COMBINATÓRIA E TEORIA DE CÓDIGOS

TPC 6 (para entregar na aula de 30/5/2014)

Observação: Os exercícios 1 a 4 valem 20 pontos no total, o exercício bónus A vale 4 pontos extra.

1. Seja $C = \mathrm{Ham}(3,2)$ o código de Hamming binário de redundância 3 e com polinómio gerador $g(t) = 1 + t + t^3$
   (a) Determine os parâmetros $[n,k,d]$ do código entrelaçado $C^{(3)}$.
   (b) Determine o polinómio gerador e o de paridade de $C^{(3)}$.
   (c) Mostre que $C^{(3)}$ corrige todos os erros-m acumulados com $m \leq 3$, mas não corrige todos os erros acumulados de comprimento 4.
   (d) Usando o Algoritmo Caça ao Erro Acumulado, descodifique o vector recebido
   $$y(t) = t + t^3 + t^4 + t^9 + t^{13} \ .$$

2. Seja $C = \langle (0,\alpha,\alpha^2,1),(1,1,1,1)\rangle \subset \mathbb{F}_4^4$, onde $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ com $\alpha^2 = 1+\alpha$.
   (a) Determine uma matriz geradora e os parâmetros do código concatenação $C^* = \phi^*(C)$, onde $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2$ é a aplicação linear sobre $\mathbb{F}_2$ definida por $\phi(1) = 10$ e $\phi(\alpha) = 01$.
   (b) Justifique que o código C^* é equivalente a $\widehat{\mathrm{Ham}}(3,2)^{\perp}$.

3. (Exercício 9.9 das notas.) Seja C um código $[q-1,k]$ sobre $\mathbb{F}_q$ com matriz geradora
   $$G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \alpha^{3(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{bmatrix} ,$$
   onde α é um elemento primitivo de $\mathbb{F}_q$.
   (a) Mostre que C é um código cíclico.
   (b) Determine o polinómio gerador e conclua que C é um código de Reed-Solomon.

4. Seja $C \subset \mathbb{F}_5^4$ o código cíclico com polinómio gerador $g(t) = (t-2)(t-4)$.
   (a) Justifique que C é um código Reed-Solomon e indique os seus parâmetros.
   (b) Indique os parâmetros e uma matriz geradora da extensão $\widehat{C}$.
   (c) Seja $\widetilde{C}$ um código cíclico de comprimento 5 e dimensão 2. Escreva uma matriz geradora para $\widetilde{C}$ e mostre que este código é linearmente equivalente a $\widehat{C}$.
   (d) Conclua que qualquer código cíclico, não nulo, de comprimento 5 sobre $\mathbb{F}_5$ é MDS.

A. (Exercício 9.7 das notas.)

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