Teoria da Informação (2000-2001) Exame de 1ª chamada (12-6-2001)

Resolução

3 - a) Cada palavra de código pode ser obtida por adição das linhas de G: $Y = a_1 \underline{g}_1 + a_2 \underline{g}_2 + \ldots + a_K \underline{g}_K$, em que $a_i = 0, 1, \ldots, D-1$ e $\underline{g}_i$ é a linha de ordem i de G. As K linhas da matriz G são linearmente independentes, isto é, somadas não dão zero, ou seja $Y = 0$ se e só se todos os a_i forem zero. Considerem-se duas palavras de código, Y_1 e Y_2. Então $Y_1 + Y_2 = (a_1 + b_1)\underline{g}_1 + (a_2 + b_2)\underline{g}_2 + \ldots + (a_K + b_K)\underline{g}_K$ é sempre diferente de zero a não ser que $a_i = b_i$, $i = 1, 2, \ldots K$. Quer dizer que todas as diferentes combinações dos coeficientes a_i originam diferentes palavras de código. Como cada coeficiente pode ter D valores existem D^K palavras de código. c.q.d.

b) Código 1: H_1 c/ palavras de código Y_1

Código 2: H_2 c/ " " " Y_2

Ora $Y_2 H_2 = 0 \Rightarrow Y_2 H_1 Q = 0 \Rightarrow Y_2 H_1 = 0$

$\Rightarrow Y_2$ pertence ao código 1

Inversamente, de $H_2 = H_1 Q \Rightarrow H_1 = H_2 Q^{-1}$, obtemos

$Y_1 H_1 = Y_1 H_2 Q^{-1} = 0 \Rightarrow Y_1 H_2 = 0 \Rightarrow Y_1$ pertence ao código 2 $\Rightarrow Y_1 = Y_2$ necessariamente.

4 - Código 1: (n, K); Cód. 2: $(2n, n+K)$; ambos são gerados por $g(p)$. Assim os polinómios $p^n + 1$ e $p^{2n} + 1$ são ambos múltiplos de $g(p)$. Acontece que $p^n + 1$ tem grau inferior a $2n$ pelo que, sendo múltiplo de $g(p)$, é um polinómio do código 2. Mas este polinómio corresponde a um vector com peso 2. Em conclusão: o cód. 1 tem $d_{min} = 3$ e o cód. 2 tem $d_{min} = 2 \Rightarrow$ escolheria o Código 1.

(Lição a tirar: n deve ser o menor possível tal que $p^n + 1$ seja múltiplo de $g(p)$!!)

5- Fonte binária com símbolos independentes.

a) Entropia: $\Omega\left(\frac{3}{4}\right) = H\left(\frac{1}{4}, \frac{3}{4}\right) = 0{,}8113$ bits/símbolo.

b) $P(0) = \frac{3}{4}$ e $P(1) = \frac{1}{4}$. Sendo os símbolos independentes:

$P(000) = \left(\frac{3}{4}\right)^3 = \frac{27}{64}$ $P(001) = P(010) = P(100) = \frac{1}{4} \times \frac{9}{16} = \frac{9}{64}$

$P(011) = P(101) = P(110) = \frac{3}{64}$ e $P(111) = \frac{1}{64}$

Ordenando e codificando:

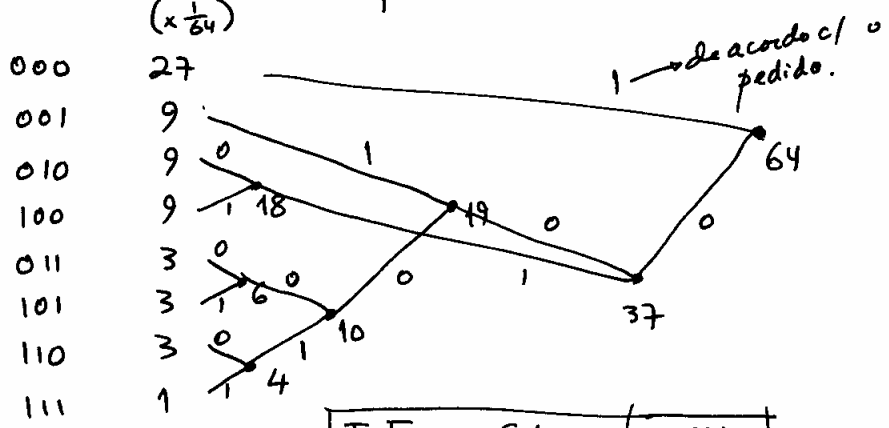


Tabela:

Fonte	Código	n_i
000	1	1
001	001	3
010	010	3
100	011	3
011	00000	5
101	00001	5
110	00010	5
111	00011	5

c) Entropia da fonte binária: $\Omega\left(\frac{3}{4}\right) = H\left(\frac{1}{4}, \frac{3}{4}\right) = 0{,}8113$ bits/símb.

$\overline{N} = \frac{1}{3} \times \left(1 \times 27 + (3+3+3) \times 9 + (5+5+5) \times 3 + 5 \times 1\right) \times \frac{1}{64} = \frac{79}{96} = 0{,}823$

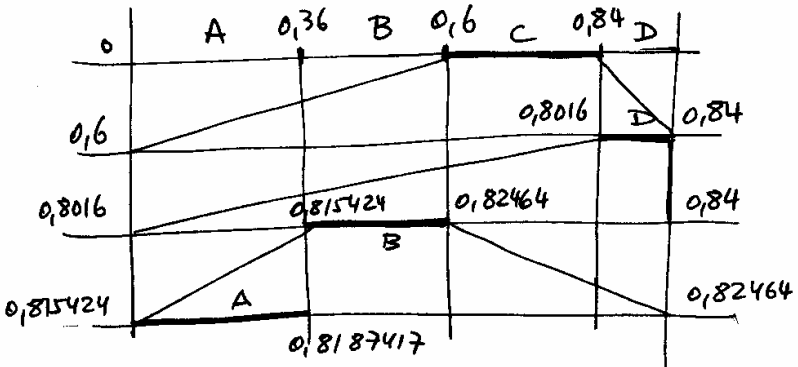
Eficiência: $\frac{H(x)}{\overline{N}} = 98{,}6\,\%$

d) $P(0) = 0{,}6$, Extensão de 2ª ordem, símbolos independentes

	Probab.
A = 00	0,36
B = 01	0,24
C = 10	0,24
D = 11	0,16

Sequência a codificar: 10 11 01 00

C D B A



Intervalo final: $[0{,}815424 ; 0{,}8187417[$

Poderia ser o nº: 0,816, por exemplo.

6. Por permutação e soma de linhas chegamos à matriz G "sistemática":

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

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

a) De G tirava-se logo que $d_{min} \leq 3$. Ora em H vemos que não há 2 linhas iguais, logo $d_{min} \geq 3$. Concluímos imediatamente que $d_{min} = 3$. (Confirmação: a soma das linhas 2, 4 e 5 de H é zero $\Rightarrow d_{min} = 3$; outra maneira seria calcular as oito palavras de código)

b) Está acima.

c) Existem $2^3 = 8$ "coset leaders": um é nulo, seis têm peso 1 ($\Rightarrow \alpha_1 = 6$) e um tem peso 2 ($\Rightarrow \alpha_2 = 1$).

Assim, $P_{enc} = 1 - \sum_{i=0}^{n} \alpha_i\, p^i (1-p)^{n-i} = 1 - [(1-p)^6 + 6p(1-p)^5 + p^2(1-p)^4]$

Com $p = 10^{-4} \Rightarrow P_{enc} = 1{,}3996 \cdot 10^{-7} \simeq 1{,}4 \cdot 10^{-7}$

d) Síndrome correspondente a $z = [101001]$:

$$s = zH = [111] + [011] + [001] = [101]$$

(1ª linha de H; 3ª; 6ª)

Como $d_{min} = 3$ e $t = 1$ e a síndrome não é igual a nenhuma linha de H concluímos que a palavra z contém 2 ou mais erros.

Intencionalmente em branco

7 – $(127, 120)$, $g(p) = p^7 + p + 1$

a) $X(p) = p^{49} \Rightarrow C(p) = p^7 X(p) \bmod g(p) = p^{56} \bmod g(p)$

Vamos achar múltiplos de $g(p)$:

$(p^7+p+1)^2 = p^{14} + (p+1)^2 = p^{14} + p^2 + 1$

$(p^7+p+1)^4 = p^{28} + (p^2+1)^2 = p^{28} + p^4 + 1$

$(p^7+p+1)^8 = p^{56} + (p^4+1)^2 = p^{56} + p^8 + 1$

Quer dizer que se dividirmos p^{56} por $g(p)$ o resto é o mesmo da divisão de p^8+1 por $g(p)$!

$(p^{56}+p^8+1) \bmod g(p) = 0$

$\Rightarrow p^{56} \bmod g(p) + (p^8+1) \bmod g(p) = 0$

$\Rightarrow p^{56} \bmod g(p) = (p^8+1) \bmod g(p) = p^2+p+1$

Modo prático alternativo:

$p^7+p+1 = 0 \Longrightarrow p^7 = p+1$

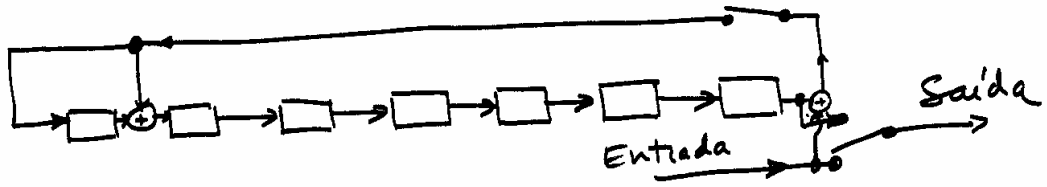
$p^{14} = (p+1)^2 = p^2+1$

$\vdots$

$p^{56} = p^2+p+1$ ← Resto da divisão de p^{56} por $g(p)$.

Polinómio de código: $Y(p) = p^{56}+p^2+p+1$.

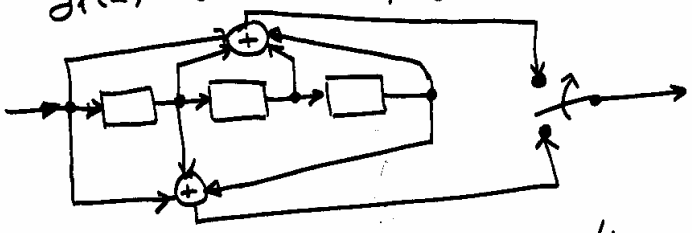
b)



c) $Z(p) = p^{11}+p^8+p^5+p^2+p+1$

$S(p) = Z(p) \bmod g(p) = p^4+1$

8. $g_1(\omega) = \omega^3+\omega^2+\omega+1$; $g_2(\omega) = \omega^2+\omega+1$ (menor potência à esquerda ←)

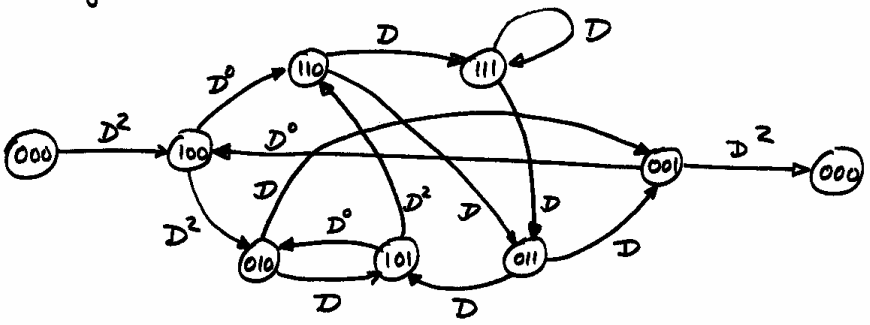


a) Comprimento de restrição: 4

b) Nº de estados: $2^3 = 8$

(6)

c) Diagrama de estados:



Distância livre: $000 \longrightarrow 100 \longrightarrow 110 \longrightarrow 011 \longrightarrow 001 \longrightarrow 000$

$2 + 0 + 1 + 1 + 2 = 6$

$d_f = 6$

Os outros percursos têm métricas maiores.

d) Percurso de métrica 7: há três

$000 \longrightarrow 100 \longrightarrow 010 \longrightarrow 001 \longrightarrow 000 \Rightarrow D^2D^2DD^2 = D^7$

$000 \longrightarrow 100 \longrightarrow 110 \longrightarrow 011 \longrightarrow 101 \longrightarrow 010 \rightarrow 001 \rightarrow 000 \Rightarrow D^2D^0DDD^0DD^2 = D^7$

$000 \longrightarrow 100 \longrightarrow 110 \longrightarrow 111 \longrightarrow 011 \longrightarrow 001 \longrightarrow 000 \Rightarrow D^2D^0DDDD^2 = D^7$

Os cálculos em c) e d) poderiam ter sido realizados calculando a função de transferência do código.