IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises III.

1. Decide whether the following binary codes are cyclic and whether they are equivalent to a cyclic code:
   (a) $C_1 = \{0000, 1000, 0100, 0010, 0001, 1111\}$
   (b) $C_2 = \{000, 100, 001, 101\}$
2. Consider the binary cyclic code of length 7 with the generating polynomial $g(x) = x^4 + x^2 + x + 1$.
   (a) Find the generator matrix.
   (b) Find the parity check polynomial and the parity check matrix.
   (c) Encode 110.
3. For each code C with codewords of length n a reverse code $\bar{C}$ is defined as

$$\bar{C} = \{x_1 x_2 \dots x_n \mid x_n x_{n-1} \dots x_1 \in C\}.$$

   (a) Show that for each cyclic code C, its reverse code $\bar{C}$ is also cyclic.
   (b) Show that for each binary cyclic code C with codewords of length $n \leq 6$, $C = \bar{C}$.
   (c) Find an example of a binary code with codewords of length 7, such that $C \neq \bar{C}$.
4. Prove the following. Let C_1 and C_2 be cyclic codes with generator polynomials $g_1(x)$ and $g_2(x)$. Then $C_1 \subseteq C_2$ if and only if $g_2(x)$ divides $g_1(x)$.
5. (a) How many binary cyclic codes of length 7 are there?
   (b) How many ternary cyclic codes of length 7 are there?
   (c) Is there a ternary cyclic code of length 10 and dimension 7?
6. Find the generator polynomial of the code

$$C = \{a_1 \cdots a_n \mid a_1, \dots, a_n \in \mathbb{Z}_p, \sum_{i=1}^{n} a_i \equiv 0 \pmod{p}\},$$

   where p is prime.
7. Consider the convolution code defined by the generator matrix

$$G = \begin{pmatrix} x^2 + x + 1 & 1 & x + 1 \\ 1 & x^2 & x^2 + x \end{pmatrix}$$

   and encode the message $(x + 1, x^2)$ using this code.
8. Let $k \in \mathbb{N}_0$ be a non negative integer. How many binary cyclic codes of length 2^k are there?