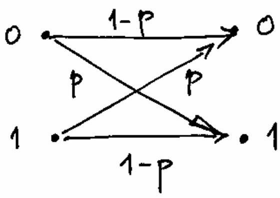
Teoria da Informação (2000-2001) Exame de Recurso (24-7-2001)

Resolução

1.



a) Nenhum erro em 15 bits: $P(0,n) = \binom{n}{0} p^0 (1-p)^n = (1-p)^n$

Deverá ser $P(0,n) \geq 0{,}95$, isto é, $(1-p)^n \geq 0{,}95$, ou

$$1-p \geq 0{,}95^{1/15} \Longrightarrow p \leq 1-0{,}95^{1/15} = 0{,}0034$$

b) Agora deverá ser $P(0,n)+P(1,n) \geq 0{,}95$

$$\Rightarrow (1-p)^n + \binom{n}{1} p (1-p)^{n-1} = (1-p)^n + np(1-p)^{n-1} \geq 0{,}95$$

$$\Rightarrow (1-p)^{15} + 15p(1-p)^{14} \geq 0{,}95$$

ou ainda $(1-p)^{14}(1+14p) \geq 0{,}95$

O valor máximo de p pode ser determinado sabendo que $(1-p)^{14} \approx 1-14p$ (se $p \ll 1$):

$$\Rightarrow (1-14p)(1+14p) = 1-(14p)^2 = 1-256p^2 \geq 0{,}95$$

$$p^2 \leq \frac{1-0{,}95}{256} \Longrightarrow p \leq \frac{\sqrt{5}}{110} = 0{,}0203$$

Confirmação: alínea a) $P(0,15) = (1-0{,}0034)^{15} = 0{,}95$ ✓

alínea b) $P(0,15)+P(1,15) = (1-0{,}0203)^{15} + 15 \times 0{,}0203 \times (1-0{,}0203)^{14} = 0{,}9636$ ✓

2. A : 0
B : 01
C : 011
D : 111

$\Rightarrow$ O código não satisfaz a condição de prefixação pois a palavra binária correspondente a A ("0") é prefixo das palavras correspondentes a B e C (e a palavra de B é prefixo da palavra de C).

Embora possa não parecer, o código é unicamente descodificável. Não o seria se houvesse um par de sequências literais diferentes (u e y, por exemplo) que fossem codificadas da mesma maneira.

Vejamos então:

- Se se receber "00" é possível que $\underline{u}$ comece por AA, AB ou AC.

- Se tivermos recebido "001111" já não temos dúvidas quanto à primeira letra (só pode ser A) mas a segunda ainda é ambígua. Mas à medida que os bits forem surgindo para descodificação esta torna-se única. (se por exemplo surgir agora um "0" é porque antes temos

$$\Big(\overset{A}{\overset{\uparrow}{0}}\ \overset{B}{\overset{\uparrow}{\overbrace{01}}}\ \overset{D\,\ldots}{\overset{\uparrow}{\overbrace{111}}}\ 0\ \ldots\Big)$$

Não é preciso usar a desigualdade de Kraft. Claro que se não for obedecida podemos logo dizer que não é unicam. descodificável. Só que aqui $\sum_i 2^{-n_i} = 1$ e não podemos concluir nada.

3. O truque é usar duas matrizes de verificação de paridade diferentes no codificador e no descodificador (mas que sejam "equivalentes" a nível das colunas). Assim, para que um só erro na posição $\underline{i}$ produza uma síndrome com a representação binária de $\underline{i}$ a matriz de verificação de paridade no descodificador tem de ser

$$H_{descod.} = \begin{array}{cl} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} & \begin{array}{l} \leftarrow 1 \\ \leftarrow 2 \\ \leftarrow 3 \\ \vdots \\ \\ \\ \leftarrow 7 \end{array} \end{array}$$

Esta matriz não tem a forma sistemática. Para que a codificação seja sistemática temos de efectuar algumas operações nas colunas de modo a obter

$$H_{codif.} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ \hdashline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Longrightarrow \begin{cases} c_1 = m_2 + m_3 + m_4 \\ c_2 = m_1 + m_3 + m_4 \\ c_3 = m_1 + m_2 + m_4 \end{cases}$$

4. Suponhamos que os polinómios de erro $e_1(p)$ e $e_2(p)$ têm ambos peso inferior a $d_{min}/2$ e a mesma síndrome $S(p)$. Então

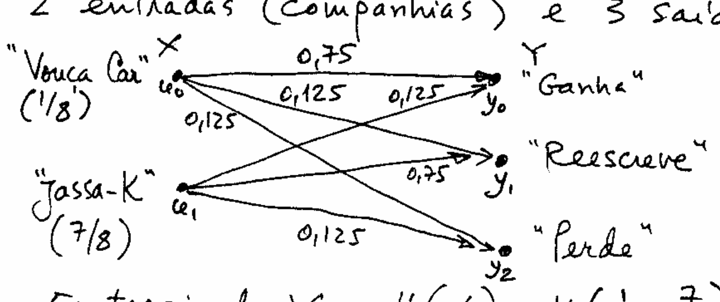
$$e_1(p) = Q_1(p)\, g(p) + S(p)$$
$$e_2(p) = Q_2(p)\, g(p) + S(p)$$

e

$$e_1(p) - e_2(p) = \left[Q_1(p) - Q_2(p)\right] g(p)$$

Como $e_1(p)$ e $e_2(p)$ têm peso inferior a $d_{min}/2$, a sua diferença, $e_1(p) - e_2(p)$, terá peso <u>inferior</u> a d_{min}. No 2.º membro temos uma palavra de código. Se não for a palavra nula o seu peso será, no mínimo, d_{min} (por definição de d_{min}). Então o 2.º membro terá de ser nulo $\Longrightarrow e_1(p) = e_2(p)$, concluindo-se que, de facto, "não há dois polinómios de erro diferentes com peso menor que $d_{min}/2$ com a mesma síndrome $S(p)$".

5- A situação é semelhante à retratada no seguinte "canal" de 2 entradas (companhias) e 3 saídas (resultados):



Probabil. (Vouça Car) $= \frac{1}{8}$

Probab. (Jassa-K) $= \frac{7}{8}$

Entropia de X: $H(X) = H\left(\frac{1}{8}, \frac{7}{8}\right) = 0{,}5436$ bits/símbolo

a) É a informação ganha sobre X, isto é, é a redução da incerteza sobre X (informação mútua).

Vamos precisar das probabilidades de y_j:

$$P(Y=\text{"Ganha"}) = \frac{3}{4}\times\frac{1}{8} + \frac{1}{8}\times\frac{7}{8} = \frac{13}{64} \qquad (P(y_0))$$

$$P(Y=\text{"Reescreve"}) = \frac{1}{8}\times\frac{1}{8} + \frac{3}{4}\times\frac{7}{8} = \frac{43}{64} \qquad (P(y_1))$$

$$P(Y=\text{"Perde"}) = \frac{1}{8}\times\frac{1}{8} + \frac{1}{8}\times\frac{7}{8} = \frac{8}{64} \qquad (P(y_2))$$

(Para simplificar vamos passar a usar y_0, y_1 e y_2, respectivam.)

a₁) $Y = y_0 = \text{"Ganha"}$: $H(X) - H(X|y_0)$ ... Generalizando:

$$H(X|y_j) = -\sum_{i=0}^{1} P(x_i|y_j)\log P(x_i|y_j) \quad \text{e}$$

$$P(x_i|y_j) = \frac{P(x_i)}{P(y_j)} \times P(y_j|x_i)$$

X só tem dois valores, x_0 e x_1 $\Rightarrow$ $H(X|y_j)$ é igual à entropia de uma fonte binária com probabilidades $P(x_0|y_j)$ e $P(x_1|y_j)$

Assim: $$P(x_0|y_0) = \frac{P(x_0)}{P(y_0)}P(y_0|x_0) = \frac{1/8}{13/64}\cdot\frac{3}{4} = \frac{6}{13}$$

$$P(x_1|y_0) = \frac{P(x_1)}{P(y_0)}P(y_0|x_1) = \frac{7/8}{13/64}\times\frac{1}{8} = \frac{7}{13}$$

O que queremos então é:

$$Y = y_0 = \text{"Ganha"} : H(X) - H(X|y_0) = H\left(\frac{1}{8}, \frac{7}{8}\right) - H\left(\frac{6}{13}, \frac{7}{13}\right) =$$

$$= 0{,}5436 - 0{,}9957 = -0{,}4522$$

a₂) Do mesmo modo, se $Y = y_1 = \text{"Reescreve"}$:

$$P(x_0|y_1) = \frac{1/8}{43/64}\cdot\frac{1}{8} = \frac{1}{43} \Rightarrow P(x_1|y_1) = \frac{42}{43}$$

$$\Rightarrow H(X) - H(X|y_1) = 0{,}5436 - \overbrace{H\left(\frac{1}{43}, \frac{42}{43}\right)}^{0{,}1594} = 0{,}3842$$

$a_3)$ $Y = y_2 =$ "Perde" : $H(X) - H(X|y_2) =$

$$= H(X) - H\left[P(x_0|y_2), P(x_1|y_2)\right]$$

$$P(x_0|y_2) = \frac{P(x_0)}{P(y_2)} \cdot P(y_2|x_0) = \frac{1/8}{8/64} \times \frac{1}{8} = \frac{1}{8}$$

Portanto: $H(X) - H(X|y_2) = 0{,}5436 - \overbrace{H\left(\frac{1}{8}, \frac{7}{8}\right)}^{0{,}5436} = 0$

b) Agora pretende-se a informação mútua média, $I(X;Y)$:

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

Como já dispomos de todas as probabilidades $P(x_i|y_j)$ podemos usar a 1ª igualdade (na maior parte dos casos usaríamos a 2ª igualdade):

$$H(X|Y) = \sum_{j=0}^{2} P(y_j) H(X|y_j) = P(y_0)H(X|y_0) + P(y_1)H(X|y_1) +$$

$$+ P(y_2)H(X|y_2) = \frac{13}{64} \times 0{,}9957 + \frac{43}{64} \times 0{,}1594 + \frac{8}{64} \times 0{,}5436 =$$

$$= 0{,}3773$$

$$\Rightarrow I(X;Y) = H(X) - H(X|Y) = 0{,}5436 - 0{,}3773 = 0{,}1663 \text{ bits/simb.}$$

(Se usássemos a 2ª igualdade seria:

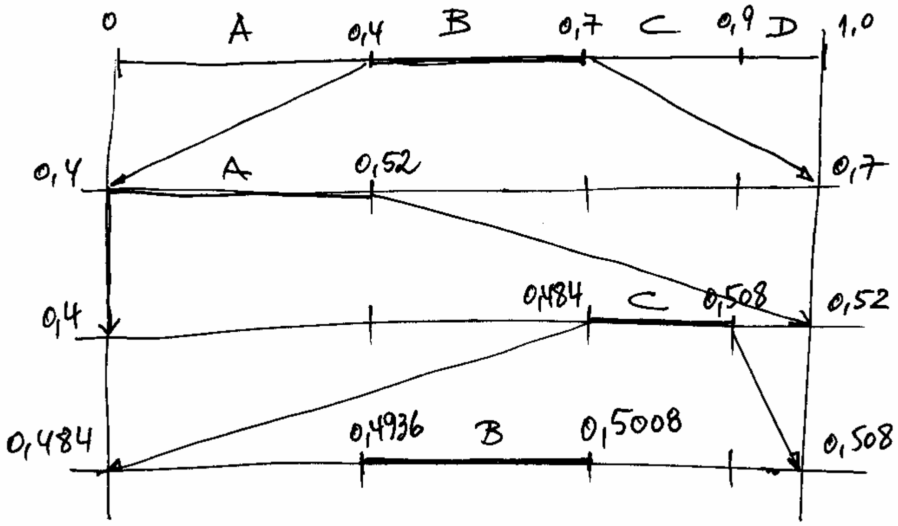
$$I(X;Y) = H(Y) - H(Y|X) = H(Y) - \sum_{i=0}^{1} P(x_i) H(Y|x_i)$$

$$= H\left(\frac{13}{64}, \frac{43}{64}, \frac{8}{64}\right) - \left[P(x_0) H(0{,}75; 0{,}125; 0{,}125) + P(x_1) H(0{,}75; 0{,}125; 0{,}125)\right]$$

$$= 1{,}2276 - 1{,}0613 = 0{,}1663 \text{ bits/simb.}$$

(como antes))

6.



a) O intervalo final é $[0{,}4936\,;\,0{,}5008[$

b) O nº real $0{,}5 = \frac{1}{2}$ pertence ao intervalo final. Logo, a sequência BACB pode ser representada pelo nº real 0,5, que corresponde ao bit "1"

($0{,}5 = \frac{1}{2^1} \Rightarrow 0{,}1$. Retirando o zero e a vírgula fica apenas "1".)

c) $\frac{449}{512} \approx 0{,}877 \longrightarrow$ 1ª letra : C

$\frac{0{,}877 - 0{,}7}{0{,}2} = 0{,}8848 \longrightarrow$ 2ª letra : C

$\frac{0{,}8848 - 0{,}7}{0{,}2} = 0{,}9238 \longrightarrow$ 3ª letra : D

$\frac{0{,}9238 - 0{,}9}{0{,}1} = 0{,}2383 \longrightarrow$ 4ª letra : A

Portanto: $\frac{449}{512} \longrightarrow$ CCDA

7 - $$G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$ (7)

a) Usando linhas (permutações, adições) obtém-se

$$G' = \left[\begin{array}{cccc:cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Todas as linhas têm peso par $\Rightarrow$ todas as palavras têm peso par

b) $$H' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Linhas $\neq 0$ e diferentes $\Rightarrow d_{min} \geq 3$

Como em G' todas as linhas têm peso par $\Rightarrow$ as palavras têm peso par $\Rightarrow d_{min} \geq 4$. Terá de ser $d_{min} = 4$ (peso das palavras das linhas de G).

c) Se retirarmos o 1.º bit de informação então:

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

(código 7, 3)

(retira-se a 1.ª linha e a 5.ª coluna)

porque os bits de informação aparecem no fim!!

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

(retira-se a quinta linha)

d) (8,4) . O polinómio gerador tem grau 4 e é factor de p^8+1. Como 8 é par então: (8)

$$p^8+1 = (p^4+1)^2 = (p^2+1)^4 = (p+1)^8$$

Só há um polinómio nessas condições: $g(p) = (p+1)^4 =$
$= p^4+1$

$g(p)$ representa também uma palavra de código e tem peso 2. Como todas as palavras têm peso par
$\Rightarrow d_{mín} = 2$

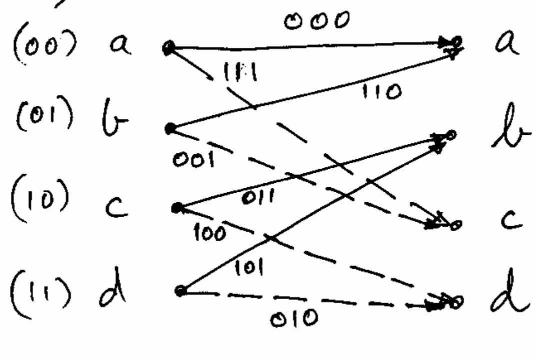
e)
$$g(p) = p^4+p^3+p^2+1 \quad ; \quad X(p) = p \Rightarrow p^{n-k}X(p) = p^5$$

$$C(p) = p^5 \bmod g(p) = p^2+p+1$$

$$Y(p) = p^5+p^2+p+1 \Rightarrow Y = [0\,1\,0\,0\,1\,1\,1]$$

8. Existem 4 estados: 00 (a), 01 (b), 10 (c) e 11 (d)

a)



b) O percurso de peso mínimo é o percurso $a \to c \to b \to a$.
O peso é $3+2+2 = 7$
$\Rightarrow d_f = 7$

Pelo diagrama de estados concluiríamos o mesmo: