COMBINATÓRIA E TEORIA DE CÓDIGOS

Homework 5 (deadline 10/5/2013, in class)

1. (a) Write $t^{12} - 1$ as a product of irreducible polynomials in $\mathbb{F}_2[t]$.
   (b) How many binary cyclic codes with length 12 are there?
   (c) Determine for which k there is a binary cyclic $[12, k]$ code.
   (d) How many binary cyclic $[12, 9]$ codes are there?
   (e) Determine all self-dual binary cyclic codes with length 12, and their generator polinomials.

2. Determine the generator polynomial and the dimention of the smallest ternary cyclic code which contains the word $c = 220211010000 \in \mathbb{F}_3^{12}$.

3. (Exercise 8.8 in the notes.) Let C be a binary cyclic code with generator polynomial $g(t)$.
   (a) Show that, if $t - 1$ divides $g(t)$, then all code words have even weight.
   (b) Assuming C has odd length, show that C contains an odd weighted word if and only if the vector $\vec{1} = (1, \ldots, 1)$ is a code word.

4. (Exercises 8.14 and 8.15 in the notes.)
   (a) Let $g(t)$ be the generator polynomial of a binary Hamming code $\mathrm{Ham}(r, 2)$, with $r \geq 3$. Show that the parameters of $C = \langle (t-1)g(t) \rangle$ are $[2^r - 1, 2^r - r - 2, 4]$. [Sugestion: apply exercise 3.]
   (b) Show that the code C can be used to correct all adjacent double errors.
   (c) (Generalization of the previous part.) Let $C = \langle (t+1)f(t) \rangle$ be a binary cyclic code with length n, where $f(t) \mid t^n - 1$, but $f(t) \nmid t^i - 1$, for $1 \leq i \leq n-1$. Show that C corrects all simple errors and also the adjacent double errors.

5. (Exercise 8.16 in the notes.) Consider binary cyclic code with length $n = 15$ generated by the polynomial $g(t) = 1 + t^3 + t^4 + t^5 + t^6$.
   (a) Justify that $g(t)$ is indeed the generator polynomial of this code.
   (b) Write a generator matrix, the check polynomial and a parity-check matrix for this code.
   (c) Write a generator matrix in the form $G = \begin{bmatrix} R & I \end{bmatrix}$ for this code and the corresponding parity-check matrix.
   (d) Use systematic coding to encode the message vector $m = 010010001$.
   (e) Given that this code has minimum distance $d(C) = 5$, decode the received vector $y = 010011000111010$, and carefully justify your procedure.