 + \tfrac{1}{2} \log 2 = 1 \text{ bit} \quad \forall x_i$$

uguale a prima

$$H(Y|X) = \sum_i P_X(x_i) \cdot H(Y|x_i)$$
$$= p + (1-2p) + p = 1 \text{ bit}$$

(una cosa in più)

$$I(X;Y) = H(Y) - H(Y|X)$$
$$= 1 - H_2(p) - 1 = H_2(p)$$

$$C = \max_p I(X;Y) = 1 \text{ bit/uso canale} \quad (p = 1/2)$$

Es: sorgente binaria $X = \{0,1\}$ $p_X(x) = \{1/2, 1/2\}$ con legge

$$p_{X_n|X_{n-1},X_{n-2}}(X_n|01) = p_{X_n|X_{n-1},X_{n-2}}(X_n|10) = 1/2 \qquad X_n = 0,1$$
$$p_{X_n|X_{n-1},X_{n-2}}(1|11) = p_{X_n|X_{n-1},X_{n-2}}(0|00) = p$$
$$p_{X_n|X_{n-1},X_{n-2}}(0|11) = p_{X_n|X_{n-1},X_{n-2}}(1|00) = 1-p$$

1) Calcolare $H(X)$ discutere i casi $p = (0, 1/2, 1)$

$$H(X) = \lim_{L\to\infty} H(X_n|X_{n-1},\dots,X_{n-L})$$
$$= \lim_{L\to\infty} \frac{1}{L} H(X_n, X_{n-1},\dots,X_{n-L})$$

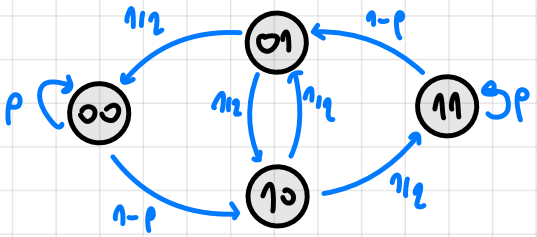
sorgente Markoviana con $m=2$ dipendente dai 2 simb precedenti

$$= H(X_n|X_{n-1},X_{n-2})$$
$$= \sum_{X_{n-1},X_{n-2}} p(X_{n-1},X_{n-2}) \cdot H(X_n|X_{n-1},X_{n-2})$$
$$= \sum\sum p_{X_n,X_{n-1},X_{n-2}}(X_n,X_{n-1},X_{n-2}) \cdot \log\left(\frac{1}{p_{X_n|X_{n-1},X_{n-2}}(X_n|X_{n-1},X_{n-2})}\right)$$
$$= \sum\sum p_{X_n|X_{n-1},X_{n-2}}(X_n|X_{n-1},X_{n-2}) \cdot p_{X_{n-1},X_{n-2}}(X_{n-1},X_{n-2}) \cdot I(X_n|X_{n-1},X_{n-2})$$

ottenibile tramite probabilità di stato

$$H(X_n|\text{fissati } X_{n-1},X_{n-2}) = \sum_{n=1}^{2} p_{X_n|X_{n-1},X_{n-2}}(X_n|X_{n-1},X_{n-2}) \cdot \log\left(\frac{1}{p_{X_n|X_{n-1},X_{n-2}}(X_n|X_{n-1},X_{n-2})}\right)$$
$$= E[I(X_n|X_{n-1},X_{n-2})]$$

Diagramma di Markov: evoluzione tra stati



Prob. di transizione
Per simmetria stati: anche solo 2 stati:
$p_d = p(01) = p(10)$
$p_u = p(00) = p(11)$
Prob. stazionarie

Equazioni totali:
n stati + 1 di normalizzazione - 1 ridondante

$$\begin{cases} p_u = 1/2\, p_d + p \cdot p_u & \text{eq. entrante nello stato} \\ 2p_u + 2p_d = 2 & \text{eq. di normalizzazione} \end{cases}$$

$$\begin{cases} 1/2\, p_d + (p-1)p_u = 0 \\ p_u = 1/2 - p_d \end{cases} \qquad \begin{cases} 1/2\, p_d + (p-1)(1/2 - p_d) \\ \text{''} \end{cases}$$

$$\begin{cases} 1/2\, p_d + 1/2\, p - p p_d - 1/2 + p_d = 0 \\ \text{''} \end{cases} \qquad \begin{cases} \frac{3}{2} p_d - p p_d = 1/2 - 1/2\, p \end{cases}$$

$$\begin{cases} p_d = \frac{1-p}{3/2 - p} \cdot \frac{1}{2} = \frac{1-p}{3-2p} \\ p_u = \frac{1}{2} - \frac{1-p}{3-2p} = \frac{1}{2}\,\frac{1}{3-2p} \end{cases}$$

$$H(X_n|X_{n-1},X_{n-2}) = \frac{H_2(p) + 2 - 2p}{3-2p}$$

- con $p = 0$: $H(X_n|X_{n-1},X_{n-2}) = \frac{2}{3}$ bit
  $p_u = 1/6$ e $p_d = 1/3$

se sono nello stato 01 o 10 la transizione di un bit è un bit zero di informazione. ⇒ equipro.

Se nello stato 00 o 10 il bit trasmesso non ha nessuna informazione ⇒ deterministico.

- con $p=1$ $\quad H(X_u|X_{u-1},X_{u-2}) = 0$ bit

  $p_u = \eta_2$ e $p_d = 0$

Se stato 01 o 10 "inizialmente" il bit x_u trasmesso è un vero bit di informazione. Se stato 00 o 11 rimango sempre dentro questi stati emettendo un bit senza alcuna informaz. ⇒ sorgente non stazionaria

- con $p=\eta_2$ $\quad H(X_u|X_{u-1},X_{u-2}) = 1$ bit $\quad p_u = p_d = \eta_4$

  tutti gli stati dato la trasmissione di 1 bit emettono 1 bit vero di informazione ⇒ sorgente senza memoria

Calcolando $H(X_u|X_{u-1},X_{u-2})$ stesso:

$$H(x_u|00) = p(1|00)\cdot \log_2\left(\frac{1}{p(1|00)}\right) + p(0|00)\cdot \log_2\left(\frac{1}{p(0|00)}\right)$$

$$H(x_u|01) = p(1|01)\cdot \log_2\left(\frac{1}{p(1|01)}\right) + p(0|01)\cdot \log_2\left(\frac{1}{p(0|01)}\right)$$

$$H(x_u|10) = p(1|10)\cdot \log_2\left(\frac{1}{p(1|10)}\right) + p(0|10)\cdot \log_2\left(\frac{1}{p(0|10)}\right)$$

$$H(x_u|11) = p(1|11)\cdot \log_2\left(\frac{1}{p(1|11)}\right) + p(0|11)\cdot \log_2\left(\frac{1}{p(0|11)}\right)$$

$$H(x_u|x_{u-1},x_{u-2}) = p(00)\cdot\left[p(1|00)\cdot \log_2\left(\frac{1}{p(1|00)}\right) + p(0|00)\cdot \log_2\left(\frac{1}{p(0|00)}\right)\right] +$$
$$+ p(01)\cdot\left[p(1|01)\cdot \log_2\left(\frac{1}{p(1|01)}\right) + p(0|01)\cdot \log_2\left(\frac{1}{p(0|01)}\right)\right] +$$
$$+ p(10)\cdot\left[p(1|10)\cdot \log_2\left(\frac{1}{p(1|10)}\right) + p(0|10)\cdot \log_2\left(\frac{1}{p(0|10)}\right)\right] +$$
$$+ p(11)\cdot\left[p(1|11)\cdot \log_2\left(\frac{1}{p(1|11)}\right) + p(0|11)\cdot \log_2\left(\frac{1}{p(0|11)}\right)\right] =$$
$$= \frac{1}{2}\left(\frac{1}{3-2p}\right)\left[(1-p)\log_2\left(\frac{1}{1-p}\right) + p\cdot\log_2\left(\frac{1}{p}\right)\right] +$$
$$+ \left(\frac{1-p}{3-2p}\right)\left[\frac{1}{2}+\frac{1}{2}\right] +$$
$$+ \left(\frac{1-p}{3-2p}\right)\left[\frac{1}{2}+\frac{1}{2}\right] +$$
$$+ \frac{1}{2}\left(\frac{1}{3-2p}\right)\left[(1-p)\log_2\left(\frac{1}{1-p}\right) + p\cdot\log_2\left(\frac{1}{p}\right)\right] = \left(\frac{1}{3-2p}\right)\left[(1-p)\log_2\left(\frac{1}{1-p}\right) + p\cdot\log_2\left(\frac{1}{p}\right)\right] + \left(\frac{2-2p}{3-2p}\right)$$
$$= \left(\frac{1}{3-2p}\right) H_2(p) + \frac{2-2p}{3-2p}$$
$$= \frac{H_2(p) + 2 - 2p}{3-2p}$$

dove: $p(10) = p(01) = p_d$
$p(11) = p(00) = p_u$

Esame 16/9/2009

$\mathcal{X} = \{-1, 0, 1\}$ sorgente discreta X

$p_{X_n|X_{n-1}}(0|0) = 1/2$

$p_{X_n|X_{n-1}}(1|0) = p_{X_n|X_{n-1}}(-1|0) = 1/4 \Rightarrow p_{X_n|X_{n-1}}(X_n|0) = 1/4$

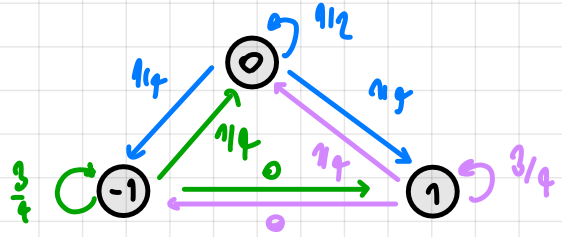
$p_{X_n|X_{n-1}}(0|-1) = p_{X_n|X_{n-1}}(0|1) = 1/4 \Rightarrow p_{X_n|X_{n-1}}(0|X_{n-1}) = 1/4$

$p_{X_n|X_{n-1}}(-1|-1) = p_{X_n|X_{n-1}}(1|1) = 3/4$

$\Rightarrow$ altrimenti $\emptyset$

Si tratta di una sorgente con memoria l'evento X_n è influenzato dall'evento X_{n-1}.

1) Si tratta di una sorgente Markoviana di parametro $m = 1$. Dal diagramma di Markov abbiamo che:



Probabilità di stato: $P(0), P(1), P(-1)$ $\Rightarrow$ Prob. marginali.

dove: $P(\text{stato}) = P(0) = P(1) = P(-1)$

$$\begin{cases} P(0) = 1/2\, P(0) + 2 \cdot 1/4\, P(1) \\ 2P(1) + P(0) = 1 \end{cases} \rightarrow \begin{array}{l} P(0) = 1/2 P(0) + 1/2 P(1) \\ P(1) = P(0) = 1/3 \\ P(0) = 1/3 \end{array}$$

sorta memoria $\rightarrow$ $p_{X_n}(x_n) = \frac{1}{3}$ $\forall\, x_n \in \{-1, 0, 1\}$

$$H(X) = 3 \cdot \tfrac{1}{3} \cdot \log_2(3) = 1{,}59 \text{ bit}$$

2) Calcolare entropie condizionate:

$$H(X_n|X_{n-1}) = \sum_{n=1}^{3} p_{X_n|X_{n-1}}(X_n|X_{n-1}) \cdot \log_2\left(\frac{1}{p_{X_n|X_{n-1}}(X_n|X_{n-1})}\right)$$

$$H(Y_n|0) = 1/4 \log(4) + 1/2 \log(2) + 1/4 \log(4) = 1{,}5 \text{ bit}$$

$$H(X_n|1) = 0 + 1/4 \log(4) + 3/4 \log(4/3) = 0{,}8 \text{ bit}$$

$$H(X_n|-1) = 0 + 1/4 \log(4) + 3/4 \log(4/3) = 98 \text{ bit}$$

da stato 1 e -1 è viceversa la probabilità di transizione risulta sempre nulla, dunque non ho alcun contributo in termini informativi $\Rightarrow$ determinismo da maggior impossibile compiere direzione improvvisamente.

3) Calcolo entropia condizionata: $H(X) = H(X_n|X_{n-1})$

$$\begin{aligned} H_{X_n|X_{n-1}}(X_n|X_{n-1}) &= \sum_{i=1}^{3} p_{X_{n-1}}(x_{n-1}) \cdot H(X_n|x_{n-1}) \\ &= P(-1) \cdot H(X_n|-1) + P(0) \cdot H(X_n|0) + P(1) \cdot H(X_n|1) \\ &= 1/3 \cdot 0{,}8 + 1/3 \cdot 1{,}5 + 1/3 \cdot 0{,}8 = 1{,}03 \text{ bit} \end{aligned}$$

$\Rightarrow$ la conoscenza dello stato precedente diminuisce l'informazione/incertezza dello stato attuale, ossia:

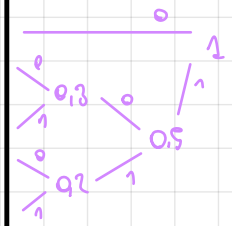
$$H(X|Y) \leq H(X)$$

Esame 17/6/2010

X sorgente discreta $\quad \mathcal{X} = \{A, B, C, D, E\}$

$$p_X(x) = \{0.1, 0.1, 0.3, 0.15, 0.15\}$$

Codifica Huffman: definisce un codice C ottimo per la sorgente X che sia istantaneamente decodificabile impiegando i teoremi sull'ottimalità

x	$p_X(x)$		$n(x_i)$	$C(x_i)$	
C	0.5		1	0 → C_1	0
D	0.15		3	100 → C_3	100
E	0.15		4	101 → C_8	1100
B	0.1		4	110 → C_7	1101
A	0.1		3	111 → C_4	111

Non posso scegliere i seguenti perché iniziano come un'altra sequenza:

$$C_1, C_6, C_5, C_9, C_{10}$$

Disuguaglianza di Kraft:

$$\sum_{i=1}^{9} 2^{-n(x_i)} \leq 1$$

$$2^{-1} + 2^{-3} + 2^{-3} + 2^{-4} + 2^{-4} \leq 1$$

$$1/2 + 2/8 + 2/16 \leq 1$$

$$\frac{8+4+2}{16} = \frac{14}{16} \leq 1$$

Il codice risulta essere istantaneamente decodificabile

Limite di Shannon: $\quad \bar{n}_C \geq H(x)$

$$\bar{n}_0 = \sum p_X(x_i) \cdot n(x_i)$$

$$= 0.5 \cdot 1 + 0.15 \cdot 3 + 0.15 \cdot 4 + 0.1 \cdot 4 + 0.1 \cdot 3$$

$$= 0.5 + 0.45 + 0.6 + 0.4 + 0.3$$

$$= 2.3 \text{ bit}$$

$$H(x) = 0.5 \log \tfrac{10}{5} + 0.3 \log \tfrac{100}{15} + 0.2 \log_2 10 \simeq 1.99 \text{ bit}$$

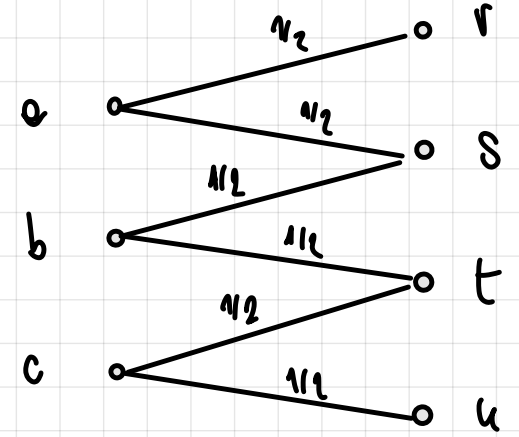
dunque $\bar{n}_C > H(x)$

Utilizzando la codifica ottima di Huffman otteniamo:

$$\bar{n}_C = 0.8 + 0.90 + 0.60 = 2.1 \text{ bit}$$

si avvicina molto di più al limite teorico con una compressione migliore senza perdita di informazione.

Esame 31/01/2006



$p(r|a) = 1/2$

$p(s|a) = 1/2$] $\sum_x p(s,x_i) = p(s)$; $p(s,a) = p(s|a)\cdot p_a$; $p(s,b) = p(s|b)\cdot p_b$

$p(s|b) = 1/2$

$p(t|b) = 1/2$

$p(t|c) = 1/2$

$p(u|c) = 1/2$

1) Calcolare $I(X;Y)$ assumendo $p_X(x)$ uniforme

2) Sfruttando le simmetrie assumere $p_X(x)$ dipendente da un solo parametro e trovare C. Discutere il risultato ottenuto e l'utilità del canale alla luce delle p_X ottime individuate.

1) $p_X(x_i) = \{1/3, 1/3, 1/3\}$

x	y	$p_X(x)$	$p_{Y\|X}(y\|x)$	$p_{Y,X}(y,x)$
a	r	1/3	1/2	1/6
a	s	1/3	1/2	1/6
b	s	1/3	1/2	1/6
b	t	1/3	1/2	1/6
c	t	1/3	1/2	1/6
c	u	1/3	1/2	1/6

$p_Y(y_j) = \sum_{i=1}^{3} p_X(x_i)\cdot p_{Y|X}(y_j|x_i)$

$p_Y(r) = p_X(a)\cdot p_{Y|X}(r|a) = 1/6$

$p_Y(s) = p_X(a)\cdot p_{Y|X}(s|a) + p_X(b)\cdot p_{Y|X}(s|b) = 1/3$

$p_Y(t) = p_X(b)\cdot p_{Y|X}(t|b) + p_X(c)\cdot p_{Y|X}(t|c) = 1/3$

$p_Y(u) = p_X(c)\cdot p_{Y|X}(u|c) = 1/6$

$p_{Y,X}(y,x) = p_{Y|X}(y|x)\cdot p_X(x)$

$H(Y|X) = \sum_i p_X(x_i)\cdot H(Y|x_i)$ (con x_i fissato)

$= \sum_i p_X(x_i)\cdot \sum_j p_{Y|X}(y_j|x_i)\cdot \log\frac{1}{p_{Y|X}(y_j|x_i)}$

$= \sum_i \sum_j p_{Y,X}(y_j,x_i)\cdot \log\frac{1}{p_{Y|X}(y_j|x_i)}$

$= 6\cdot\left(\frac{1}{6}\cdot 1\right) = 1$ bit

$H(Y|x_i) = \sum_j p_{Y|X}(y_j|x_i)\cdot I(y_j|x_i)$

$= 1/2 + 1/2 + 0 + 0$

$= 1$ bit

$H(Y) = \sum_j p_Y(y_j)\cdot \log\frac{1}{p_Y(y_j)}$

$= 2\cdot\left(\frac{1}{6}\cdot\log 6\right) + 2\cdot\left(\frac{1}{3}\log 3\right) = 1.92$ bit

$I(X;Y) = H(Y) - H(Y|X) = 1.92 - 1 = 0.92$ bit/uso canale

2) Sfruttando le simmetrie del grafico di trasmissione del canale otteniamo che:

$\begin{cases} p(a) = p(c) = p \\ p(a)+p(b)+p(c) = 1 \end{cases}$ $\begin{cases} " \\ 2p + p(b) = 1 \rightarrow p(b) = 1-2p \end{cases}$

x	y	$p_X(x)$	$p_{Y\|X}(y\|x)$	$p_{Y,X}(y,x)$
a	r	p	1/2	1/2 p
a	s	p	1/2	1/2 p
b	s	1-2p	1/2	1/2 (1-2p)
b	t	1-2p	1/2	1/2 (1-2p)
c	t	p	1/2	1/2 p
c	u	p	1/2	1/2 p

$p_Y(y_j = r) = p_Y(y_j = u) = 1/2\, p$

$p_Y(y_j = s) = p_Y(y_j = t) = 1/2\, p + 1/2 - p$

$= -1/2\, p + 1/2$

$= 1/2\,(1-p)$

$H(Y) = 2\cdot\left(\frac{1}{2}p\cdot\log\frac{2}{p}\right) + 2\cdot\left(\frac{1}{2}(1-p)\log\frac{2}{1-p}\right)$

$= p\cdot\log\frac{2}{p} + (1-p)\log\left(\frac{2}{1-p}\right) = 1 + H_2(p)$

$= p\log\frac{1}{p} + p\log 2 + (1-p)\log\left(\frac{1}{1-p}\right) + (1-p)\log 2$

$$= p \log \frac{1}{p} + p \log 2 + (1-p) \log \left(\frac{1}{1-p}\right) + (1-p) \log 2$$

$$= p \log \frac{1}{p} + (1-p) \log \left(\frac{1}{1-p}\right) + p + 1 - p$$

$$= H_2(p) + 1$$

$H(Y|X) = 4\left(\frac{1}{2} p \cdot 1\right) + 2 \cdot \left(\frac{1}{2}(1-2p) \cdot 1\right) = 2p + 1 - 2p = 1$ bit

Se prima abbiamo che

$$H(Y|x_i) = \sum_j p_{Y|X}(y_j|x_i) \cdot \log_2 \left(\frac{1}{p_{Y|X}(y_j|x_i)}\right)$$

$$= \frac{1}{2} \log 2 + \frac{1}{2} \log 2 + 0 + 0 \qquad \forall x_i$$

- fissato x_i
- non cambia con le cambiare di $p_X(x_i)$!!

Infatti con il cambio $p_X(x_i)$ potevo:

$$H(Y|X) = \sum_i p_X(x_i) \cdot H(Y|x_i)$$ uguale a prima

$$= \sum_i p_X(x_i) \cdot 1 = 1 \text{ bit}$$

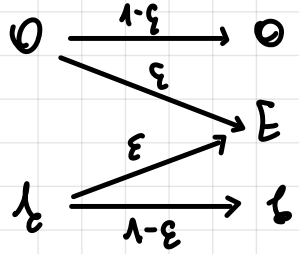
$$I(X;Y) = H(Y) - H(Y|X) =$$

$$= 2H_2(p) - 1$$

$$C = \max_p I(X;Y) = 1 \text{ bit/uso canale} \quad \text{con } p = 1/2$$

Esame 23/1/2005

Calcolare la capacità del canale BEC.



1) Determinare $I(X;Y)$ con p_X uniforme

2) Con p_X generica calcolo l'equivocazione quindi la $I(X;Y)$ e mostrerò che la I del punto 1) è la C.

1) $p_X(x_i) = \{\frac{1}{2}, \frac{1}{2}\}$

$$p_Y(y_j) = \sum_i p_X(x_i) \cdot p_{Y|X}(y_j|x_i)$$

$$p_Y(y_j) = \left\{\frac{1}{2}(1-\varepsilon),\ \varepsilon,\ \frac{1}{2}(1-\varepsilon)\right\}$$

$$H(Y) = \sum_j p_Y(y_j) \cdot \log \left(\frac{1}{p_Y(y_j)}\right) = 2 \cdot \frac{1}{2}(1-\varepsilon) \log \frac{2}{1-\varepsilon} + \varepsilon \log \frac{1}{\varepsilon}$$

$$= (1-\varepsilon) \log \frac{1}{1-\varepsilon} + \varepsilon \log \frac{1}{\varepsilon} + 1 - \varepsilon$$

$$= H_2(\varepsilon) + 1 - \varepsilon$$

$$H(Y|x_i) \overset{0,1}{=} \sum_j p_{Y|X}(y_j|x_i) \cdot \log \left(\frac{1}{p_{Y|X}(y_j|x_i)}\right) = H_2(\varepsilon)$$

$$H(Y|X) = \sum_i \sum_j p_{Y,X}(y_j, x_i) \cdot \log \left(\frac{1}{p_{Y|X}(y_j|x_i)}\right)$$

$$= \sum_i p_X(x_i) \cdot H(Y|x_i)$$

$$H(Y|X) = \frac{2}{3} H_2(\varepsilon) + \frac{1}{3} H_2(\varepsilon) = H_2(\varepsilon)$$

$$I(X;Y) = H(Y) - H(Y|X) = H_2(\varepsilon) + 1 - \varepsilon - H_2(\varepsilon)$$

$$= 1 - \varepsilon \quad \text{bit/uso canale}$$

2) Calcolare equivocazione

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

$$H(X) = \sum_i p_X(x_i) \cdot \log \frac{1}{p_X(x_i)} = 1 \text{ bit}$$

$$H(X|Y) = 1 - (1-\varepsilon) = \varepsilon$$

$$C = \max_{p} I(X,Y) = 1 - \varepsilon$$

C non è una proprietà della sorgente X ma del TX

Dimostrazione: $p_X(x_i) = \{p, 1-p\}$ generico

$$p_Y(y_i) = \{p(1-\varepsilon),\ p\varepsilon + (1-p)\varepsilon,\ (1-p)(1-\varepsilon)\}$$

$$H(Y) = p(1-\varepsilon) \log \frac{1}{p(1-\varepsilon)} + 0 + (1-p)(1-\varepsilon) \log \frac{1}{(1-p)(1-\varepsilon)}$$

$$H(Y|x_i) =$$

$$H(Y|X) =$$

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

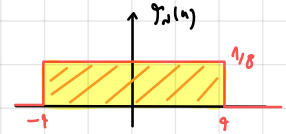
Esame 15/2/2007

$X \in \{-1; +1\}$ ingresso discreto

$p_X(x) = \{\frac{1}{2}, \frac{1}{2}\}$

Con rumore additivo indipendente da X con ddp uniforme nell'intervallo $[-4, 4]$. Calcolare:

- $H(X)$, $H(Y)$, $H(N)$, $H(Y|X)$, $I(X;Y)$ e C.
- e fornire una spiegazione intuitiva del valore ottenuto per C



$$E(X) = \frac{-4+4}{2} = 0$$

$$\text{Var}(X) = \frac{(b-a)^2}{12} = \frac{64}{12} = \frac{16}{3}$$

$$f_{N(n)} = \frac{1}{b-a} = \frac{1}{8}$$

$$Y = X + N$$

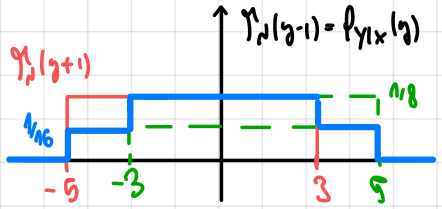
N continua $\rightarrow$ Y continua

$$f_{Y|X}(y|x_i) = f_{Y|X}(y - x_i | x_i) = f_N(y - x_i) = f_N(n)$$

$$I(X,Y) = H(Y) - H(Y|X) = H(Y) - H(N) \Rightarrow H(Y|X) = H(N)$$

$$f_Y(y) = \sum_i p_X(x_i) \cdot f_{Y|X}(y|x_i) = \sum_i p_X(x_i) \cdot f_N(y - x_i)$$

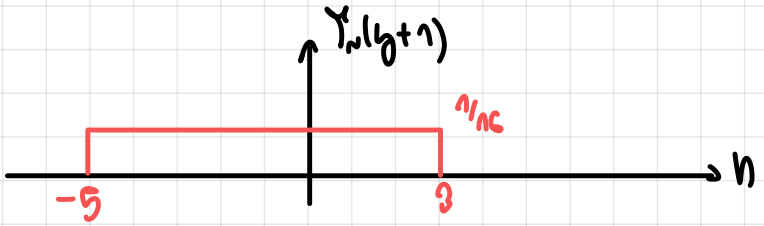
$$= \frac{1}{2} f_N(y+1) + \frac{1}{2} f_N(y-1)$$



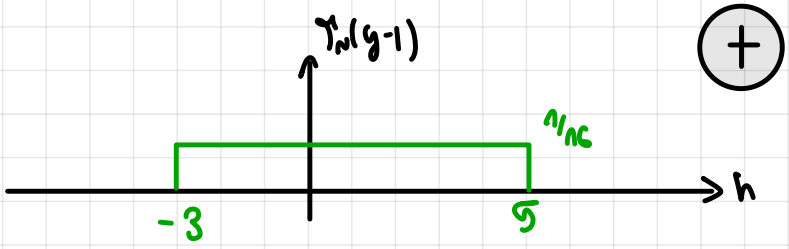
traslazione a dx di 1 rispetto a $f_N(n)$

traslazione a sx di 1 rispetto a $f_N(n)$

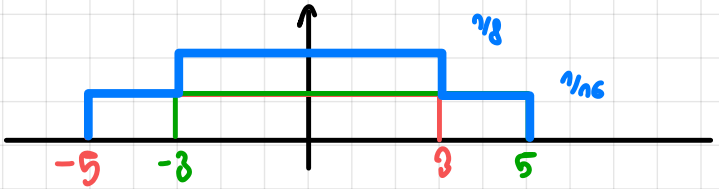
l'ampiezza della densità è metà di $f_N(n)$ ossia $\frac{1}{8} \cdot \frac{1}{2} = \frac{1}{16}$



+



=



$$H(N) = \int_{-\infty}^{+\infty} \gamma_n(h) \cdot \log \frac{1}{\gamma_n(h)}\, dh = \int_{-4}^{+4} \frac{1}{8} \cdot \log 8\, dh$$

$$= \frac{3}{8} \cdot \int_{-4}^{4} dh = \frac{3}{8} \cdot (x)_{-4}^{4}$$

$$= \frac{3}{8}\left[4 - (-4)\right] = 3$$

$$H(y) = \int_{-\infty}^{+\infty} \gamma_y(k) \cdot \log \frac{1}{\gamma_y(k)}\, dy = 2 \cdot \int_{-5}^{-3} \frac{1}{16} \cdot \log 16\, dy + \int_{-3}^{3} \frac{3}{8} \log 8\, dy$$

$$= \frac{1}{2} \cdot 2 + \frac{3}{8} \cdot 6 = 1 + \frac{18}{8} = \frac{26}{8}$$

$$\mathcal{I}(x;y) = H(y) - H(y|x) = H(y) - H(N)$$

$$= \frac{13}{4} - 3 = \frac{1}{4} \text{ bit/uso canale}$$

Esame: 12/9/2008

Si consideri: $GF(17)$

1) È un campo? Quali e quanti elementi e quali primitivi?

Sì, è un campo di Galois prime $GF(p)$ contenente 17 elementi:

$$GF = \{0, \dots, 16\}$$

L'ordine di un elemento del campo α^h è dato da:

$$n = \frac{(q-1)}{\text{massimo comun divisore } MCD(q-1, h)} \qquad h = 0, \dots, q-2$$

supponendo che α sia primitivo

(tutti multipli o divisori di 16)

ordine	elementi distinti del campo
16	$\alpha^1, \alpha^3, \alpha^5, \alpha^7, \alpha^9, \alpha^{11}, \alpha^{13}, \alpha^{15}$
8	$\alpha^2, \alpha^6, \alpha^{14}$
4	α^4, α^{12}
2	α^8
1	$\alpha^0 = 1$

(in notazione esponenziale con α incognito)

8 elementi primitivi distinti del campo

esempio: α^{15} ha ordine 16 $\Rightarrow \alpha^{15 \cdot 16} = 1$

2 è un elemento di questo gruppo

$\alpha^2 \Rightarrow \frac{16}{MCD(16,2)} = 8$ è l'ordine dell'elemento α^2

Cerchiamo un elemento primitivo per stabilire la conversione tra le due notazioni:

partiamo con gli elementi più piccoli $\rightarrow$ che 2

2^n	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
	2	4	8	16	32	$16 \cdot 2$	$13 \cdot 2$	$9 \cdot 2$
mod 17	2	4	8	16	15	13	9	1

$\Rightarrow$

- partiamo dire che 2 non ha ordine 2 o 4
- 2 ha ordine 8, non primitivo

$\Rightarrow$ $2^2 \bmod 17 = 4 \neq 1$
$2^4 \bmod 17 = 16 \neq 1$
$2^8 \bmod 17 = 1$

3^1	3^2		3^4				3^8
3	9	27	30	39	13	15	33
		10	13	5		11	16

Sono arrivato a 3^8 di cui 8 non è l'ordine $\Rightarrow$ risulta essere sicuramente un elemento primitivo

NB: gli ordini di tutti gli elementi devono dividere 16

α^h	0	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6
h	$-\infty$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

$\Rightarrow 3^{16} = 18 \bmod 17 = 1$

elementi primitivi

2) Determinare opposto di

a) $(9+8) \bmod 17 = 0$
b) $(1+16) \bmod 17 = 0$
c) $(5+12) \bmod 17 = 0$
d) $(0+0) \bmod 17 = 0$ non esiste l'elemento 17 in $GF(17)$

3) Determinare l'inverso:

a) $(9 \cdot 2) \bmod 17 = 1$
b) $(1 \cdot 1) \bmod 17 = 1$
c) $(5 \cdot 7) \bmod 17 = 1$
d) $\nexists$ inverso di 0

Def: $\alpha^h \cdot \alpha^{q-1-h} = 1$

$(3^5 \cdot 3^{11}) \bmod 17 = 1$
$3^{16} \bmod 17 = 1$

4) Quanto valgono:

$3^{18} = 3^{16} \cdot 3^2 = 1 \cdot 3^2 = 9$

$2^{148} = 2^{144} \cdot 2^4 = 16$

oppure $2^{148 \bmod 16} = 2^4 = 16$?

abbiamo visto che ordine di 2 è 8 $\Rightarrow 2^8 = 1$
quanti multipli di 8 ci stanno in 148

$2^{144} = 2^{8 \times 18}$

5) Calcolare $\beta = \sqrt[2]{15}$

$\beta = \sqrt{15} \Rightarrow \beta^2 = 15 \Rightarrow$ teorema dell'algebra lineare o al più 2 radici

in notazione esponenziale $\beta^2 = 15 \Rightarrow (\alpha^k)^2 = \alpha^6$

$(\alpha^k)^2 = \alpha^6$ — n·2 può darmi un esponente maggiore di 15, dunque devo ridurlo modulo 16

$(\alpha^u)^2 = \alpha^6 \iff (2u) \bmod 16$

NB: gli esponenti si riducono mod p-1 ⇒

$(\alpha^k)^2 = \alpha^6 \Rightarrow (2u) \bmod 16 = 6$

$2u = 6 \rightarrow u = 3$

$2u = 16+6 \rightarrow 2u = 22 \rightarrow u = 11$

al più 2 soluzioni:

- $\beta_1 = \alpha^3 = 10$
- $\beta_2 = \alpha^{11} = 7$

6) Quante e quali soluzioni hanno le equazioni:

1) $x^2 + 2 = 0$ → al più 2 soluzioni

2) $x^{89} + x = 0$ → al più 17 soluzioni GF(17)

3) $x^2 + 13x + 2 = 0$ → al più 2 soluzioni

1) $x^2 + 2 = 0$

$x^2 = -2$

$x^2 = 15$ ⇒ $(\alpha^4)^2 = 15$, $(\alpha^4)^2 = \alpha^6$

$(-2) \bmod 17 = (15) \bmod 17$

$u = 3 \rightarrow x_1 = \alpha^3 = 10$

$u = 11 \rightarrow x_2 = \alpha^{11} = 7$

2) $x^{89} + x = 0$

$x(x^{88} + 1) = 0$

$x(x^8 + 1) = 0$

$x = 0$

$x^8 + 1 = 0$

$x^8 = -1$

$x^8 = 16$

$(\alpha^4)^8 = \alpha^8$

quindi:

$(4 \cdot 8) \bmod 16 = 8$

$8u = 8 \rightarrow u = 1$

$8u = 24 \rightarrow u = 3$

$8u = 40 \rightarrow u = 5$

$8u = 56 \rightarrow u = 7$

$8u = 72 \rightarrow u = 9$

$8u = 88 \rightarrow u = 11$

$8u = 104 \rightarrow u = 13$

$8u = 120 \rightarrow u = 15$

Le soluzioni sono:

$0, \alpha^1, \alpha^2, \alpha^5, \alpha^7, \alpha^9, \alpha^{11}, \alpha^{13}, \alpha^{15}$

$0, 3, 10, 5, 11, 14, 7, 12, 6$

NB: - 0 è l'unico elemento 0 del campo non rappresentabile tramite notazione esponenziale.

3) $x^2 + 13x + 2 = 0$

$x_1, x_2 = \frac{-13 \pm \sqrt{13^2 - 8}}{2} = \frac{-13 \pm \sqrt{161}}{2} = \frac{-13 \pm \sqrt{8}}{2}$

$(161) \bmod 17 = 8$

$(\alpha^4)^2 = \alpha^{10}$

$(2u) \bmod 16 = 10 \rightarrow u = 5$

$x_{1,2} = \frac{-13 \pm 5}{2}$

$x_1 = -9 \Rightarrow 8$

$x_2 = -4 \Rightarrow 13$

Esame 7/2/2013

$p(\alpha) = \alpha^3 + \alpha + 1$ generatore del campo $GF(8)$

1) Quanti e quali sono gli elementi primitivi:

$(q-1) = 7$ è primo allora:

$\forall a \in GF(8)$ con $a \neq 0$ e $a \neq 1$ dove:

$GF(8) = GF(2^3)$

a_2	a_1	a_0	
0	0	0	0
0	0	1	1
0	1	0	α
0	1	1	$\alpha+1$
1	0	0	α^2
1	0	1	α^2+1
1	1	0	$\alpha^2+\alpha$
1	1	1	$\alpha^2+\alpha+1$

elementi primitivi

$GF(8) =$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
	0	α^0	α^1	α^3	α^2	α^6	α^4	α^5

Notazione polinomiale / Notazione esponenziale

1) Opposto di α^2+1

$(\alpha^2+1) + (\alpha^2+1) = 0$

2) Inverso di $\alpha^2+\alpha$

$(\alpha^2+\alpha) = \alpha^4$ inverso $\alpha^{7-1-4} = \alpha^3$

$\alpha^4 \cdot \alpha^3 = \alpha^7 = 1$

dove $\alpha^3 = \alpha + 1$

$\alpha^2+1 = \alpha^6$

inverso α^6: $\alpha^{7-1-6} = \alpha$

$\alpha^6 \cdot \alpha = \alpha^7 = 1$

oppure: $\alpha^6 \cdot \alpha^{-6} = 1$

dove $\alpha^{-6 \bmod 7} = \alpha$

3) Tutte le radici di:

- $x^2 = 0 \rightarrow x = 0$ 2 soluzioni coincidenti
- $x^2 = 1$ $(\alpha^u)^2 = \alpha^0$ dunque avremo

$(2u) \bmod 7 = 0 \rightarrow k = 0 \rightarrow \alpha^0 = 1$

- $x^2 + x = 0$

$x(x+1) = 0$ $x_1 = 0$

$x_2 = -1 \Rightarrow x_2 = (-1+2) = 1$

- $x^3 + x + 1 = 0$

per sostituzione (vedremo una proprietà dopo) trovo che $x_1 = \alpha$ è soluzione perché $\alpha^3 + \alpha + 1 = 0$:

infatti: $\alpha^3 + \alpha + 1 = 0$

$(\alpha+1) + \alpha + 1 = 0$

$x^3 + x + 1 \;|\; x + \alpha$

$x^3 + \alpha x^2$

$\alpha x^2 + x + 1$

$\alpha x^2 + \alpha^2 x$

$(1+\alpha^2)x + 1$

$x^2 + \alpha x + (1+\alpha^2)$

$\alpha(1+\alpha^2) = \alpha + \alpha^3$

$= \alpha + \alpha + 1 = 1$

$\Rightarrow x^3 + x + 1 = (x+\alpha)(x^2 + \alpha x + (1+\alpha^2))$

$x_1 = \alpha$

$x_2 = \alpha^3$

$x_3 = \alpha^4$ che controllo

Al più 2 soluzioni:

somma: $x_2 + x_3 = \alpha$

prodotto: $x_2 \cdot x_3 = 1 + \alpha^2$

guardando le tabelle

4) La radice $\sqrt{\alpha^2+\alpha}$ $\quad p^2 = \alpha^2 + \alpha$

$(\alpha^u)^2 = \alpha^2 + \alpha = \alpha^4 \Rightarrow (2u) \bmod 4 = 4$

$u = 2 \Rightarrow \alpha^2 = \alpha^2$

$2u = 11 \rightarrow \not\exists$

Esame 15/1/15

$GF(9) = GF(3^2)$

1) È un campo esteso di 9 elementi

2) $GF(3^2) =$

0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0								

Notazione polinomiale

3) opposto $\alpha+2+(2\alpha+1)=0$

4) Determinare inverso $2\cdot 2 = 1 \quad 4 \bmod 3 = 1$

$2^{-1} \Rightarrow -1 \bmod 8 = 7 \Rightarrow 2^7 \bmod 3 = 2$

5) Polinomio generatore primitivo del campo:

- deve avere grado $m=2$
- deve essere irriducibile
- deve avere coefficienti in $GF(3)=\{0,1,2\}$
- $\alpha^n \bmod p(\alpha)$ ottengo tutti i polinomi di $GF(9)$ con $n=0\dots 7$

$p(\alpha) = p_2\alpha^2 + p_1\alpha + p_0 \rightarrow$ p_2 può essere qualsiasi in $GF(3)$ tanto se divido il polinomio per p_2 ottengo comunque un fattore α^2 dunque $p_2 = 1$

$\Rightarrow p(\alpha) = \alpha^2 + p_1\alpha + p_0$ con $p_1, p_0 \in GF(3)$

$GF(3)$

	I tentativo	II tentativo
$p(0) = p_0 \neq 0$	$\rightarrow p_0 = 1$	$p_0 = 1$
$p(1) = 1 + p_1 + p_0 \neq 0$	$\rightarrow p_1 = 2$	$p_1 = 0$
$p(2) = 4 + 2p_1 + p_0 \neq 0$		
$= 1 + 2p_1 + p_0 \neq 0$	la terza = 0 non va bene	la buona ↓ $p(\alpha) = \alpha^2 + 1$

non $4 \bmod 3 = 1$

I valori li fisso e vedo se la III eq. torna

$p(\alpha) = \alpha^2 + 1 \Rightarrow \alpha^2 + 1 = 0 \Rightarrow \alpha^2 = -1 \bmod 3 = 2$

NB: α scelto come radice del polinomio irriducibile

$\alpha^2 \bmod \alpha^2+1 = 2$

α^2	α^2+1
α^2+1	1
$+1$	

$\Rightarrow -1 \bmod 3 = 2$

$\alpha^3 \bmod \alpha^2+1 = 2\alpha$

α^3	α^2+1
$\alpha^3+\alpha$	α
$+\alpha$	

$-\alpha = 2\alpha$

$\alpha^4 \bmod \alpha^2+1 = 1$

α^4	α^2+1
$\alpha^4+\alpha^2$	α^2-1
$+\alpha^2$	
$-\alpha^2-1$	
1	

$\Rightarrow$ $p(\alpha)$ non è un polinomio generatore primitivo

$\alpha^2 = (\alpha^2)^2 = (2)^2 = 4$

$4 \bmod 3 = 1$

Scegliamo un'altra soluzione:

III tentativo: $p_0 = 2$, $p_1 = 1$ → $p(\alpha) = \alpha^2 + \alpha + 2$

Vediamo se $p(\alpha)$ è primitivo: $x = r + kp$, $r = kp - x$

$\alpha^2 \bmod \alpha^2+\alpha+2 = (-\alpha-2) = 2\alpha+1$

$\alpha^3 \bmod p(\alpha) = 2\alpha^2 + \alpha = -\alpha - 4 = 2\alpha + 2$

$\alpha^4 \bmod p(\alpha) = 2\alpha^2 + 2\alpha = -4 = 2$

$\alpha^5 \bmod p(\alpha) = 2\alpha$

va bene

$\alpha^6 \bmod p(\alpha) = 2\alpha^2 = -2\alpha - 4 = \alpha + 2$

$\alpha^7 \bmod p(\alpha) = \alpha^2 + 2\alpha = \alpha - 2 = \alpha + 1$

$\alpha^8 \bmod p(\alpha) = \alpha^2 + \alpha = -2 \bmod 3 = 1$

$p(\alpha) = \alpha^2 + \alpha + 2$

$p(\alpha)$ è un generatore primo $\alpha^{q+1} = \alpha^8 = 1$

6) Trovare le soluzioni

- $x^1 = 0 \rightarrow x_{1,2} = 0$
- $x^2 = 1 \quad (\alpha^k)^2 = \alpha^0$
  $2k \bmod (9-1) = 0$
  $2k \bmod 8 = 0$
  $\rightarrow k = 0 \Rightarrow \alpha^0 = 1 = x_1$
  $\rightarrow k = 4 \Rightarrow \alpha^4 = 2 = x_2$
- $x^2 + x = 0 \quad x(x+1) = 0$
  $x_1 = 0$
  $x_2 = -1 = 2$
  $(\alpha^k = \alpha^{(q-1)} = \alpha^8$
  $k \bmod 8 = 4$
  $k = 4 \rightarrow \alpha^4 = 2$
  $x_2 = 1$
- $x^3 + x + 1 = 0$

per sostituzione

$x^3+x+1=0$ grado 3 al più 3 soluzioni

la risolvo per costituzione, dunque:

$$Gf(8) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

- $x_1 = 0$: $1 \neq 0$
- $x_1 = 1$: $3 \bmod 3 = 0 \Rightarrow 0=0$
- $x_2 = 2$: $8+2+1 \neq 0$
- $x_2 = \alpha$: $\alpha^3+\alpha+1=0$
  $(2\alpha+2)+\alpha+1=0 \Rightarrow 0=0$
- $x_3 = \alpha+1$: $(\alpha+1)^3+(\alpha+1)+1=0$
  $\alpha^3+1+\alpha+1+1=0$
  $2\alpha+2+1+\alpha+1+1=0$
  $3\alpha+2 \neq 0$
- $x_3 = 2\alpha+2$: $(2\alpha+2)^3+(2\alpha+2)+1=0$
  $(8\alpha^3+8)+2\alpha=0$
  $8(2\alpha+2)+8+2\alpha=0$
  $16\alpha+16+8+2\alpha=0$
  $18\alpha+24=0$ in mod 3
  $0=0$

Un altro modo sarebbe stato fattorizzando: dove γ radice $(x_1-\gamma)$

$x^3+x+1 \mid x+2$

$x^3+2x^2 \mid x^2+x+2$

x^2+x+1

x^2+2x

$2x+1$

$2x+4$

$5 \bmod 3 = 2$

$x_1 = 1$

$(x_1-1) = (x_1+2)$

$(x+2)(x^2+x+2)=0$

fattorizzando

$x^2+x+2 = (x-\gamma)(x-\beta) \Rightarrow \begin{cases} \gamma = x_2+x_3 = 1 \\ \beta = x_2 \cdot x_3 = 2 \end{cases}$

con tutti i dati trovati si ottiene come prima:

$x_2 = \alpha \rightarrow \gamma = \alpha+2\alpha+2 = 2$

$x_3 = 2\alpha+2$ $\beta = (2\alpha+2)(\alpha) = 2\alpha^2+2\alpha \bmod p(\alpha)$

$= 2(2\alpha+1)+2\alpha$

$= 4\alpha+2+2\alpha$

$= 6\alpha+2 = 2$

Dunque le radici sono:

$x_1 = 1$

$x_2 = \alpha$ $\Rightarrow$ $(x_1+2)(x_2-\alpha)(x_3-(2\alpha+2))=0$

$x_3 = 2\alpha+2$ $(x_1+2)(x_2+2\alpha)(x_3+(\alpha+1))=0$

$x_1 = -2 = 1$

$x_2 = -2\alpha = \alpha$

$x_3 = -\alpha-1 = 2\alpha+2$

$$\Omega(x) = \sum_{h=1}^{J} e_{\xi_h} \cdot \beta^{j_0 \cdot \xi_h} \cdot \prod_{\substack{u=1 \\ u \neq h}}^{J} (1 - \underbrace{\beta^{\xi_u} \cdot x}_{\beta^{\xi_u - \xi_i}})$$

$x = \beta^{-\xi_i}$

$u \neq h \ e \ h = i$

$$= e_{\xi_i} \cdot \beta^{j_0 \xi_i} \prod_{\substack{h=1 \\ h \neq i}}^{J} (1 - \beta^{\xi_h} \cdot x)$$

$$e_{\xi_i} = \frac{\Omega(x)}{\beta^{j_0 \xi_i} \prod_{\substack{h=1 \\ h \neq i}}^{J} (1 - \beta^{\xi_h} \cdot x)} \rightarrow \frac{\Omega(\beta^{-\xi_i})}{V'(\beta^{-\xi_i})}$$

$$V(x) = \sum_{h=1}^{J} (1 - \beta^{\xi_h} \cdot x) \rightarrow \frac{dV(x)}{dx} = - \sum_{h=1}^{J} \beta^{\xi_h} \cdot \sum_{\substack{u=1 \\ u \neq h}}^{J} (1 - \beta^{\xi_u} \cdot x)$$

$u \neq h \ e \ h = i$

$$V'(\beta^{-\xi_i}) = - \beta^{\xi_i} \cdot \sum_{\substack{h=1 \\ h \neq i}}^{J} 1 - \beta^{\xi_h - \xi_i}$$

$$\beta^{j_0 \xi_i} = \beta^{-\xi_i} \cdot \beta^{\xi_i} \cdot \beta^{j_0 \xi_i} = \beta^{-\xi_i} \cdot \beta^{\xi_i (0+1) j_0}$$

Esempio: Hamming (n, k, d) $\quad (7, 4, 3)$

$g(x) = x^3 + x + 1 \qquad (N-k) = 3 \rightarrow k = 7-3 = 4$ bit

evendo: $\underline{i} = [i_0\ i_1\ i_2\ i_3] = [0\ 1\ 0\ 1] \Rightarrow i(x) = x^3 + x$

rappresentazione non sistematica:

$$\begin{aligned} c(x) &= i(x) \cdot g(x) \\ &= (x^3 + x)(x^3 + x + 1) \\ &= x^6 + x^4 + x^3 + x^4 + x^2 + x \\ &= x^6 + 2x^4 + x^3 + x^2 + x \\ &= x^6 + x^3 + x^2 + x \end{aligned}$$ xor

$\underline{c} = [c_0\ c_1\ c_2\ c_3\ c_4\ c_5\ c_6] = [0\ 1\ 1\ 1\ 0\ 0\ 1]$

rappresentazione sistematica:

$$c(x) = i(x) \cdot x^{N-k} + \text{resto}\left[\frac{i(x) \cdot x^{N-k}}{g(x)}\right]$$

$x^6 + x^4$ | $x^3 + x + 1$

$x^6 + x^4 + x^3$ | $x^3 + 1$

x^3

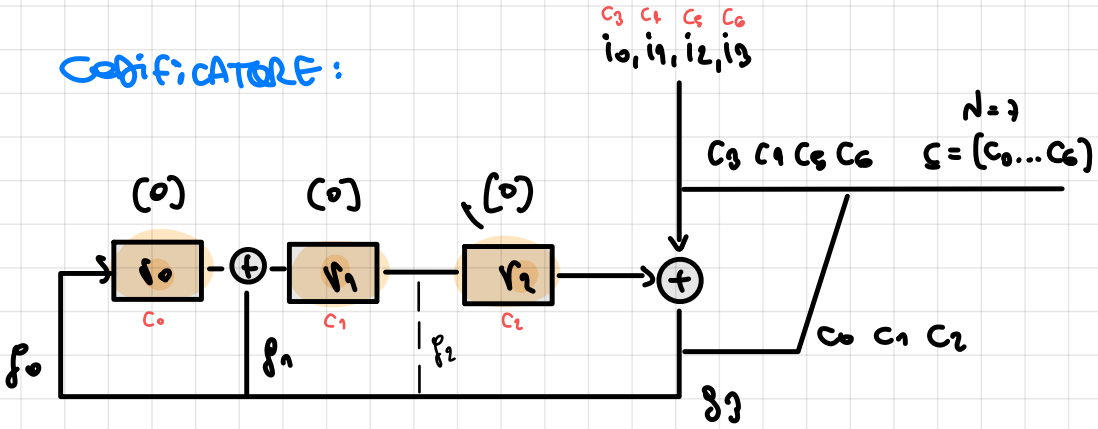
$x^3 + x + 1$

$x + 1$

$\Rightarrow c(x) = x^6 + x^4 + x + 1$

$\underline{c} = [1\ 1\ 0\ 0\ 1\ 0\ 1]$

CODIFICATORE:



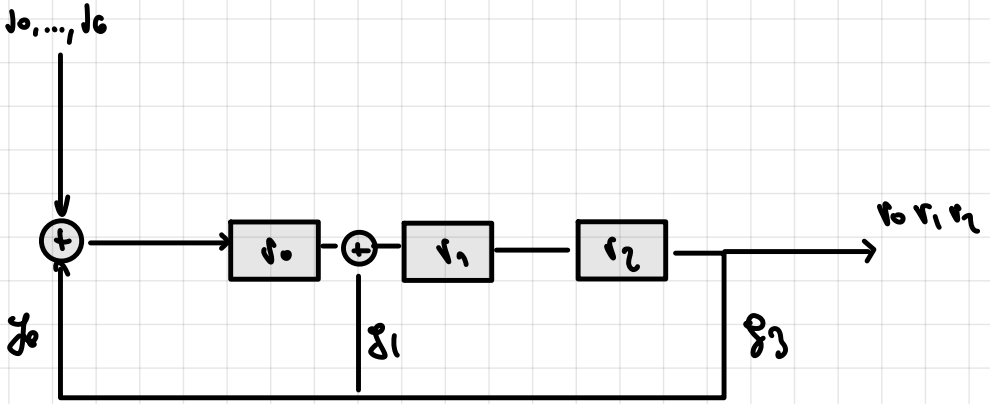
$g(x) = x^3 + x + 1$

$r(x) = r_2 x^2 + r_1 x + r_0$

Decodificatore:

Data una ricevuta generica $J(x)$

$$\text{resto}\left[\frac{J(x)}{g(x)}\right] \begin{cases} = 0 \Rightarrow J(x) \in C \\ \neq 0 \Rightarrow J(x) \notin C \end{cases}$$



Esame 27/08/2008

C binario non sistematico $N = 7 \Rightarrow GF(2^3)$

$g(x) = x^4 + x^3 + x^2 + 1$ $\quad (N-n) = 4 \rightarrow n = 3$ bit

1) Quanti e quali sono le parole di codice?

$M = 2^n = 8$ sequenze lecite

i_2 i_1 i_0	$i(x)$	$C(x) = i(x) \cdot g(x)$	$\underline{c}$ c_0 c_1 c_2 c_3 c_4 c_5 c_6
0 0 0	0	0	0 0 0 0 0 0 0
0 0 1	1	$x^4 + x^3 + x^2 + 1$	1 0 1 1 1 0 0
0 1 0	x	$x^5 + x^4 + x^3 + x$	0 1 0 1 1 1 0
0 1 1	$x+1$	$x^5 + x^2 + x + 1$	1 1 1 0 0 1 0
1 0 0	x^2	$x^6 + x^5 + x^4 + x^2$	0 0 1 0 1 1 1
1 0 1	x^2+1	$x^6 + x^3 + x^2 + 1$	1 0 0 1 0 1 1
1 1 0	x^2+x	$x^6 + x^4 + x^3 + x$	0 1 1 1 0 0 1
1 1 1	x^2+x+1	$x^6 + x^4 + x + 1$	1 1 0 0 1 0 1

$(x+1)(x^4+x^3+x^2+1) = x^5 + \cancel{x^4} + \cancel{x^3} + x + \cancel{x^4} + \cancel{x^3} + x^2 + 1$
$= x^5 + x^2 + x + 1$

$(x^2+1)(x^4+x^3+x^2+1) = x^6 + x^5 + \cancel{x^4} + \cancel{x^3} + x^2 + \cancel{x^4} + \cancel{x^3} + x^2 + 1$
$= x^6 + x^5 + x^2 + 1$

$(x^2+x)(x^4+x^3+x^2+1) = x^6 + \cancel{x^5} + \cancel{x^4} + x^2 + \cancel{x^5} + \cancel{x^4} + x^3 + x$
$= x^6 + x^3 + x^2 + x$

$(x^2+x+1)(x^4+x^3+x^2+1) = x^6 + \cancel{x^5} + \cancel{x^4} + x^2 + \cancel{x^5} + \cancel{x^4} + \cancel{x^3} + x + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + 1$
$= x^6 + x^4 + x + 1$

3) $d, t, r = ?$

Dato che si tratta di un codice lineare allora che:

$d_H = w_H(\underline{c}) = 4$ $\quad \forall \underline{c} \in C, \underline{c} \neq \underline{0}$ $\quad r = d - 1 = 3$

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

4) p_{tw} probabilità di sbagliare a correggere una parola (word) su BSC(p)

$$p_{tw} = \sum_{t=d+1}^{N} \binom{N}{e} \cdot \varepsilon^e \cdot (1-\varepsilon)^{N-e} = \sum_{t=d+1}^{N} N_e$$

$t+1 \gg N \cdot \varepsilon$
$N \gg t+1$
$\varepsilon = p \approx 0$

Utilizzando le seguenti approssimazioni avremo che:

$$p_{tw} \simeq \frac{N^{t+1}}{(t+1)!} \cdot (\varepsilon)^{t+1} (1-\varepsilon)^{N-(t+1)}$$

$$\simeq \frac{N^{t+1}}{(t+1)!} \cdot (\varepsilon)^{t+1} (1-\varepsilon)^{N} \simeq \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1}$$

$$\simeq \frac{7^2}{2} \cdot p^2$$

5) p_w su canale BSC(p)?

Spettro di Hamming di C: numero di parole in C con peso di Hamming e

$$p_w = \sum_{e=d}^{N} A_e \cdot \varepsilon^e \cdot (1-\varepsilon)^{N-e} = \sum_{e=4}^{7} A_e \cdot p^e \cdot (1-p)^{7-e}$$

$A_e = w_H(\underline{c}) = e$ $\quad \forall \underline{c} \in C, \underline{c} \neq \underline{0}$

$\simeq_{e=4} 7 \cdot p^4 \cdot (1-p)^3$

probabilità dominante

Esame 19/2/2009

Codice di Hamming : $p(x) = x^{10} + x^3 + 1$ $\quad (N-k) = 10$

$N = 2^{N-k} - 1 = 1023$

$k = 1023 - 10 = 1013$

$R = \frac{k}{N} = \frac{1013}{1023}$

In un codice di Hamming la distanza di Hamming vale:

$$d = 3 \rightarrow r = d-1 = 2$$
$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = 1$$

2) Quali sono parole di codice:

- $C_1(x) = 0$ Sì, $C_1(x) \in C$ sempre
- $C_2(x) = x^{11} + x^{10} + x^8 + x^3 + x + 1$

$$\begin{array}{l|l} x^{11} + x^{10} + x^8 + x^3 + x + 1 & x^{10} + x^3 + 1 \\ \hline x^{11} + x^8 + x & x + 1 \\ \hline x^{10} + x^3 + 1 & \\ \hline 11 & \end{array}$$

Sì, $C_2(x) \in C$ perché è divisibile per $g(x)$

- $C_3(x) = x^8 + x^2 + x$ No, $C_3(x) \in C$, $C_3(x)$ non è divisibile per $g(x)$
- $C_4(x) = x^{991} + x^{21}$ No, non è divisibile per $g(x) \Rightarrow C_4(x) \notin C$

Inoltre $d_H = 3 = w_H$ cioè devono esserci almeno 3 bit a 1 rispetto a 0

- $C_5(x) = x^{1022} + x^9 + x^2$ rotazione ciclica:

• grado max polinomio $N-1 = 1023-1 = 1022$

diventa se ruoto a dx ancora:

$$x^{1022} + x^9 + x^2$$
$$\downarrow \quad \downarrow \quad \downarrow$$
$$1 + x^{10} + x^3 = x^{10} + x^3 + 1 = g(x)$$

$\Rightarrow C_5(x) \in C$

- $C_6(x) = x^{1024} + x^{11} + x^9$ $\quad 1024 \bmod 1023 = 1$

$= x^{11} + x^9 + x$

$= (x^{10} + x^3 + 1) \cdot x \Rightarrow$ è una parola di codice

Esame 31/8/2006

Sapendo che: in $GF(2^4)$

$C = (c_0 \dots c_{14})$ con $c_i \in GF(2)$

$\underline{C} = (C_0 \dots C_{14})$ con $C_i \in GF(2^4)$ 'trasformate'

$N = 15 \Rightarrow \alpha^{15} = \alpha^{2^4-1} \Rightarrow$ BCH primitivo

Impongo che $i_0 = 1$

In $GF(2^4)$ abbiamo che:

(a_0, a_1, a_2, a_3) : $\forall a_i \in GF(2)$

a_3	a_2	a_1	a_0		
0	0	0	0	0	0
0	0	0	1	1	α^0
0	0	1	0	α	α
0	0	1	1	$\alpha+1$	α^4
0	1	0	0	α^2	α^2
0	1	0	1	α^2+1	α^8
0	1	1	0	$\alpha^2+\alpha$	α^9
0	1	1	1	$\alpha^2+\alpha+1$	α^{10}
1	0	0	0	α^3	α^3
1	0	0	1	α^3+1	α^{14}
1	0	1	0	$\alpha^3+\alpha$	α^1
1	0	1	1	$\alpha^3+\alpha+1$	α^6
1	1	0	0	$\alpha^3+\alpha^2$	α^{13}
1	1	0	1	$\alpha^3+\alpha^2+1$	α^{11}
1	1	1	0	$\alpha^3+\alpha^2+\alpha$	α^{12}
1	1	1	1	$\alpha^3+\alpha^2+\alpha+1$	α^5

$15-1=15$ elementi $\Rightarrow$ tutti elem. sono primitivi tranne 0 e 1.

Con $p(x) = x^4 + x + 1$

Polinomi minimi: $M_i(x) = \prod_{q=0}^{q-1} (x - (\alpha^i)^{2^q})$ dove $(\alpha^i)^{2^q} = \alpha^{i \cdot 2^q}$

$M_1(x) = M_2(x) = M_4(x) = M_8(x)$
$= (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$
dove $16 \bmod 15 = 1$

$M_3(x) = M_6(x) = M_{12}(x) = M_9(x)$
$(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$
$24 \bmod 15 = 9$

$M_5(x) = M_{10}(x)$
$(x-\alpha^5)(x-\alpha^{10})$

$M_7(x) = M_{11}(x) = M_{13}(x) = M_{14}(x)$
$(x-\alpha^7)(x-\alpha^{14})(x-\alpha^{13})(x-\alpha^{11})$

Utilizzando una sola radice $j_0 = 1$ avremo che:

sapendo che $g(x) = x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$

$g(x) = M_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$
$= x^4 + x^3(\alpha+\alpha^2+\alpha^4+\alpha^8)$
$+ x^2(\alpha^3+\alpha^5+\alpha^6+\alpha^9+\alpha^{10}+\alpha^{12})$
$+ x(\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14})$
$+ \alpha^{15}$
$= x^4 + x + 1 = (1\,0\,0\,1\,1)$

→ $\binom{4}{1} = 4$
→ $\binom{4}{2} = \frac{4!}{2!(4-2)!} = \frac{24}{4} = 6$
→ $\binom{4}{3} = 4$
→ $\binom{4}{4} = 1$

elementi prodotto a 2 a 2:
$(x-\alpha)(x-\alpha^2) = (x^2 + (\alpha+\alpha^2)x + \alpha^3)$
$(x-\alpha^8)(x-\alpha^9) = (x^2 + (\alpha^8+\alpha^9)x + \alpha^{17})$
e moltiplicare tra di loro.

N	n	d	t	g(x) ottenuto
15	11	3	0	23

- $x(\dots)$ esempio fisso $(x-\alpha)$ e moltiplico gli altri 3
- $x^2(\dots)$ esempio fisso $(x-\alpha)(x-\alpha^2)$ e moltiplico gli altri 2
- $x^3(\dots)$ esempio fisso 3 moltiplico gli altri

Con $d-1 \Rightarrow d-1$ radici consecutive

$M_3(x) = x^4 + x^3(\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9) + x^2(\alpha^9 + \alpha^{13} + \alpha^{12} + \alpha^{18} + \alpha^{13} + \alpha^{21}) + x(\alpha^{21} + \alpha^{18} + \alpha^{24} + \alpha^{24}) + \alpha^{20}$

$= x^4 + x^3 + x^2 + x + 1$

$g(x) = mcm(M_1(x), M_3(x)) = (x^4+x+1)(x^4+x^3+x^2+x+1)$

$= x^8 + x^7 + x^6 + x^5 + x^4 + x^5 + x^4 + x^3 + x^2 + x + x^4 + x^3 + x^2 + x + 1$

$= x^8 + x^7 + x^6 + x^4 + 1$

$(1\ 1\ 1 \mid 0\ 1\ 0 \mid 0\ 0\ 1)$

7 2 1

N	u	N-u	d	t	g(x) ottenuto
15	11	4	3	1	23
15	7	8	5	2	721

Con $d = 5$:

$M_5(x) = (x-\alpha^5)(x-\alpha^{10}) = x^2 + x(\alpha^{10} + \alpha^5) + \alpha^{15}$

$= x^2 + x + 1$

$g(x) = mcm(M_1(x), M_3(x), M_5(x))$

$= (x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$

$= (x^8 + x^7 + x^6 + x^4 + 1)(x^2+x+1)$

$= x^{10} + x^9 + x^8 + x^6 + x^2 + x^9 + x^8 + x^7 + x^5 + x + x^8 + x^7 + x^6 + x^4 + 1 = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$

$= 2467_8$

N	u	N-u	d	t	g(x) ottenuto
15	11	4	3	1	23
15	7	8	5	2	721
15	5	10	7	3	2467
15	1	14	15	7	7777

$M_7(x) = x^4 + x^3(\alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11}) + x^2(\alpha^6 + \alpha^5 + \alpha^3 + \alpha^{12} + \alpha^{10} + \alpha^9) + x(\alpha^4 + \alpha^2 + \alpha + \alpha^8) + 1$

$= x^4 + x^3$

$\alpha^3 + \alpha + 1$
$\alpha^3 + 1$
$\alpha^3 + \alpha^2 + 1$
$\alpha^3 + \alpha^2 + \alpha$

$\alpha^3 + \alpha^2$
$\alpha^2 + \alpha$
α^3
$\alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^2 + \alpha + 1$
$\alpha^3 + \alpha$

$\alpha + 1$
α^2
α
$\alpha^2 + 1$

$g(x) = mcm(M_1(x), M_3(x), M_5(x), M_7(x))$

$= (x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1)(x^8 + x^3)$

$= x^{18} + x^{12} + x^9 + x^8 + x^6 + x^5 + x^3 + x^{13} + x^{11} + x^8 + x^7 + x^5 + x^4 + x^3$

$= x^{18} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3$

Esame 17/11/2016

$GF(4) = GF(2^2)$ generato da $p(\alpha) = \alpha^2 + \alpha + 1$

1)

Notazione esponenziale	$\alpha^{-\infty}$	α^0	α	α^2
Notazione polinomiale	0	1	α	$\alpha+1$

2) $q^m - 1 = 3$ disperi $\Rightarrow \forall a \in GF(2^2)$ con $a \neq 0$ e 1 sono elementi primitivi.

3) $\underline{v} = (v_0\ v_1\ v_2)$ con $v_i \in GF(4)$

Lunghezza $\underline{v}$ è $N = 2 \Rightarrow$ ai degli altri $\alpha^{2^n - 1} = 1$, $\alpha^3 = 1$

$$J_j = \sum_{i=0}^{N-1} v_i \cdot \alpha^{ij}$$

$$\begin{cases} J_0 = v_0 + v_1 + v_2 \\ J_1 = v_0 + v_1\alpha + v_2\alpha^2 \\ J_2 = v_0 + v_1\alpha^2 + v_2\alpha^4 \end{cases} \qquad \begin{cases} J_0 = v_0 + v_1 + v_2 \\ J_1 = v_0 + \alpha v_1 + (\alpha+1)v_2 \\ J_2 = v_0 + (\alpha+1)v_1 + \alpha v_2 \end{cases}$$

4) Quante terne distinte $(v_0\ v_1\ v_2)$? $L^N = 4^3 = 64$

5) Consideriamolo $(v_0\ v_1\ v_2)$ con $v_i \in GF(4)$ e $J_0 = 0$.

$J_0 = 0 \Rightarrow$ distanza di Hamming $d = 2$

polinomio generatore: $g(x) = (x - \alpha^0) = (x-1)$

$N = 3 \quad N - u = 1 \quad u = 2 \Rightarrow q^2 = 16$ sequenze

Reed Solomon $RS(\overset{N}{3}, \overset{u}{2}, \overset{d}{2})$ ni è ciclico $GF(4)$

Elencare le sequenze a titolo di esempio:

$J_0 = v_0 + v_1 + v_2$

	v_0	v_1	v_2
$\underline{c}_1 =$	0	0	0
$\underline{c}_2 =$	0	α	α

$\text{mod } 2 = 0$

$\alpha + \alpha = 2\alpha$

6) $(v_0\ v_1\ v_2)$ con $v_i \in GF(2)$ e $J_j \in GF(4)$ e $J_0 = 0$

Si è un codice ciclico $J_0 = 0 \Rightarrow BCH(\overset{N}{3}, \overset{u}{2}, \overset{d}{2})$

con generatore $g(x) = x - 1$ $\quad RSC(3, 2, 2)$

$q^u = q^2 = 4$ sequenze

$\underline{c}_1 = 0\ 0\ 0$
$\underline{c}_2 = 1\ 0\ 1$
$\underline{c}_3 = 1\ 1\ 0$
$\underline{c}_4 = 0\ 1\ 1$

7) $(v_0\ v_1\ v_2)$ con $v_i \in GF(2)$ e $J_j \in GF(4)$ con $J_1 = 0$

Sì, è un codice ciclico $J_1 = 0 \Rightarrow BCH(\overset{N}{3}, \overset{u}{1}, \overset{d}{2})$

$$p(x) = M_1(x) = (x - \alpha)(x - \alpha^2)$$

$q^u = q^1 = 2$ sequenze lecite $\Rightarrow J_1 = 0$ cioè $v_0 + \alpha v_1 + (\alpha+1)v_2 = 0$

$\underline{c}_1 = 0\ 0\ 0$
$\underline{c}_2 = 1\ 1\ 1$

Esame 13/9/2007

- Decodificatore primitivo BCH lunghezza $N = 15$
- con $g(x)$ di radici: $\alpha, \alpha^2, \alpha^3, \alpha^4$
- sindromi:

$j_0 = 1$

$S_0 = E_1 = \alpha^3$
$S_1 = E_2 = \alpha^6$
$S_2 = E_3 = \alpha^9$
$S_3 = E_4 = \alpha^{12}$

1) Scrivere le key equation
2) Determinare $\Lambda(x)$ il n° e le posizioni degli errori.

Assunzioni:

- 4 radici consecutive $\rightarrow$ $d = 5$
- n° max errori $v = \frac{d-1}{2} = 2$ errori
- $N = 15 \Rightarrow \beta^d = 1$ lunghezza sequenza dunque

$$S_i, C_j \in GF(2^4)$$

Polinomio locatore:

$$\Lambda(x) = \prod_{n=1}^{2} (1 - \beta^{E_n} x) = \Lambda_0 + \Lambda_1 x + \Lambda_2 x^2$$

($\Lambda_0 = 1$)

key equation:

$$\sum_{n=0}^{N-1} \Lambda_n \cdot E_{k-n} = \Lambda_0 \cdot E_k + \sum_{n=1}^{N-1} \Lambda_n \cdot E_{k-n} \quad \forall k < N$$

$$\sum_{n=1}^{N-1} \Lambda_n \cdot E_{k-n} = -E_k \quad j_0+v \le k \le j_0+d-2$$

$$\sum_{n=1}^{v} \Lambda_n \cdot E_{k-n} = -E_k$$

$$\sum_{n=1}^{v} \Lambda_n \cdot S_{k-n} = S_k \quad \forall k : v \le k \le d-2$$

Totale equazioni: $d - v - 1 = 5 - 2 - 1 = 2$ equazioni

$$\sum_{n=1}^{2} \Lambda_n \cdot S_{k-n} = -S_k \qquad v \le k \le d-2, \quad 2 \le k \le 3$$

$$\begin{cases} \Lambda_1 \cdot S_1 + \Lambda_2 \cdot S_0 = -S_2 & (k=2) \\ \Lambda_1 \cdot S_2 + \Lambda_2 \cdot S_1 = -S_3 & (k=3) \end{cases}$$

Λ_i sono le incognite

$$\Lambda_1 = -\frac{\Lambda_2 \cdot S_0 - S_2}{S_1} \Rightarrow \frac{(-\Lambda_2 S_0 - S_2) S_2}{S_1} + \Lambda_2 S_1 = -S_3$$

$$-\Lambda_2 S_0 S_2 - S_2^2 + \Lambda_2 S_1^2 = -S_1 S_3$$

$$\Lambda_2 (S_1^2 - S_0 S_2) = S_2^2 - S_1 S_3$$

$S_1^2 - S_0 S_2 \neq 0$
$\alpha^{12} - \alpha^{12} \neq 0 \Rightarrow$ indeterminato

$$S_1^2 - S_0 S_2 \neq 0$$

Indeterminato se $v = 2$ e $v = 1$:

$d - v - 1 = 5 - 1 - 1 = 3$ n° equazioni

$$\sum_{n=1}^{1} \Lambda_n \cdot S_{k-n} = -S_k \qquad v \le k \le d-2, \quad 1 \le k \le 3$$

$$\begin{cases} \Lambda_1 \cdot S_0 = -S_1 \rightarrow \Lambda_1 = -\frac{S_1}{S_0} = \alpha^3 \\ \Lambda_1 \cdot S_1 = -S_2 \quad \Lambda_1 = \alpha^3 \\ \Lambda_1 \cdot S_2 = -S_3 \quad \Lambda_1 = \alpha^3 \end{cases}$$

$\Lambda(x) = \Lambda_0 + \Lambda_1 x = 1 + \alpha^3 x$

β^{-E_n} radici polinomio locatore: $\Lambda(x) = 0$

$1 + \alpha^3 x = 0$
$\alpha^3 x = -1$
$x = -\alpha^{-3}$
$x = \alpha^{-3} \Rightarrow$ posizione α^3

radice in $\Lambda(x) \rightarrow \beta^{-E_n}$
posizione $\beta^{E_n} = \alpha^3$

Il bit da complementare è y_3

Esame 27/6/2013

BCH $(7,4)$ primitivo con $j_0 = 1$ e bit c_3 errato

1) Potere correttore codice?

- $g(x)$ grado $N-k = 7-4 = 3$
- $\beta^N = \beta^{2^m - 1} = \beta^7 \Rightarrow GF(2^3)$ $\quad p(\beta) = \beta^3 + \beta + 1$ polinomio
- $j_0 = 1 \Rightarrow C_1 \Rightarrow$ codice $d \Rightarrow$ polinomio minimo d:

$$M_{\beta_1}(x) = (x-\beta)(x-\beta^2)(x-\beta^4) \Rightarrow g(x) = (x-\beta)(x-\beta^2)(x-\beta^4)$$

$C_1, C_2, C_4 = 0$ $\quad$ radici consecutive $= 2$

$\Rightarrow d = 2+1 = 3$

BCH bound

$$t = \frac{d-1}{2} = 1$$

2) Determinare $\Lambda(x)$

errori $\quad j_{max} = \frac{d-1}{2} = t = 1$

$$\Lambda(x) = \prod_{h=1}^{1} (1 - \beta^{c_h} x) = \Lambda_0 + \Lambda_1 x$$

$\Lambda_0 = 1$

key equation:

$$\prod_{h=1}^{j=1} \Lambda_h \cdot S_{k-h} = -S_k$$

$j = u \le d-2$

$1 \le k \le 1 \Rightarrow u = 1$

$$\Lambda_1 \cdot S_0 = S_1 \rightarrow \Lambda_1 = \frac{S_1}{S_0}$$

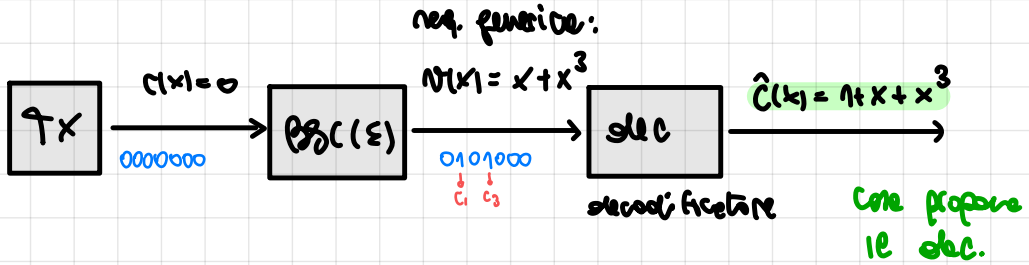
Una volta trovato Λ_1 viene sostituito in $\Lambda(x)$ e ricavate le posizioni degli errori.

$$S_0 = E_{0+j_0} = J_{0+j_0} = \sum_{h=0}^{N-1=6} e_h \cdot \beta^{h \cdot 1} = \beta^3 + \beta^3$$
$$= \epsilon_{1+} = J_1$$

$$S_1 = E_{1+j_0} = J_{1+j_0}$$
$$= E_2 = J_2 = \sum_{h=0}^{7} e_h \cdot \beta^{h \cdot 2} = (\beta^2 + \beta^4) \bmod p(\beta) = 1$$

$$\Lambda_1 = \frac{S_1}{S_0} = \frac{1}{\beta^3 + \beta^3} = 1 \Rightarrow \Lambda(x) = 1 + x$$
$$x = (-1) \bmod 2 = 1 = \beta^0$$

Dunque il decodificatore complementa il bit 0. Ossia:



In un caso base: $\quad \hat{x}_{ML} = \arg\min_{x \in \text{Lcode}} d_H(y, x) \Rightarrow$ scelta errata del decodificatore

Esame 17/7/2014

RS(7,5) $j_0 = 1$ simbolo errato c_6 con $e_6 = \alpha^2$

1) Potere correttore t? Supponendo RS(7,5) primitivo (N lungo)

- $\alpha^N = \alpha^{q^m - 1} = \alpha^7 \Rightarrow GF(8)$
- Non devo includere polinomi minimi dunque altro:

Sapendo che $j_0 = 1$ e $d = 2$ sappiamo che: $c_1 = 0$ e $c_2 = 0$

$g(x)$ grado $(N-u) = 7 - 5 = 2$

$\Rightarrow d - 1 = N - u = 2 \Rightarrow g(x) = (x-\alpha)(x-\alpha^2)$

$d = N - u + 1 = 3 \quad = x^2 + x(\alpha + \alpha^2) + \alpha^3$

$\Rightarrow t = \frac{d-1}{2} = 1$

2) Polinomio locatore: supponendo $\nu = t = 1$

$$\Lambda(x) = \prod_{h=1}^{\nu=1} (1 - \alpha^{e_h} x) = \Lambda_0 + \Lambda_1 x = 1 + \alpha^6 x$$

→ posizione errore 6 $\quad \alpha^{-e_h} = \alpha^{-6}$

3) Polinomio valutatore degli errori:

$$\Omega(x) = (\Lambda(x) \cdot S(x)) \bmod x^{d-1}$$

Sapendo che: $\Lambda(x) = 1 + \alpha^6 x$

$S(x) = S_0 + S_1 x$ da cui:

$$S_0 = E_{0+j_0} = \sum_{h=0}^{N-1} e_h \cdot \alpha^{h \cdot 1} = \alpha^1 \cdot \alpha^6 = \alpha^3 = \alpha$$

$$S_1 = E_{1+j_0} = \sum_{h=0}^{N-1} e_h \cdot \alpha^{h \cdot 2} = \alpha^2 \cdot \alpha^{12} = \alpha^{14} = 1$$

$$\Lambda(x) \cdot S(x) = (1 + \alpha^6 x) \cdot (\alpha + x) = \alpha + x + \alpha^7 x + \alpha^6 x^2$$

$$\Omega(x) = (\alpha + x + \alpha^7 x + \alpha^6 x^2) \bmod x^2 = \alpha + x(1 + \alpha^7) = \alpha + x(1+1) = \alpha$$

$$e_6 = -\frac{\Omega(\alpha^{-6})}{\Lambda'(\alpha^{-6})} = -\frac{\alpha}{\alpha^6} = -\alpha^{-5} = \alpha^2 \qquad \Lambda'(x) = \alpha^6$$

4) Controllare con algoritmo di Euclide

$$\Omega(x) = (\Lambda(x) S(x)) \bmod x^2 = \Lambda(x) S(x) - \Phi x^2$$

cond. terminazione: grado$(\Omega(x)) >$ grado$(\Lambda(x))$

$$\begin{cases} \Omega_{-1}(x) = x^2 \\ \Lambda_{-1}(x) = 0 \\ \Phi_{-1}(x) = 1 \end{cases} \qquad \begin{cases} \Omega_0(x) = S(x) = \alpha + x \\ \Lambda_0(x) = 1 \\ \Phi_0(x) = 0 \end{cases}$$

$x^2 \mid x+\alpha$

$x^2 + \alpha x \mid x + \alpha$

αx

$\alpha x + \alpha^2$

α^2

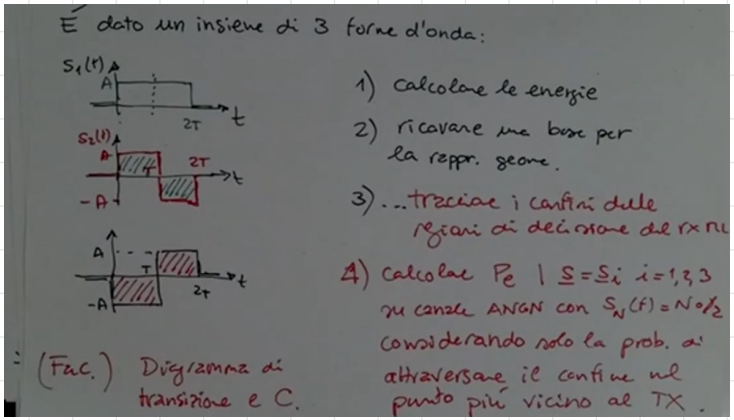
$$\Phi_h = \frac{\Omega_{h-2}(x)}{\Omega_{h-1}(x)} \rightsquigarrow q_1 = \frac{\Omega_{-1}(x)}{\Omega_0(x)} = \frac{x^2}{\alpha + x} = x + \alpha$$

$$\begin{cases} \Omega_h(x) = \Omega_{h-2}(x) - q_h \Omega_{h-1}(x) \rightarrow (\Omega_{-1}(x)) \bmod \Omega_0(x) \\ \Lambda_h(x) = \Lambda_{h-2}(x) - q_h \Lambda_{h-1}(x) \\ \Phi_h(x) = \Phi_{h-2}(x) - q_h \Phi_{h-1}(x) \end{cases}$$

$$\begin{cases} \Omega_1(x) = \Omega_{-1}(x) - q_1 \Omega_0(x) = x^2 - (x+\alpha)\cdot(x+\alpha) = \alpha^2 \quad (x^2 + \alpha^2) \\ \Lambda_1(x) = \Lambda_{-1}(x) - q_1 \Lambda_0(x) = x + \alpha \\ \Phi_1(x) = \Phi_{-1}(x) - q_1 \Phi_0(x) = 1 \end{cases}$$

Una sola iterazione avendo dell'algoritmo. Non garantisce $\Lambda_0 = 1$ (monico).

Esame 26/1/2006



1) $\int s_1(t)^2 dt = \int_0^{2T} A^2 dt = 2A^2T = E_1 = E_2 = E_3 = E$

2) Utilizzando G.S. otteniamo:

$$\varphi_1(t) = \frac{s_1(t)}{\sqrt{E}} \quad \text{dove } s_1(t) = A\,\text{rect}\left(\frac{t-T}{2T}\right) \quad \text{dove } \|s_1(t)\| = \sqrt{E}$$

$$\Rightarrow \underline{s}_1 = (\sqrt{E}, 0, \dots)$$

Utilizzo la seconda forma d'onda ottenuamo:

$$s_{21} = \int s_2(t)\cdot\varphi_1(t)\,dt = \int_0^T A\cdot\frac{A}{\sqrt{E}}dt + \int_T^{2T} -A\cdot\frac{A}{\sqrt{E}}dt = \frac{A^2}{\sqrt{E}}T - \frac{A^2}{\sqrt{E}}T = 0$$

$$s_2(t) \perp \varphi_1(t) \Rightarrow \varphi_2(t) = \frac{s_2(t)}{\sqrt{E}}$$

$$\Rightarrow \underline{s}_2 = (0, \sqrt{E}, \dots)$$

Utilizzando $s_3(t)$ otteniamo:

$$s_{31} = \int s_3(t)\cdot\varphi_1(t)\,dt = \int_0^T -A\cdot\frac{A}{\sqrt{E}}dt + \int_T^{2T} A\cdot\frac{A}{\sqrt{E}} = 0 \Rightarrow s_3(t) \perp \varphi_1(t)$$

$$s_{32} = \int s_3(t)\cdot\varphi_2(t)\,dt = \int_0^T -A\cdot\frac{A}{\sqrt{E}}dt + \int_T^{2T} A\cdot-\frac{A}{\sqrt{E}}dt = -\frac{2A^2T}{\sqrt{E}} = -\sqrt{E}$$

$\Downarrow$ $s_3(t) \parallel \varphi_2(t)$, $\|s_3(t)\| = s_{32}$ modulo

$\underline{s}_3 = (0, -\sqrt{E}, 0\dots)$ infatti se:

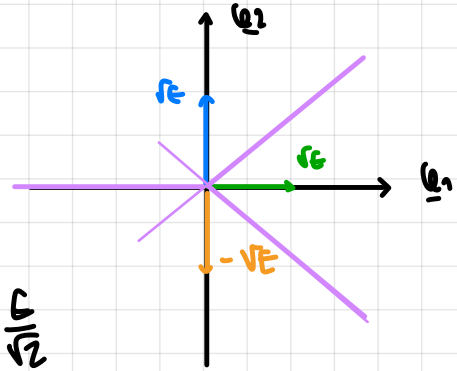
$$s_3(t) - s_{32}\varphi_2(t) = s_3(t) + \sqrt{E}\varphi_2(t)$$

$$= s_3(t) + \sqrt{E}\frac{s_2(t)}{\sqrt{E}} = s_3(t) + s_2(t) = 0$$

Uno è la combinazione lineare dell'altro

3) Tracciare confini:

Legenda: $\underline{s}_1$ $\underline{s}_2$ $\underline{s}_3$

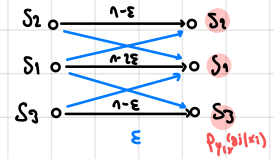


4) Calcolare P_e: $\frac{d}{2} = \frac{\sqrt{2E}}{2} = \frac{E}{\sqrt{2}}$

$$P_e(n_\perp > \tfrac{d}{2}) = Q\left(\frac{\frac{d}{2}-m_x}{\sqrt{N_0/2}}\right) = Q\left(\frac{d}{\sqrt{2N_0}}\right)$$

$$P_{e1}(n_\perp > d/2) = 2\cdot Q\left(\sqrt{\frac{E}{N_0}}\right) = 2\varepsilon$$
$$P_{e2}(n_\perp > d/2) = Q\left(\sqrt{\frac{E}{N_0}}\right) = \varepsilon$$
$$P_{e3}(n_\perp > d/2) = Q\left(\sqrt{\frac{E}{N_0}}\right) = \varepsilon$$

Diagramma di Transizione:



5) $P_X(x) = \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$

$P_Y(y) = \{\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\}$

$$H(Y) = \sum_{j=1}^{3} P_Y(y_j)\cdot\log\left(\frac{1}{P_Y(y_j)}\right) = \log 3$$

$$H(Y|S_2) = \sum_{j=1}^{3} P_{Y|x}(y_j|x_i)\cdot\varepsilon(y_j|x_i) = H_2(\varepsilon)$$

$$H(Y|S_1) = (1-2\varepsilon)\cdot\log\left(\frac{1}{1-2\varepsilon}\right) + (2\varepsilon)\cdot\log\left(\frac{1}{2\varepsilon}\right) = H_2(2\varepsilon)$$

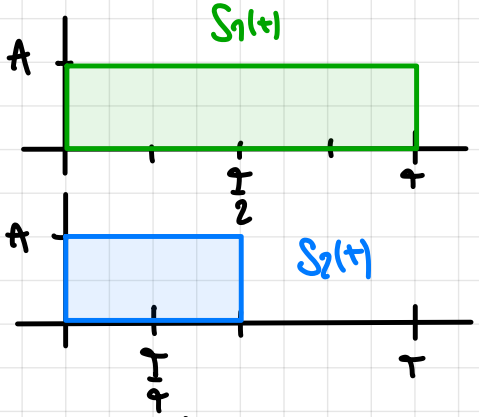
$$I(X;Y) = H(Y) - H(Y|X) = \log 3 - \frac{1}{3}H_2(\varepsilon) - \frac{2}{3}H_2(2\varepsilon)$$

Esame 8/9/16

$s_1(t) = A\,\mathrm{rect}\left(\frac{t-\frac{T}{2}}{T}\right)$

$s_2(t) = A\,\mathrm{rect}\left(\frac{t-\frac{T}{4}}{\frac{T}{2}}\right)$

Canale AWGN $S_w(f) = \frac{N_0}{2}$



1) $R_b = \frac{1}{T}$ trasmetto 1 bit su un periodo T

2) $E_1 = \int_0^T s_1(t)^2\,dt = A^2T$ $\quad E_2 = \int_0^{T/2} s_2(t)^2\,dt = A^2\frac{T}{2} = \frac{E_1}{2}$

3) 4) Rappresentazione geometrica tramite G.S.:

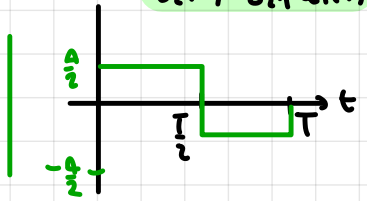
$\varphi_1(t) = \frac{s_1(t)}{\sqrt{E_1}} = \frac{s_1(t)}{\sqrt{A^2T}}$ $\quad \underline{s}_1 = (\sqrt{E_1}, 0, \dots)$

non è $\parallel \varphi_1(t)$

$s_{21} = \int s_2(t)\cdot\varphi_1(t)\,dt = \int_0^{T/2} A\cdot\frac{A}{\sqrt{A^2T}}\,dt = \frac{AT}{2} = \frac{\sqrt{E_1}}{2} \neq \|s_2(t)\|$

$s_2(t) - s_{21}\varphi_1(t) \perp \varphi_1(t)$

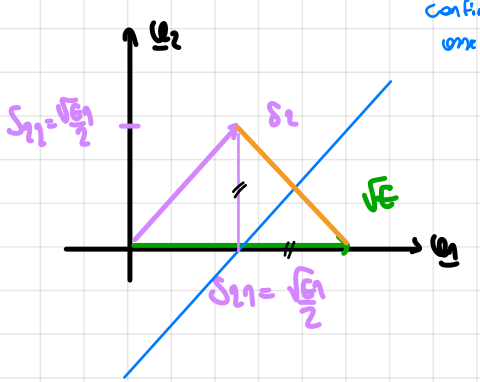
$\varphi_2(t) = \frac{s_2(t) - s_{21}\varphi_1(t)}{\|s_2(t) - s_{21}\varphi_1(t)\|} = \frac{s_2(t) - \frac{s_1(t)}{2}}{\|s_2(t) - s_{21}\varphi_1(t)\|} = \frac{s_2(t) - \frac{1}{2}s_1(t)}{\sqrt{\frac{E_1}{2}}}$



dove:
$E = \int_0^{T/2}\left(\frac{A}{2}\right)^2 dt + \int_{T/2}^{T}\left|-\frac{A}{2}\right|^2 dt$
$= \frac{A^2T}{4\cdot 2} + \frac{A^2T}{4\cdot 2} = \frac{A^2T}{4} = \frac{E_1}{4}$

$\Rightarrow \underline{s}_2 = \left(0, \sqrt{\frac{E_1}{2}}, \dots\right)$

Legenda:
$\underline{s}_1$
$\underline{s}_2$
$\underline{s}_1 - \underline{s}_2$



dove $d = \sqrt{2}\cdot\frac{\sqrt{E_1}}{2} = \frac{\sqrt{E_1}}{\sqrt{2}}$

6) Calcolo P_e e confrontare con 2-PAM:

$P_e(n_1 > \frac{d}{2}) = Q\left(\frac{\frac{d}{2}\cdot w_x}{\sqrt{\frac{N_0}{2}}}\right) = Q\left(\frac{d}{\sqrt{2N_0}}\right) = Q\left(\frac{\sqrt{E_1}}{2\sqrt{N_0}}\right)$

$E_b = \frac{E_1 + E_1/2}{2} = \frac{3}{4}E_1 \Rightarrow E_1 = \frac{4}{3}E_b$

2 forme d'onda diverse

$P_e(n_1 > \frac{d}{2}) = Q\left(\frac{\sqrt{\frac{4}{3}E_b}}{\sqrt{4N_0}}\right) = Q\left(\sqrt{\frac{E_b}{3N_0}}\right)$

2-PAM $\rightarrow Q\left(\sqrt{\frac{2E_b}{N_0}}\right)$

Perde $\frac{1}{6}$ cioè $-7{,}8$ dB rispetto a 2-PAM

$10\log_{10}\frac{1}{6} \simeq -7{,}8$ dB

Esame 9/2/2012

RS in GF(4) con $g(x) = x+1$

1) Quanto vulgono:

codice α e α^{N-1} è $N-1$

- con Rb primitivo $\alpha^n = \alpha^{4^{n-1}} = \alpha^3 \Rightarrow N = 3$
- N-k grado polinomio $g(x) \Rightarrow N-k=1$ che coi $k=2$
- $d-1 = N-k = 1 \Rightarrow d = 2$ (teri in TDF $C_j = 1$)

$t = 0$

$r = 1$

2) Alfabeto:

$$GF(2^2) = \{0, 1, \alpha, \alpha+1\}$$

alfabeto, codice e TDF $\in GF(2^2)$ $\quad c_i, C_j \in GF(4)$

$\underbrace{C_0 C_1 C_2}_{N-2} \in GF(4)$

$C_0 C_1 C_2 \in GF(4)$

bit di parità

bit di informaz

Affinché un sequenza c sia di codice oblieuno che:

$g(x) = x+1 \rightarrow x=1 \rightarrow C(x)|_{x=1} = 0 \quad \forall C(x) \in \mathcal{C}$

sapendo che $\alpha^0 = 1$ avremo che:

$c(\alpha^0) = 0 = C_0 \rightarrow$ deve essere a altrimenti la sequenza non è ricevibile.

3) Sindromi:

- $e_0 = 1, \ e_1 = e_2 = 0 \qquad j_0 = 0 \qquad \Rightarrow S_0 = J_0 = E_0$

$$S_0 = E_0 = \sum_{h=0}^{N-1} e_{E_h} \cdot \alpha^{0 \cdot E_h} = 1$$

$\Rightarrow$ la sequenza ricevuta non è di codice $\notin \mathcal{C}$ contiene errori

- $e_0 = e_2 = 0 \quad e_1 = 1$

$$S_0 = J_0 = E_0 = \sum_{h=0}^{N-1} e_h \cdot \alpha^{0 \cdot h} = 1 \neq 0$$

$\Rightarrow$ la sequenza $\notin \mathcal{C}$ contiene errori.

- $e_0 = 0 \quad e_1 = e_2 = \alpha$

$$S_0 = J_0 = E_0 = \sum_{h=0}^{d-1} e_h \cdot \alpha^{0 \cdot h} = 0 + \alpha + \alpha = 0$$
$$= 0 + 2\alpha = 0$$
$$2 \bmod 2 = 0$$

$\Rightarrow O(x) \in \mathcal{C}$

$r = 1 \neq 2 \Rightarrow$ sequenza lecita

$r = d$

NB: $\quad C(\alpha^0) = 0 \Rightarrow C_0 = 0 \Rightarrow j_0 = 0$

Esame: 19/1/2012

Codice sistematico binario, $N=4$, $g(x)=x+1$

- Quante e quali parole di codice?

$c_i \in GF(2) = [0,1]$ $\quad \underline{c} = c_0\, c_1\, c_2\, c_3$

$c(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3$

Una sequenza lecita e sistematica è:

$$c(x) = i(x)\cdot x^{N-k} + \text{resto}\left[\frac{i(x)\cdot x^{N-k}}{g(x)}\right] \qquad c(x) \in \mathcal{C}$$

$c(x) = l_e(x)\cdot g(x)$ $\quad c(x) \in \mathcal{C}$

Oss: $g(1)=0 \rightarrow c(1)=0 \quad \forall c(x)\in C$

Questo vuol dire che: $c(1) = c_0+c_1+c_2+c_3 = 0$

Ovvio che se $\sum_{i=0}^{N-1} c_i = 0 \Rightarrow$ SPC

$N-k=1 \Rightarrow k=3$

una sola radice
$\Rightarrow d-1=1$
$d=2, r=1, t=0$

Sequenze lecite: $2^k = 8 \in \mathcal{C}$
Sequenze totali: $2^N = 16$

Le sequenze lecite sono: $\underline{c}\cdot \underline{H} = \underline{0}$

Ne è solo se somma bit a 1 = 0

0 0 0 0	0 1 0 0	1 0 0 0	1 1 0 0
0 0 0 1	0 1 0 1	1 0 0 1	1 1 0 1
0 0 1 0	0 1 1 0	1 0 1 0	1 1 1 0
0 0 1 1	0 1 1 1	1 0 1 1	1 1 1 1

- Si tratta di un codice SPC: ne sequenze sempre parity check

- P_{fw} su BSC:

$$P_{fw} = \sum_{e=d}^{N} A_e \cdot \varepsilon^e \cdot (1-\varepsilon)^{N-e} \simeq A_{t+1}\cdot \varepsilon^{t+1}$$

dominante $\varepsilon \to 0$

dove

$A_e = d_H(\underline{c}_R, \underline{c}_T) = d_H(\underline{c}_R + \underline{c}_T, \underline{0}) = w_H(\underline{c}_R + \underline{c}_T) = e$ errori

spettro di Hamm. del $\mathcal{C}$

Nel nostro caso (guardare sequenze):

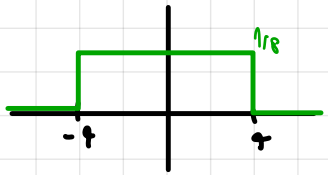
$A_0 = 1$
$A_3 = A_1 = 0$ solo pesi 1 leciti
$A_2 = 6$
$A_4 = 1$

- No non si potrebbe usare su canale BSC(p):

non ho potere correttore e non so individuare l'errore per effettuare una correzione.

Esame: 13/2/2007

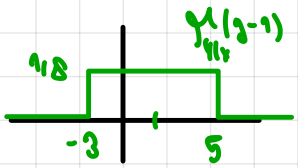
$Y = X + N$ $\quad X \perp N$ $\quad X = \{-1, +1\}$ $\quad P_X(x_i) = \{\eta_2, \eta_2\}$



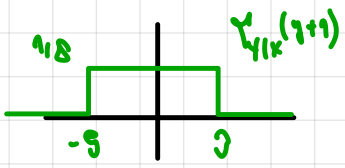
$$f_{Y|X}(y|x) = f_{Y|X}(y-x|x) = f_N(y-x|x) = f_N(y-x) = f_N(n)$$

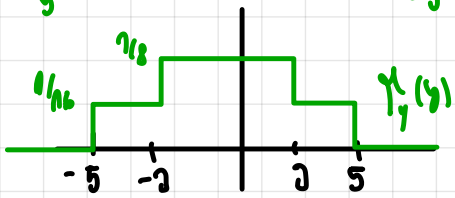
$$H(Y|X) = H(N) \rightarrow I(X;Y) = H(Y) - H(Y|X) = H(Y) - H(N)$$

se trasmetto 1 traslato a dx



se trasmetto -1:





$$f_Y(y) = \sum_i f_{Y|X}(y|x_i) \cdot P(x_i) = \frac{1}{2} f_{Y|X}(y-1) + \frac{1}{2} f_{Y|X}(y+1)$$

$$H(Y) = \int_{-\infty}^{+\infty} f_Y(y) \cdot \log\left(\frac{1}{f_Y(y)}\right) dy$$

$$= \int_{-8}^{-3} \frac{1}{16} \cdot \log 16 \, dy + \int_{-3}^{3} \frac{1}{8} \log 8 \, dy + \int_{3}^{5} \frac{1}{16} \log 16 \, dy$$

$$= \frac{1}{16} \cdot (-3+5) \cdot 4 + \frac{1}{8} \cdot (3+3) \cdot 3 + \frac{1}{16} \cdot (5-3) \cdot 4$$

$$= \eta_2 + \frac{18}{8} + \eta_2 = \frac{2+9+2}{4} = \frac{13}{4}$$

$$H(N) = \int_{-\infty}^{+\infty} f_N(n) \cdot \log \frac{1}{f_N(n)} \, dn = \int_{-4}^{4} \frac{1}{8} \log 8 \, dn = \frac{1}{8} \cdot (4+4) \cdot 3 = 3$$

$$H(X) = \sum_i P_X(x_i) \log \frac{1}{P_X(x_i)} = \frac{1}{2} \cdot \log 2 + \frac{1}{2} \log 2 = \log 2 = 1$$

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

$$= H(Y) - H(N) = \frac{13}{4} - 3 = \frac{13-12}{4} = \eta_4 \text{ bit/use canale}$$

$$C = \max_{P_X(x_i)} I(X;Y) = \max_{P_X(x_i)} H(Y)$$

ma la distribuzione dell'ingresso è equiprobabile $\Rightarrow$ capacità massima.

Esame 19/7/2011

GF(5), definire sequenze con N=4, RS

- Elemento opposto in GF(5) = {0,1,2,3,4} → $3^N = 1$

$$2^N = 2^4 = 16 \bmod 5 = 1$$

$$3^N = 3^4 = 6 \bmod 5 = 1$$

- Carattere di Jn solo errori $3^0\ 3^1\ 3^2\ 3^3$ / 1 3 4 2

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

$d = 2t+1 = 3$ BCH Lower $d-1$ trasformata è 0

$N-k = d-1 \Rightarrow N-k = 2 \Rightarrow k = 2$

- Le radici possibili di g(x) sono:

g(x) deve avere grado (N-k) con (N-k) radici consecutive α^i

- Parole di codice:

$c_i, c_j \in GF(5)$ sequenze totali: $5^N = 625$ sequenze lecite: $5^2 = 25$

- Si assume che $j_0 = 1 \Rightarrow C_1 = 0 \Rightarrow$ radice 3^0, $C_3 = 0 \Rightarrow$ radice 3^1

$g(x) = (x-1)(x-3)$

- La sequenza $c = \overset{C_0}{0}\ \overset{C_1}{0}\ \overset{C_2}{0}\ \overset{C_3}{3}$ è di codice?

$C(x) = 3x^3$ $C(1) = 3 \neq 0 \Rightarrow C(x) \notin \mathcal{C}$

$C(3) = 3^4 = 1 \neq 0$

- Calcolare le sindromi

$$S_0 = V_{0+j_0} = V_1 = \sum_{n=0}^{N-1} v_n \cdot 3^{1 \cdot n} = 3 \cdot 3^3 = 3^4 = 1$$

$$S_1 = V_{1+j_0} = V_2 = \sum_{n} v_n \cdot 3^{2 \cdot n} = 3 \cdot 3^6 = 3^7 = 3^3$$

- Calcolare $\Lambda(x)$ t_{max} errori $= t = 1$

$$\Lambda(x) = \prod_{n=1}^{t} (1 - \alpha^n x) = \Lambda_0 + \Lambda_1 x$$

t^2 equazioni $d-1-1 = 3-1-1 = 1$ eq. Key equation:

$$\sum_{h=1}^{N-1} \Lambda_h \cdot S_{k-h} = -S_k \quad \text{con} \quad \begin{matrix} 1 \le k \le d-2 \\ 1 \le k \le 1 \Rightarrow k=1 \end{matrix}$$

$$\Lambda_1 \cdot S_0 = -S_1$$

$$\Lambda_1 = \frac{-S_1}{S_0} = -3^3 = -2 = 3$$

$\Lambda(x) = \Lambda_0 + \Lambda_1 x = 1 + 3x$ $1 + 3x = 0$

$x = -\frac{1}{3} = -3^{-1}$

$\Lambda(x=3) = 1 + 3^2 = 0$

$= 1 + 2 = 3 = 0$ $= -3^2 = -2 = 3$

posizione $\Rightarrow 3$

$\Omega(x) = (\Lambda(x) \cdot S(x)) \bmod x^{d-1}$

$= ((1+3x)\cdot(1+2x)) \bmod x^{d-1}$

$= (1 + 2x + 3x + 6x^2) \bmod x^{d-1}$

$= 1$

$$e_3 = -\frac{\Omega(3)}{\Lambda'(3)} = -\frac{1}{3} < 3$$

Esame 17/1/2019

$X = \{D_0, M_1, F_A, L_A\}$

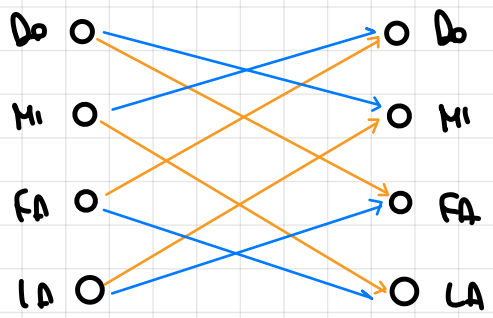
$p_{Y|X}(D_0|F_A) = p_{Y|X}(F_A|D_0) = p$

$p_{Y|X}(M_1|L_A) = p_{Y|X}(L_A|M_1) = 1-p$

$p_{Y|X}(D_0|M_1) = p_{Y|X}(M_1|D_0)$

$p_{Y|X}(F_A|L_A) = p_{Y|X}(L_A|F_A)$

Diagramma di transizione:



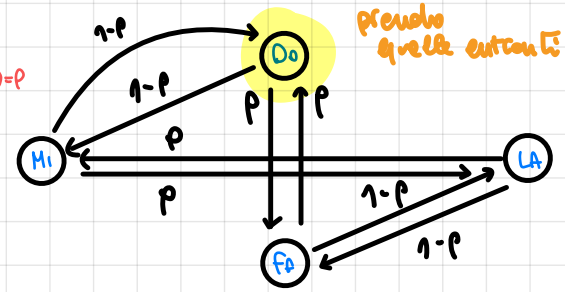
1) È una sorgente con memoria limitata ⇒ sorgente di Markov con parametro $M = 1$ ossia

$$H(X) = H(X_n|X_{n-1}, \dots, X_{n-L}) \quad L \to \infty$$
$$= \frac{H(X_n, X_{n-1}, \dots, X_{n-L})}{L}$$

$$X(k) = H(X_n|X_{n-1}) = \frac{H(X_n, X_{n-1})}{L} \quad L = 1$$

Probabilità di stato ⇒ Diagramma di Markov

Notato e fine esercizio per simmetria ho: $P(M_1) = P(L_A) = P(F_A) = P(D_0) = p$, $4p = 1 \Rightarrow p = \frac{1}{4}$, rovato fare tutti i passaggi



prendo quelli entranti

Simmetrie:
$P(D_0) = P(F_A) = P(a)$
$P(M_1) = P(L_A) = P(b)$
2 incognite
2 eq. indipendenti

$$\begin{cases} P(a) = (1-p)P(b) + pP(a) \\ 2P(a) + 2P(b) = 1 \end{cases} \qquad \begin{cases} P(a)(1-p) = (1-p)P(b) \\ P(a) = \frac{1-2P(b)}{2} \end{cases}$$

$$\begin{cases} P(a)(1-p) = (1-p)P(b) \\ P(a) = \frac{1-2P(b)}{2} \end{cases} \longrightarrow \frac{1-2P(b)}{2}\cdot(1-p) = (1-p)P(b)$$

$$(1-2P(b))(1-p) = 2P(b) - 2pP(b)$$

$$1 - p - 2P(b) + 2pP(b) = 2P(b) - 2pP(b)$$

$$4pP(b) - 4P(b) = p - 1$$

$$P(b) = \frac{p-1}{4p-4}$$

$$2P(a) = 1 - \frac{p-1}{2p-2}$$

$$(4p-4)P(a) = 2p - 2 - p + 1$$

$$P(a) = \frac{p-1}{4p-4}$$

$\Rightarrow P(a) = P(b) \Rightarrow 2P(a) + 2P(a) = 1 \to P(b) = \frac{1}{4}$

$P(a) = \frac{1}{4}$

$P_X(x) = \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\} \to P_Y(y_j) = \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\}$

$$H(X) = \sum_i P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} = 4 \cdot \frac{1}{4} \cdot 2 = 2 \text{ bit}$$

$$H(Y|x_i = D_0) = \sum_j P_{Y|X}(y_j|x_i) \cdot \log \frac{1}{P_{Y|X}(y_j|x_i)} = (1-p)\log\frac{1}{1-p} + p\log\frac{1}{p}$$

$$= H_2(p)$$

$$H(Y|X) = \sum_i H(Y|x_i) \cdot P_X(x_i) = \sum_i P_{Y,X}(y_j, x_i) \cdot \log \frac{1}{P_{Y|X}(y_j|x_i)}$$

$$= 4 \cdot H_2(p) \cdot \frac{1}{4} = H_2(p)$$

$$P_Y(y_j) = \sum_i P_{Y,X}(y_j, x_i) = \sum_i P_{Y|X}(y_j|x_i) \cdot P_X(x_i) = (1-p)\cdot\frac{1}{4} + p \cdot \frac{1}{4} = \frac{1}{4}$$

$$H(Y) = \sum_j P_Y(y_j) \cdot \log \frac{1}{P_Y(y_j)} = 4 \cdot \frac{1}{4} \cdot 2 = 2 \text{ bit}$$

$$\gamma(X,Y) = H(Y) - H(Y|X) = 2 - H_2(p) \ \frac{\text{bit}}{\text{uso}} \text{ come } p$$

$H(X)$ con memoria:

$$H(X) = H(X_n^Y | X_{n-1}^X) = H(Y|X) = H_2(P)$$

Esame 18/2/2016

	1	2	3	...	10
1		min(1,1) = 1	1	1	1
2	1		2	2	2
3	1	2			
⋮	1	2		9	9
10	1	2		9	

Probabilità di vincere x come carte più basse:

$$p_X(1) = \frac{9+9}{90} = \frac{18}{90}$$

$$p_X(2) = \frac{8+8}{90} = \frac{16}{90}$$

$$p_X(3) = \frac{7+7}{90}$$

$$\vdots$$

$$p_X(9) = \frac{2}{90}$$

- una coppia = 1 evento
- tutti gli eventi sono equiprobabili:

P(estrarre una coppia di carte Jolade) = equiprobabile

Le coppie estratte possibili sono: 90

- Quanti valori può assumere X:

X: risultato coppie estratta, la valore carte più basso

X: $\{1, 2, 3, \dots 9\}$ esiti possibili

p_X: $\{\frac{18}{90}, \dots, \frac{2}{90}\}$

- Memorizzare N prove, senza codifica di sorgente:

$$N \cdot \lceil \log_2 9 \rceil = N \cdot 4 \text{ bit}$$

- Codifica di sorgente: $N \cdot H(X)$
- Utilizzando una codifica sensibile: $N \cdot \bar{n}$ < Huffman, Gilbert, Moore

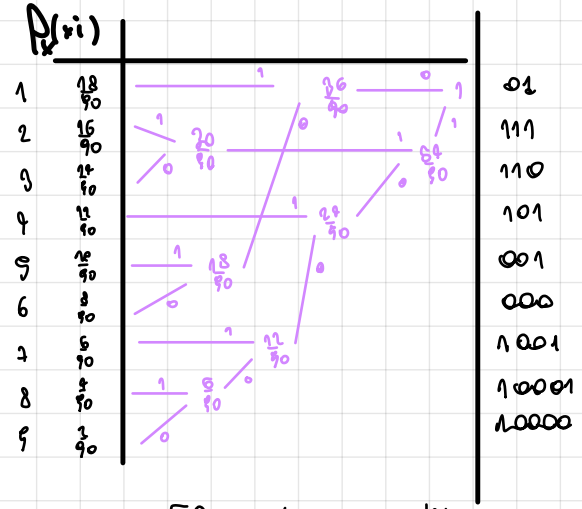
Gilbert

	$p_X(x_i)$	$n(x_i)$	$c(x_i)$
1	$\frac{18}{90}$	3	000
2	$\frac{16}{90}$	3	001
3	$\frac{14}{90}$	3	010
4	$\frac{12}{90}$	3	111
5	$\frac{10}{90}$	4	1000
6	$\frac{8}{90}$	4	1001
7	$\frac{6}{90}$	4	1010
8	$\frac{4}{90}$	5	11111
9	$\frac{2}{90}$	5	11110

$$n(x_i) = \left\lceil \log_2 \frac{1}{p_X(x_i)} \right\rceil$$

$$\bar{n} = \sum_i p_X(x_i) \cdot n(x_i) = \frac{17}{5} = 3{,}4$$

Huffman



$$\bar{n} = \sum_i p_X(x_i) \cdot n(x_i) = 2{,}96 \text{ bit}$$

Esame 8/11/2018

$X = \{a, b, c, d\}$ X: estrazione carte

	1	2	3	4	5	6	7	8	9	10	
a	0	1	0	1	0	0	0	1	0	1	$\frac{4}{10}$
b	0	0	1	0	0	0	0	0	1	0	$\frac{2}{10}$
c	0	0	0	0	0	1	0	0	0	0	$\frac{1}{10}$
d	1	0	0	0	1	0	1	0	0	0	$\frac{3}{10}$

$\Sigma = 1$

$p_X(x) = \{\frac{16}{40}, \frac{8}{40}, \frac{4}{40}, \frac{12}{40}\}$ su 40 carte

1) bit codifica senza sorgente su N prove: $N \cdot 2$ bit

2) Con codifica sorgente ideale: $N \cdot H(x)$

$$H(x) = \sum_i p_X(x_i) \cdot \log \frac{1}{p_X(x_i)} =$$

$$= \frac{16}{40} \cdot \log \frac{40}{16} + \frac{8}{40} \cdot \log \frac{40}{8} + \frac{1}{10} \log 10 + \frac{12}{40} \log \frac{40}{12} = 1{,}85 \text{ bit}$$

Shannon

$p_X(x_i)$	$h(x_i)$	$C(x_i)$
$\frac{16}{40}$	2	01
$\frac{8}{40}$	3	111
$\frac{4}{40}$	4	0000
$\frac{12}{40}$	2	10

$h(x_i) = \lceil \log_2 (\frac{1}{p_X(x_i)}) \rceil$

$\bar{n} = \frac{16}{40} \cdot 2 + \frac{8}{40} \cdot 3 + \frac{4}{40} \cdot 4 + \frac{12}{40} \cdot 2 = 2{,}67$ bit

Huffman

	$p_X(x_i)$		$C(x_i)$
$x_i = a$	$\frac{16}{40}$		0
$x_i = b$	$\frac{8}{40}$		111
$x_i = c$	$\frac{4}{40}$		110
$x_i = d$	$\frac{12}{40}$		10

$\bar{n} = \frac{16}{40} + \frac{24}{40} + \frac{12}{40} + \frac{28}{40} = 1{,}95$ bit

3) Codifica a coppie

Parola sorgente	
$p(a,a)$	
$p(a,b)$	
$p(a,c)$	
$p(a,d)$	

Esame 8/9/2022

β^0	β^1	β^2	β^3	β^4	β^5	β^6
1	3	2	6	4	5	1

$RS(6,4)$ in $GF(7) = \{0,1,2,3,4,5,6\}$

$t = 2$ • Scelte α^N: $\alpha^N = \alpha^6 = 1$

$N = 6$

$\beta^3 = 1 \rightarrow$ NO

$\beta^6 = 1 \rightarrow$ SÍ $\quad \alpha = 3$

• Quante sequenze contiene $\mathcal{C}$ e d ?

$t = 2 \rightarrow d = 2t + 1 = 5 \rightarrow d-1$ radici consecutive

$N - k = d - 1 \Rightarrow k = 6 - 4 = 2$

sequenze scelte $c \in \mathcal{C}$: $7^2 = 49$ con $c_i, c_j \in GF(7)$

• Assumendo $j_0 = 1$ determinare $g(x)$:

$j_0 = 1 \Rightarrow C_1 = 0$ dunque altri sette $d-2$ successive nulle

$\alpha^0 = \beta^0 = C_1 = 0$
$\alpha^1 = \beta^1 = C_3 = 0$
$\alpha^2 = \beta^2 = C_2 = 0$
$\alpha^3 = \beta^3 = C_6 = 0$
$\alpha^4 = \beta^4 = C_4 = 0$

$$g(x) = (x-\alpha^0)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$$

• Quali sequenze appartengono a $\mathcal{C}$:

$v_1(x) = 1 + x$ $\quad v_1(x)$ è resto di $g(x) \Rightarrow$ NO.

$v_2(x) = 0$ $\quad v_2(x)$ è divisibile $g(x) \Rightarrow$ SÍ

$$v_3(x) = 6 + 6x + 6x^2 + 6x^3 + 6x^4 + 6x^5$$

$v_3(1) \neq 0 \Rightarrow v_3(x)$ non è una sequenza di codice

$6 \cdot 5 \bmod 7 \neq 0$

$v_4(x) = 1 + 1x^2 + 1x^4 \rightarrow$ non $\in \mathcal{C}$ distanza di Hamming del codice è $d_H = w_H = 3$

• Polinomio locatore $\Lambda(x)$

$v_{num} = t = 2 \qquad \Lambda(x) = \prod_{h=1}^{J} (1 - \alpha^{j_h} x) = \Lambda_0 + \Lambda_1 x + \Lambda_2 x^2 = 1 + \Lambda_1 x + \Lambda_2 x^2$

$$S_0 = v_{0+j_0} = v_1 = \sum_{h=0}^{N-1} v_h \cdot \alpha^{j \cdot h} = 2 + 2\alpha = 2 + 6 = 8 = 1$$
$$S_1 = v_2 = = 2 + 2\alpha^2 = 2 + 4 = 6$$
$$S_2 = v_3 = = 2 + 2\alpha^3 = 2 + 12 = 14 = 0$$
$$S_3 = v_4 = = 2 + 2\alpha^4 = 2 + 8 = 10 = 3$$
$$S_5 = v_5 = = 2 + 2\alpha^5$$

$J \leq h \leq d-2$ con $d - J - 1 = 2$

$2 \leq h \leq 3$

key equation $\quad \sum_{h=1}^{J} \Lambda_h \cdot S_{n-h} = -S_n$

$$\begin{cases} \Lambda_1 \cdot S_1 + \Lambda_2 \cdot S_0 = -S_2 \\ \Lambda_1 \cdot S_2 + \Lambda_2 \cdot S_1 = -S_3 \end{cases} \rightarrow \Lambda_1 = \frac{-\Lambda_2 S_0 - S_2}{S_1} = \frac{-2}{6} = \frac{5}{6}$$

$\Lambda_2 = 2$

$$\left(\frac{-\Lambda_2 S_0 - S_2}{S_1}\right) \cdot S_2 + \Lambda_2 S_1 = -S_3$$

$$-\Lambda_2 S_0 S_2 - S_2^2 + \Lambda_2 S_1^2 = -S_3$$

$$\Lambda_2 (S_1^2 - S_0 S_2) = S_2^2 - S_3 \qquad \frac{1}{\Lambda_2} = \frac{S_1^2 - S_0 S_2}{S_2^2 - S_3} = \frac{0 - 3}{1 - 6} = \frac{-3}{-5} = \frac{4}{2} = 2$$

Esame 10/11/2022

dato una soglia $\bar{x}$:

se $x_u = x_u \leq \bar{x}$ $\quad c = 0\, c_1 \dots c_m$ $\quad p_x(x_i \leq \bar{x}) = p$

se $x_u = x_u > \bar{x}$ $\quad c = 1\, c_1 \dots c_h$ $\quad p_x(x_i > \bar{x}) = 1-p$

$$\bar{n}_c = p\cdot(m+1) + (1-p)(h+1)$$

$$H(x) = \sum_i p_x(x_i)\cdot \log \frac{1}{p_x(x_i)} = 2{,}94 \text{ bit}$$

$$\bar{n}_c \geq H(x) \Rightarrow \bar{n}_c = H(x)$$

$$p(m+1) + (1-p)(h+1) = 2{,}94$$
$$pm + p + h + 1 - p - p = 2{,}94$$
$$p(m-h) = 1{,}94$$
$$p = \frac{1{,}94}{m-h}$$

- Senza codifica di sorgente : $\bar{n}_c = \log_2 6 = 2{,}58$
- Codifica sorgente :

Huffman : $\bar{n}_c = 2{,}94$

Huffman : $\bar{n}_c = 2{,}86$ bit

x_i	$p_x(x_i)$	$h(x_i)$	$c(x_i)$
1	$\frac{1}{32}$	2	
2	$\frac{2}{32}$	3	
3	$\frac{6}{32}$	3	
4	$\frac{6}{32}$	3	
5	$\frac{8}{32}$	4	
6	$\frac{1}{32}$	4	

x_i	$p_x(x_i)$	$c(x_i)$
1	$\frac{1}{32}$	10
2	$\frac{2}{32}$	01
3	$\frac{6}{32}$	00
4	$\frac{6}{32}$	111
5	$\frac{8}{32}$	110
6	$\frac{1}{32}$	1100

Maggior efficienza possibile : codice deve generare 0 e 1 in maniera equiprobabile

$p_x(x_i \leq \bar{x}) = \frac{1}{2}$ genero uno 0

$p_x(x_i > \bar{x}) = \frac{1}{2}$ genero uno 1

con un valore di soglia $\bar{x} = \frac{9}{32}$ divido l'alfabeto in 2 parti equivalenti che mi generano 0 e 1 equiprobabili.

$$\bar{n}_c = \frac{1}{2}(m+1) + \frac{1}{2}(h+1)$$
$$= \frac{1}{2}m + \frac{1}{2}h + 2 \qquad m, h \geq 0$$

Esame 11/11/2021

$X = \{+1, -1\}$

$N \perp X \rightarrow Y = X + N$

1) $E[n] = \int_{-\infty}^{+\infty} n \cdot p_N(n)\, dn = \int_{-2}^{0} \frac{1}{3} n\, dn + \int_{0}^{2} \frac{1}{6} n\, dn$

$= \frac{1}{3}\left[\frac{n^2}{2}\right]_{-2}^{0} + \frac{1}{6}\left[\frac{n^2}{2}\right]_{0}^{2}$

$= \frac{1}{3}(-2) + \frac{1}{6}(2)$

$= -\frac{2}{3} + \frac{1}{3} = -\frac{1}{3}$

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

$= H(Y) - H(N)$

$p_{Y|X}(y|x) = p_{Y|X}(y-x|x) = p_N(y-x) = p_N(n)$

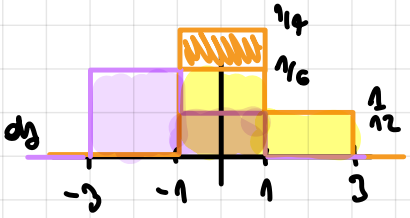
$p_Y(y) = \sum_i p_{Y|X}(y|x_i) \cdot p_X(x_i) = \sum_i p_N(y-x_i) \cdot p_X(x_i)$

$= \frac{1}{2} p_N(y+1) + \frac{1}{2} p_N(y-1)$

$H(Y) = \int p_Y(y) \cdot \log \frac{1}{p_Y(y)}\, dy$

$= \int_{-3}^{-1} \frac{1}{6} \cdot \log 6\, dy + \int_{-1}^{1} \frac{1}{4} \log 4\, dy + \int_{1}^{3} \frac{1}{12} \log 12\, dy$

$= \frac{2}{6}\log 6 + 1 + \frac{1}{6}\log 12$



$H(N) = \int_{-\infty}^{+\infty} p_N(n) \cdot \log \frac{1}{p_N(n)}\, dn = \int_{-2}^{0} \frac{1}{3} \log 3\, dn + \int_{0}^{2} \frac{1}{6} \log 6\, dn$

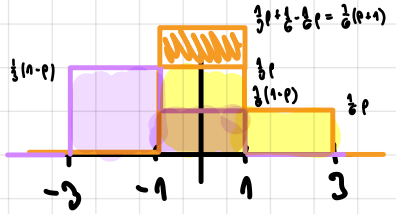
$= \frac{2}{3}\log 3 + \frac{1}{3}\log 6$

$I(X;Y) = H(Y) - H(N) = \frac{2}{6}\log 6 + 1 + \frac{1}{6}\log 12 - \frac{2}{3}\log 3 + \frac{1}{3}\log 6$

$= \log 6 + 1 + \frac{1}{6}\log 12 - \frac{2}{3}\log 3$

con $p_X(x_i) = \{p, 1-p\}$

$p_Y(y) = (1-p)p_N(y+1) + p\, p_N(y-1)$



$H(Y) = \int_{-3}^{-1} \frac{1}{3}(1-p) \cdot \log \frac{3}{(1-p)}\, dy + \int_{-1}^{1} \frac{1}{6}(p+1) \cdot \log \frac{6}{p+1}\, dy + \int_{1}^{3} \frac{1}{6} p \log \frac{6}{p}\, dy$

$= \frac{2}{3}(1-p)\log \frac{3}{1-p} + \frac{1}{3}(p+1)\log \frac{6}{p+1} + \frac{1}{3} p \log \frac{6}{p}$

$= -\frac{2}{3}(1-p)\log \frac{1}{1-p} + \frac{2}{3}(1-p)\log 3$

$+ \frac{1}{3}(p+1)\log 6 - \frac{1}{3}(p+1)\log \frac{1}{p+1} + \frac{1}{3} p \log 6 - \frac{1}{3}\log \frac{1}{p}$

$= \frac{1}{3} H_2(p) + \frac{2}{3} p \log 6 + \log 6 - \frac{2}{3}(1-p)\log(1-p)\frac{1}{1-p} + \frac{2}{3}(1-p)\log 3$

$I(X;Y) = H(Y) - H(N)$

$= -\frac{1}{3} H_2(p) + \frac{2}{3} p \log 6 + \log 6 - \frac{2}{3}(1-p)\log(1-p)$

Esame 13/12/2020

$$s_2(t) = \begin{cases} A\frac{2t}{T} & -\frac{T}{2} \le t \le 0 \\ A - \frac{2t}{T} & 0 \le t \le \frac{T}{2} \end{cases}$$

$$E_1 = \int s_1(t)^2 dt = \int_{-T/2}^{T/2} A^2 dt = A^2 T = 3E$$

$$E_2 = \int s_2(t)^2 dt = \int_{-T/2}^{0} \left(\frac{A2t}{T}\right)^2 dt + \int_{0}^{T/2} \left(-\frac{A2t}{T}\right)^2 dt$$

$$= \frac{A^2 4}{T^2}\left(\frac{t^3}{3}\right)_{-T/2}^{0} + \frac{A^2 4}{T^2}\left(\frac{t^3}{3}\right)_{0}^{T/2}$$

$$= \frac{A^2 4}{T^2}\left(\frac{T^3}{24} + \frac{T^3}{24}\right) = \frac{4A^2}{T^2}\cdot\frac{2T^3}{24\cdot 2} = \frac{A^2 T}{3} = E$$

$$E_b = \frac{E + 3E}{2} = 2E$$

Rappresentazione geometrica G.S.:

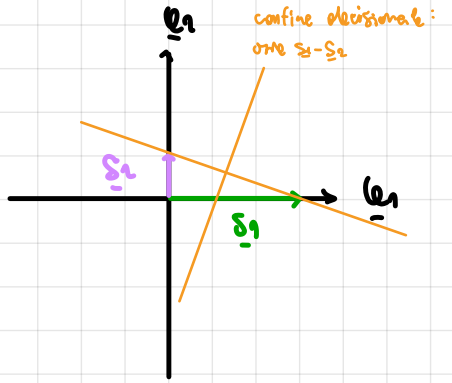
$$\varphi_1(t) = \frac{s_1(t)}{\sqrt{E_1}} \qquad \underline{s}_1 = (\sqrt{E_1}, 0, \dots)$$

$$s_{21} = \int s_2(t)\cdot\varphi_1(t)\,dt = \int_{-T/2}^{0} \frac{A2t}{T}\cdot A\,dt + \int_{0}^{T/2} -\frac{A2t}{T}\cdot A\,dt$$

$$= \frac{2A^2}{T}\left[\frac{t^2}{2}\right]_{-T/2}^{0} + -\frac{2A^2}{T}\left[\frac{t^2}{2}\right]_{0}^{T/2} = 0$$

$s_{21} \perp \varphi_1(t) \rightarrow \varphi_2(t) = \frac{s_2(t)}{\sqrt{E_2}} \qquad \underline{s}_2 = (0, \sqrt{E_2}, \dots)$

sono forme d'onda ortogonali, servirebbero 2 dimensioni oppure φ_1 e φ_2



$$d = \sqrt{E + 9E} = \sqrt{10E}$$

$$P(n_1 > \tfrac{d}{2}) = P_{el} = Q\left(\frac{\frac{d}{2}}{\sqrt{\frac{N_0}{2}}}\right) = Q\left(\frac{d}{\sqrt{2N_0}}\right) = Q\left(\frac{\sqrt{10E}}{\sqrt{2N_0}}\right) =$$

2-PAM: $Q\left(\frac{\sqrt{2\mathcal{E}_b}}{\sqrt{N_0}}\right)$ $\qquad = Q\left(\frac{\sqrt{5E}}{\sqrt{N_0}}\right)$

perdo di $\frac{5}{2}$ rispetto a 2-PAM ovvio $-4\,dB$ $\qquad E = \frac{E_b}{2}$ $\qquad = Q\left(\frac{\sqrt{5E_b}}{\sqrt{2N_0}}\right)$

Brune

9/9/2021

$L = 4$ {A,B,C,D} alfabeto

$\underline{x}_T = (x_1, \dots, x_N) : \forall x_i \in L$ — sequenze codificate

$\underline{x}_T = AABCD$ $(N=5)$ → ne lecite 101

$C = (\underline{c}_1, \dots, \underline{c}_M)$ — Codice: rilevatore → r; correttore → t; sistematico; lineare: $\underline{G}$, $\underline{H}$; ciclico: $(x^N + 1) \bmod g(x) = 0$

$\forall \underline{c} \in C \Rightarrow \underline{c} = (\underline{i} \; \underline{r})$ — $1 \times N$, $1 \times K$, $1 \times (N-K)$

$I(x;y) \to C$

ε: prob. errore

$H(x|y)$ equivocazione

Linearità K=3 — una sequenza $\underline{c}_i = 101$ • BSC, BEC, AGN

TX — sorgente X — $I(x_i)$, $H(x)$ → CANALE → 101, rx = $(y_1, \dots, y_N)$ — Rx sorgente Y

La sequenza viene 101 decodificata in: ⟹ $\underline{c}$ lineare lecito se: $\underline{c} \cdot \underline{H} = \underline{w} = \underline{0}$

viene soggetta a ε

Codificatore: codifica una sequenza $x \to 101$

Decodificatore sceglie qua

il decodificatore è integrato nel ricevitore che ha il compito di verificare e se necessario correggere la sequenza ricevuta durante la trasmissione

N lunghezza sequenza
k bit di info nel canale
R rate $= \frac{K}{N}$
M combinazioni lecite $= 2^k$

$2^N \geq 2^k$
$N \log L \geq k$

• Ridondanza
• errore nel singolo bit

Codice Lineare:

$\forall C \to \underline{G}$ matrice di generazione: $\underline{c} = \underline{i} \cdot \underline{G}$

$\underline{c}$ lecito se: $\underline{c} \cdot \underline{H} = \underline{w}$ dove $\underline{w} = \underline{0}$ $\quad 1 \times (N-K)$

Codice lineare sistematico:

$\underline{G} = [\underline{I} \;\; \underline{P}]$ — $K \times N$, $K \times K$, $K \times (N-K)$

$\underline{H} = \begin{bmatrix} P \\ I \end{bmatrix}$ — $N \times (N-K)$; $K \times (N-K)$; $(N-K) \times (N-K)$

Notazione esponenziale

$\underline{c} = (c_0, \dots, c_{N-1})$ lungo N

$c(x) = c_{N-1} x^{N-1} + \dots + c_0$ $\quad (N-1)$ grado

$i(x) = i_{K-1} x^{K-1} + \dots + i_0$ $\quad (K-1)$

Polinomio generatore del codice C $g(x)$: $\forall \underline{c} \in C \Rightarrow c(x) \bmod g(x) = 0$; $g(x)$ ha grado $(N-K)$

codice lecito: $c(x) = i(x) \cdot g(x)$

codice sistematico: $c(x) = x^{N-K} \cdot i(x) - \text{resto}\left[\frac{x^{N-K} \cdot i(x)}{g(x)}\right]$ — bit di info; bit di parità

Secondo Shannon: $I(x_i) = \log\left(\frac{1}{P_x(x_i)}\right)$

$\sum_i P_x(x_i) \cdot n(x_i) = \bar{n} \geq H(x)$ 1° Teorema di Shannon: (limite di Shannon)

Teorema della codifica di canale:

$E_x[P_{e,M}(x)] \leq 2^{NR} \cdot 2^{-E_0(\rho) \cdot N}$ $\quad \rho \in (0,1)$
$= 2^{-N(E_0(\rho) - R\rho)}$
$= 2^{-N E(R)}$

• $E_x[P_{e,M}(x)] \downarrow$ $N \uparrow$ se $E(R) > 0$
• $R \uparrow$ $E(R) \downarrow$ $\rho \downarrow$ $E_0(\rho) \downarrow$ $E_x[P_{e,M}(x)] \uparrow$

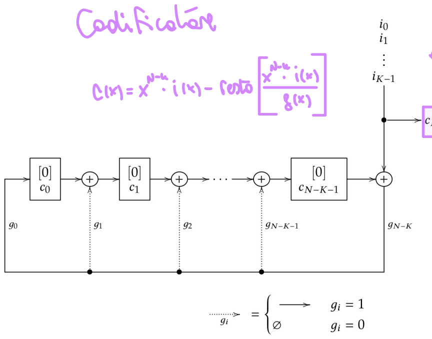
$\max_{P_X} \lim_{\rho \to 0} \frac{E_0(\rho)}{\rho} = \max_{P_X} I(x;y) = C$

→ se $R > C$ $\uparrow N$ $E_x[P_{e,M}(x)]$ invariato
→ se $R \leq C$ $\uparrow N$ $E_x[P_{e,M}(x)] \downarrow$

Codificatore

$c(x) = x^{N-K} \cdot i(x) - \text{resto}\left[\frac{x^{N-K} \cdot i(x)}{g(x)}\right]$

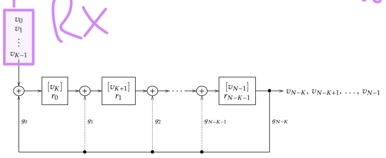
lunghezza iniziale N
k bit di info



Tx → canale → Rx

Decodificatore:

se $\frac{v(x)}{g(x)} = 0 \Rightarrow v(x)$ lecito, $v(x) \in C$



|| lunghezza N

$h(x_i) = k$ bit di informazione → codifica sorgente
$h(x_i) = N > k + (N-k)$ → codifica di canale

Campi finiti di Galois

proprietà	Galois	
ciclico	∃ generatore α^k	

$E_j = \sum_{h=0}^{N-1} e_h \cdot \beta^{jh}$

$\underline{e} = (e_0 \dots e_{N-1}) \longrightarrow \underline{E} = (E_0, \dots, E_{N-1})$

$\underline{e} = (0 \dots 1 \dots 1 \dots 0)$ — $\sum_{h=1}^{d-1} e_h = \sum_{h=1}^{v} e_{E_h}$

Dato un codice di Hamming: $d \to d-1$ elementi nulli consecutivi in $\underline{E}$

$e(x) = e_{N-1} x^{N-1} + \dots + e_0$

$e(\beta^j) = 0 \Rightarrow E_j = 0$ ⟹ l'errore viene rilevato proprio in posizione β^j ⟹ $\sum_{h=1}^{N-1} e_h \cdot \beta^{xh}$

$g(x) = \prod_{j \in L} (x - \beta^j)$ + polinomio minimo $\forall \beta^j$

$\underline{E} = (E_0, \dots, E_x, \dots, E_{N-1})$

$\sum_{h=1}^{N-1} e_h \cdot \beta^{0 \cdot h}$ $\quad$ $\sum_{i=1}^{N-1} e_h \cdot \beta^{(N-1)h}$

Se ho un errore in posizione e_6 ↓ ottengo il termine β^6 apparirà nella sindrome ⇓ posso dunque correggere e_6 con l'info di S

Incognite: β^{E_1} $\quad \beta^{E_v}$

$\underline{e} = (e_0, \dots, e_1, \dots, e_{N-1})$

incognite: e_{E_1} $\quad e_{E_v}$

- utilizzo semplicemente Ei perché nel punto deve fare Vi perché Ci = 0
- in questo modo posso calcolare tutte le posizioni dei miei errori
- dunque utilizzo i vari Ei = Vi per determinare le equazioni da cui determino le posizioni
- per risolvere v incognite ⇒ v equazioni indipendenti

$e_6 = \alpha^2$ → posizione β^6 → valore $= \alpha^2$

$g(x) = (x - \alpha_1)(x - \alpha_2)$

$V_1 = E_1 + C_1 = E_1$ $\quad$ Sindrome $S_0 = 1$

eq I) $E_1 = \sum_{h=1} e_{E_h} \cdot \beta^{1 \cdot E_h}$ → S_0

$V_2 = E_2 + C_2 = E_2$

eq II) $E_2 = \sum_{h=1} e_{E_h} \cdot \beta^{2 \cdot E_h}$ → S_1

$\Lambda(x) = \prod_{h=1} (1 - \beta^{E_h} x) = \Lambda_0 + \dots + \Lambda_v x^v$

key equation: $\sum_{h=1} \Lambda_h \cdot S_{k-h} = -S_k$

equazioni $= d - 1 - 1$ $\quad$ $v \leq k \leq d_2$

SORGENTI SENZA MEMORIA

$I(x=x_i) = \log \frac{1}{p_x(x_i)}$ $\quad \downarrow p_x(x_i) \geq 0 \quad \uparrow I(x_i) \geq 0$ (bit/mat)

$H(X) = \sum_i p_x(x_i) \cdot I(x_i) = \sum_i p_x(x_i) \cdot \log \frac{1}{p_x(x_i)} = E_x(I(x_i)) \geq 0$ (bit)

$H_2(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p}$ (bit)

$p = \frac{1}{2} \Rightarrow H_2(p) = 1$

$p = 0,1 \Rightarrow H_2(p) = 0$

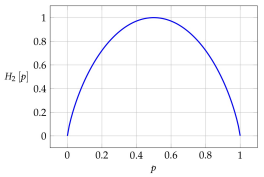


Figura 2.1.: Funzione $H_2(p)$.

$H(x)$ max con d di X uniforme $\Rightarrow$ incertezza massima

dato $X \Rightarrow p_x(x_i) = \frac{1}{M}$

$H(x) = \log_2 M$

$\uparrow$

$0 \leq H(x) \leq \log_2 M$

$\ln x \leq (x-1)$

$\log_2 x \leq (x-1) \log_2 e$

CODIFICA SORGENTI SENZA MEMORIA

$X = \{x_1, \dots, x_M\}$ $\quad$ dove $C(x_i)$ è lunga $n(x_i)$ bit $\quad \Rightarrow$

$Y = (C(x_1), \dots, C(x_M))$ M-upla $\quad$ $C(x_i)$ sequenza di bit

Notazione: $\underline{x}' = (x', x'', \dots)$ dove $x \in X$ ossia una sequenza di X

codice univocamente decodificabile (LOSSLESS) : $C(\underline{x}') \neq C(\underline{x}'')$ con $\underline{x}' \neq \underline{x}''$

codice istantaneamente decodificabile

ragionamento per assurdo

$p_x(0) = p_x(1) = 1/2 \Rightarrow H(x) = 1$ bit

assegno 1 bit a 2 eventi equiprobabili

$\overline{n_c} \rightsquigarrow H(x)$

max info per simbolo bit

stesso modo, C:

- $\uparrow H(x)$ $\uparrow$efficienza ma spreco
- Nella codifica $H(x)$ dipende da $p_x(x_i)$

Obiettivo: $\uparrow$efficienza $\downarrow \overline{n_c}$

1 bit contiene 1 bit di informazione utile $\Rightarrow$ codifica ma genera:

$\Rightarrow$ 0 e 1 equiprobabili

$n(x_i) =$ n bit di informazione $\rightarrow$ codifica sorgente

$l(x_i) = N > n + (N-n) \rightarrow$ codifica di canale

$$E_x(P_{em}(\varepsilon)) \leq M^\rho \cdot \left(\sum_{y \in Y} \left(\sum_{x \in X} p_x(x) \cdot p_{y|x}(y|x)^{\frac{1}{1+\rho}} \right)^{1+\rho} \right)^N$$

$M = q^{N \cdot R}$

$= q^{N \cdot R \cdot \rho} \cdot q^{-E_0(\rho) \cdot N}$

$= q^{-N(E_0(\rho) - R\rho)}$

$= q^{-N E(R)}$

$\uparrow N \Rightarrow \downarrow E_x(P_{em}(\varepsilon))$

$E(R) > 0$

$p_{tw} = \binom{N}{e} \varepsilon^e (1-\varepsilon)^{N-e}$ $\quad t+1 \gg N \cdot \varepsilon$, $N \gg t+1$, $\varepsilon \approx 0$

$= \binom{N}{e} \varepsilon^{t+1} (1-\varepsilon)^{N-t-1}$

$= \frac{N^{t+1}}{(t+1)!} \varepsilon^{t+1} (1-\varepsilon)^N \simeq \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1}$

$p_{tb} = \frac{e+1}{N} \cdot \binom{N}{e} \cdot \varepsilon^e \cdot (1-\varepsilon)^{N-e}$

$= \frac{2t+1}{N} \frac{N^{t+1}}{(t+1)!} \cdot \varepsilon^{t+1} \simeq 2 \cdot \frac{N^t}{t!} \cdot \varepsilon^{t+1}$

$\frac{N^t}{t!} \cdot \varepsilon^{t+1} \leq p_{tb} \leq 2 \cdot \frac{N^t}{t!} \cdot \varepsilon^{t+1}$

$\Omega(x)_u = \Omega(x)_{u-2} - p_u \Omega(x)_{u-1}$

$\Lambda(x)_u = \Lambda(x)_{u-2} - p_u \Lambda(x)_{u-1}$

$\Phi(x)_u = \Phi(x)_{u-2} - p_u \Phi(x)_{u-1}$

dove $p_u = \frac{\Omega(x)_{u-2}}{\Omega(x)_{u-1}}$

$g(\Omega(x)) > g(\Lambda(x))$

$H(X) \le \log_2 M$

$$H(X) = \sum_i^M P_X(x_i) \cdot \log \frac{1}{P_X(x_i)} \cdot \frac{M}{M} = \sum_i^M P_X(x_i) \log M + \sum_i^M P_X(x_i) \cdot \log \frac{1}{M \cdot \log P_X(x_i)}$$

$$= \log M + \sum_i^n P_X(x_i) \cdot \log \frac{1}{M \cdot P_X(x_i)}$$

$\ln x \le (x-1)$

$\frac{\log_2 x}{\log_2 e} \le (x-1) \Rightarrow \log_2 x \le (x-1) \log e$

$$\le \log M + \sum_i^n P_X(x_i) \cdot \log e \cdot \left(\frac{1}{M \cdot P_X(x_i)} - 1 \right)$$

$$= \log M + \log e \sum_i^M \cancel{P_X(x_i)} \cdot \frac{1}{M \cdot \cancel{P_X(x_i)}} - \sum_i^M P_X(x_i) \cdot \log e$$

$$= \log_2 M$$

fare tabelle partire sempre da $p(y)$

$$H(Y) = \sum_j p_Y(y_i) \cdot \log \frac{1}{p_Y(y_i)}$$

$$H(Y|x_i) = \sum_j p_{Y|X}(y_j|x_i) \cdot \log \frac{1}{p_{Y|X}(y_j|x_i)}$$

$$H(Y|X) = \sum_i p_X(x_i) \cdot H(Y|x_i)$$

$$p_Y(y_j) = \sum_i p_{Y,X}(y_j, x_i) = \sum_i p_{Y|X}(y_j|x_i) \cdot p_X(x_i)$$

$\Sigma(x)$

$\alpha^6 \neq p(\alpha) = 1$ spazio ne.