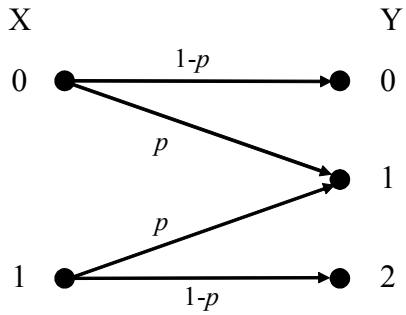
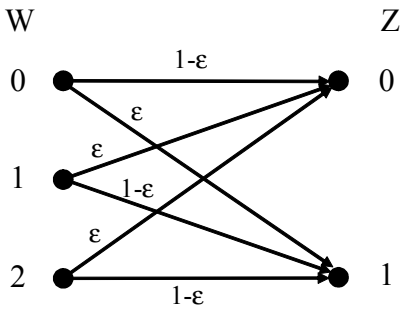
Resolução

1. Canais discretos sem memória e $p = 0{,}2$:



Canal A



Canal B

Vamos representar $P(X = i)$ por $P(X_i)$, etc.

a) $P(Y_0) = P(X_0)P(Y_0 \mid X_0) = \frac{1}{2}(1-p)$; $P(Y_2) = P(Y_0) = \frac{1}{2}(1-p)$; $P(Y_1) = p$.

Entropia de Y: $H(Y) = H\left(\frac{1}{2}(1-p), \frac{1}{2}(1-p), p\right) = H(0{,}4; 0{,}4; 0{,}2) = 1{,}522$

b) Cálculo de $H(Y|X)$:

$$H(Y \mid X) = \sum_{i=0}^{1} P(X_i) H(Y \mid X_i) =$$

$$= \frac{1}{2} H(p, 1-p) + \frac{1}{2} H(p, 1-p) = \Omega(p)$$

Sendo $p = 0{,}2$ então $H(Y \mid X) = \Omega(0{,}2) = 0{,}722$ bits/símbolo.

c) Como $I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$ então a entropia condicional pedida (equivocação do canal) é $H(X \mid Y) = H(X) - H(Y) + H(Y \mid X)$. Substituindo valores:

$$H(X \mid Y) = H(X) - H(Y) + H(Y \mid X) = 1 - 1{,}522 + 0{,}722 = 0{,}2$$

d) Matrizes de transição dos canais:

$$\left[P(Y \mid X)\right] = \begin{bmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{bmatrix} \qquad \left[P(Z \mid Y)\right] = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}$$

A matriz de transição do canal-série é igual ao produto das matrizes individuais:

$$[P(Z|X)] = [P(Y|X)][P(Z|Y)] =$$
$$= \begin{bmatrix} (1-p)(1-\varepsilon)+p\varepsilon & (1-p)\varepsilon+p(1-\varepsilon) \\ p\varepsilon+(1-p)\varepsilon & p(1-\varepsilon)+(1-p)(1-\varepsilon) \end{bmatrix}$$

Este canal é inútil (e o canal B também) se ε = 0,5 pois nesse caso todas as entradas da matriz [P(Z|X)] são iguais a 0,5, independentemente de *p*. Uma moeda ao ar seria muitíssimo mais simples.

e) Capacidade do canal B:

$$C = \max I(Y;Z) = \max\left[H(Z) - H(Z|Y)\right] =$$
$$= \max H(Z) - H(Z|Y)$$

Entropia condicional $H(Z|Y)$:

$$H(Z|Y) = P(Y_0)H(Z|Y_0) + P(Y_1)H(Z|Y_1) + P(Y_2)H(Z|Y_2) =$$
$$= \Omega(\varepsilon)\left[P(Y_0) + P(Y_1) + P(Y_2)\right] =$$
$$= \Omega(\varepsilon)$$

Z é uma variável binária. A sua entropia vale

$$H(Z) = \Omega\left[P(Y_0)(1-\varepsilon) + P(Y_1)\varepsilon + P(Y_2)\varepsilon\right].$$

Se ε = 1/2 teremos $H(Z|Y) = \Omega(0,5) = 1$ e $H(Z) = \Omega(0,5) = 1$ pelo que $I(Y;Z) = 1-1 = 0$ independentemente da distribuição de probabilidades de Y. Nessas circunstâncias a capacidade do canal é $C = 0$ (canal inútil, como se disse).

2. Com codificação de canal o limite de Shannon é dado, em canais AWGN, por $\frac{E_b}{N_0} \geq \frac{2^{2R_c}-1}{2R_c}$, em que $R_c = k/n$ é a taxa do código. Como $k/n = 1/2$ então $\frac{E_b}{N_0} \geq 1$, isto é, $\left(E_b/N_0\right)_{dB} \geq 0$ dB. Concluímos que o menor valor de E_b/N_0 que o código inventado permite usar é 0 + 0,5 = 0,5dB.

3. Código de Hamming (7,4) gerado por

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

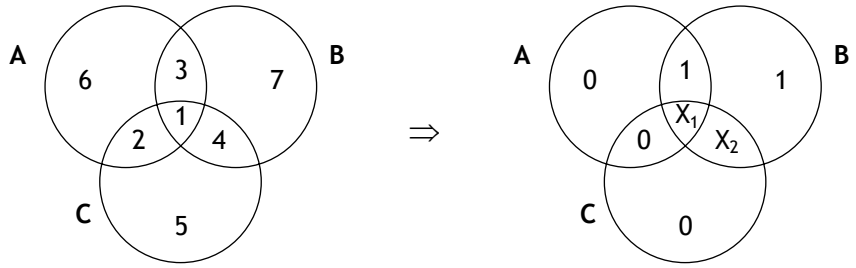
a) Codificação de 1110: basta somar as primeiras três linhas de **G**: 1110010.

b) Descodificação da sequência **Z** = [1010101]: precisamos da matriz **H** e da síndrome **S**:

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \Rightarrow \qquad \mathbf{S} = \mathbf{ZH} = [1010101]\mathbf{H} = [001]$$

Num código de Hamming a síndrome é igual a uma das linhas de **H**, neste caso a última, o que quer dizer que na sequência recebida o último bit está errado. Assim, a palavra de código enviada terá sido 1010100 e a mensagem terá sido 1010.

c) Vamos eliminar as duas rasuras de $X_1 01 X_2 001$ com diagramas de Venn. Para os desenhar precisamos das equações de paridade ou… da matriz **H**, que é a que vamos usar. Assim, nesta vemos que o bit da mensagem de 4 bits que está nas três equações de paridade é o primeiro (pois a linha 1 de **H** só tem "uns"), logo, será colocado na área de intersecção dos três círculos do diagrama de Venn. A numeração das restantes áreas tem em conta os bits 1 em cada coluna de **H**.



Do ponto de vista de **A** a rasura X_1 tem de representar o bit 1 (para que haja um número par de "uns" dentro do círculo). Depois desta decisão a rasura X_2 terá de ser 1 para que dentro de cada um dos restantes círculos o número de "uns" também seja par. Concluímos, portanto, que a palavra de código estimada é 1011001 e a mensagem correspondente é 1011.

É de notar que, sendo o código de Hamming um código corrector de apenas erros simples, consegue corrigir duas rasuras por palavra de sete bits.

4. No código A as palavras de código têm comprimentos {2, 2, 3, 3, 4}. Vamos ver se satisfazem a desigualdade de Kraft:

$$\sum_{i=1}^{5} 2^{-n_i} = \frac{1}{2^2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^4} = \frac{13}{16} < 1 \qquad \text{(Satisfaz a desigualdade de Kraft)}$$

Quanto ao código B: $\sum_{i=1}^{5} 2^{-n_i} = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^4} = \frac{17}{16} > 1$ (não satisfaz). Concluímos que este não é um código de Huffman binário porque os códigos de Huffman, tal como todos os códigos unicamente descodificáveis, satisfazem a desigualdade de Kraft. No entanto, não podemos afirmar que o código A seja um código de Huffman, nem sequer que seja unicamente descodificável, pois a desigualdade de Kraft é uma condição necessária mas não suficiente.

5. Codificação LZ78 com dicionário de tamanho 32 iniciado com A, B e C. Sequência a codificar: ACBBACBABAABBC.

a) Seccionamento da sequência: AC/BB/ACB/AB/AA/BBC

Dicionário:

Índice	Entrada	Código
1	A	0A
2	B	0B
3	C	0C
4	AC	1C
5	BB	2B
6	ACB	4B
7	AB	1B
8	AA	1A
9	BBC	5C

b) Sequência codificada: 1C 2B 4B 1B 1A 5C

c) Cada palavra de código é constituída por duas partes: a primeira indica o índice da secção repetida e a segunda representa a última letra da secção corrente. Como o dicionário tem capacidade para 32 entradas cada índice é representado por 5 bits; como o alfabeto da fonte tem 3 letras (A, B e C) precisamos de 2 bits para as representar. Portanto, em binário cada secção é representada por uma palavra de código de 7 bits. A sequência dada é representada por $6 \times 7 = 42$ bits.

6. Polinómio gerador: $g(p) = p^3 + p^2 + p + 1$. O grau de $g(p)$ indica-nos que n-k = 3. Mas… quanto vale n e $k > 1$?

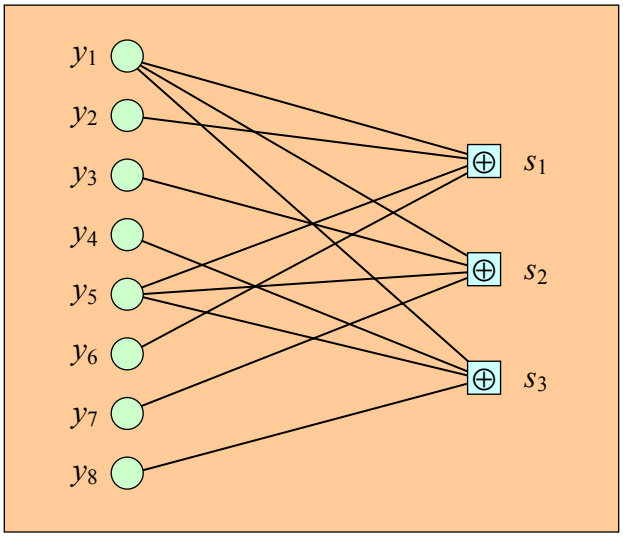
a) Sabemos que $p^n + 1$ é múltiplo de $g(p)$, ou seja, $p^n \bmod g(p) = 1$. Os menores valores de n que obtemos dividindo $p^n = 10000\ldots$ por $g(p) = 1111$ são $n = 4$ e $n = 8$. O primeiro tem de ser

abandonado porque o código correspondente é um código (4,1) (código de repetição) e nós sabemos que, por hipótese, $k > 1$. Portanto, retemos $n = 8$ e $k = 5$ (código (8,5)).

b) O polinómio gerador é o polinómio de código de menor grau e pode ser imediatamente colocado na quinta e última linha de **G**: 00001111. Tratando-se de um código cíclico qualquer deslocamento cíclico de uma palavra de código é outra palavra de código. Então deslocando a última linha de um bit obtemos 10000111, que devemos considerar como a primeira linha de **G**. A segunda linha pode ser obtida somando a primeira com o seu deslocamento de um bit: 01000100. Prosseguindo de modo idêntico com deslocamentos e convenientes somas de linhas obteríamos

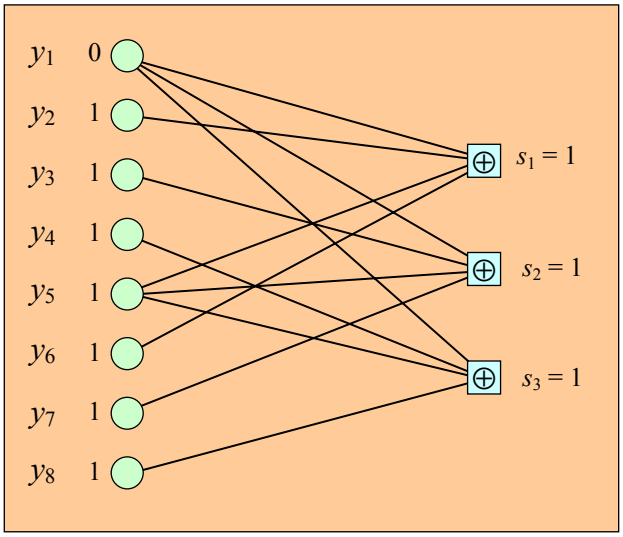
$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

c) No gráfico de Tanner temos $n = 8$ nós de variáveis e $n - k = 3$ nós de paridade ligados assim:

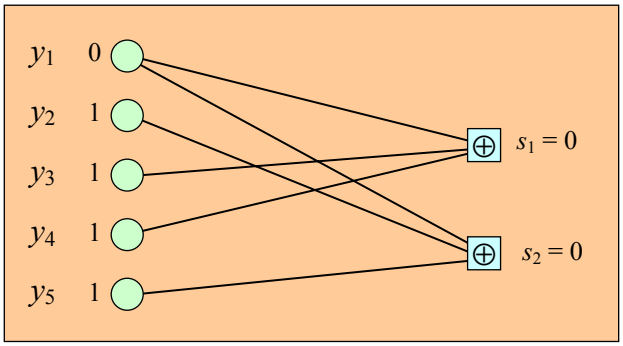


À matriz geradora alternativa corresponde o gráfico de Tanner apresentado na alínea seguinte. Tem cinco nós de variáveis e dois nós de paridade.

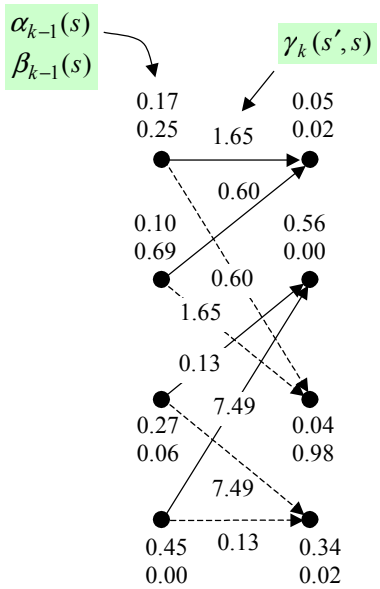
d) Síndrome da sequência 01111111 recorrendo ao gráfico de Tanner: cada elemento da síndrome é obtido somando em módulo 2 os bits que confluem no respectivo nó de paridade. Como se vê na figura seguinte, a síndrome vale **S** = 111.



A síndrome obtida com o código alternativo é igual a **S** = 00, como se observa no gráfico de Tanner respectivo:



7. Algoritmo BCJR.



A LLR a posteriori $L(u_k|\mathbf{y}) = \ln \dfrac{P(u_k = +1|\mathbf{y})}{P(u_k = -1|\mathbf{y})}$ (em que +1 corresponde ao bit 1 e -1 corresponde ao bit 0) é calculada através do quociente da soma de produtos $\alpha\beta\gamma$:

$$L(u_k|\mathbf{y}) = \ln \frac{\sum\limits_{R_1} P(s', s, \mathbf{y})}{\sum\limits_{R_0} P(s', s, \mathbf{y})} = \ln \frac{\sum\limits_{R_1} \alpha_{k-1}(s')\gamma_k(s', s)\beta_k(s)}{\sum\limits_{R_0} \alpha_{k-1}(s')\gamma_k(s', s)\beta_k(s)}$$

No numerador consideramos os quatro ramos gerados por bits de entrada 1 (ramos tracejados) e no denominador consideramos os outros ramos, ou seja,

$$L(u_k|\mathbf{y}) = \ln \frac{P(0,2,\mathbf{y}) + P(1,2,\mathbf{y}) + P(2,3,\mathbf{y}) + P(3,3,\mathbf{y})}{P(0,0,\mathbf{y}) + P(1,0,\mathbf{y}) + P(2,1,\mathbf{y}) + P(3,1,\mathbf{y})}.$$

Cada probabilidade $P(s', s, \mathbf{y})$ não normalizada vale

$$P(0,2,\mathbf{y}) = 0{,}17 \times 0{,}6 \times 0{,}98 = 0{,}1 \qquad P(1,2,\mathbf{y}) = 0{,}1 \times 1{,}65 \times 0{,}98 = 0{,}16$$
$$P(2,3,\mathbf{y}) = 0{,}27 \times 7{,}49 \times 0{,}02 = 0{,}04 \qquad P(3,3,\mathbf{y}) = 0{,}45 \times 0{,}13 \times 0{,}02 = 0{,}001$$

$$\Rightarrow P(0,2,\mathbf{y}) + P(1,2,\mathbf{y}) + P(2,3,\mathbf{y}) + P(3,3,\mathbf{y}) = 0{,}303$$

$$P(0,0,\mathbf{y}) = 0{,}17 \times 1{,}65 \times 0{,}02 = 0{,}006 \qquad P(1,0,\mathbf{y}) = 0{,}1 \times 0{,}6 \times 0{,}02 = 0{,}001$$
$$P(2,1,\mathbf{y}) = 0{,}27 \times 0{,}13 \times 0 = 0 \qquad P(3,1,\mathbf{y}) = 0{,}45 \times 7{,}49 \times 0 = 0$$

$$\Rightarrow P(0,0,\mathbf{y}) + P(1,0,\mathbf{y}) + P(2,1,\mathbf{y}) + P(3,1,\mathbf{y}) = 0{,}007$$

Na prática deve proceder-se à normalização das probabilidades anteriores dividindo cada uma pela soma de todas, $\sum\limits_{R_0, R_1} P(s', s, \mathbf{y}) = 0{,}31$, para evitar problemas de instabilidade numérica. Como 0,31 aparece quer no numerador quer no denominador da expressão de $L(u_k|\mathbf{y})$ o resultado final é o mesmo, com ou sem normalização. Aqui optámos por não normalizar as probabilidades pois não há instabilidade numérica nestes pequenos cálculos.

a) $P(0,2,\mathbf{y}) = 0{,}17 \times 0{,}6 \times 0{,}98 = 0{,}1$.

b) Substituindo valores temos $L(u_k|\mathbf{y}) = \ln \dfrac{0{,}303}{0{,}007} = 3{,}80$. Como o valor de $L(u_k|\mathbf{y})$ é positivo estimamos $\hat{u}_k = 1$.