# COMBINATÓRIA E TEORIA DE CÓDIGOS
# TPC 1

(para entregar até 4/3/2011)

**Justifique cuidadosamente todas as suas respostas.**

1. Problema 5 da Ficha 1: Na palavra binária

$$01111000000?001110000?0011001100101011100000000?01110$$

codificou-se uma data. O sistema utilizado consistiu em escrevê-la primeiro na forma de 6 dígitos decimais seguidos (por exemplo, 290296 quer dizer 29 de Fevereiro de 1996) e passar esse número para a base 2 (no exemplo acima 290296 transforma-se em 1000110110111111000) e em seguida codificar de acordo com a regra

$$\begin{aligned} \{0,1\}^2 &\longrightarrow \mathcal{C} \subseteq \{0,1\}^6 \\ 00 &\longmapsto 000000 \\ 01 &\longmapsto 001110 \\ 10 &\longmapsto 111000 \\ 11 &\longmapsto 110011 \end{aligned}$$

Na palavra recebida há 3 bits que não se conhecem (foram apagados) e possivelmente outros que estão trocados.

(a) Encontrar os 3 bits apagados;

(b) Dizer quantos bits e em que posições estão errados;

(c) De que data se trata?

(d) Repetir o problema trocando os bits das posições 15 e 16.

2. Problema 1 da Ficha 1: Quais as capacidades de correcção e detecção *simultâneas* de erros de um código de distância mínima d. Discuta e comente separadamente os casos de d par e ímpar. Dê exemplos ilustrativos.

3. Mostre que $A_2(5,4) = 2$ e $A_2(8,5) = 4$.

4. Problema 1 da Ficha 2:

(a) Dados dois vectores $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_m)$, define-se $(u|v) = (u_1, \ldots, u_n, v_1, \ldots, v_m)$. Sejam $C_1$ e $C_2$ códigos binários de parâmetros $(n, M_1, d_1)$ e $(n, M_2, d_2)$, respectivamente. A Construção de Plotkin dos códigos $C_1$ e $C_2$ é o código dado por

$$C_1 * C_2 = \{(u|u+v) : u \in C_1, v \in C_2\} .$$

Mostre que os parâmteros de $C_1 * C_2$ são $(2n, M_1M_2, d)$, onde $d = \min\{2d_1, d_2\}$.

(b) A importante família de Códigos de Reed-Muller binários pode ser obtida por recorrência do seguinte modo:

$$\forall\, r, m \in \mathbb{N}_0 : \begin{cases} RM(0,m) = \{\vec{0}, \vec{1}\} & \text{código de repetição binário de comprimento } 2^m \\ RM(m,m) = (\mathbb{F}_2)^{2^m} & \\ RM(r,m) = RM(r,m-1) * RM(r-1,m-1)\ , & 0 < r < m \end{cases}$$

onde $C_1 * C_2$ designa a Construção de Plotkin obtida dos códigos $C_1$ e $C_2$.

Estudar esta família de códigos, mostrando que $RM(r,m)$ tem parâmetros: $n = 2^m$, $M = 2^{\delta(r,m)}$, onde $\delta(r,m) = \sum_{i=0}^{r} \binom{m}{i}$, $d = 2^{m-r}$.