IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises III.

1. Suppose that a cyclic shift of each row of a generator matrix G of a linear code C belongs to C. Show that C is a cyclic code.

2. Determine d and find generator polynomials and generator matrices for

   (a) all binary cyclic codes in R_4;

   (b) all ternary cyclic codes in R_5.

3. (a) How many binary cyclic codes of length 7 are there?

   (b) Find a binary cyclic code of length 7 which contains exactly 32 codewords or show that such a code does not exist.

4. Let C be a binary cyclic code and $g(x)$ its generator polynomial. Show that $C = C^{\perp}$ if and only if $x^{n-k}g(x)g(x^{-1}) = x^n - 1$.

5. (a) Which Hamming codes are maximum distance separable?

   (b) Let C be a q-ary $[n, k]$-code that is maximum distance separable. What is the number of words with minimum weight $d = n - k + 1$ in C?

6. Show that $C^{\perp}$ is equivalent to the cyclic code $\langle h(x) \rangle$ where $h(x)$ is the check polynomial of a cyclic code C.