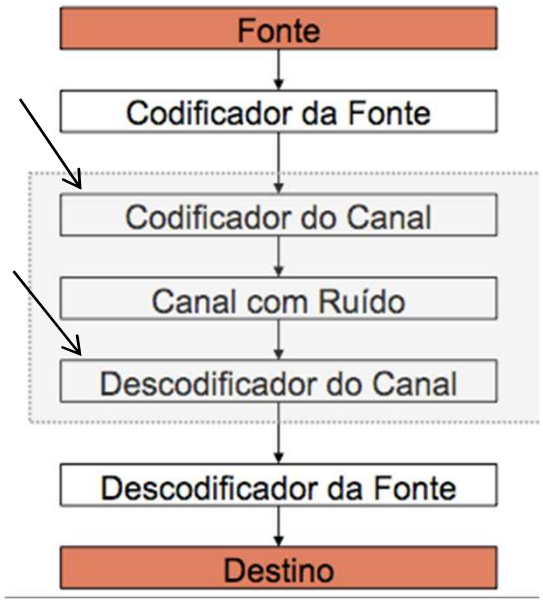
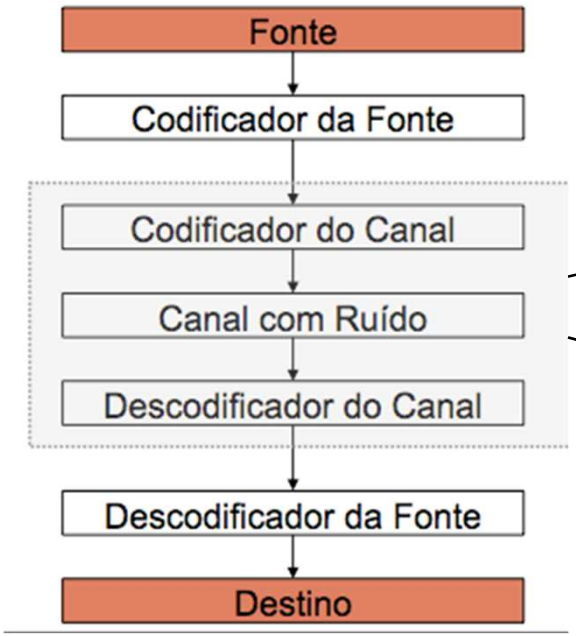
VII. CÓDIGOS PARA CONTROLO DE ERROS

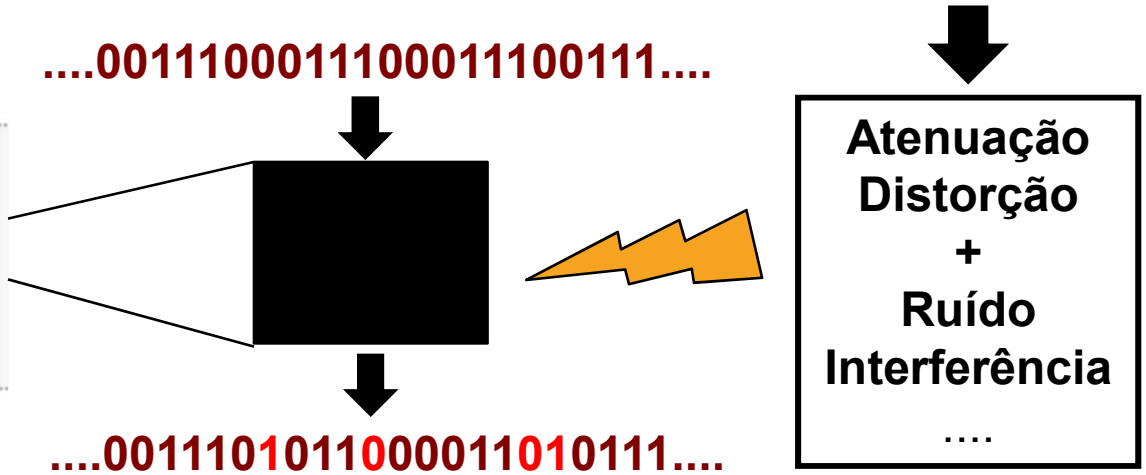


- Códigos utilizados na codificação de canal para controlar os erros de transmissão em sistemas de telecomunicações não fiáveis ou ruidosos.
- Considera-se somente o caso da transmissão digital binária.
- Existem variadas técnicas utilizadas em diversas tecnologias de comunicações... (e não só...)

VII. CÓDIGOS PARA CONTROLO DE ERROS



Os canais/sistemas de transmissão não são "perfeitos"

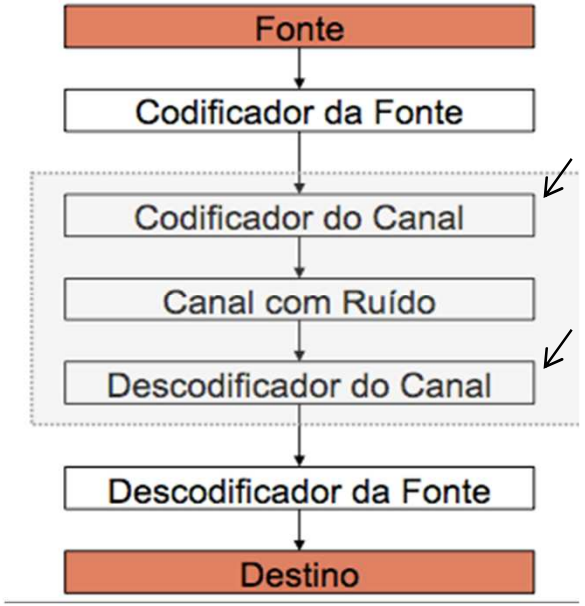


Que dígitos/bits estão errados na receção?

VII. CÓDIGOS PARA CONTROLO DE ERROS

Teoria da Informação

Dado um canal de comunicação e uma fonte cujo débito de informação não excede a capacidade do canal, existe um código tal que a informação pode ser transmitida através do canal com uma frequência de erros arbitrariamente pequena, apesar da presença de ruido.



VII. CÓDIGOS PARA CONTROLO DE ERROS

Tipos de Erros

- **Ruído branco**: erros de transmissão causados por este ruído num determinado dígito não afeta os dígitos subsequentes (ocorrências de erros estatisticamente independentes, ou seja, os erros são de natureza aleatória).

- **Ruído impulsivo**: a sua presença caracteriza-se por longos intervalos de tempo em que os dígitos não são corrompidos, intercalados por molhos (*burts*) de dígitos corrompidos (ou seja, erros num dígito não são estatisticamente independentes dos dígitos adjacentes).

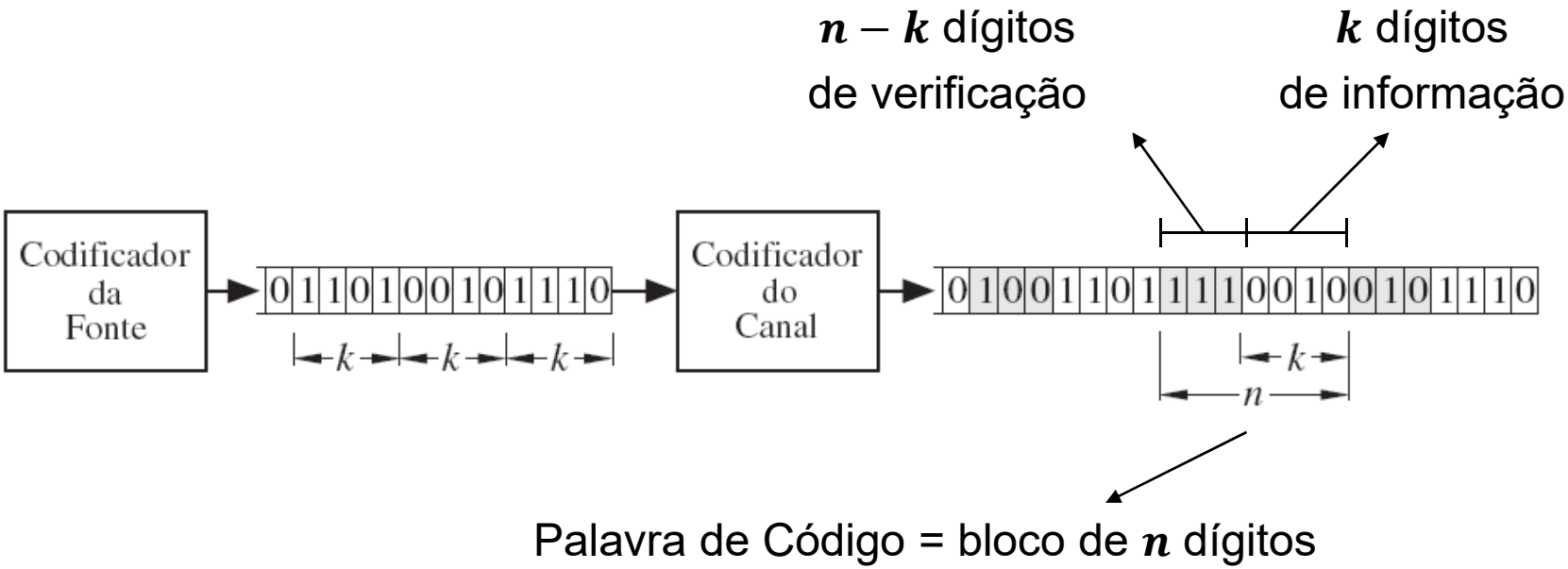
VII. CÓDIGOS PARA CONTROLO DE ERROS

Tipos de Códigos

- Neste capítulo serão abordadas as bases para a construção de códigos de correção de erros aleatórios através de **códigos sistemáticos de bloco**, em que cada conjunto de k dígitos de informação é acompanhado de $n - k$ dígitos redundantes (dígitos de verificação de paridade) calculados a partir dos dígitos de informação, formando assim um bloco de tamanho fixo, de n dígitos, designada por palavra de código.
- Quando os dígitos da mensagem aparecem destacados num sub-bloco da palavra de código, o código diz-se sistemático ou separável.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Lineares de Bloco



VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Lineares de Bloco C(n,k)

- Um bloco de dígitos de informação será um tuplo D, tal que $\mathbf{D = (d_0\ d_1\ d_2\ \ldots\ d_{k-1})}$ com $\mathbf{d_j \in \{0,1\}}$
- Existem 2^k blocos de dígitos de informação
- Cada bloco **D** de informação é transformado numa palavra de código representada por um tuplo C, tal que $\mathbf{C = (c_0\ c_1\ c_2\ \ldots\ c_{n-1})}$ com $\mathbf{c_j \in \{0,1\}}$
- Existem 2^n palavras de código mas apenas 2^k palavras de código são válidas e distintas
- As restantes palavras ($2^n - 2^k$) não fazem parte do dicionário do código e se forem recebidas no destino identificam ocorrência de erro na transmissão.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Lineares de Bloco C(n,k)

Rendimento de um código $\boldsymbol{C(n,k)}$ é $\boldsymbol{\rho = \frac{k}{n}}$

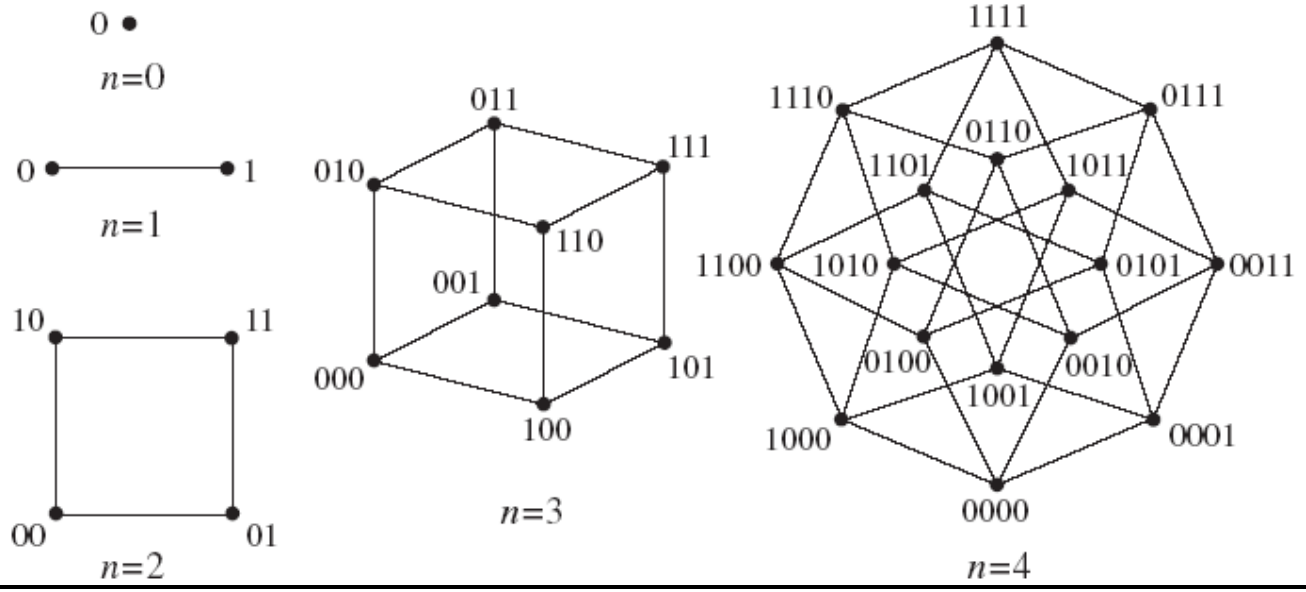
Definição 9.1 *Distância de Hamming entre duas palavras de um código de bloco, $d(C_i, C_j)$, é o número de posições em que as duas palavras, C_i e C_j, diferem.*

- Duas palavras de código idênticas estarão à distância zero;
- Duas palavras de código distintas estarão a uma distância igual ou superior a uma unidade;
- O conceito de distância de *Hamming* é passível de uma interpretação geométrica semelhante à distância euclidiana entre dois pontos.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Lineares de Bloco C(n,k)

Interpretação geométrica do conceito de distância de *Hamming*: correspondência entre 2^n palavras distintas (n dígitos) com 2^n vértices de um hipercubo (num espaço de n dimensões):



VII. CÓDIGOS PARA CONTROLO DE ERROS

Distância Mínima em Códigos C(n,k)

Definição 9.2 *Distância mínima de um código de bloco, d_{min}, é a menor das distâncias de Hamming entre quaisquer duas palavras desse código.*

- A distância mínima de um código condiciona a sua capacidade de controlo de erros (tanto de deteção como de correção).
- Quantos erros poderão ser detetados/corrigidos por um código com uma determinada distância mínima?

VII. CÓDIGOS PARA CONTROLO DE ERROS

Distância Mínima em Códigos C(n,k)

Definição alternativa mais fácil de calcular:

Definição 9.3 *Peso de uma palavra C_i de um código de bloco, $p(C_i)$, é o número de dígitos 1 que a palavra C_i contém.*

Definição 9.4 *Peso mínimo de um código de bloco, $[p(C_i)]_{\min}$ é o peso da palavra de menor peso desse código, exceptuando a palavra de peso zero.*

Teorema 9.1 — Distância mínima
A distância mínima de um código de bloco é igual ao seu peso mínimo.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Deteção & Correção de Erros em Códigos C(n,k)

Se a distância mínima dum código for $d_{\min}$, então esse código pode:

- detetar até e_d dígitos errados, em que $e_d = d_{\min} - 1$
- corrigir até e_c dígitos errados, em que $e_c = \frac{d_{\min}-1}{2}$

Exemplos:

- Com um código com distância mínima de 2 pode detetar-se um erro que resulte da modificação dum único dígito mas não se pode/sabe corrigir esse digito.
- Com um código com distância mínima de 3 pode detetar-se um erro que resulte da modificação de até 2 dígitos e pode corrigir-se um erro quando este é de um dígito.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Cíclicos Binários C(n,k)

São uma subclasse dos códigos lineares de bloco sendo fáceis de realizar (estrutura matemática simples).

- Nestes códigos utiliza-se uma representação polinomial;
- Operações são realizadas em aritmética módulo 2;
- A partir de uma palavra de código é possível obter outras.

Definição 9.5 *Um código linear de bloco $C(n,k)$ é cíclico se possuir a seguinte propriedade:*

Se o tuplo $C = (c_0, c_1, c_2, \ldots, c_{n-1})$ fôr uma palavra de código então o tuplo $C^{(1)} = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ obtido por deslocação cíclica direita de uma posição de C também é uma palavra de código.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Cíclicos Binários C(n,k)

Para gerar estes códigos C(n,k) utiliza-se um polinómio gerador $g(x)$ de grau n-k para dividir o polinómio $x^n + 1$.

As palavras de código podem ser geradas de duas formas:

- Originando palavras de código em que os dígitos de informação e de verificação estão misturados (códigos criptográficos);
- Ou de forma sistemática, em que os dígitos de verificação e de informação aparecem separados. É esta forma que veremos em mais detalhe.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Cíclicos Sistemáticos Binários C(n,k)

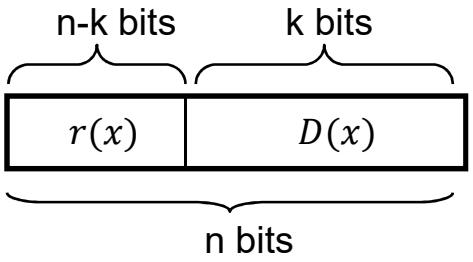
$$C = (\underbrace{r_0, r_1, r_2, \ldots, r_{n-k-1}}_{\substack{n-k \text{ dígitos} \\ \text{de verificação} \\ \text{de paridade}}}, \underbrace{d_0, d_1, d_2, \ldots, d_{k-1}}_{\substack{k \text{ dígitos} \\ \text{da mensagem}}})$$

$$D(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_{k-1} x^{k-1}$$

$$r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-k-1} x^{n-k-1}$$

$r(x)$ é o resto da divisão de $x^{n-k} D(x)$ por $g(x)$

Palavra de Código (n,k) :



VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Cíclicos Sistemáticos Binários C(n,k)

Exemplo: Seja $g(x) = 1 + x + x^3$ o polinómio gerador de um código cíclico C(7,4). Determinar a palavra de código (sistemática) correspondente à mensagem de dados D = (1110).

> $D(x) = 1 + x + x^2$

> $x^{n-k} * D(x) = x^3\, D(x) = x^3 + x^4 + x^5$

> $r(x) = x$

> $C(x) = r(x)|D(x) = x|1 + x + x^2$

$$C = (\underbrace{0\,1\,0}_{r(x)}\ \underbrace{1\,1\,1\,0}_{D(x)})$$

$$\begin{array}{l|l} x^5+x^4+x^3 & x^3+x+1 \\ \hline x^5+\quad x^3+x^2 & x^2+x \\ \hline 0+x^4+0+x^2 & \\ \quad x^4+\quad x^2+x & \\ \hline 0+\quad 0+x & = r(x) \end{array}$$

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Cíclicos Sistemáticos Binários C(n,k)

Exemplo C(7,4) com $g(x) = 1 + x + x^3$

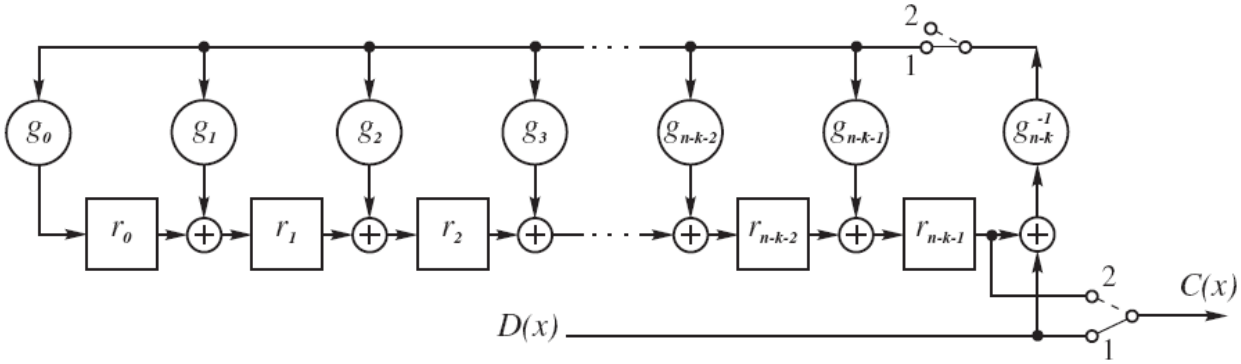
Informação $D(x)$	Código criptográfico $C(x) = D(x) \cdot g(x)$	Código sistemático $C(x) = r(x) + x^{n-k}D(x)$	Peso $p(C_i)$	
0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0	
0 0 0 1	0 0 0 1 1 0 1	1 0 1 0 0 0 1	3	
0 0 1 0	0 0 1 1 0 1 0	1 1 1 0 0 1 0	4	4 ←
0 0 1 1	0 0 1 0 1 1 1	0 1 0 0 0 1 1	3	
0 1 0 0	0 1 1 0 1 0 0	0 1 1 0 1 0 0	3	
0 1 0 1	0 1 1 1 0 0 1	1 1 0 0 1 0 1	4	5 ←
0 1 1 0	0 1 0 1 1 1 0	1 0 0 0 1 1 0	3	
0 1 1 1	0 1 0 0 0 1 1	0 0 1 0 1 1 1	4	7 ←
1 0 0 0	1 1 0 1 0 0 0	1 1 0 1 0 0 0	3	
1 0 0 1	1 1 0 0 1 0 1	0 1 1 1 0 0 1	4	3 ←
1 0 1 0	1 1 1 0 0 1 0	0 0 1 1 0 1 0	3	
1 0 1 1	1 1 1 1 1 1 1	1 0 0 1 0 1 1	4	6 ←
1 1 0 0	1 0 1 1 1 0 0	1 0 1 1 1 0 0	4	2 ←
1 1 0 1	1 0 1 0 0 0 1	0 0 0 1 1 0 1	3	
1 1 1 0	1 0 0 0 1 1 0	0 1 0 1 1 1 0	4	1 →
1 1 1 1	1 0 0 1 0 1 1	1 1 1 1 1 1 1	7	

Obtenção de outras palavras de código, a partir da primeira D(1110), por rotação cíclica…

VII. CÓDIGOS PARA CONTROLO DE ERROS

Circuitos para Códigos Cíclicos Sistemáticos C(n,k)

Geração por hardware através dum circuito gerador:



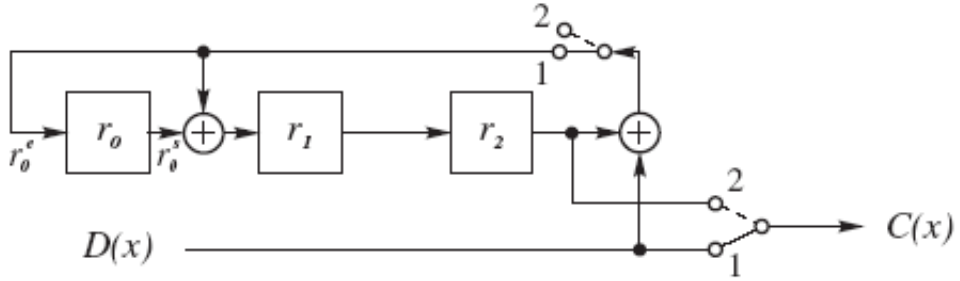
O circuito contém:

- registos para n-k bits (dígitos de verificação);
- conjunto de ou-exclusivos (XOR);
- conjunto de ligações abertas ou fechadas conforme os coeficientes do polinómio $g(x)$.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Circuitos para Códigos Cíclicos Sistemáticos C(n,k)

Circuito para C(7,4) com $g(x) = 1 + x + x^3$ e $r(x) = x$



Verificar a operação do circuito para a palavra de dados D=(0101)

bit de entrada	entrada nos registos				saída dos registos		
$D(x)$	r_0^e	r_1^e	r_2^e		r_0^s	r_1^s	r_2^s
—	0	0	0		0	0	0
1	1	1	0	→	1	1	0
0	0	1	1	→	0	1	1
1	0	0	1	→	0	0	1
0	1	1	0	→	1	1	0

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

VII. CÓDIGOS PARA CONTROLO DE ERROS

Circuitos para Códigos Cíclicos Sistemáticos C(n,k)

As palavras de código são transmitidas através do canal e no caso de ocorrência de erro(s) a palavra que chega ao descodificador poderá permitir saber qual a palavra transmitida:

- O descodificador divide $r(x)$ por $g(x)$ obtendo um resto $S(x)$, designado por **Síndroma** de $r(x)$.
- Se $S(x) = 0$ o receptor toma a palavra como válida.
- Se $S(x) \neq 0$ o receptor assume então que houve erro e pode (ou não, se for só detetor) tentar corrigir a palavra recorrendo a circuitos específicos e à informação presente em $S(x)$.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Circuitos para Códigos Cíclicos Sistemáticos C(n,k)

Exemplos de circuitos no descodificador

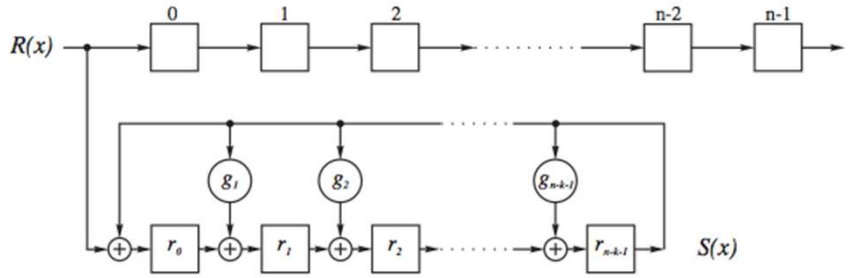


Figura 9.6: Divisão de $R(x)$ por $g(x)$ no descodificador

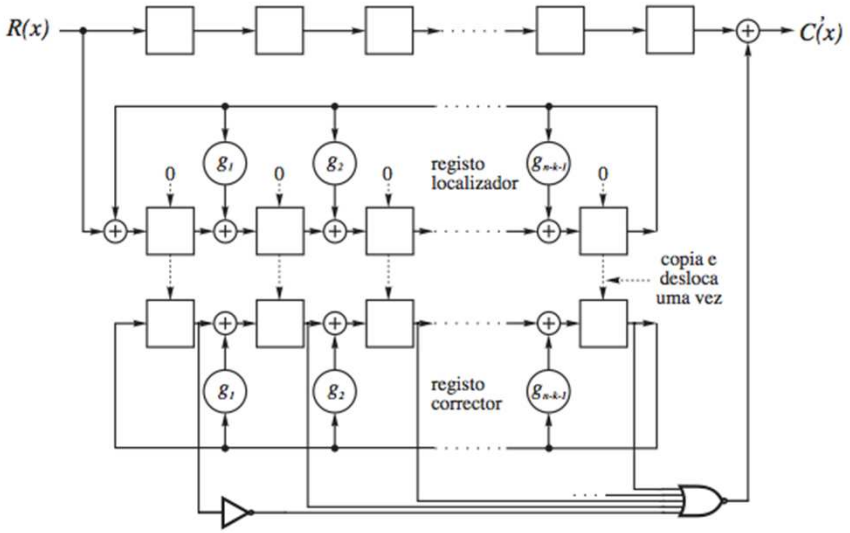


Figura 9.7: Circuito corrector de erros simples

VII. CÓDIGOS PARA CONTROLO DE ERROS

Códigos Cíclicos Sistemáticos C(n,k)

Nem todos os polinómios geradores são capazes de gerar um bom código, depende da sua utilização. Existe sempre um compromisso entre rendimento, capacidade de deteção e correção e complexidade de implementação.

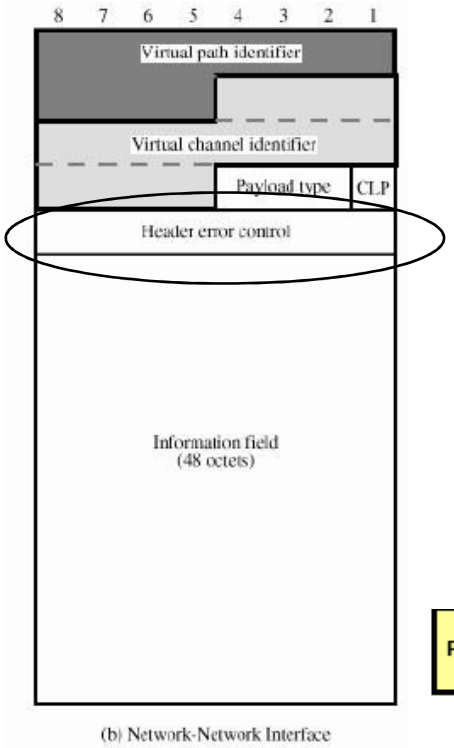
Exemplos de alguns códigos reais usados em diversas aplicações:

Tipo	n	k	ρ	d_{min}	$g(x)$
códigos de Hamming	7	4	0.57	3	x^3+x+1
	15	11	0.73	3	x^4+x+1
	31	26	0.84	3	x^5+x^2+1
códigos BCH	15	7	0.46	5	$x^8+x^7+x^6+x^4+1$
	31	21	0.68	5	$x^{10}+x^9+x^8+x^6+x^5+x^3+1$
	63	45	0.71	7	$x^{18}+x^{17}+x^{16}+x^{15}+x^9+x^7+$ $+x^6+x^3+x^2+x+1$
código Golay	23	12	0.52	7	$x^{11}+x^9+x^7+x^6+x^5+x+1$

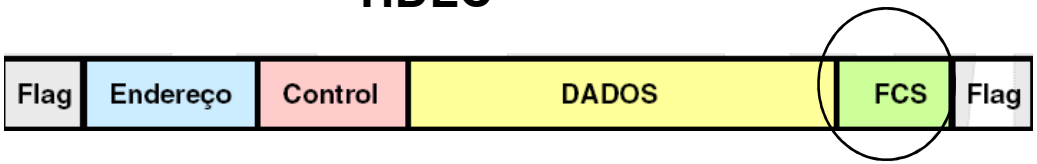
VII. CÓDIGOS PARA CONTROLO DE ERROS

Outros tipos de mecanismos de controlo de erros

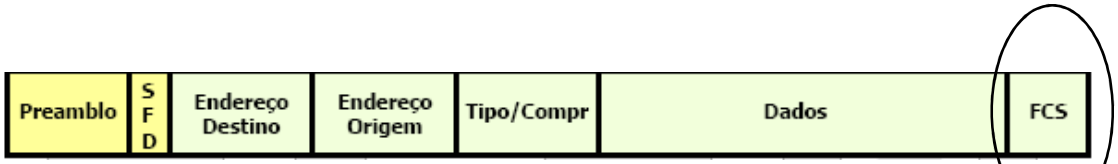
ATM



HDLC



Diferentes tipos de códigos são utilizados por diferentes tecnologias; normalmente é referido o polinómio gerador utilizado.



ETHERNET

VII. CÓDIGOS PARA CONTROLO DE ERROS

Outros tipos de mecanismos de controlo de erros

Forward Error Correction/Error Correction Codes (FEC/ECC)

- Correção de erros progressiva, quando os códigos para controlo de erros são utilizados como corretores.
- Pouco usados em sistemas de transmissão de dados, exceto em condições/protocolos especiais.
- Usado em canais simplex onde não é possível/praticável um mecanismo suportado na retransmissão.
- Cenários em que o tempo de propagação é muito elevado (e.g. comunicação com sondas espaciais).
- Técnicas também usadas em gravações digitais (CD, DVD, ...), memórias flash, hard drives, SSD, etc.

VII. CÓDIGOS PARA CONTROLO DE ERROS

Outros tipos de mecanismos de controlo de erros

Automatic Repeat Request (ARQ)

- Código usado só como detetor.
- Correção processa-se por repetição (pedido de retransmissão das palavras).
- Só possível num canal de comunicação duplex.
- Técnicas utilizadas nos sistemas/tecnologias de transmissões de dados mais comuns.
- Técnicas ARQ - Tópico expandido e coberto em detalhe noutra UC (Redes de Computadores).

VII. CÓDIGOS PARA CONTROLO DE ERROS

Erro - pág. 241

$$= (1+x)\cdot(1+x+x^3) = 1+x+x^3+x+x^2+x^4$$
$$= 1+x+x^2+x^5$$

dado que $x^3+x^3=(1+1)\cdot x^3=0\cdot x^3=0$. *Portanto a palavra de código é* $C=(1110010)$. *Podem obter-se outras palavras do código por deslocação cíclica desta. A segunda coluna da tabela 9.1 lista o código completo assim calculado.*

b) Na forma sistemática os três primeiros dígitos são os de verificação e os últimos quatro são os da mensagem. Os dígitos de verificação são os coeficientes do polinómio $r(x)$ *que é o resto da divisão de* $x^{n-k}D(x)$ *por* $g(x)$, *isto é,*

$$\frac{x^{n-k}D(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

Considere-se uma sequência qualquer de mensagem, por exêmplo $D=(1110)$, *a que corresponde* $D(x)=1+x^2+x^3$. *Como* $n-k=7-4=3$, *tem-se* $x^3D(x)=x^3+x^4+x^5$ *e executando a divisão polinomial:*

deve ler-se $D(x) = 1 + x + x^2$