COMBINATÓRIA E TEORIA DE CÓDIGOS
TPC 6

(para entregar até 11/6/2011)

Justifique cuidadosamente todas as suas respostas.

1. Seja $C = \mathrm{Ham}(3,2)$ o código de Hamming binário de redundância 3, com polinómio gerador $g(t) = 1 + t + t^3$.

   (a) Determine os parâmetros e o polinómio gerador de $C^{(3)}$.

   (b) Mostre que o código $C^{(3)}$ corrige todos os erros-m acumulados com $m \leq 3$.

   (c) Usando o Algoritmo Caça ao Erro Acumulado, descodifique o vector recebido

   $$y(t) = t + t^3 + t^5 + t^7 + t^8 + t^9 + t^{11} \ .$$

2. Seja C o código binário linear com a seguinte matriz de paridade

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

   Determine a distância mínima $d(C)$ e indique a capacidade de detecção e de correcção de erros deste código. Mostre ainda que C detecta todos os erros-m acumulados com $m \leq 3$.

   NOTA: Neste exercício, está-se a considerar apenas vectores erros-m acumulados no sentido "estrito", i.e., vectores da forma $(0,\ldots,0,1,*,\ldots,*,1,0,\ldots,0)$ com as coordenadas não nulas entre os índices $i \geq 1$ e $i+m-1 \leq n$.

3. Um código cíclico q-ário de comprimento n diz-se *degenerado* se existe $r \in \mathbb{N}$ tal que r divide n e cada palavra do código se escreve na forma $c = c'c'\cdots c'$ com $c' \in \mathbb{F}_q^r$, isto é, cada palavra do código consiste em n/r cópias idênticas de uma sequência c' de comprimento r.

   (a) Seja C o código do exercício anterior. Mostre que o pontuado, na última coordenada, do dual $C^\perp$ é um código cíclico e degenerado, e determine o seu polinómio gerador.

   (b) Determine todos os códigos binários, cíclicos e degenerados de comprimento 9, indicando os respectivos polinómios geradores e a correspondente sequência de comprimento r.

4. Seja C o código Reed-Solomon sobre $\mathbb{F}_8$ com polinómio gerador $g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)$, onde $\alpha \in \mathbb{F}_8$ é uma raíz de $1 + t + t^3$.

   (a) Justifique que α é um elemento primitivo de $\mathbb{F}_8$.

   (b) Determine os parâmetros de C.

   (c) Determine os parâmetros do código dual $C^\perp$.

   (d) Determine os parâmetros da extensão $\widehat{C}$.

   (e) Determine os parâmetros da concatenação $C^* = \phi^*(C)$, onde $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ é a aplicação linear definida por $\phi(1) = 100$, $\phi(\alpha) = 010$ e $\phi(\alpha^2) = 101$.

5. Um código linear C diz-se *auto-ortogonal* se $C \subseteq C^\perp$. Determine o polinómio gerador de todos os códigos Reed-Solomon, sobre $\mathbb{F}_{16}$, auto-ortogonais. Quais desses códigos são auto-duais?