

10

Codificação de Canal (Códigos de Controlo de Erros)

Comunicação Digital

(21 de abril de 2023)



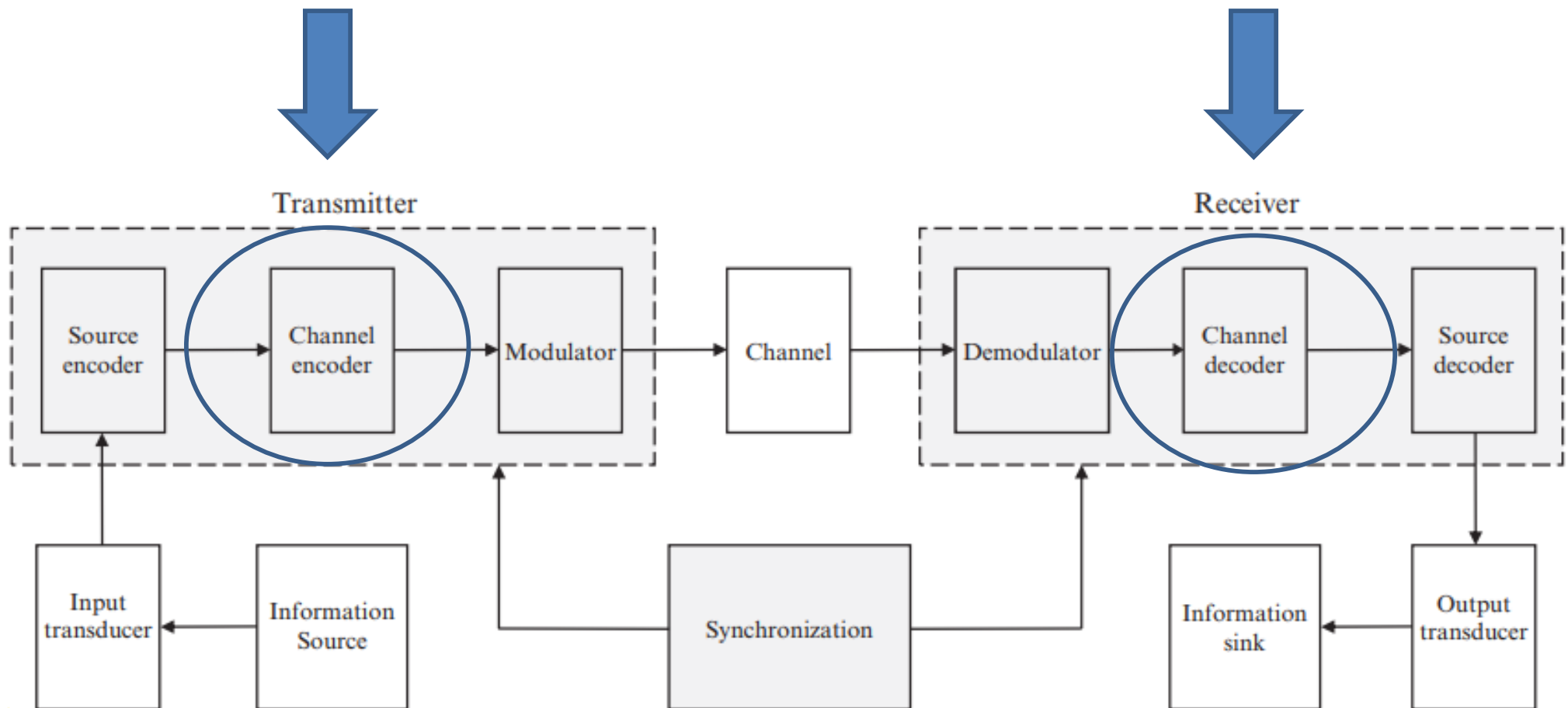
Sumário

1. Aspectos gerais sobre a comunicação digital
 - Comportamento do canal
 - Causas da existência de erros
2. Códigos detetores e corretores de erros
 - Códigos de bloco linear (n,k)
 - Características dos códigos
 - Capacidades de deteção e correção
 - Códigos de repetição e bit de paridade
 - Código de *Hamming*
 - CRC – *Cyclic Redundancy Check*
3. Deteção e Correção
4. Análise matricial dos códigos
5. Aplicações
6. Exercícios

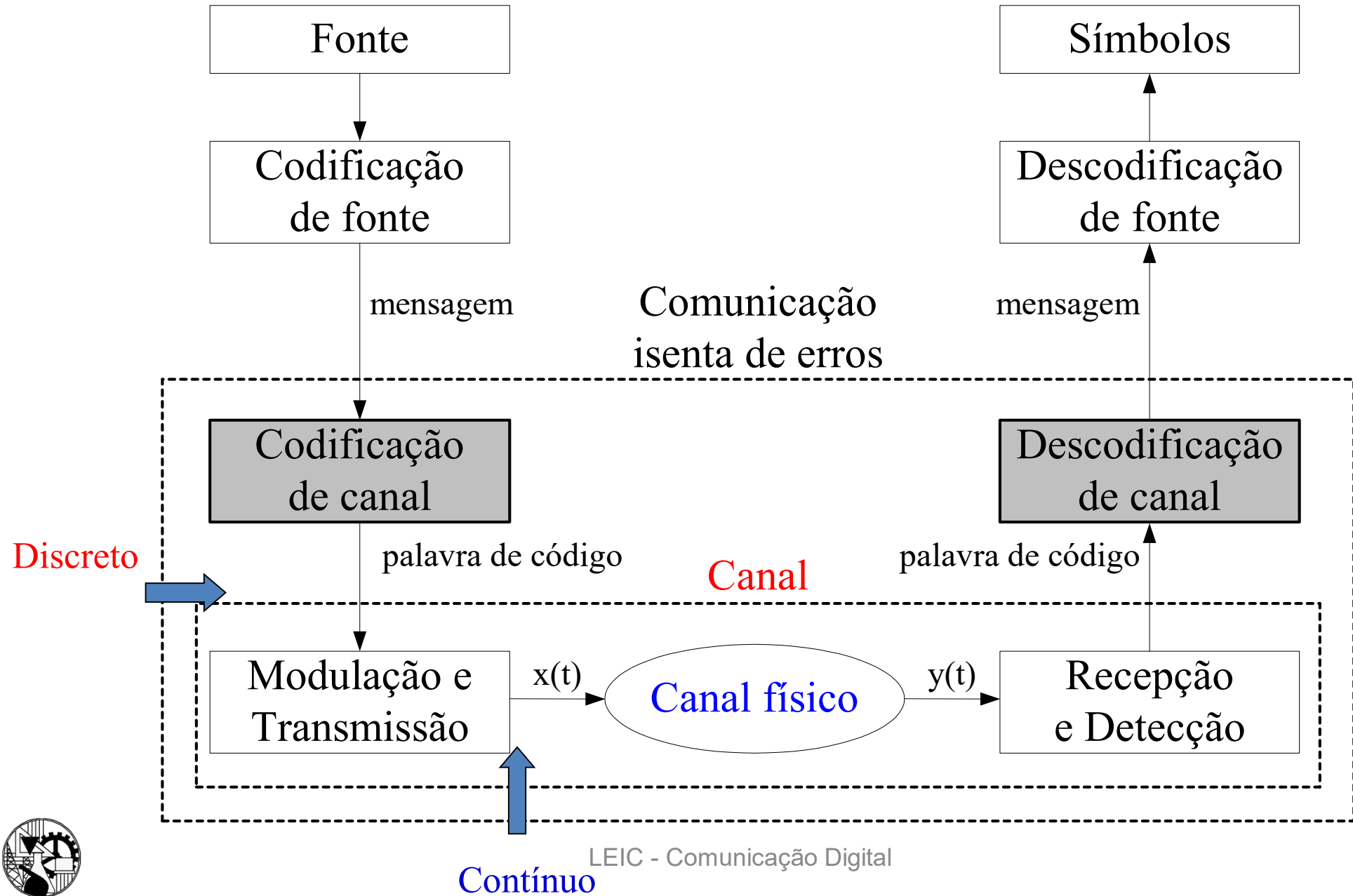


Sistemas de Comunicação

- Diagrama de blocos genérico



1. Cenário de utilização



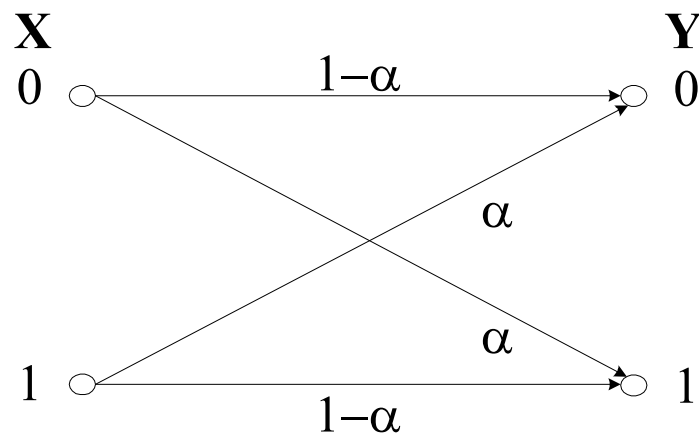
1. Modelo de canal discreto

- O canal é analisado através de modelo discreto usando variáveis aleatórias (v.a.)
- Do ponto de vista da transmissão, um SCD pode ser visto através de modelo probabilístico
- A probabilidade de erro por troca de bit não é nula



1. Modelo de canal discreto

- O canal é analisado através de modelo discreto usando variáveis aleatórias (v.a.)
- Modelo BSC - *binary symmetric channel*



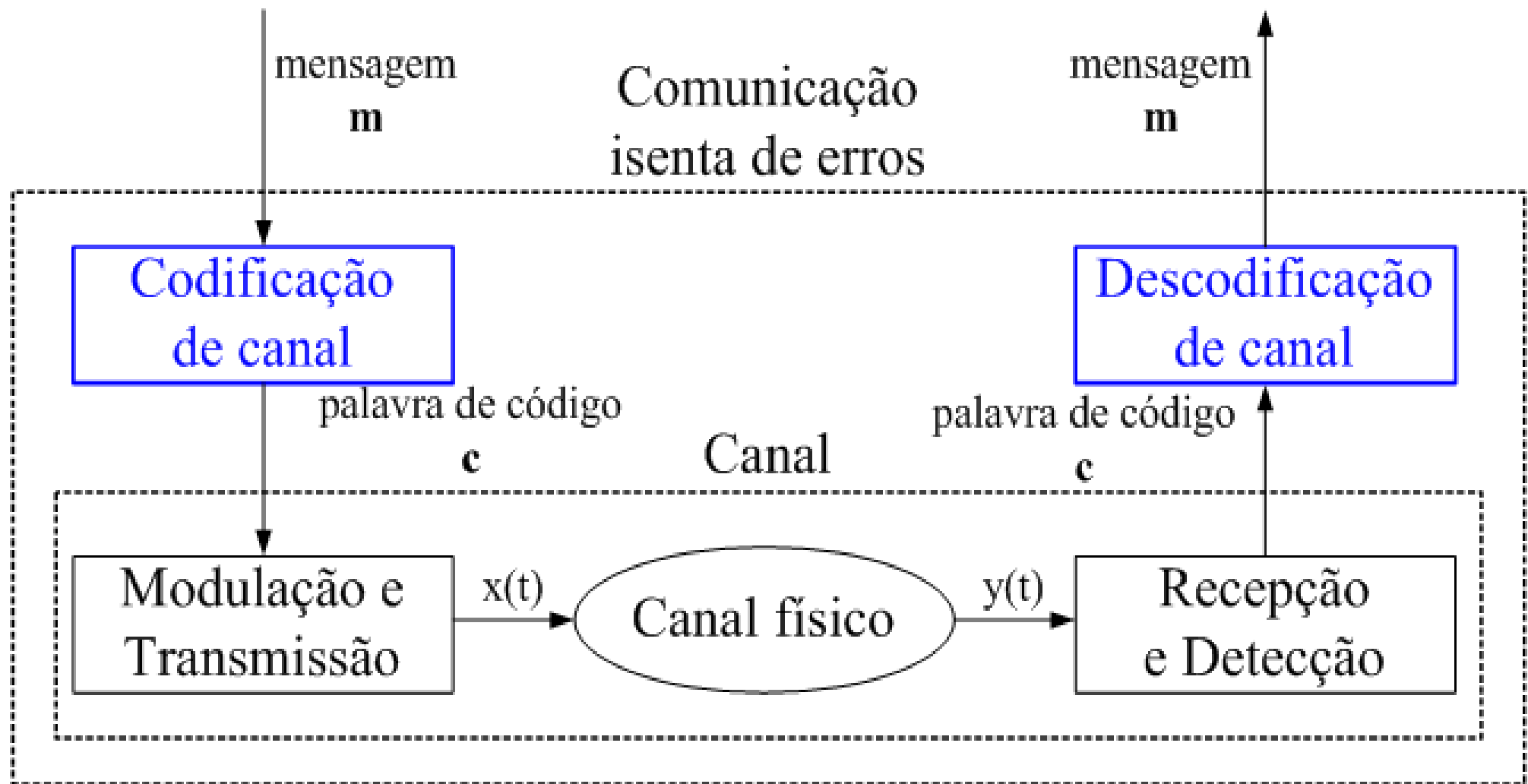
Probabilidade de erro de bit

$$\begin{aligned} P_e &= P(y_0, x_1) + P(y_1, x_0) \\ &= P(y_0|x_1)P(x_1) + P(y_1|x_0)P(x_0) \\ &= \alpha P(x_1) + \alpha P(x_0) \\ &= \alpha \end{aligned}$$

A probabilidade de erro define o **BER (*Bit Error Rate*)** do canal.
É a taxa de erros por bit.



1. Cenário de Utilização: detalhe



2. Códigos de controlo de erros

- A deteção e correção são obtidas pela introdução de redundância na mensagem original
- Essa redundância é função da mensagem
- Códigos a analisar: repetição; bit de paridade par; Hamming e CRC
- Os códigos de canal são utilizados nos modos:
 - FEC - **F**orward **E**rror **C**orrection
 - ARQ - **A**utomatic **R**epeat **R**e**Q**uest



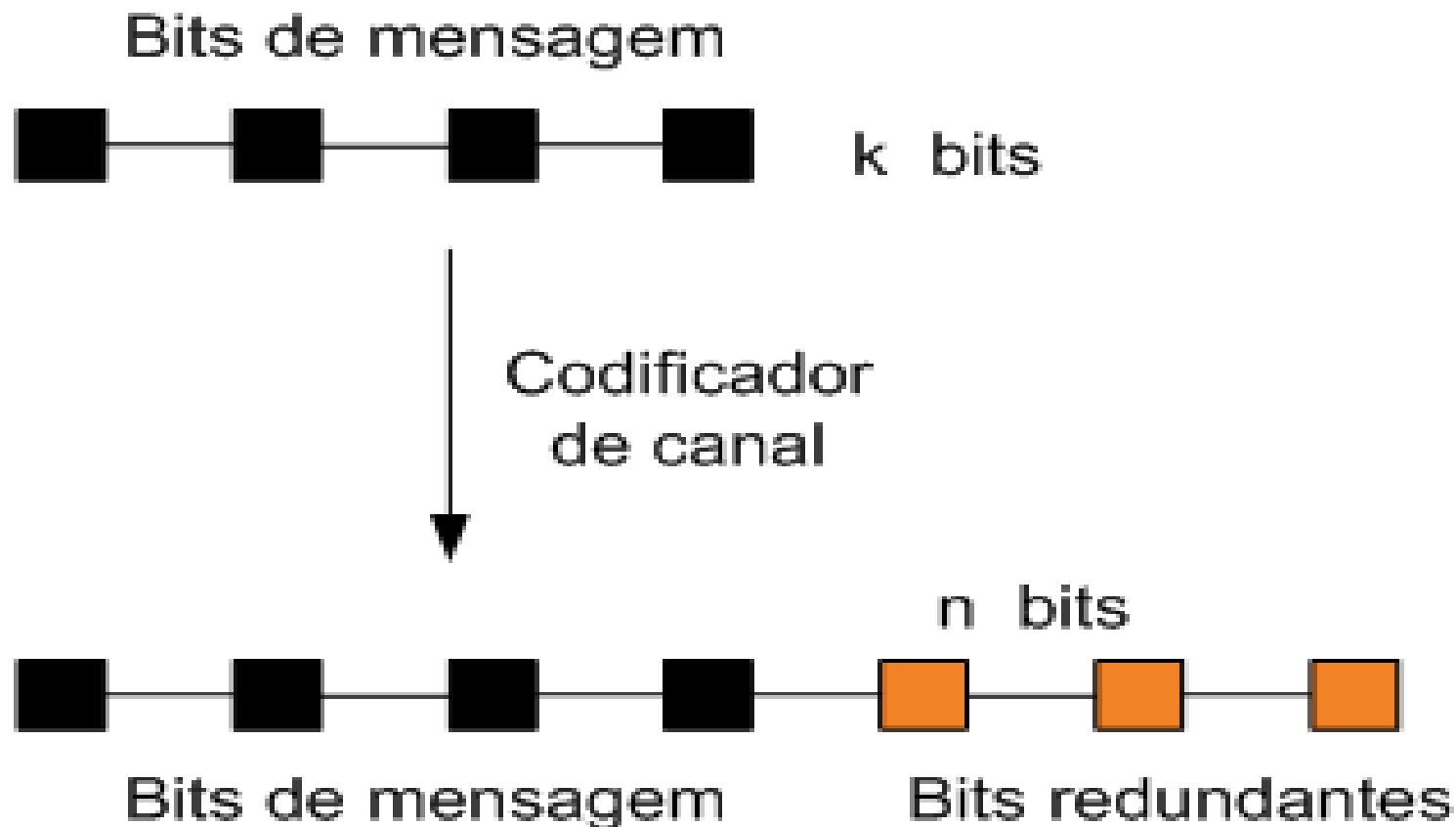
2. Modos de funcionamento

- **FEC - Forward Error Correction**
 - Modo de correção de erros
 - O recetor recebe as palavras, deteta eventuais erros e corrige-os
- **ARQ - Automatic Repeat ReQuest**
 - Modo de deteção de erros
 - O recetor recebe as palavras e deteta eventuais erros; em caso de erro, solicita a retransmissão




2. Códigos de bloco (n,k)

- Codificador de bloco
- Cada bloco de k **bits de mensagem** origina uma **palavra de código** com n bits
- k = número de bits de mensagem
- n = número de bits de palavra de código



2. Códigos de bloco (n,k): propriedades

1. *Code rate* (ritmo) $R = \frac{k}{n}$, medida de eficiência
2. Distância de **Hamming (dH)**: número de dígitos em que diferem duas quaisquer palavras do código
3. **Distância mínima (dmin)**: é a menor distância de Hamming entre duas quaisquer palavras do código; depende da redundância:
Majorante  $d_{\min} \leq 1 + q, \quad q = n - k$
4. Deteta todos os padrões até “l” erros: $l \leq d_{\min} - 1$
5. Corrige todos os padrões até “t” erros: $t \leq \lfloor \frac{d_{\min} - 1}{2} \rfloor$
6. Deteta “l” erros e corrige “t” erros: $d_{\min} \geq l + t + 1$, com $l > t$



Richard Wesley Hamming (1915 – 1998)



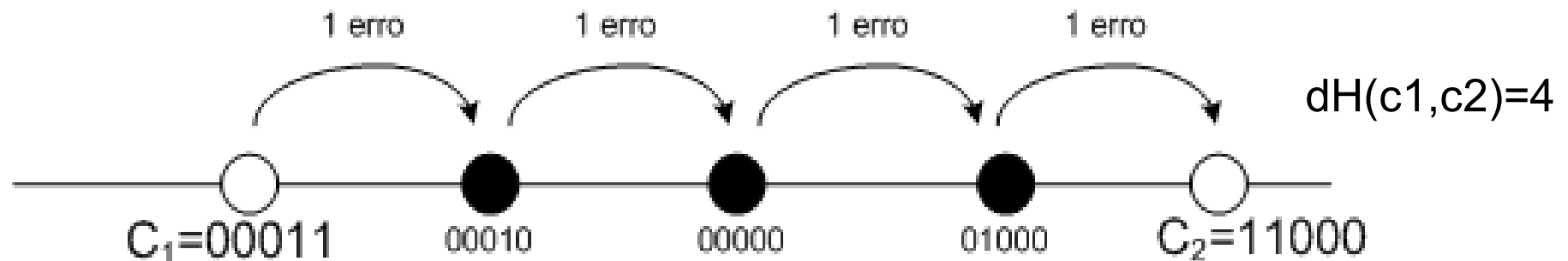
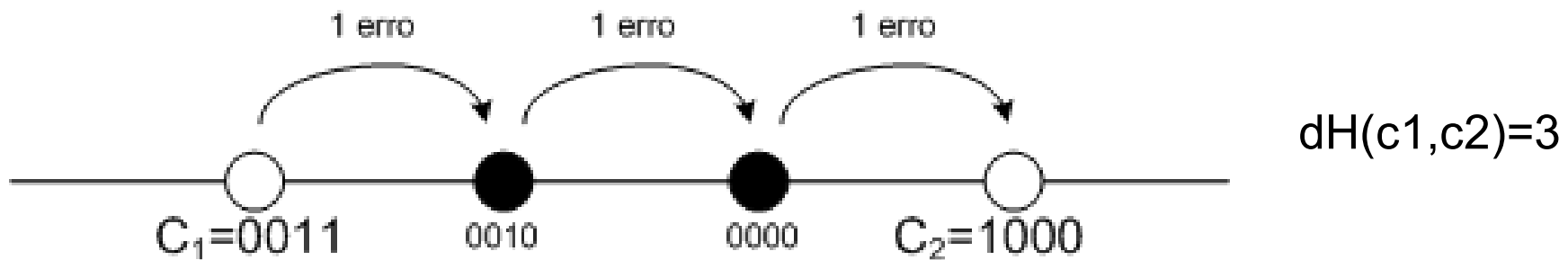
<http://www-history.mcs.st-and.ac.uk/Biographies/Hamming.html>

https://en.wikipedia.org/wiki/Richard_Hamming



2. Códigos de bloco (n,k): distância

- Distância de Hamming entre palavras



2. Códigos lineares de bloco (n,k)

- Bloco: todas as palavras têm a mesma dimensão
- Linear:
 - o vetor nulo pertence ao código
 - a soma modular de quaisquer duas palavras do código é ainda uma palavra do código

n = número de bits da palavra de código

2^n palavras possíveis

k = número de bits da mensagem

2^k palavras de código

$q = n - k$, é o número de bits redundantes

Seja $\mathbf{m} = [m_0 \ m_1 \ \dots \ m_{k-1}]$ a mensagem e \mathbf{c} a palavra de código

Podem ser sistemáticos ou não sistemáticos; exemplos destas formas:

• sistemática: $\mathbf{c} = [m_0 \ m_1 \ \dots \ m_{k-1} \ b_0 \ b_1 \ \dots \ b_{q-1}]$

• não sistemática: $\mathbf{c} = [m_0 \ b_1 \ b_0 \ m_1 \ \dots \ m_{k-1} \ \dots \ b_{q-1}]$



2. Códigos lineares de bloco (n,k)

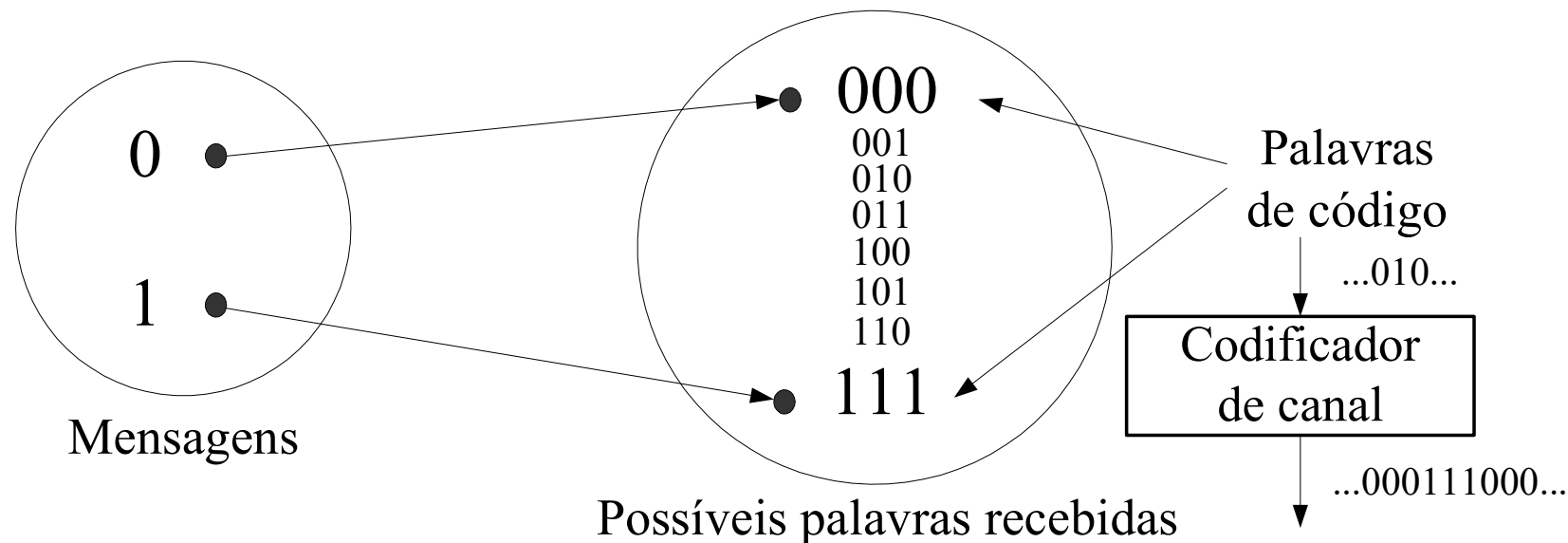
- O desenho de códigos eficientes é um problema complexo: maximizar d_{\min} com restrição R ou maximizar R com restrição d_{\min}
- São problemas adicionais: memória ocupada e complexidade do codificador e do decodificador
- Através dos conceitos de estrutura algébrica e espaço vetorial definem-se os códigos lineares (elementos de sub-espaço vetorial)
- Os códigos lineares são um sub-conjunto de todos os códigos; requerem menos memória e existem codificadores e decodificadores simples



2. Código de repetição (3,1)

- Consiste na repetição da mensagem
- Exemplo: código (3,1), na forma (n,k) com k=1 bit de mensagem e n=3 bit na palavra de código

m	c
0	000
1	111



Usa $2^k = 2^1 = 2$ palavras de $2^n = 2^3 = 8$ possíveis



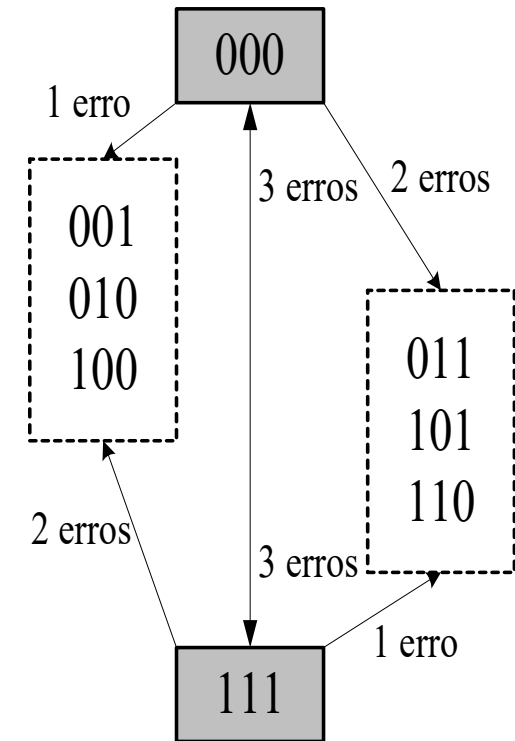
2. Código de repetição (3,1)

- Descodificação realizada por maioria
- A **distância** entre as palavras de código, garante que:
 - Deteta todos os erros de 1 e 2 bit
 - Corrige todos os erros de 1 bit

Considerando um BSC com $\alpha = 10^{-5}$,
tem-se que:

$$\begin{aligned} P(1, 3) &= C_1^3 \alpha^1 (1 - \alpha)^2 = \frac{3!}{2!1!} \alpha (1 - \alpha)^2 \\ &= 3\alpha - 6\alpha^2 + 3\alpha^3 \approx 3 \times 10^{-5} \end{aligned}$$

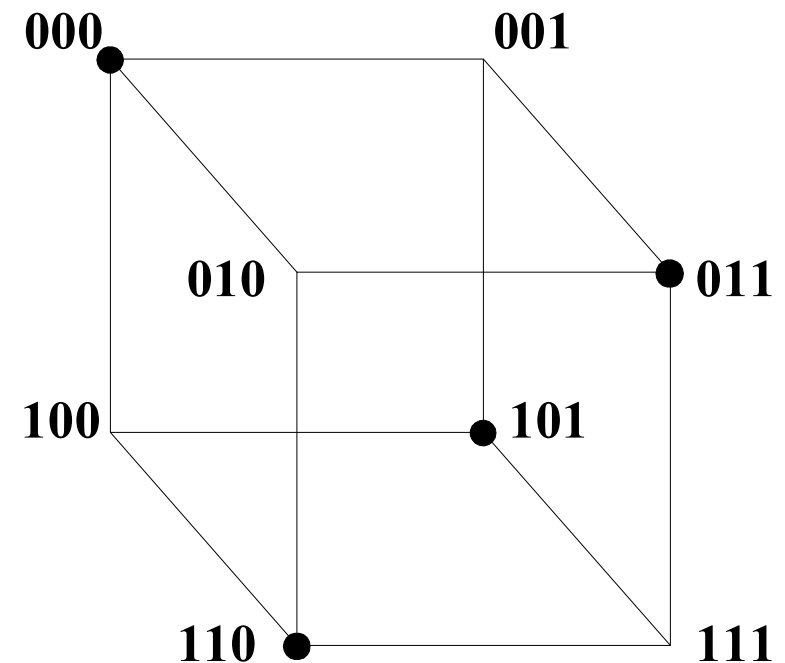
$$\begin{aligned} P(2, 3) &= C_2^3 \alpha^2 (1 - \alpha)^1 = \frac{3!}{1!2!} \alpha^2 (1 - \alpha) \\ &= 3\alpha^2 - 3\alpha^3 \approx 3 \times 10^{-10} \end{aligned}$$



2. Código bit de paridade (3,2) - paridade par

- Adicionar um bit no final da mensagem; este bit é a soma módulo 2 dos bits da mensagem
- A palavra de código é $\mathbf{c} = [m_0 \ m_1 \ m_0 \oplus m_1]$

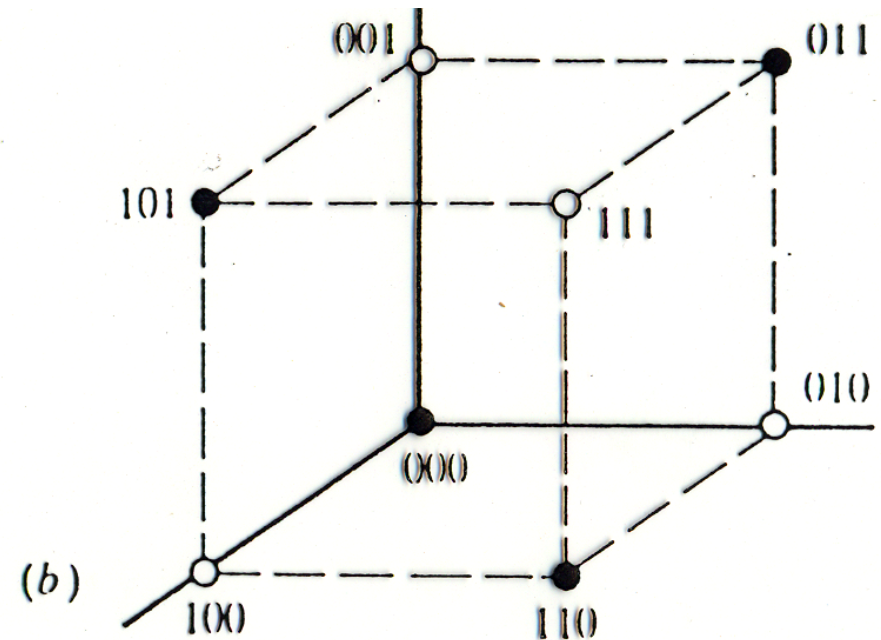
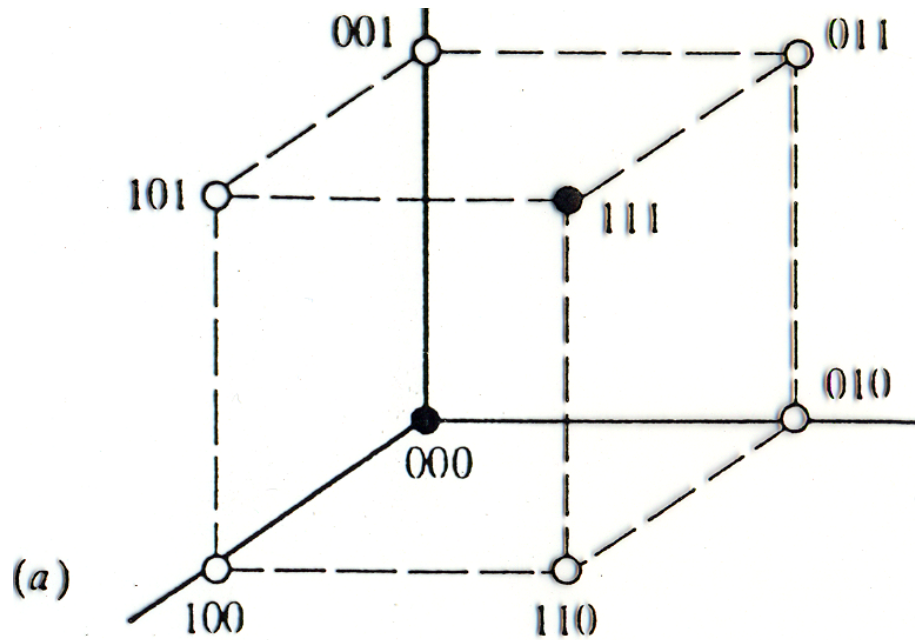
m	c
00	000
01	011
10	101
11	110



- Deteta a presença de 1 e 3 bits errados
- Não tem capacidade de correção; não realiza FEC



2. Palavras de código: vetores



- Palavras de 3 bit

(a) código de repetição (3,1); 3 arestas entre as 2 palavras de código

(b) código de bit de paridade (3,2); 2 arestas entre 2 palavras de código mais próximas



2. Peso de Hamming

- Define-se peso de Hamming (w) como o número de dígitos não nulos numa palavra
- Sejam c_i e c_j duas palavras distintas de um código linear de bloco; tem-se por definição que $d_{\min} = \min_{i \neq j} dH(c_i, c_j)$
- Dado que o código é linear, tem-se:

$$d_{\min} = \min w(c_i \oplus c_j) = \min w(c_k), \quad \text{soma modular}$$

sendo c_k palavra do código, diferente do vetor nulo

Exemplos:

Código de repetição (3,1)

m	c	w(c)	$d_{\min} = 3$
0	000	0	$l = 2$
1	111	3	$t = 1$

Código de bit de paridade par (3,2)

m	c	w(c)	$d_{\min} = 2$
00	000	0	$l = 1$
01	011	2	$t = 0$
10	101	2	
11	110	2	



2. Códigos de Hamming

- Família de códigos lineares de bloco
- Têm $d_{\min}=3$, logo corrigem todos os erros de 1 bit
- A motivação: $P(2, n) \ll P(1, n)$
- Definidos por um parâmetro inteiro $m (\geq 2)$ tal que:

$$(n, k) = (2^m - 1, 2^m - 1 - m)$$

Por exemplo, com $m=3$ tem-se o código (7,4)

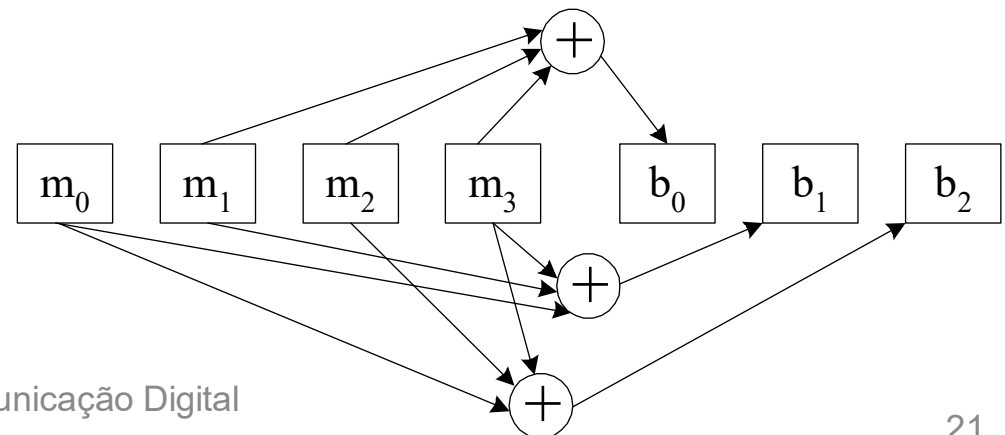
$$\mathbf{c} = [m_0 \ m_1 \ m_2 \ m_3 \ b_0 \ b_1 \ b_2]$$

Equações de paridade:

$$b_0 = m_1 \oplus m_2 \oplus m_3$$

$$b_1 = m_0 \oplus m_1 \oplus m_3$$

$$b_2 = m_0 \oplus m_2 \oplus m_3$$



2. Hamming (7,4): todas as palavras

Listagem das 16 palavras de código e respectivos pesos de Hamming

<u>Palavra de código</u>							<u>Peso</u>	<u>Palavra de código</u>							<u>Peso</u>
0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	3
0	0	0	1	1	1	1	4	1	0	0	1	1	0	0	3
0	0	1	0	1	0	1	3	1	0	1	0	1	1	0	4
0	0	1	1	0	1	0	3	1	0	1	1	0	0	1	4
0	1	0	0	1	1	0	3	1	1	0	0	1	0	1	4
0	1	0	1	0	0	1	3	1	1	0	1	0	1	0	4
0	1	1	0	0	1	1	4	1	1	1	0	0	0	0	3
0	1	1	1	1	0	0	4	1	1	1	1	1	1	1	7

O menor peso de Hamming para palavras não nulas é 3, logo:

$$d_{\min} = 3, \quad l = 2 \text{ e } t = 1$$



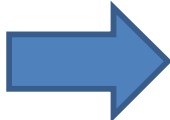
2. Códigos de Hamming (caraterísticas)

- Seja k o número de *bits* da mensagem a transmitir e n o número de *bits* efetivamente transmitidos
- Códigos de Hamming são códigos de bloco linear (n,k) onde:
 - $q \geq 3$, sendo $q = n - k$ o número de *bits* redundantes
 - $n = 2^q - 1$
 - para $q = \{1, 2, 3, \dots\}$, temos então $(7,4), (15,11), (31,26), \dots$
- A eficiência do código (*code rate*) é $r_c = k/n = 1 - q/(2^q - 1)$
 - $r_c \rightarrow 1$, se $q \gg 1$
- $d_{\min} = 3$, independentemente de q



2. Códigos Cíclicos - CRC

- Os códigos cíclicos são uma sub-classe dos códigos lineares de bloco
 - Linear:** o vetor nulo pertence ao código; a soma modular de duas palavras do código é ainda uma palavra do código
 - Bloco:** todas as palavras têm a mesma dimensão de n bits
- Nos códigos cíclicos tem-se que qualquer rotação cíclica de qualquer ordem sobre uma palavra de código é ainda uma palavra de código
- Exemplo: código de bit de paridade par (3,2)



m	c
00	000
01	011
10	101
11	110



2. Códigos Cíclicos

- Tem-se $\mathbf{c(X) = m(X)g(X)}$ em que:
 - $c(x)$ é a palavra de código – polinómio de grau $n-1$
 - $m(x)$ depende da mensagem – polinómio de grau $k-1$
 - $g(x)$ – polinómio gerador de grau q
- As palavras de código $\mathbf{c=[c_{n-1} \ c_{n-2} \ \ c_1 \ c_o]}$ podem ser analisadas como polinómios:
 - $\mathbf{c(X) = c_{n-1} X^{n-1} + c_{n-2} X^{n-2} + + c_1 X + c_o}$
- O número de bits redundantes (de paridade) corresponde ao grau do polinómio gerador



2. Polinómio Gerador

- Determinado polinómio $g(X)$ de grau q é gerador de um código (n,k) , com $q=n-k$, caso seja factor de X^n+1
- Ser fator de X^n+1 implica que $\text{resto}\left[\frac{X^n+1}{g(X)}\right]=0$
- Assim, a fatorização do polinómio X^n+1 é importante, neste contexto
- Através desta fatorização, conseguimos obter polinómios geradores para códigos de diferentes dimensões



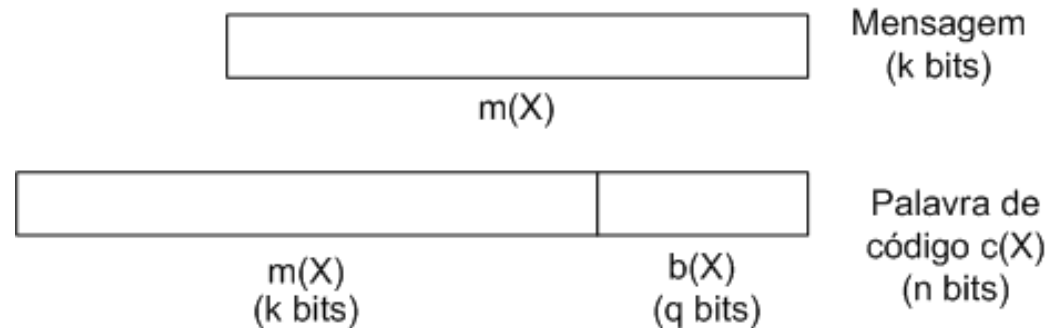
2. Polinómios Geradores

Código	Polinómio gerador $g(X)$
CRC4	$X^4+X^3+X^2+X+1$
CRC7	$X^7+X^6+X^4+1$
CRC12	$X^{12}+X^{11}+X^3+X^2+X+1$
CRC16	$X^{16}+X^{15}+X^2+1$
CRC-CCITT	$X^{16}+X^{12}+X^5+1$
CRC32	$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$



2. CRC – Cyclic Redundancy Check

- Num código cíclico sistemático, as palavras têm a seguinte organização



- Os bits $b(X)$, que constituem um polinómio de grau $q-1$ designam-se por **CRC-Cyclic Redundancy Check**
- A palavra de código é dada por

$$c(X) = m(X)X^q + b(X) = m(X)X^q + \text{resto} \left[\frac{m(X)X^q}{g(X)} \right]$$



2. CRC – Cyclic Redundancy Check

- O CRC resulta do resto da divisão de polinómios entre:
 - A mensagem deslocada de q bits para a esquerda
 - O polinómio gerador do código

$$CRC = b(X) = \text{resto} \left[\frac{m(X)X^q}{g(X)} \right]$$

- Dado que $g(X)$ tem grau q , resulta que $b(X)$ terá grau $q-1$, sendo constituído por q bits
- Assim, temos palavra de código com n bits (k de mensagem e q de paridade)



2. CRC – Cyclic Redundancy Check

- Exemplo de cálculo do CRC para código (7,4)

- $m(X) = X^3 + 1 = [1 \ 0 \ 0 \ 1]$
- $g(X) = X^3 + X^2 + 1 = [1 \ 1 \ 0 \ 1]$

$$\begin{aligned} CRC = b(X) &= \text{resto} \left[\frac{m(X)X^q}{g(X)} \right] = \text{resto} \left[\frac{(X^3 + 1)X^3}{X^3 + X^2 + 1} \right] = \text{resto} \left[\frac{X^6 + X^3}{X^3 + X^2 + 1} \right] \\ &= X + 1 \end{aligned}$$

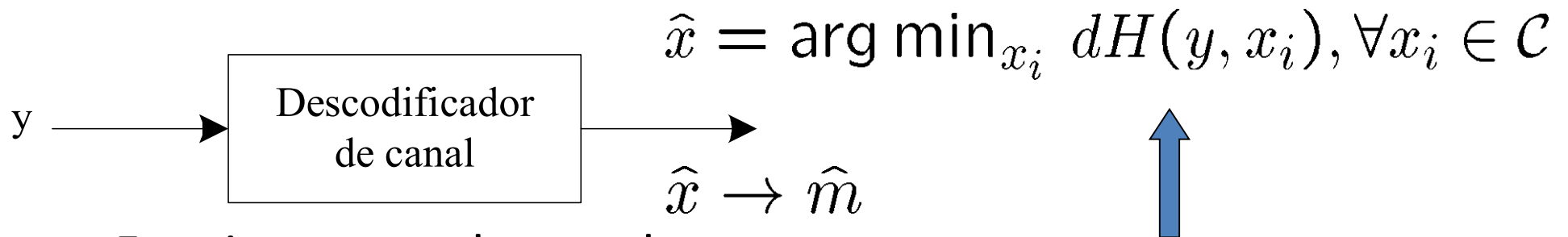
$$\begin{array}{r} 1001000 \\ 1101 \\ 01000 \\ 1101 \\ 01010 \\ 1101 \\ 01110 \\ 1101 \\ 0\mathbf{011} \end{array} \quad \begin{array}{r} 1101 \\ \hline 1111 \end{array}$$

$$\begin{aligned} c(X) &= m(X)X^3 + b(X) = (X^3 + 1)X^3 + (X + 1). \\ &= X^6 + X^3 + X + 1 \\ &= [1001 \ 011] \end{aligned}$$



3. Descodificador de canal: características

- O decodificador:
 1. recebe a palavra \mathbf{y} (possivelmente com erros)
 2. estima a palavra de código \hat{x} que lhe deu origem
 3. estima a mensagem \hat{m}

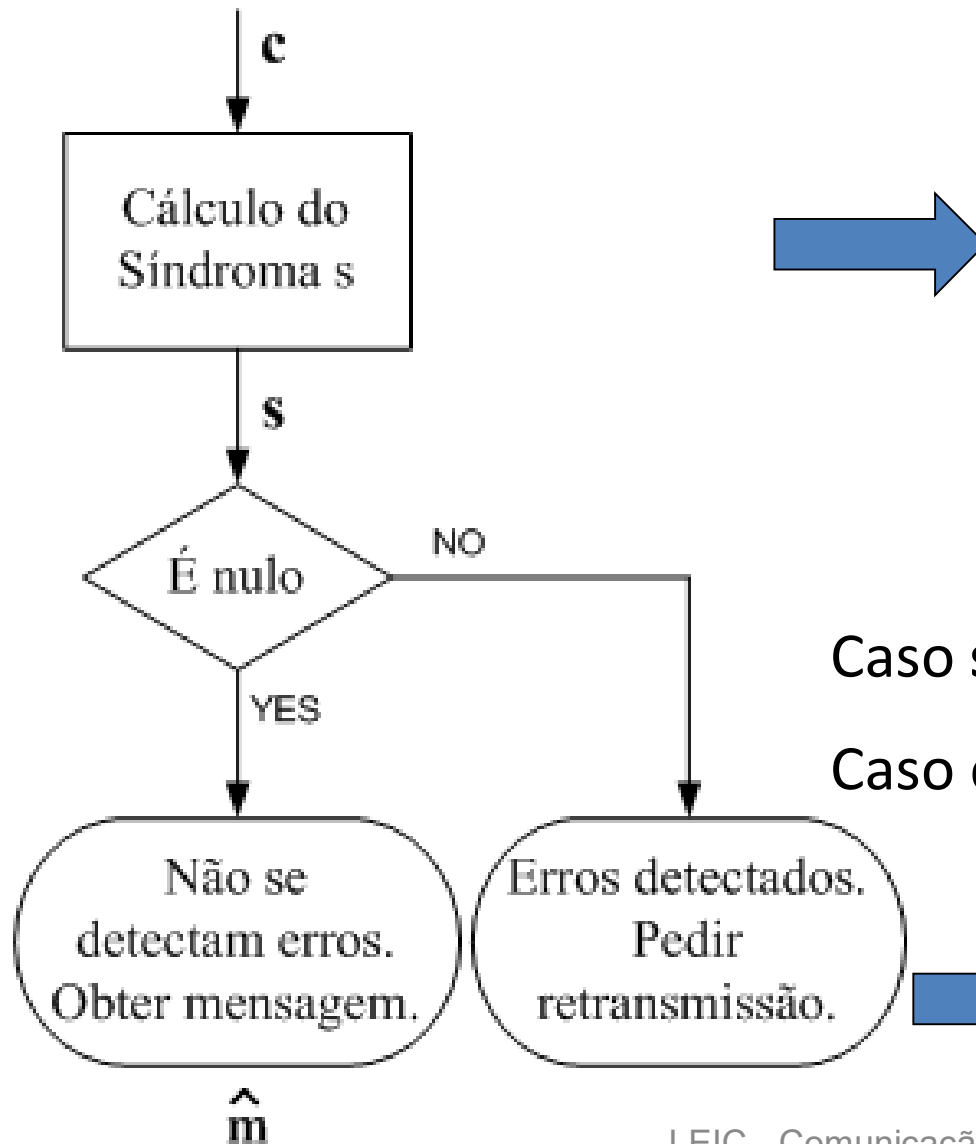


- Funciona num dos modos:
 1. deteção
 2. correção
 3. deteção e correção
- Se a palavra recebida \mathbf{y} não pertence ao código, houve erro(s)



3. Descodificação: deteção

- Processo de descodificação em modo **deteção (ARQ)**



Síndroma

= conjunto de sintomas

= comparação bit a bit entre os bits de paridade transmitidos e recalculados no decodificador

Caso s seja nulo, não se detetam erros

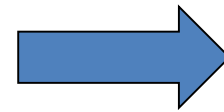
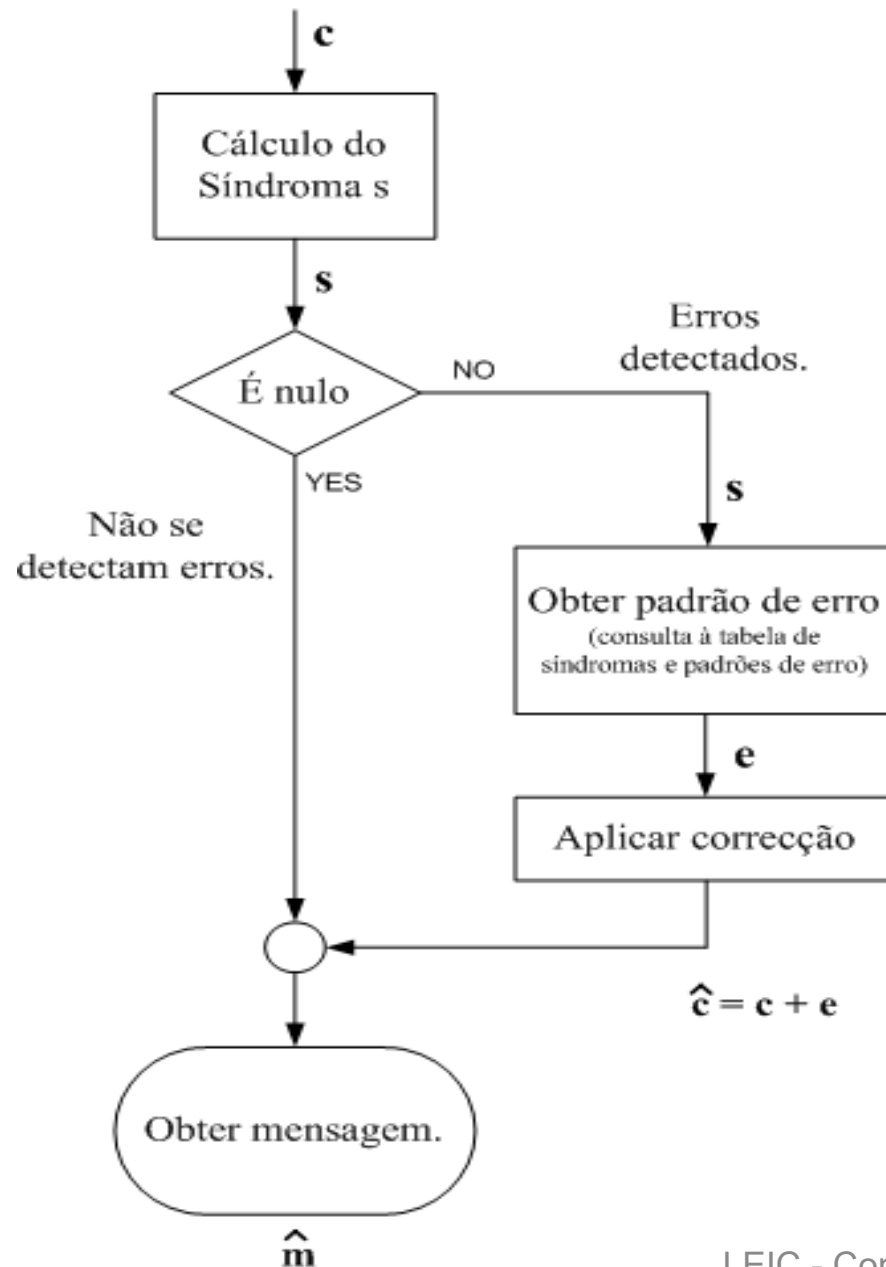
Caso contrário, existem erros detetados

É necessário que o SCD possibilite este pedido de retransmissão



3. Descodificação: correção

- Processo de descodificação em modo **correção (FEC)**



Mecanismo de
correção



3. Descodificação: correção

- Tabela de síndromas para o código Hamming(7,4)
- O código tem $2^3=8$ síndromas: síndrome nulo - ausência de erro; os outros 7 correspondem aos padrões de um bit em erro por palavra

Síndrome	Padrão de Erro	Observações
000	0000000	Ausência de erro
011	1000000	1.º bit em erro
110	0100000	2.º bit em erro
101	0010000	3.º bit em erro
111	0001000	4.º bit em erro
100	0000100	5.º bit em erro
010	0000010	6.º bit em erro
001	0000001	7.º bit em erro



3. Descodificação: correção

s	e
000	0000000
011	1000000
110	0100000
101	0010000
111	0001000
100	0000100
010	0000010
001	0000001

- Sejam as palavras de código
 - $c_1 = [1\ 0\ 0\ 0\ 0\ 1\ 1]$
 - $c_2 = [0\ 0\ 1\ 1\ 0\ 1\ 0]$
- Sejam as palavras recebidas no decodificador
 - $y_1 = c_1 + [1\ 0\ 0\ 0\ 0\ 0\ 0] = [\underline{0}\ 0\ 0\ 0\ 0\ 1\ 1]$
 - $y_2 = c_2 + [0\ 0\ 1\ 0\ 0\ 0\ 0] = [0\ 0\ \underline{0}\ 1\ 0\ 1\ 0]$
 - $y_3 = c_1 + [1\ 1\ 0\ 0\ 0\ 0\ 0] = [\underline{0}\ \underline{1}\ 0\ 0\ 0\ 1\ 1]$
- Os síndromas obtidos são
 - $s_1 = [0\ 1\ 1]$
 - $s_2 = [1\ 0\ 1]$
 - $s_3 = [1\ 0\ 1]$



Dois erros na palavra



3. Descodificação: correção

s	e
000	0000000
011	1000000
110	0100000
101	0010000
111	0001000
100	0000100
010	0000010
001	0000001

- Os padrões de erro associados são
 - $e_1 = [1\ 0\ 0\ 0\ 0\ 0\ 0]$
 - $e_2 = [0\ 0\ 1\ 0\ 0\ 0\ 0]$
 - $e_3 = [0\ 0\ 1\ 0\ 0\ 0\ 0]$
- As palavras estimadas são
 - $c_1 = y_1 + e_1 = [\underline{0}\ 0\ 0\ 0\ 0\ 1\ 1] + [1\ 0\ 0\ 0\ 0\ 0\ 0] = [1\ 0\ 0\ 0\ 0\ 1\ 1]$
 - $c_2 = y_2 + e_2 = [0\ 0\ \underline{0}\ 1\ 0\ 1\ 0] + [0\ 0\ 1\ 0\ 0\ 0\ 0] = [0\ 0\ 1\ 1\ 0\ 1\ 0]$
 - $c_3 = y_3 + e_3 = [\underline{0}\ \underline{1}\ 0\ 0\ 0\ 1\ 1] + [0\ 0\ 1\ 0\ 0\ 0\ 0] = [0\ 1\ 1\ 0\ 0\ 1\ 1]$
- As mensagens obtidas após correção

- $m_1 = [1\ 0\ 0\ 0]$

- $m_2 = [0\ 0\ 1\ 1]$

- $m_3 = [0\ 1\ 1\ 0]$

Os dois erros na palavra implicaram erro após correção (t=1)



3. CRC – Cyclic Redundancy Check

- O decodificador, em modo de deteção calcula o síndrome $s(X)$
- Dado que $c(X)=m(X)g(X)$, tem-se que qualquer palavra de código é fator do polinómio gerador
- Seja $y(X) = c(X) + e(X)$ a palavra recebida, em que $e(X)$ é o padrão de erro

- **Caso $e(X)$ seja nulo o síndrome é nulo**

$$s(X) = \text{resto} \left[\frac{y(X)}{g(X)} \right] = \text{resto} \left[\frac{c(X)}{g(X)} \right] = \text{resto} \left[\frac{m(X)g(X)}{g(X)} \right] = 0$$

- **Caso $e(X)$ seja não nulo o síndrome é não nulo e depende do valor de $e(X)$**

$$s(X) = \text{resto} \left[\frac{y(X)}{g(X)} \right] = \text{resto} \left[\frac{m(X)g(X) + e(X)}{g(X)} \right] = \text{resto} \left[\frac{e(X)}{g(X)} \right]$$



3. CRC – Cyclic Redundancy Check

- Na descodificador temos divisão de polinómios $s(X) = \text{resto} \left[\frac{c(X)}{g(X)} \right]$
- Recorrendo ao MATLAB, podemos usar a função *deconv*
- Sejam $c(X) = X^6 + X^3 + X + 1$ $g(X) = X^3 + X^2 + 1$
 $= [1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1]$ $= [1 \ 1 \ 0 \ 1]$

```
>> c = [1 0 0 1 0 1 1];
```

```
>> g = [1 1 0 1];
```

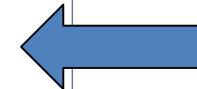
```
>> [q, s] = deconv(c, g);
```

```
>> mod(s,2)
```

```
ans =
```

```
0 0 0 0 0 0 0
```

Síndrome nulo



**Ausência de
erros**



3. CRC – Cyclic Redundancy Check

- Introduzindo 1 erro no penúltimo bit na palavra $c(X)$ temos

$$y(X) = c(X) + e(X) = (X^6 + X^3 + X + 1) + (X)$$

$$= X^6 + X^3 + 1$$

$$= [1\ 0\ 0\ 1\ 0\ 0\ 1]$$

$$g(X) = X^3 + X^2 + 1$$
$$= [1\ 1\ 0\ 1]$$

```
>> c = [1 0 0 1 0 0 1];
```

```
>> g = [1 1 0 1];
```

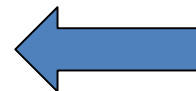
```
>> [q, s] = deconv(c, g);
```

```
>> mod(s,2)
```

```
ans =
```

```
0 0 0 0 0 1 0
```

Síndrome não nulo



Erros detetados



3. CRC - *Cyclic Redundancy Check*

- Tipicamente é utilizado em modo de **deteção** de erros
- Quando a distância mínima do código for maior ou igual a 3, também pode ser usado em modo **correção**
- Tipicamente temos um número reduzido de bits de paridade calculado para elevado número de bits de mensagem
 - $n \gg q > 1$
- O CRC tem elevada capacidade de deteção de erros, especialmente de *burst* de erros (rajada de erros)
- Um *burst* ou rajada de erros define-se como um bloco contíguo de bits recebidos em erro; o primeiro e último *bit* distam B bits entre si, sendo B o comprimento do *burst*



3. CRC - *Cyclic Redundancy Check*

- Elevada capacidade de deteção de erros:
 - todos os *burst* de dimensão q ou menor
 - uma fração dos *burst* de dimensão $q+1$; a fração é $1-2^{-(q-1)}$
 - uma fração dos *burst* de dimensão superior a $q+1$; a fração é $1-2^{-q}$
 - todas as combinações de d_{\min} ou menos erros
 - todos os padrões com número ímpar de erros, quando o gerador tem número par de coeficientes não nulos
- Por exemplo, para o código CRC7 com $g(X)=X^7+X^6+X^4+1$ temos
 - todos os *burst* de dimensão 7 ou menor
 - $1-2^{-(q-1)} = 1 - 2^{-(7-1)} = 98,44\%$ dos *burst* de dimensão 8
 - $1-2^{-(q)} = 1 - 2^{-(7)} = 99,22\%$ dos *burst* de dimensão superior a 8
 - todos os padrões com número ímpar de erros



3. Comparação de códigos

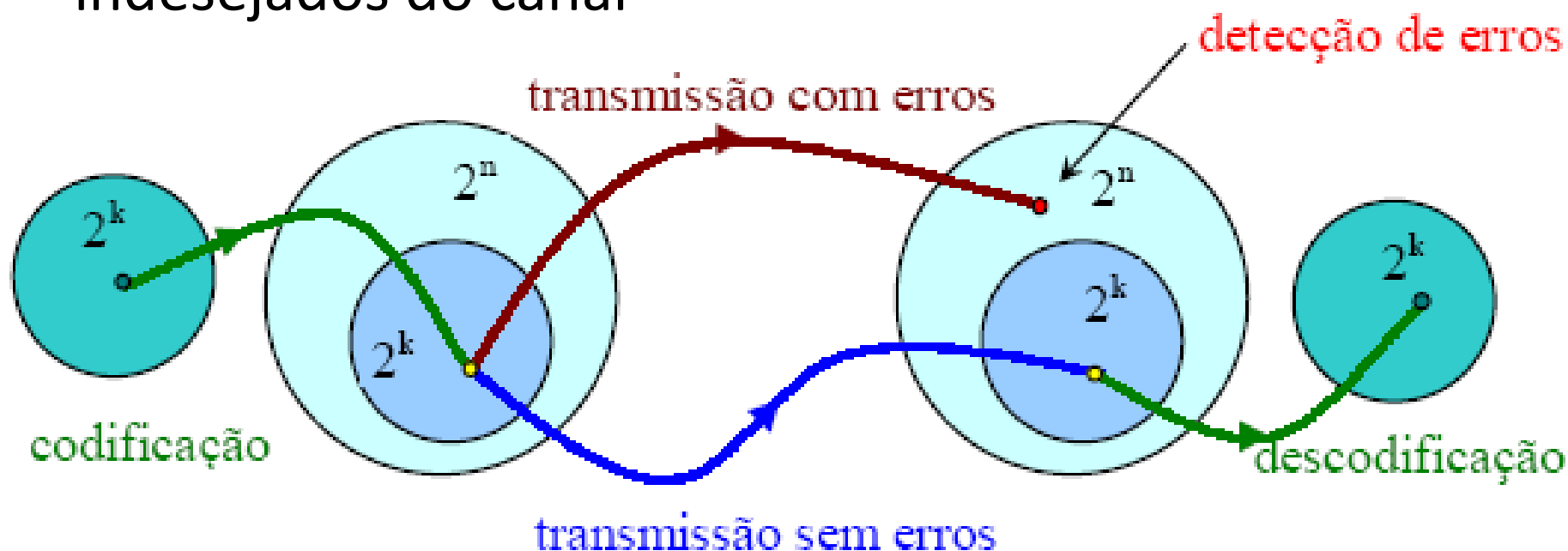
Análise comparativa de códigos: ritmo e capacidades de deteção e correção de erros.

Código	$R = k/n$	d_{min}	Deteta l	Corrige t
Repetição (2,1)	0.500	2	1	0
Repetição (3,1)	0.333	3	2	1
Repetição (4,1)	0.250	4	3	1
Repetição (5,1)	0.200	5	4	2
Paridade (3,2)	0.666	2	1	0
Paridade (8,7)	0.875	2	1	0
Hamming (7,4) m=3	0.571	3	2	1
Hamming (15,11) m=4	0.733	3	2	1
Hamming (31,26) m=5	0.838	3	2	1



4. Análise matricial dos códigos

- Aumentar a robustez do SCD relativamente aos efeitos indesejados do canal



- Cada bloco de k bits de mensagem dá origem a uma palavra de código com n bits
 - 2^k palavras de código no espaço de 2^n palavras



4. Matriz Geradora

- As palavras de código **c** são obtidas através do produto do vetor mensagem **m** pela matriz geradora do código **G**

$$\mathbf{c} = \mathbf{m} \times \mathbf{G}$$

- c** é vetor de dimensões $1 \times n$; **m** é vetor $1 \times k$
- G** é matriz $k \times n$; nos códigos sistemáticos temos
 - G** = $[\mathbf{I}_k \mid \mathbf{P}]$ ou **G** = $[\mathbf{P} \mid \mathbf{I}_k]$ sendo **P** a **sub-matriz geradora de paridade**, ou seja, a matriz que estabelece as equações de paridade do código
 - Cada coluna de **P** constitui uma equação de paridade
 - P** tem dimensões $k \times q$



4. Matriz Geradora

- Exemplos de matrizes geradoras
- Código de repetição (3,1)

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

- Código de bit de paridade par (3,2)

$$G = [I_2 \ P] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \text{ou} \quad G = [P \ I_2] = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$



4. Códigos de Hamming

- Família de códigos lineares de bloco
- Têm $d_{\min}=3$, logo corrigem todos os erros de 1 bit
- A motivação: $P(2, n) \ll P(1, n)$
- Definidos por um parâmetro inteiro $m (\geq 2)$ tal que:

$$(n, k) = (2^m - 1, 2^m - 1 - m)$$

Por exemplo, com $m=3$ tem-se o código (7,4)

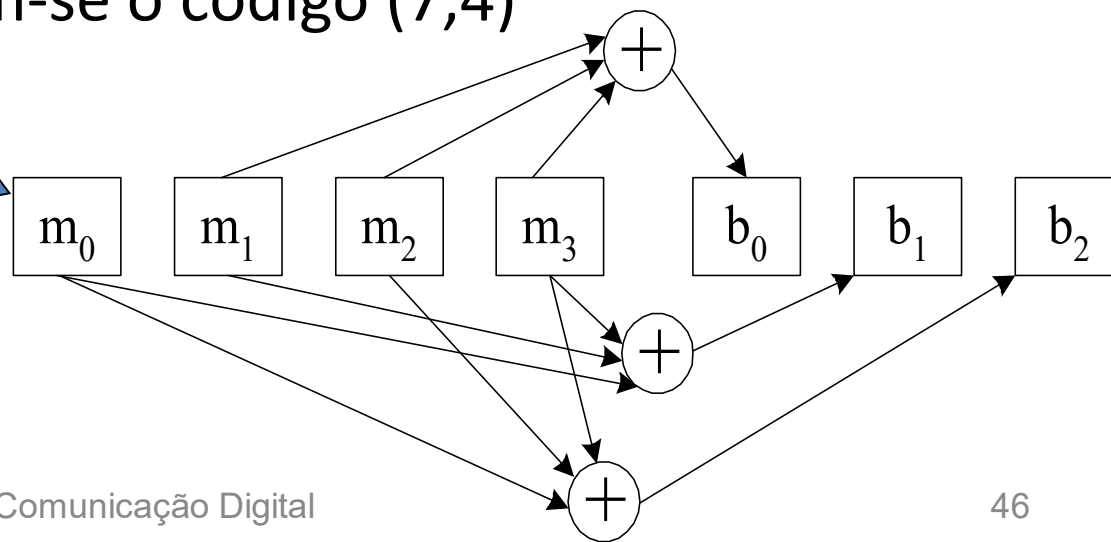
$\mathbf{c} = [m_0 \ m_1 \ m_2 \ m_3 \ b_0 \ b_1 \ b_2]$

Equações de paridade:

$$b_0 = m_1 \oplus m_2 \oplus m_3$$

$$b_1 = m_0 \oplus m_1 \oplus m_3$$

$$b_2 = m_0 \oplus m_2 \oplus m_3$$



4. Códigos de Hamming: forma matricial

$$c = mG = m [I_4 \mid P]$$

$$= \begin{bmatrix} m_0 & m_1 & m_2 & m_3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} m_0 & m_1 & m_2 & m_3 & b_0 & b_1 & b_2 \end{bmatrix}$$

- **G** é a matriz geradora do código
- Cada linha de **G** é uma palavra do código
- Todas as palavras do código são obtidas por combinação linear das linhas de **G**
- **G** é um conjunto de vetores linearmente independentes
- Gera 16 vetores de um total possível de 128; base de sub-espço vetorial



4. Cálculos em MATLAB

```
>> [H,G,n,k] = hamngen(3);
```

```
>> G
```

```
G =
```

1	1	0	1	0	0	0
0	1	1	0	1	0	0
1	1	1	0	0	1	0
1	0	1	0	0	0	1

```
>> n, k
```

```
n =
```

```
7
```

```
k =
```

```
4
```

← m=3

- **G** está na forma sistemática

$$G = [P \mid I_4]$$

- As equações de paridade são diferentes das apresentadas no exemplo anterior



4. Cálculos em MATLAB

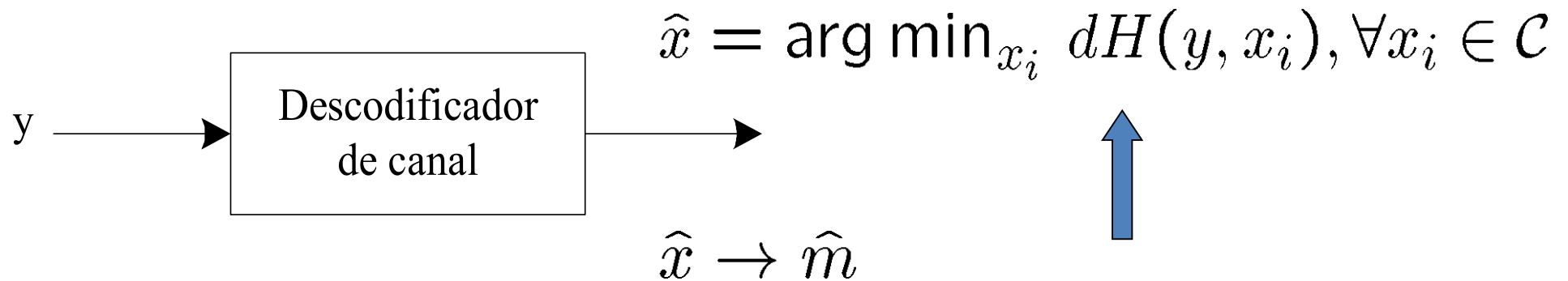
```
>> m1 = [0 1 0 1]; m2 = [1 1 0 1];  
>> c1 = mod ( m1*G, 2 )  
c1 =  
    1    1    0    0    1    0    1  
>> c2 = mod ( m2*G, 2 )  
c2 =  
    0    0    0    1    1    0    1
```

- Entre as mensagens m1 e m2 muda apenas um bit; entre as palavras de código c1 e c2 mudam três bits
- c1 resulta da soma módulo 2 da segunda e quarta linhas de **G**
- c2 resulta da soma módulo 2 da primeira, segunda e quarta linhas de **G**



4. Descodificador de canal: características

- O decodificador:
 1. recebe a palavra \mathbf{y} (possivelmente com erros)
 2. estima a palavra de código \hat{x} que lhe deu origem
 3. estima a mensagem \hat{m}



- Funciona num dos modos:
 1. deteção
 2. correção
 3. deteção e correção
- Se a palavra recebida \mathbf{y} não pertence ao código, houve erro(s)



4. Codificação / decodificação

- O codificador gera as palavras de código através da **matriz geradora G** , com

$$\mathbf{c} = \mathbf{m} \times \mathbf{G}$$

- No caso dos códigos sistemáticos temos $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{P}]$ sendo \mathbf{P} a **submatriz geradora de paridade**.
- A **matriz de controlo de paridade H** definida por $\mathbf{H} = [\mathbf{P}^T \mid \mathbf{I}_{n-k}]$ permite verificar se existem erros na palavra recebida \mathbf{c} , através do cálculo do **síndroma** (conjunto de sintomas)

$$\mathbf{s} = \mathbf{c} \times \mathbf{H}^T$$

- Caso \mathbf{s} seja nulo, não se detetam erros
- Caso contrário, existem erros detetados



4. Codificação / decodificação

- Codificação e decodificação matricial
- Na codificação temos

$$\mathbf{c} = \mathbf{m} \times \mathbf{G} = \mathbf{m} \times [\mathbf{I}_k \mid \mathbf{P}] = [\mathbf{m}_0 \mathbf{m}_1 \dots \mathbf{m}_{k-1} \quad \mathbf{b}_0 \mathbf{b}_1 \dots \mathbf{b}_{q-1}],$$

de forma a obter a concatenação *k bits mensagem / q bits de paridade*.

- Na decodificação é necessário obter os bits de mensagem, recalculer a paridade sobre estes e comparar com os bits de paridade enviados
- Para tal usa-se a **matriz de controlo de paridade** $\mathbf{H} = [\mathbf{P}^T \mid \mathbf{I}_{n-k}]$ no cálculo do **síndroma**

$$\mathbf{s} = \mathbf{cH}^T = \mathbf{mGH}^T = \mathbf{m} \begin{bmatrix} \mathbf{I}_k & \mathbf{P} \end{bmatrix} \begin{bmatrix} \mathbf{P} \\ \mathbf{I}_q \end{bmatrix} = [s_0 s_1 \dots s_{q-1}]$$



4. Descodificação

- O **síndroma** é um vetor de q bits (\mathbf{H}^T tem dimensões $n \times q$).
- Cada bit do síndrome corresponde à verificação da presença de erros no respectivo bit de paridade
- Na ausência de erros temos síndrome nulo porque \mathbf{GH}^T são ortogonais

$$\mathbf{s} = \mathbf{cH}^T = \mathbf{mGH}^T = m \begin{bmatrix} I_k & P \end{bmatrix} \begin{bmatrix} P \\ I_q \end{bmatrix} = [00 \cdots 0]$$

- Erros são detetados sempre que o síndrome não é nulo
- O valor do síndrome só depende do padrão de erro \mathbf{e} ; não depende da palavra de código

$$\mathbf{s} = (\mathbf{c} + \mathbf{e})\mathbf{H}^T = \mathbf{cH}^T + \mathbf{eH}^T = [00 \cdots 0] + \mathbf{eH}^T = \mathbf{eH}^T.$$



4. Descodificação

- Cada padrão de 1 bit em erro, tem um síndromea único associado
- Sejam os padrões de erro
 - $e_1 = [1\ 0\ \dots\ 0]$, que corresponde ao primeiro bit errado
 - $e_2 = [0\ 1\ \dots\ 0]$, que corresponde ao segundo bit errado
- Para uma palavra de código \mathbf{c} temos

$$\mathbf{s}_1 = \mathbf{e}_1 \mathbf{H}^T = \text{primeira linha de } \mathbf{H}^T.$$

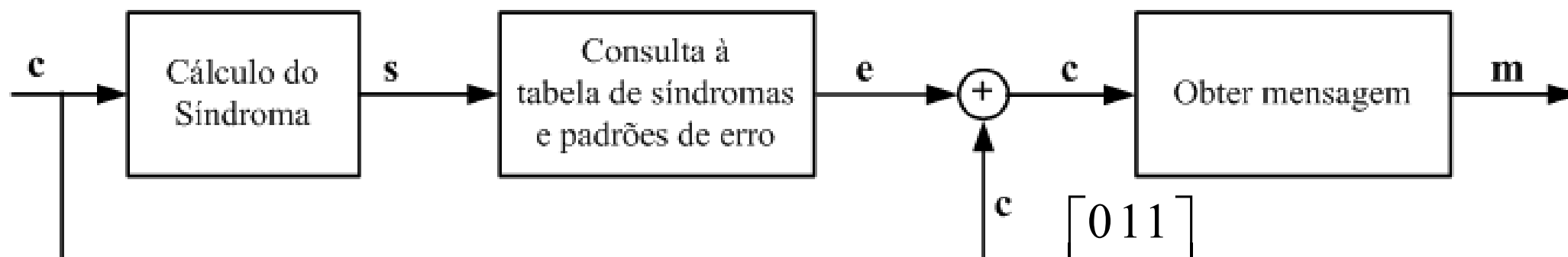
$$\mathbf{s}_2 = \mathbf{e}_2 \mathbf{H}^T = \text{segunda linha de } \mathbf{H}^T.$$

- As linhas de \mathbf{H}^T são sempre não nulas



4. Descodificação: correção

- Mecanismo de **correção**: exemplo para o código Hamming (7,4)
- Matrizes geradora **G** e de teste de paridade **H^T**



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

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



4. Descodificação: correção

- Tabela de síndromas para o código Hamming (7,4)
- O código tem $2^3=8$ síndromas:
 - síndrome nulo - ausência de erro;
 - os outros 7 correspondem aos padrões de um bit em erro por palavra

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

Síndrome	Padrão de Erro	Observações
000	0000000	Ausência de erro
011	1000000	1.º bit em erro
110	0100000	2.º bit em erro
101	0010000	3.º bit em erro
111	0001000	4.º bit em erro
100	0000100	5.º bit em erro
010	0000010	6.º bit em erro
001	0000001	7.º bit em erro



4. Descodificação: correção

- Sejam as palavras de código
 - $c_1 = [1\ 0\ 0\ 0\ 0\ 1\ 1]$
 - $c_2 = [0\ 0\ 1\ 1\ 0\ 1\ 0]$
- Sejam as palavras recebidas no descodificado
 - $y_1 = c_1 + [1\ 0\ 0\ 0\ 0\ 0\ 0] = [\underline{0}\ 0\ 0\ 0\ 0\ 1\ 1]$
 - $y_2 = c_2 + [0\ 0\ 1\ 0\ 0\ 0\ 0] = [0\ 0\ \underline{0}\ 1\ 0\ 1\ 0]$
 - $y_3 = c_1 + [1\ 1\ 0\ 0\ 0\ 0\ 0] = [\underline{0}\ \underline{1}\ 0\ 0\ 0\ 1\ 1]$
- Os síndromas obtidos são
 - $s_1 = y_1 H^T = [0\ 1\ 1]$
 - $s_2 = y_2 H^T = [1\ 0\ 1]$
 - $s_3 = y_3 H^T = [1\ 0\ 1]$

s	e
000	0000000
011	1000000
110	0100000
101	0010000
111	0001000
100	0000100
010	0000010
001	0000001



Dois erros na palavra



4. Descodificação: correção

s	e
000	0000000
011	1000000
110	0100000
101	0010000
111	0001000
100	0000100
010	0000010
001	0000001

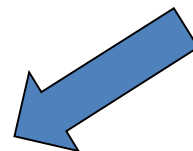
- Os padrões de erro associados são
 - $e_1 = [1\ 0\ 0\ 0\ 0\ 0\ 0]$
 - $e_2 = [0\ 0\ 1\ 0\ 0\ 0\ 0]$
 - $e_3 = [0\ 0\ 1\ 0\ 0\ 0\ 0]$
- As palavras estimadas são
 - $c_1 = y_1 + e_1 = [\underline{0}\ 0\ 0\ 0\ 0\ 1\ 1] + [1\ 0\ 0\ 0\ 0\ 0\ 0] = [1\ 0\ 0\ 0\ 0\ 1\ 1]$
 - $c_2 = y_2 + e_2 = [0\ 0\ \underline{0}\ 1\ 0\ 1\ 0] + [0\ 0\ 1\ 0\ 0\ 0\ 0] = [0\ 0\ 1\ 1\ 0\ 1\ 0]$
 - $c_3 = y_3 + e_3 = [\underline{0}\ \underline{1}\ 0\ 0\ 0\ 1\ 1] + [0\ 0\ 1\ 0\ 0\ 0\ 0] = [0\ 1\ 1\ 0\ 0\ 1\ 1]$

- As mensagens obtidas após correção

- $m_1 = [1\ 0\ 0\ 0]$

- $m_2 = [0\ 0\ 1\ 1]$

- $m_3 = [0\ 1\ 1\ 0]$



Os dois erros na palavra
implicaram erro após correcção
(t=1)



5. Aplicações - Bit de paridade e Hamming

- Comunicação série assíncrona
 - 1 bit de paridade por cada byte
- Memórias RAM
 - 1 bit de paridade por cada byte
 - mais do que 1 bit de paridade - ECC (*Error Correcting Code*) RAM
- Teletexto
 - Hamming (8,4) - extensão do Hamming (7,4)
- Discos rígidos
 - Alguns usam código de Hamming – existem bits de paridade por cada setor



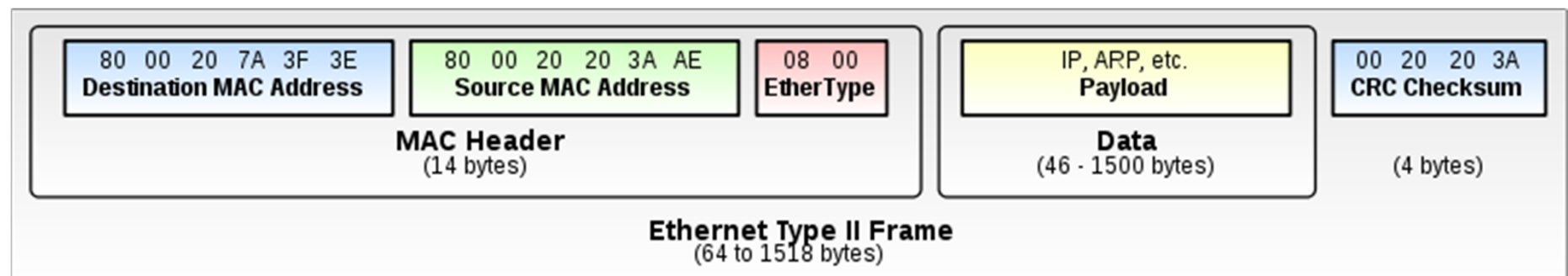
5. Aplicações - Bit de paridade, repetição e Hamming

- RAID (*Redundant Array of Independent Disks*)
 - RAID 1 – *mirroring*; código de repetição
 - RAID 2 - *Hamming system*; no caso do Hamming (7,4) usa 7 discos rígidos (4 dados + 3 paridade)
 - RAID 3 - *parallel transfer with parity drive*; usa código bit de paridade, no qual existem vários discos de dados e um de paridade
- *Bluetooth* (comunicação sem fios)
 - Usa código de repetição (3,1) - *packet header*
 - Usa Hamming modificado (15,10) - *application data*



5. Aplicações - CRC32

- Norma Ethernet 802.3 (Rede Local - LAN)
- Usa CRC32 (32 bits / 4 bytes) para verificação da integridade da trama;
$$g(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$$
- O campo *FCS-Frame Check Sequence* no cabeçalho da trama tem sempre 32 bits, independentemente da dimensão da trama
- A dimensão máxima da trama é 1518 bytes (12144 bits)



5. Aplicações - CRC32

- Norma Ethernet 802.3

$$g(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$$

- Existem sempre 32 bits de paridade
- A trama tem dimensão mínima e dimensão máxima; esta última é 1518 bytes (12144 bits); temos um código $(n, n-32)$

Distância mínima em função da dimensão da trama n

n	d_{\min}
3007 a 12144	4
301 a 3006	5
204 a 300	6
124 a 203	7
90 a 123	8

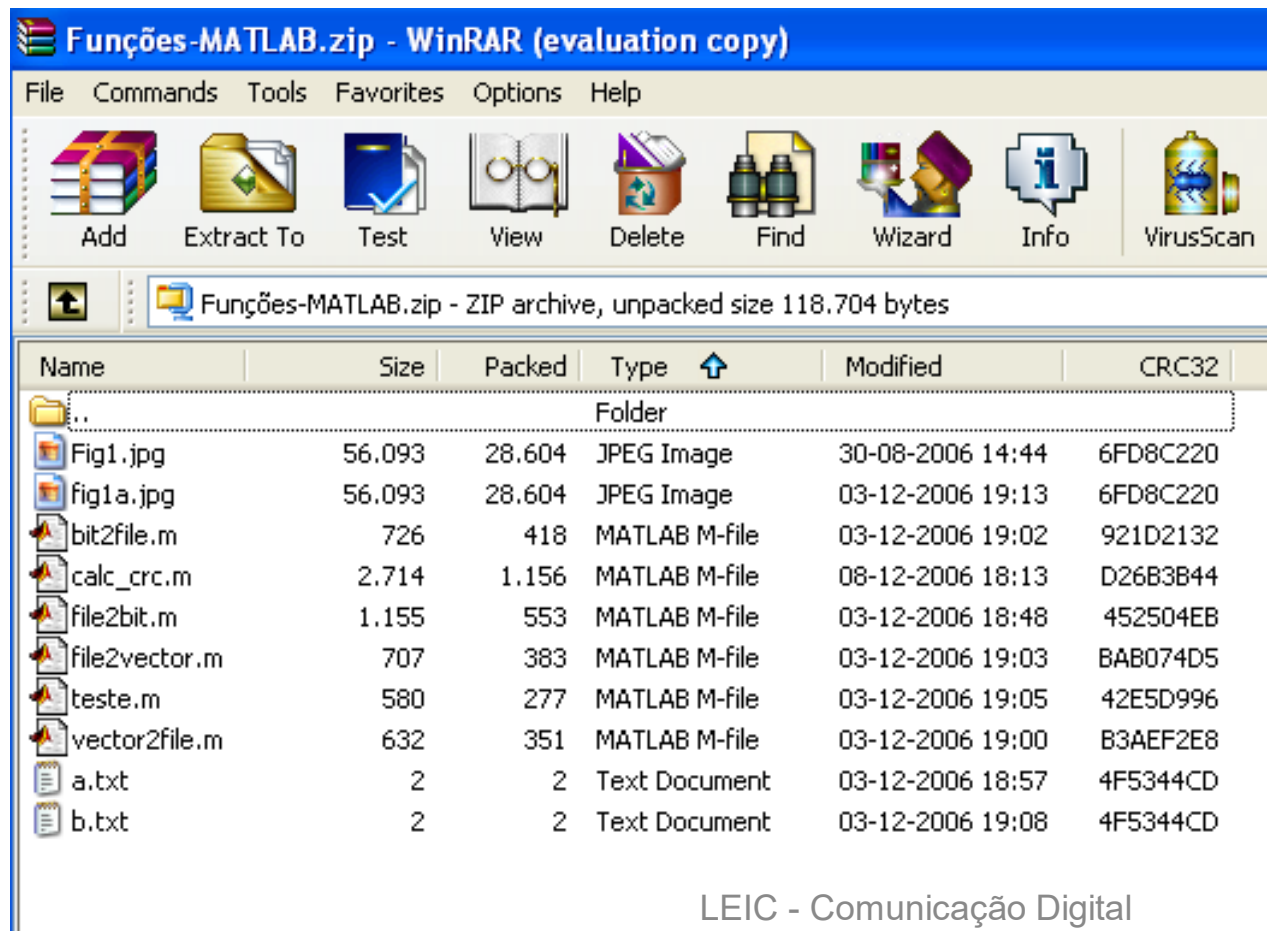
Fonte:

J. Moreira and P. Farrell, **Essentials of Error-Control Coding**, 2006, John Wiley and sons.
[Pág. 93]



5. Aplicações - CRC32

- Codificador de fonte WinRAR (e outros)
 - Usa CRC32 para verificação da integridade de cada ficheiro comprimido
 - Antes de descomprimir o ficheiro, verifica a integridade do ficheiro comprimido (cálculo do síndrome)



CRC32



5. Aplicações - Outras aplicações

- Dígitos de controlo do Bilhete de Identidade/Cartão de Cidadão
 - O último dígito do número do BI/CC serve para a deteção de erros
 - <http://www.mat.uc.pt/~picado/SistIdent/mistBI.html>
 - <http://www.cognoscomm.com/arquivo/3067/101-cartao-do-cidadao/>
- Dígitos de controlo do ISBN (*International Standard Book Number*) tem uma funcionalidade idêntica
 - http://en.wikipedia.org/wiki/International_Standard_Book_Number
- Outros dígitos de controlo (códigos de barras,...)
 - http://en.wikipedia.org/wiki/Check_digit
 - https://en.wikipedia.org/wiki/International_Article_Number
 - https://en.wikipedia.org/wiki/International_Article_Number#Check_digit



6. Exercícios

Tenha em conta os mecanismos de deteção e correção de erros usados nos códigos de bloco (n, k) .

- a) Quais as vantagens e desvantagens da utilização destes códigos? Justifique.
- b) Indique, justificando, quais as técnicas normalmente utilizadas para estabelecer os bits redundantes para proceder à deteção/correção de erros. Exemplifique e relacione o número de bits redundantes com as capacidades de deteção e correção de erros.
- c) Considere que o ficheiro f demorou 5 segundos a ser transmitido, sem a utilização de códigos detetores e corretores de erros. Passando a transmitir o ficheiro f , no mesmo sistema, usando um código $(8, 4)$, quanto tempo demorará essa transmissão?



6. Exercícios

Solução

a) Vantagens: controlo de erros, diminuição de BER, aumento da qualidade de serviço (QoS).

Desvantagens: maior complexidade, mais tempo necessário para a transmissão (e retransmissão, quando necessário) e correção.

b) Técnica de repetição e técnica de bits de paridade (XOR)

Exemplo de repetição: mensagem=010 -> palavra de código=000 111 000

Exemplo de paridade par: mensagem=0110 -> palavra de código=011 101

As capacidades de deteção e correção de erros são diretamente proporcionais ao número de bits redundantes.

c) Demorará o dobro do tempo, 10 segundos (no melhor caso).



6. Exercícios

Considere o código de controlo de erros cujas palavras estão organizadas na forma $c = [m_0 \ m_1 \ b_0 \ b_1]$, tais que $b_0 = m_0 \oplus m_1$ e $b_1 = m_1$.

- a) Apresente todas as palavras de código.
- b) Calcule a distância mínima de Hamming.
- c) Calcule as capacidades de deteção e correção de erros.
- d) Suponha que se transmite a mensagem 01 e que sobre a palavra de código resultante é aplicado o padrão de erro 1010. Qual a mensagem descodificada? Comente.



6. Exercícios

Solução

Código (4,2), com 4 palavras de código

0 0 0 0

0 1 1 1

1 0 1 0

1 1 0 1

b) $d_{\min}=2$

c) deteção $l=1$ bits por bloco, correção $t=0$ bits (não tem).

d) $m=01 \rightarrow c=0111 \rightarrow y = c + e = 0111 + 1010 = 1101$. A mensagem decodificada é 11 (os dois primeiros bits do bloco). Os dois erros introduzidos na transmissão não foram detetados.



6. Exercícios

Assuma uma transmissão digital com código Hamming (7,4), cujas palavras estão organizadas na forma $c = [m_0 \ m_1 \ m_2 \ m_3 \ b_0 \ b_1 \ b_2]$, com equações de paridade

$$b_0 = m_1 \oplus m_2 \oplus m_3 \quad b_1 = m_0 \oplus m_1 \oplus m_3 \quad b_2 = m_0 \oplus m_2 \oplus m_3$$

- a) Sabendo que o número de bits a transmitir antes da aplicação do código é 40000, qual o número de bits a transmitir após a aplicação do código?
- b) Qual a sequência transmitida quando se enviam os bits de informação 10100011?
- c) Caso seja recebida a sequência 1010001, existem erros nesta sequência?



6. Exercícios

Solução

- a) São transmitidos $40000 + 30000 = 70000$ bits, no total.
- b) A sequência transmitida é 1010 110 0011 010.
- c) A palavra 1010 001 não pertence ao código. Logo, existem erros detetados nesta sequência.



6. Exercícios

Considere o código de bloco linear com palavras definidas por $c = [m_0 \ m_1 \ m_2 \ b_0 \ b_1 \ b_2 \ b_3]$, em que $b_0 = m_0 \oplus m_1$, $b_1 = m_2$, $b_2 = m_1 \oplus m_2$ e $b_3 = m_0 \oplus m_2$.

- a) Indique as dimensões (n,k) .
- b) Qual a distância mínima do código e as respectivas capacidades de deteção e correção de erros?
- c) Exemplifique uma deteção de erros.
- d) Apresente as matrizes geradora G e de teste de paridade transposta H^T .



6. Exercícios

Solução

$(n,k) = (7,3)$.

- a) Listando as 8 palavras de código, conclui-se que a palavra de código com menor peso de Hamming tem peso igual a 3. Logo $d_{\min}=3$, $l=2$ e $t=1$.
- b) Por exemplo, se a palavra de código 0010111 sofrer um erro no último bit, temos que a palavra recebida é 0010110. Esta palavra não pertence à lista de palavras de código, logo temos a presença de erro detetada.

Em alternativa, assumindo que os bits de mensagem recebidos 001 estão corretos, e se recalcularmos os bits de paridade teremos 0111, o que difere da configuração recebida 0110, detetando-se assim o erro



6. Exercícios

Solução (Continuação)

$$d) G = [I_k \mid P] = [I_3 \mid P]$$

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

$$H^T = \begin{bmatrix} P & \\ & I_q \end{bmatrix} = \begin{bmatrix} P & \\ & I_4 \end{bmatrix}$$

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

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$



6. Exercícios

Considere o polinómio gerador $g(X) = X^4 + X^3 + X^2 + X + 1$ de código (10,6).

- a) Apresente a palavra de código $c(X)$, quando a mensagem é 1 0 0 0 0 1.
 - b) A palavra 1111111111 pertence ao código?
-

Considere o polinómio gerador $g(X) = X^3 + X + 1$ do código (7,4).

- a) Quais das palavras 0000000, 1011000 e 0000011 pertencem ao código?
- b) Apresente todas as palavras de código.



6. Exercícios

Solução

a) $c(X) = [1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0]$.

b) Sim. A palavra 1111111111 pertence ao código. Se dividirmos esta palavra pelo polinómio gerador, temos resto nulo. Isto significa que a palavra pertence ao código.

a) As palavras 0000000 e 1011000 pertencem ao código. Se dividirmos estas palavras pelo polinómio gerador, temos resto nulo. Isto significa que estas palavras pertencem ao código. Para a palavra 0000011 não se obtém resto nulo, pelo que não pertence ao código.



6. Exercícios

Solução (continuação)

b) As 16 palavras de código.

0	0	0	0	0	0	0	1	0	0	0	1	0	1
0	0	0	1	0	1	1	1	0	0	1	1	1	0
0	0	1	0	1	1	0	1	0	1	0	0	1	1
0	0	1	1	1	0	1	1	0	1	1	0	0	0
0	1	0	0	1	1	1	1	1	0	0	0	1	0
0	1	0	1	1	0	0	1	1	0	1	0	0	1
0	1	1	0	0	0	1	1	1	1	0	1	0	0
0	1	1	1	0	1	0	1	1	1	1	1	1	1



6. Exercícios

Suponha uma transmissão digital em que são enviados os bits de informação 1010. Considere que o controlo de erros é realizado através de CRC com polinómio gerador $g(X) = X^3 + X + 1$.

- a) Apresente a sequência binária transmitida.
 - b) Provoque um erro nesta sequência binária e ilustre o funcionamento da deteção de erros.
-

Determine o tempo que demora a transmissão de um ficheiro com 1 024 000 bytes, considerando a utilização de modulação 16-QAM, com tempo de símbolo $T_s = 10 \mu s$, nos seguintes cenários:

- a) Ausência de códigos detetores e corretores de erros.
- b) Deteção de erros com código CRC7, estabelecido por $g(X) = X^7 + X^6 + X^4 + 1$, aplicado a blocos de mensagem com dimensão 1024 bits.



6. Exercícios

Solução

- a) 1010011
- b) 1010001, é a sequência anterior com erro no penúltimo bit. Se dividirmos esta sequência pelo polinómio gerador obtemos o resto 010. Dado que o resto não é nulo, o decodificador/recetor deteta o erro.

Por outro lado, o resto da divisão de 1010011 pelo polinómio gerador, é nulo.

- a) Demora 20,48 segundos.
- b) Demora 20,62 segundos.



6. Exercícios

Considere o código (6,3) com matriz geradora

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

- a) Pretende-se estender este código adicionando um bit de paridade resultante da soma de todos os bits de mensagem; indique as dimensões (n,k) do código estendido e apresente as matrizes geradora e de teste de paridade.
- b) Qual o peso máximo dos padrões de erro que o código estendido consegue: i) detetar? ii) corrigir?



6. Exercícios

Solução

a) Geradora

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

$$(n,k) = (7,3)$$

Teste de paridade

$$H^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix};$$

b) O peso máximo de Hamming dos padrões de erro indica o número máximo de bits errados por palavra de código. Listando todas as palavras de código conclui-se que o menor peso de Hamming é 4. Logo $d_{\min}=4$, $l=3$, $t=1$.

Assim, detecta padrões de erro de até peso 3. Corrige padrões de erro de peso 1.



6. Exercícios

Seja o código de bloco linear sistemático (6,4) com as palavras organizadas na forma $c = [m_0 \ m_1 \ m_2 \ m_3 \ b_0 \ b_1]$. A sub-matriz geradora de paridade é

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

- a) Apresente as matrizes geradora G e de teste de paridade H^T .
- b) Verifique se as palavras 000000, 001111 e 011010 pertencem ao código.
- c) Calcule a distância mínima do código e indique as capacidades de detecção e correção de erros.



6. Exercícios

Solução

a) Geradora G

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

Teste de paridade H^T .

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

b) A palavra 000000 (Vetor nulo) pertence ao código. 0 1];

$[001111] \cdot H^T = [0 \ 1]$, logo a palavra 001111 não pertence ao código.

$[011010] \cdot H^T = [0 \ 0]$, logo a palavra 011010 pertence ao código.

c) Listando todas as palavras de código conclui-se que o menor peso de Hamming é 2. Logo $d_{\min}=2$, $l=1$, $t=0$. Assim, detecta 1 bit erro e não tem capacidade de correção.

