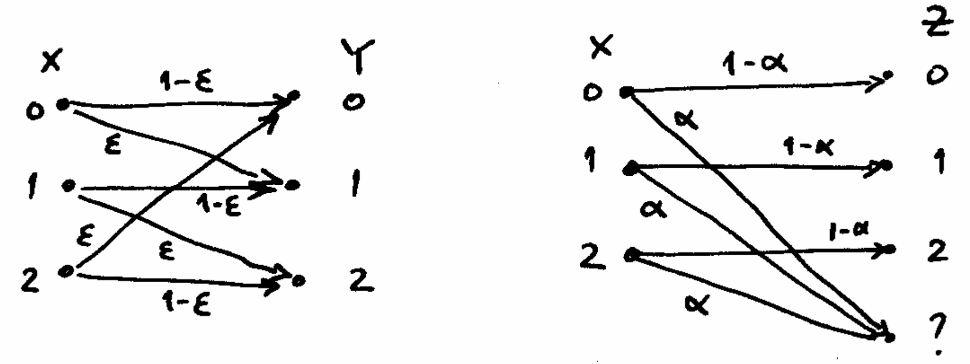
Teoria da Informação (01-02)
1ª chamada (14-6-02)

1.



a) $H(Y|X=i) = H(\varepsilon, 1-\varepsilon)$, para $i = 0, 1, 2$, então

$$H(Y|X) = \sum_{i=0}^{2} P(X=i)\, H(Y|X=i) = H(Y|X=i) = H(\varepsilon, 1-\varepsilon)$$

ou seja, $H(Y|X) = -[\varepsilon \log \varepsilon + (1-\varepsilon)\log(1-\varepsilon)]$, independentemente das probabilidades $P(X=i)$.

b) $I(X;Y) = H(Y) - H(Y|X) = H(Y) - H(\varepsilon, 1-\varepsilon)$

A capacidade obtém-se maximizando $I(X;Y)$, isto é, maximizando $H(Y)$. Como o canal é simétrico, se X for equiprovável Y também o será $\Rightarrow C = \log_2 3 - H(\varepsilon, 1-\varepsilon)$.

c) Tal como em b), $H(Z|X) = H(\alpha, 1-\alpha)$. Por outro lado, $P(Z=?) = \alpha$, independentemente de $P(X=i)$. Logo, para maximizarmos $H(Z)$ queremos que $P(Z=i)$, $i=0,1,2$, sejam iguais e, para isso, X deve ser equiprovável.

$\Rightarrow P(Z=0) = P(Z=1) = P(Z=2) = \frac{1}{3}(1-\alpha)$

$\Rightarrow H(Z)_{max} = -\left[(1-\alpha)\log\left[\frac{1}{3}(1-\alpha)\right] + \alpha\log\alpha\right] = (1+\alpha)\log 3 + H(\alpha, 1-\alpha)$

$\Rightarrow C = \max I(X;Z) = (1+\alpha)\log 3 + H(\alpha, 1-\alpha) - H(\alpha, 1-\alpha) = (1-\alpha)\log 3$.

2. a) $(7,2)$, $d_{min} = 5$: Não, porque não respeita o limite de Plotkin

$$d_{min} \leq \frac{n \cdot 2^{k-1}}{2^k - 1} = \frac{7 \times 2}{3} = \frac{14}{3}$$

2b) $(63,31)$, $t=17$: Não, porque não respeita os limites de Plotkin, Singleton e Hamming

$$d_{min} \geq 2t+1 \Rightarrow d_{min} \geq 35$$

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i} \Rightarrow t \leq 7$$

Mas $d_{min} \leq \dfrac{n \cdot 2^{k-1}}{2^k-1} = 31,5$

ou ainda $d_{min} \leq n-k+1 = 33$.

2c) $(63,45)$, $d_{min}=7$. Sim, existe (respeita os diversos limites:

$$d_{min} \leq \frac{n \cdot 2^{k-1}}{2^k-1} = 31,5$$

$$d_{min} \leq n-k+1 = 19$$

Hamming: $t \leq 3$

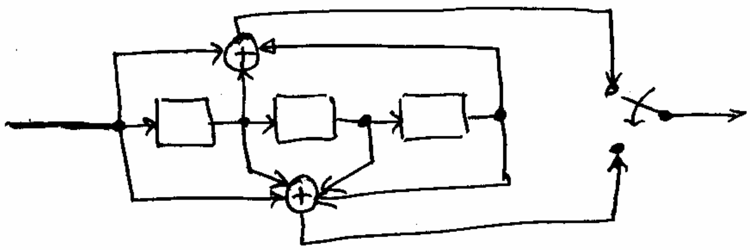
$$d_{min} \geq 2t+1$$)

Aliás existe um código BCH com estes parâmetros

Não usado [2d) $(127,109)$, $d_{min}=7$: Não, porque falha o lim. Hamming:

$$2^{18} \geq \sum_{i=0}^{t} \binom{127}{i} \Rightarrow t \leq 2$$ (com $d_{min}=7$ seria $t=3$)

3- a)



b) $N=4$

c) 8 estados

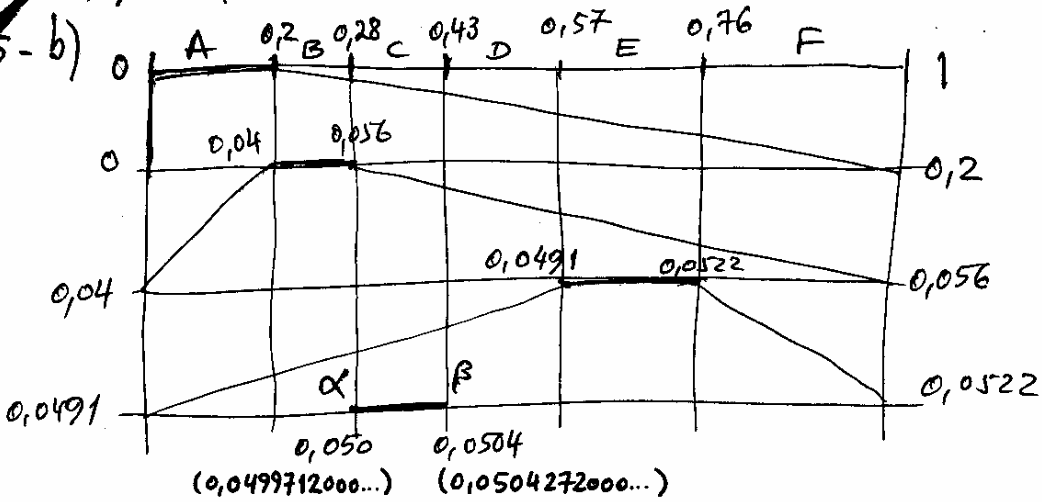
d) $g_1(D) = 1+D+D^3$

$g_2(D) = 1+D+D^2+D^3$

4.- Noutra página.

~~5a)~~ Entropia: $H = 2{,}5129$ bits/símbolo.

~~5~~ - b)



Sequência codificada: ABEC

Intervalo final: $[0{,}0500\ ;0{,}0504[$ ⟹ Qualquer valor deste intervalo serve.

c) Largura do intervalo: $L = 0{,}0004$

$$t = \lceil -\log_2 L \rceil = 12$$

$$\alpha \leq \frac{\ell}{2^t} < \beta \implies 204{,}7 \leq \ell < 206{,}5 \implies \ell = \begin{cases} 205 \\ 206 \end{cases}$$

Toma-se o valor par

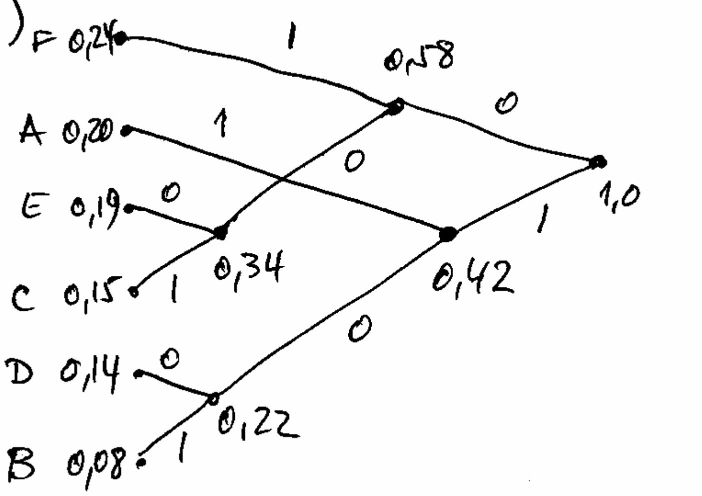
Fracção diádica c/ o menor denominador no intervalo $[\alpha\ ;\beta[$:

$$\frac{\ell}{2^t} = \frac{206}{2^{12}} = \frac{103}{2^{11}} \rightarrow (.00001100111)$$

A palavra binária mais curta tem 11 bits e é

00001100111

d)



F – 01
A – 11
E – 000 ⟹
C – 001
D – 100
B – 101

ABEC
↓
11101000001

(11 bits também)

6. $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ $(6,3)$

a) $X = [101100] \longrightarrow$ São duas mensagens de 3 bits

$\Rightarrow Y = 101100 \,.\, 100111$

b) De G vemos que $d_{min} \leq 3$. Vendo que não há nem linhas nulas nem iguais em H concluímos que $d_{min} = 3$.

c) A partir de G obtêm-se as restantes palavras de código, sendo $A_0 = 1$, $A_3 = 4$, $A_4 = 3$ e os restantes A_i nulos.

$$P_{end} = \sum_{i=d_{min}}^{6} A_i p^i (1-p)^{n-i} = A_3 p^3 (1-p)^3 + A_4 p^4 (1-p)^2 =$$

$$= 3{,}999 \cdot 10^{-12} = 4 \cdot 10^{-12}$$

d) O encurtamento no 2.º bit elimina a 2.ª linha e a 2.ª coluna de G:

$$G' = \begin{bmatrix} 1 & \cancel{0} & 0 & 1 & 1 & 1 \\ \cancel{0} & \cancel{1} & \cancel{0} & \cancel{1} & \cancel{1} & \cancel{0} \\ 0 & \cancel{0} & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Passamos a ter um código (5,2) cujas palavras de código são

00 000
10 111
01 011
11 100

7- $H(7,4)$, $g(p) = p^3+p+1$

a) $X(p) = p^3+1 \Longrightarrow p^3X(p) = p^6+p^3$

$(p^6+p^3) \bmod (p^3+p+1) = p^2+p = C(p)$

$\Longrightarrow Y(p) = p^3X(p)+C(p) = p^6+p^3+p^2+p \Longrightarrow$ ~~1001001~~ 1001110

b) linha i de P: $p^{n-i} \bmod g(p)$

$$\Longrightarrow P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \Longrightarrow H = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Substituindo o primeiro bit apagado por u e o segundo por y ficamos com $[0\ u\ 1\ y\ 0\ 0\ 1] = R$. Se a palavra não contém erros então $RH = 0$. Ficamos c/ um sistema de 3 equações a 2 incógnitas:

$$\begin{cases} u+1 = 0 \\ u+1+y = 0 \\ u+y+1 = 0 \end{cases} \Longrightarrow \begin{cases} u = 1 \\ y = 0 \end{cases}$$

Os quatro bits enviados terão sido $[0\ 1\ 1\ 0]$.

4.

(6)

$$C_s = \frac{1}{2}\log\left(1+\frac{S}{N}\right) = \frac{1}{2}\log\left(1+\frac{E_b R_s}{N_0 B}\right) \quad \left(\text{bits/símb.}\right)$$

E_b - energia de c/ bit de inform.

R_s - bit rate antes da codif.

R_s/R_c — bit rate depois da codif.

Se $B \geq \frac{R_s/R_c}{2}$ (para evitar ISI)

$$\Rightarrow C_s \leq \frac{1}{2}\log\left(1+\frac{E_b}{N_0}\cdot\frac{R_s}{R_s/2R_c}\right) = \frac{1}{2}\log\left(1+2R_c\frac{E_b}{N_0}\right)$$

Ora terá de ser $R_c < C_s \leq \frac{1}{2}\log\left(1+2R_c\frac{E_b}{N_0}\right)$

$$\Rightarrow \frac{E_b}{N_0} \geq \frac{2^{2R_c}-1}{2R_c}$$

Se $R_c = \frac{1}{2} \Rightarrow \frac{E_b}{N_0} \geq 1 \quad (0\ dB)$