



Sessão nº10

Códigos Cíclicos



Conceitos básicos da Teoria da Informação



- Medida de quantidade de informação (entropia).
- Capacidade de informação dum canal.
- Codificação:
 - codificação de fonte
 - [cifra]
 - codificação de canal



Codificação de canal



- Com a codificação de fonte **eliminou-se a redundância**, pelo que idealmente todos os símbolos binários “contêm” um bit de informação.
- Mas estes símbolos vão ser transmitidos sobre um **canal com ruído**, logo vai haver **perda de informação** sempre que existir erro num símbolo.
- A solução deste problema consiste em **adicionar redundância** de tal forma que apesar dos erros do canal ainda é possível transferir a quantidade de informação associada à mensagem; faz-se com a **codificação de canal**.



Como adicionar redundância?



- forma simples:
 - código de repetição
 - código de bit de paridade
- forma mais elaborada:
 - códigos de bloco lineares
 - Ex. Código de Hamming
 - códigos cíclicos
 - Ex. CRC, BCH, ...
 - códigos convolucionais (orientados ao símbolo)



Palavras de código como polinómios



- Os códigos cíclicos são **códigos de bloco lineares** com uma estrutura cíclica, o que leva a implementações mais práticas e daí a sua grande utilização.
- **Palavras de código como polinómios**: cada palavra do código com n dígitos binários $\mathbf{c} = c_{n-1} \dots c_2 c_1 c_0$ sobre $\text{GF}[2]$ está associada a um polinómio com coeficientes em $\text{GF}[2]$, tal que

$$c_{n-1} \dots c_2 c_1 c_0 \leftrightarrow c_{n-1} x^{n-1} + \dots + c_2 x^2 + c_1 x^1 + c_0 = p(x)$$

onde x é a variável.

- **Adição e Multiplicação escalar** de polinómios
 - $\mathbf{c} + \mathbf{d} \leftrightarrow (c_{n-1} + d_{n-1}) x^{n-1} + \dots + (c_1 + d_1) x^1 + (c_0 + d_0) = p(x) + q(x)$
 - $\alpha \mathbf{c} \leftrightarrow (\alpha c_{n-1}) x^{n-1} + \dots + (\alpha c_1) x^1 + (\alpha c_0) = \alpha p(x)$



Código linear como sub espaço vectorial



- O conjunto $P_n(\text{GF}[2])$ de todos os polinómios de grau menor que n , com coeficientes em $\text{GF}[2]$, é um espaço vectorial, com as operações de adição e de multiplicação escalar de polinómios por elementos de $\text{GF}[2]$. Além disso, se C é um código linear com palavras de dimensão n , então a cada palavra do código $\mathbf{c} \in C$ está associado um polinómio $p(x) \in P_n(\text{GF}[2])$. Mais ainda, esta associação preserva as operações de adição e de multiplicação escalar e assim podemos pensar em C como um sub espaço de $P_n(\text{GF}[2])$.
Deste modo, podemos pensar numa palavra do código com dimensão n como um polinómio de grau menor que n e um código linear C com palavras de dimensão n sobre $\text{GF}[2]$ como um sub espaço de $P_n(\text{GF}[2])$.



Rotação ou *cyclic shift* duma palavra do código



- Seja $p(x) = c_{n-1}x^{n-1} + \dots + c_2x^2 + c_1x^1 + c_0$
- Rotação para a esquerda de $p(x) \equiv p'(x)$
$$p'(x) = c_{n-2}x^{n-1} + \dots + c_2x^3 + c_1x^2 + c_0x^1 + c_{n-1}$$
- Mas
$$x p(x) = c_{n-1}x^n + \dots + c_2x^3 + c_1x^2 + c_0x^1$$

logo

$$\begin{aligned}x p(x) + p'(x) &= c_{n-1}x^n + c_{n-1}; \\p'(x) &= x p(x) + c_{n-1}x^n + c_{n-1}; \\p'(x) &= x p(x) \bmod (x^n + 1); \end{aligned}$$

- Um código linear $C \subseteq P_n$ diz-se **cíclico** se e só se $p(x) \in C$ implicar que $f(x)p(x) \in C$ para qualquer polinómio $f(x) \in P_n$.



Polinómio gerador do código cíclico



- Um código cíclico (n,k) é definido pelo **polinómio gerador**
$$g(x) = 1x^q + g_{q-1}x^{q-1} + \dots + g_2x^2 + g_1x^1 + 1$$
onde $q = n - k$ e os coeficientes g_i tais que $g(x)$ é factor de $x^n + 1$
- Cada palavra do código X obtém-se
$$X(x) = Q_M(x) g(x), \text{ onde } Q_M(x) \equiv \text{bloco de } k \text{ bits da mensagem}$$
- Polinómio verificador de paridade $h(x)$
$$p(x) h(x) = 0 \Leftrightarrow p(x) \in C$$
em que $h(x) g(x) = x^n + 1$ ou seja $h(x) g(x) \bmod (x^n + 1) = 0$
 - Nota: o polinómio gerador é o polinómio de menor grau de entre todos os que pertencem ao código.



Código cíclico sistemático



- Definem-se o polinómio dos bits da mensagem $M(x)$ e o polinómio dos bits de paridade $C(x)$ como

$$M(x) = m_{k-1}x^{k-1} + \dots + m_2x^2 + m_1x^1 + m_0$$

$$C(x) = c_{q-1}x^{q-1} + \dots + c_2x^2 + c_1x^1 + c_0$$

- Pretende-se que as palavras do código tenham a seguinte forma

$$X(x) = x^q M(x) + C(x)$$

mas como $X(x) = Q_M(x) g(x)$

logo $x^q M(x) / g(x) = Q_M(x) + C(x) / g(x)$

sendo esta a condição para o **código ser sistemático**

- os **bits de paridade** $C(x)$ obtêm-se

$$C(x) = \text{resto} [x^q M(x) / g(x)]$$



Descodificação do código cíclico sistemático



- Define-se o polinómio dos bits recebidos $Y(x)$ como

$$Y(x) = y_{n-1}x^{n-1} + \dots + y_2x^2 + y_1x^1 + y_0$$

onde $Y(x) = X(x) + E(x)$, sendo $E(x)$ o polinómio do erro

- Para verificar a paridade faz-se

$$Y(x) / g(x) = X(x) / g(x) + E(x) / g(x)$$

$$Y(x) / g(x) = M(x) + E(x) / g(x)$$

- os **síndrome** $S(x)$ obtêm-se

$$S(x) = \text{resto} [Y(x) / g(x)]$$

