IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises III.

1. Consider the following binary linear $[8,5]$-code C generated with

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

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

2. Which of the following binary codes are cyclic? Explain your reasoning.
   (a) $C_1 = \{000, 001, 100, 101\}$
   (b) $C_2 = \{000, 001, 010, 100\}$
   (c) $C_3 = \{0, 1\}$
   (d) $C_4 = \{0000, 0101, 1010, 1111\}$

3. Compute a generator polynomial and a parity check polynomial of a binary cyclic code of length 12 and dimension 5. Encode the word 00100.

4. Provide the generator polynomial of the smallest binary cyclic code containing codeword 0001001.

5. Consider a binary cyclic code C with a generator polynomial $g(x)$. Show that $g(1) = 0$ if and only if weight of each word in C is even.

6. How many quinary cyclic codes of length seven are there? Give a generator polynomial for each of them.

7. Let C be a cyclic code over $\mathbb{F}_q$ of length 7 such that 1110000 is an element of C. Show that C is a trivial code (*ie.* $\mathbb{F}_q^n$ or $\{0^n\}$) if q is not a power of 3.