IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises III.

1. Provide the generator polynomial for

   (a) the smallest cyclic code containing word 0011010;

   (b) code dual to the $[7,4,3]$ code with $g(x) = x^3 + x + 1$.

2. Let C_1 and C_2 be cyclic codes over $\mathbb{F}_q$ with generator polynomials $g_1(x)$ and $g_2(x)$, respectively. Prove that $C_1 \subseteq C_2$ if and only if $g_2(x) \,|\, g_1(x)$.

3. $(x+1) \,|\, (x^n - 1)$ over $\mathbb{F}_2$. Let C be the binary cyclic code $\langle x+1 \rangle$ of length n and let C_1 be any binary cyclic code of length n with generator polynomial $g_1(x)$.

   (a) What is the dimension of C?

   (b) Prove that C is the set of all vectors in $\mathbb{F}_2^n$ with even weight.

   (c) If C_1 has *only* even weight codewords, what is the relationship between $x+1$ and $g_1(x)$?

   (d) If C_1 has *some* odd weight codewords, what is the relationship between $x+1$ and $g_1(x)$?

4. Find irreducible factors of $x^5 - 1$ in $\mathbb{Z}_2[x]$ and hence determine all cyclic codes of length 5.

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

6. Which binary Hamming codes are maximum distance separable?

Bonus Suppose C is a linear $[n,k]$ code over $\mathbb{F}_2$ with generator matrix G. Answer the following questions. Include proofs.

   (i) Given m linearly independent codewords, how many linear codes containing all of them exist? Can you express it recursively?

   (ii) Let ρ be a transposition on columns of the class of $k \times n$ matrices over GF(2). Formulate a condition that is both necessary and sufficient for the code C' generated by matrix $\rho(G)$ to be *different* from the code C (note that the code C' is equivalent with C).

   (iii) In lecture 1 we defined that two codes are equivalent if one can be obtained from the other by a sequence of applications of rules `a)` and `b)`, where

   `a)` a permutation of the positions of the code,

   `b)` a permutation of symbols appearing in a fixed position.

   However, this definition has a flaw when applied to linear codes.

   (a) Consider both rules and answer which is flawed for linear codes. Why?

   (b) Describe as accurately as possible the assumptions that need to be made so that the flawed rule(s) produce an equivalent code in the sense of equivalence for linear codes as described in lecture 2. Consider only binary linear codes.

   (c) Describe equivalent codes the application of the flawed rule(s) produces. Consider only binary linear codes.