COMBINATÓRIA E TEORIA DE CÓDIGOS
TPC 2

(para entregar até 18/3/2011)

Justifique cuidadosamente todas as suas respostas.

1. Problema 1 da Ficha 3: (Construção do Corpo $\mathbb{F}_{2^4}$)
   (a) Verifique que o polinómio $x^4 + x + 1$ é irredutível em $\mathbb{F}_2[x]$.
   (b) Construa então $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$ idenficando os seus elementos e esboçando as respectivas tabelas de adição e multiplicação.
   (c) É capaz de identificar um elemento primitivo daquele corpo?

2. Seja V um subespaço vectorial de $\mathbb{F}_q^n$ de dimensão $1 \leq k \leq n$.
   (a) Quantos vectores contém V?
   (b) Quantas bases distintas tem V?

3. (a) Mostre que $\mathbb{F}_{q^m}$ é um espaço vectorial sobre $\mathbb{F}_q$, com a soma e o produto por um escalar definidos à custa das operações em $\mathbb{F}_{q^m}$.
   (b) Seja $f(x) \in \mathbb{F}_q[x]$ um polinómio de grau m, irredutível em $\mathbb{F}_q[x]$, e seja $\alpha \in \mathbb{F}_{q^m}$ uma raiz de $f(x)$. Mostre que $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

4. Considere a aplicação $< \cdot, \cdot >_H : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \longrightarrow \mathbb{F}_{q^2}$ definida por

$$< u, v >_H = \sum_{i=1}^{n} u_i v_i^q \ ,$$

   onde $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^2}^n$. Mostre que $< \cdot, \cdot >_H$ é um produto interno em $\mathbb{F}_{q^2}^n$.

   Nota: $< \cdot, \cdot >_H$ diz-se o *produto interno hermítico*. O *dual hermítico* do código linear C é definido por

$$C^{\perp_H} = \{v \in \mathbb{F}_{q^2}^n \ : < v, c >_H = 0 \quad \forall c \in C\} \ .$$

5. Recorde que $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle = \{0, 1, \alpha, \alpha^2\}$, onde α é uma raiz de $x^2 + x + 1 \in \mathbb{F}_2[x]$. Mostre que os seguintes códigos lineares sobre $\mathbb{F}_4$ são auto-duais em relação ao produto interno hermítico definido no problema anterior:
   (a) $C_1 = \langle (1, 1)\rangle \subset \mathbb{F}_4^2$,
   (b) $C_2 = \langle (1, 0, 0, 1, \alpha, \alpha), (0, 1, 0, \alpha, 1, \alpha), (0, 0, 1, \alpha, \alpha, 1)\rangle \subset \mathbb{F}_4^6$.

   Serão estes códigos auto-duais em relação ao produto interno euclideano?