COMBINATÓRIA E TEORIA DE CÓDIGOS
HOMEWORK 2

(deadline 18/3/2011)

Justify all your answers.

1. Problem 1 in Exercise List 3: (The field $\mathbb{F}_{2^4}$)
   (a) Show that the polynomial $x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.
   (b) Define $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$ by identifiying its elements and by sketching the addition and multiplication tables.
   (c) Find a primitive element in $\mathbb{F}_{2^4}$.

2. Let V be a vector subspace of $\mathbb{F}_q^n$, with dimention $1 \leq k \leq n$.
   (a) How many vectors does V contain?
   (b) How many distinct bases does V have?

3. (a) Show that $\mathbb{F}_{q^m}$ is a vector space over $\mathbb{F}_q$, with the vector sum and product by a scalar defined via the operations in $\mathbb{F}_{q^m}$.
   (b) Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial in $\mathbb{F}_q[x]$, with degree m, and let $\alpha \in \mathbb{F}_{q^m}$ be a root $f(x)$. Show that $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

4. Let $< \cdot, \cdot >_H : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \longrightarrow \mathbb{F}_{q^2}$ be defined by

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

   where $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^2}^n$. Show that $< \cdot, \cdot >_H$ is an inner product in $\mathbb{F}_{q^2}^n$.
   Remark: $< \cdot, \cdot >_H$ is the *hermitian inner product.* The *hermitian dual* of a linear code C is defined as

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

5. Recall that $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle = \{0, 1, \alpha, \alpha^2\}$, where α is a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$. Show that the following linear codes over $\mathbb{F}_4$ are self-dual with respect to the hermitian inner product defined in the previous problem:
   (a) $C_1 = \langle (1, 1)\rangle \subset \mathbb{F}_4^2$,
   (b) $C_2 = \langle (1, 0, 0, 1, \alpha, \alpha), (0, 1, 0, \alpha, 1, \alpha), (0, 0, 1, \alpha, \alpha, 1)\rangle \subset \mathbb{F}_4^6$.

   Are these self-dual codes with respect to the euclidean inner product?