IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises III.

1. Consider the binary cyclic code C of length 7 with the generating polynomial $g(x) = x^3 + x + 1$.

   a) Find the generating matrix G and the parity check matrix H.

   b) Decide whether the code C is perfect or not.

   c) Encode the message 1001.

2. Find a generator polynomial for the smallest binary cyclic code containing codewords 00101000 and 01001000.

3. Let $g(x) = g_k x^k + \cdots + g_1 x + g_0 \neq 0$ be a generator polynomial of some cyclic code C. Show that $g_0 \neq 0$.

4. For $k \in \{0, 1, \ldots, 5\}$ let n_k be the number of different cyclic codes over $GF(31)$ which have length 5 and dimension k. Find n_0, n_1, $\ldots$, n_5.

5. How many ternary cyclic codes of length 6 are there? Give the generator polynomial for each such code and one generator matrix for each dimension.

6. Which of the following codes are cyclic?

   a) $\{000, 111, 222\} \subset \mathbb{F}_3^3$

   b) $\{000, 100, 010, 001\} \subset \mathbb{F}_q^3$

   c) $\{x_0 x_1 ... x_{n-1} \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} x_i = 0\}$

   d) $\{x_0 x_1 ... x_{n-1} \in \mathbb{F}_8^n \mid \sum_{i=0}^{n-1} x_i^2 = 0\}$

   e) $\{x_0 x_1 ... x_{n-1} \in \mathbb{F}_2^n \mid \sum_{i=0}^{n-1} (x_i^2 + x_i) = 0\}$

7. Show that the dual code of a cyclic code is cyclic.