IV054 Coding, Cryptography and Cryptographic Protocols
2014 - Exercises III.

1. Find a cyclic code equivalent to the non-cyclic code $C = \{0000, 1100, 0011, 1111\}$.

2. Suppose a linear $[8, 5]$ code C has the following generator matrix:

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

   (a) Prove that C is a cyclic code.
   (b) Find a generator polynomial of C.

3. Show that the $[7, 4, 3]$ binary code with $g(x) = x^3 + x + 1$ and the $[7, 3, 4]$ binary code with $g(x) = x^4 + x^3 + x^2 + 1$ are duals.

4. Consider the linear code C over $\mathbb{F}_q$ with the generator matrix G

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

   Show that for all q, C is not cyclic.

5. Consider the polynomial $g(x) = x^5 + x^2 + 1$ over $\mathbb{F}_2$.

   (a) Show that $g(x)$ is the generating polynomial of a binary cyclic code of length 31.
   (b) Find the dimension of this code.
   (c) Find its parity check polynomial.

6. Find a generator matrix and a parity check matrix of a cyclic code equivalent to Hamming code $Ham(4, 2)$.

7. Let C be a binary cyclic code of odd length n. Prove that exactly one of the following holds:

   (i) Every codeword in C has even weight.
   (ii) The word $1 \ldots 1$ is a codeword.

8. Let C be a binary cyclic code of length 15 and dimension 11 such that $000111111111100 \in C$ and no word of its dual code has odd weight. Find the generator polynomial of C.