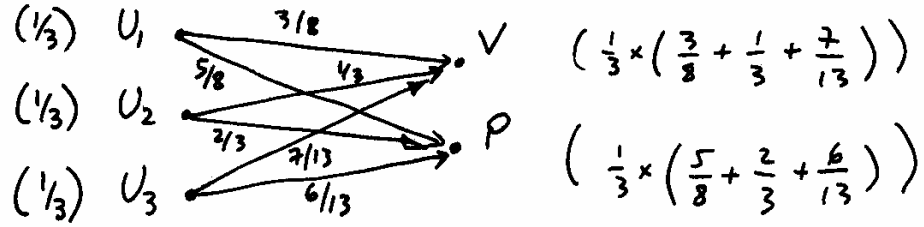
Resolução

3. a) Seja $N > n$ e $(p^N+1) \bmod g(p) = 0$ (tal como $(p^n+1) \bmod g(p) = 0$)
Então, se p^n+1 é múltiplo de $g(p)$ e dado que tem grau menor que N, é uma palavra de código (de comprim. N). O seu peso é 2, logo $d_{min} < 2$. Mas por outro lado não há nenhuma palavra nesse código de peso 1, porque se houvesse, por deslocamentos cíclicos dela obteríamos o polinómio 1, que também seria palavra de código. Só que 1 não pode ser palavra de código porque como o grau de $g(p)$ é ≥ 1, o polinómio 1 não é divisível por $g(p)$. Assim, $d_{min} > 1$, isto é, $d_{min} = 2$

b) Uma palavra de código de peso 2 é da forma $y(p) = p^i + p^j$, com $0 \leq j < i < n$. Como o código é cíclico, o deslocam. de $n-i$ posições levaria à palavra do código $p^{n-(i-j)}+1$, divisível por $g(p)$. Mas $n-(i-j) < n$ e foi dito que, por hipótese, n é o menor inteiro tal que p^n+1 é múltiplo de $g(p) \Rightarrow$ não há palavra de peso $2 \Rightarrow d_{min} \geq 3$.

5. $U = \{U_1, U_2, U_3\}$ $C = \{V, P\}$



a) $I(U;C) = \sum_{i=1}^{3} \sum_{j=1}^{2} P(u_i, c_j) I(u_i, c_j) = 0,0232$

b) $H(U) = \log_2 3 = 1,585$ (valor máximo)

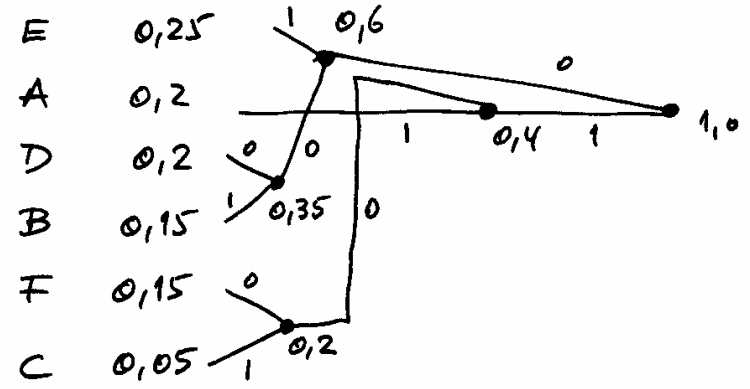
c) $H(C) = 0,9793$

d) $H(U,C) = H(U) + H(C) - I(U,C) = 2,5411$

e) $H(C|U) = H(C) - I(U,C) = 0,9793 - 0,0232 = 0,9562$

6. a)

b)

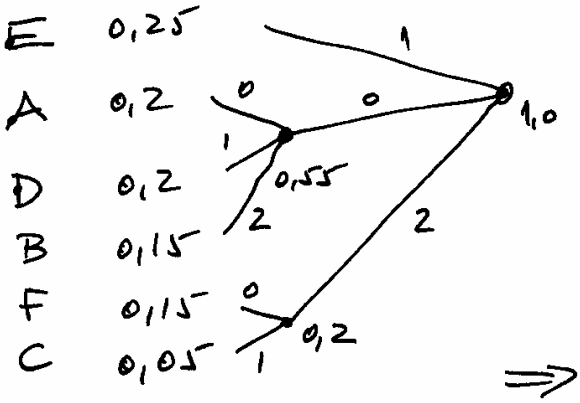


A — 11
B — 001
C — 101
D — 000
E — 01
F — 100

(árvore de variância mínima)
(para minimizar nº. erros)

c) $H(x) = 2,466$ $\quad \bar{N} = 2,55 \Rightarrow$ Efic. $= \frac{H(x)}{\bar{N}} = 96,7\%$

d) $K = 6$, $D = 3$ $\Rightarrow$ Agrupam. prévio de $2 + (k-2) \bmod (D-1) =$
$= 2 + 4 \bmod 2 = 2$



A — 00
B — 02
C — 21
D — 01
E — 1
F — 20

$\Rightarrow \bar{N} = 1,75$ dígitos tern./letra

7- a) A matriz H é igual a

$$H = \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&1&1 \\ 1&1&0&1 \\ 1&0&1&0 \\ 0&1&0&1 \\ 1&1&1&0 \\ 0&1&1&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix} \Rightarrow G = \left[\begin{array}{cccc|cccc} 1&0&0&0&0&0&0&0 & 1&1&0&0 \\ 0&1&0&0&0&0&0&0 & 0&1&1&0 \\ & & & & & & & & 0&0&1&1 \\ & & & & & & & & 1&1&0&1 \\ & & & & & & & & 1&0&1&0 \\ & & & & & & & & 0&1&0&1 \\ & & & & & & & & 1&1&1&0 \\ 0&0&0&0&0&0&0&1 & 0&1&1&1 \end{array}\right]$$

b) $X = [1\,0\,0\,1\,0\,1\,1\,0]$

$y_9 = 1+1+1 = 1$
$y_{10} = 1+1+1+1 = 0$
$y_{11} = 1$
$y_{12} = 1+1 = 0$

$\Rightarrow Y = [1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,1\,0]$

c) $S = \hat{Z}H = [1\,1\,1\,1\,0\,1\,0\,0\,0\,1\,0\,0]\,H =$

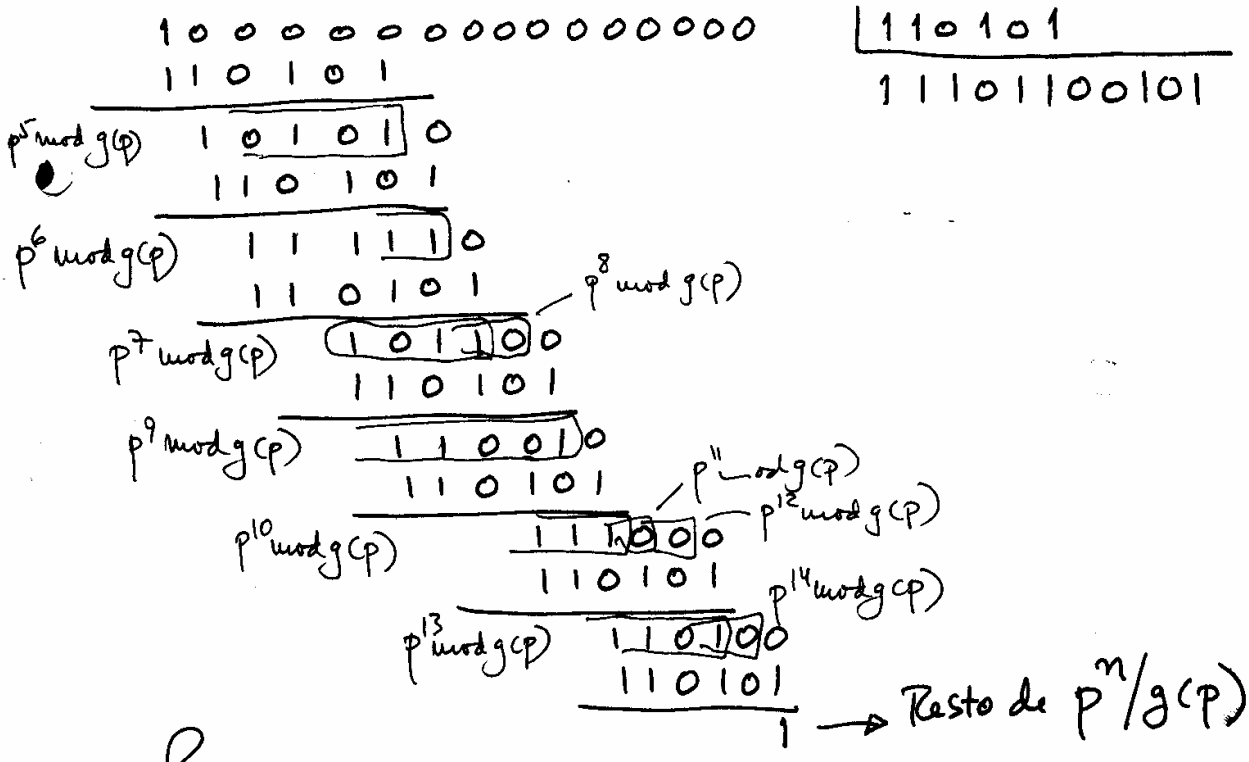
$= [1+1 \quad 1+1+1+1+1 \quad 1+1 \quad 1+1+1] = [0\,1\,0\,1]$

O código corrige erros simples. Esta síndrome é igual à 6ª linha de $H \Rightarrow \hat{E} = [0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0]$

$\Rightarrow \hat{Y} = \hat{Z} + \hat{E} = [1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0]$

$\Rightarrow \hat{X} = [1\,1\,1\,1\,0\,0\,0\,0]$

8. $g(p) = p^5 + p^4 + p^2 + 1$ é submúltiplo de $p^n + 1$.



Portanto, $n = 15$.

(4)

a) O grau de $g(p)$ é $n-k=5$. Como $n=15$, o código é $(15,10)$.

Existem $2^k = 2^{10} = 1024$ palavras de código de tamanho 15.

b) A linha i da submatriz P é $p^{n-i} \bmod g(p)$. Olhando para a divisão polinomial atrás concluímos:

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

$$\Rightarrow G = [I_{10} \mid P]$$

$$H = \begin{bmatrix} P \\ \hline I_5 \end{bmatrix}$$

c) $Z(p) = p^8 + p^6 + p + 1$

$S(p) = (p^8 + p^6 + p + 1) \bmod g(p) = p^3 + p$.

Como o vector síndrome tem $n-k=5$ elementos

$$\Rightarrow S = [0\ 1\ 0\ 1\ 0]$$

d) Rajadas de erros detectáveis c/ códigos cíclicos:

De comprimento $< n-k$: todas (100%)

" " $= n-k+1$: fracção $1 - 2^{-(n-k-1)} = 1 - 2^{-4} = 15/16$

" " $> n-k+1$: fracção $1 - 2^{-(n-k)} = 1 - 2^{-5} = 31/32$

$\Rightarrow$ Comprim. 4 e 5: 100%; Comprim. 6: 15/16; Compr. 7 e 8: 31/32 das rajadas.