COMBINATÓRIA E TEORIA DE CÓDIGOS

Homework 3 (deadline 5/4/2013, in class)

1. For each $x \in \mathbb{F}_{q^m}$, we define its trace by $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$.
   (a) Show that $(a+b)^{q^i} = a^{q^i} + b^{q^i}$ for all $a, b \in \mathbb{F}_{q^m}$ and $i \in \mathbb{N}$.
   Sugestion: First show that $(a+b)^p = a^p + b^p$, where p is the characteristic of $\mathbb{F}_{q^m}$.
   (b) Justify that, for all $a \in \mathbb{F}_{q^m}$, $a \in \mathbb{F}_q \subset \mathbb{F}_{q^m}$ if and only if $a^q = a$.
   (c) Show that $\mathrm{Tr}(x) \in \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^m}$.
   (d) Show that $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ is a linear aplication over $\mathbb{F}_q$.
   (e) If C is a $[N, K, D]$ linear code over $\mathbb{F}_{q^m}$, we define the *trace code* by

   $$\mathrm{Tr}(C) = \{(\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_N)) : (x_1, \ldots, x_N) \in C\} .$$

   Show that $\mathrm{Tr}(C)$ is a q-ary linear code, with length N and dimension $k \leq mK$.

2. Consider the linear code $C = \langle(\alpha, \alpha^2, \alpha^4, 1, \alpha^3, \alpha^6, \alpha^5)\rangle$ over $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where $\alpha^3 = 1+\alpha$.
   (a) Find the parameters of C.
   (b) Determine a generator matrix for the trace code $\mathrm{Tr}(C)$.
   (c) Find the parameters of the dual code $\mathrm{Tr}(C)^{\perp}$.
   (d) Is $\mathrm{Tr}(C)$ a self-orthogonal or a self-dual code?

   If C is a linear code over $\mathbb{F}_{q^m}$, we define the *subfield subcode* by

   $$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^N .$$

   You can use, without proof, that the subfield subcode $C|_{\mathbb{F}_q}$ is linear over $\mathbb{F}_q$.

   (e) Determine a generator matrix for the dual code $C^{\perp}$ and for the subfield subcode $(C^{\perp})|_{\mathbb{F}_2}$.
   (f) Verify that $(C^{\perp})|_{\mathbb{F}_2} = \mathrm{Tr}(C)^{\perp}$.
   Note: This relation between the trace code and the subfield subcode holds for any linear code C over $\mathbb{F}_{q^m}$, it's the Delsarte Theorem.

3. (a) For a q-ary linear code, with lenght n and minimum distance d, show that the vectors $x \in \mathbb{F}_q^n$ with weight $\mathrm{w}(x) \leq \lfloor \frac{d-1}{2} \rfloor$ are coset leaders of distinct cosets of this code.

   (b) Let C be a perfect code with $\mathrm{d}(C) = 2t + 1$. Show that the only coset leaders of C are the ones determined in part (a).

   (c) Assuming that the perfect code C in part (b) is binary, let $\widehat{C}$ be the code obtained from C by adding a parity-check digit, i.e.,

$$\widehat{C} = \Big\{(x_1, \dots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} : (x_1, \dots, x_n) \in C \,, \sum_{i=1}^{n+1} x_i = 0\Big\} \,.$$

   Show that the weight of any coset leader of $\widehat{C}$ is less or equal than $t + 1$.

4. Let C be the linear code over $\mathbb{F}_3 = \{0, 1, 2\}$, with the following parity-check matrix

$$H = \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \end{bmatrix} .$$

   (a) Find the parameters $[n, k, d]$ for C.

   (b) Find a generator matrix for C.

   (c) Show that C corrects all simple errors with magnitude 1 and all the double errors of the form

$$aa000000\,, \quad 0aa00000\,, \quad 00aa0000\,, \quad 000aa000\,,$$
$$0000aa00\,, \quad 00000aa0\,, \quad 000000aa \quad \text{and} \quad a000000a\,,$$

   where $a \in \{1, 2\}$.

   (d) Decode the following received vectors

$$y = 11111112 \qquad \text{and} \qquad z = 11211200\,.$$