Exercise 5 - Cyclic Codes Basics

Q1. Note that $g(x) = x^6 + x^3 + 1$ divides $x^9 - 1$ in $\mathbb{F}_2[x]$.

i) Show that $g(x)$ can be used as generator polynomial of a binary cyclic $(9, k)$ code C, i.e.,

$$C = \{a(x)g(x) \mid i(x) \in \mathbb{F}_2[x], \deg(a(x)) < 3\}$$

ii) What is the dimension of C ?

iii) Determine a generator matrix of C.

iv) Is $x^8 + x^6 + x^5 + x^3 + x^2 + 1$ a codeword of C ?

v) What can you say about the minimum distance of C ?

Q2. The polynomial $x^{15} - 1$ can be factored into irreducible polynomials over $\mathbb{F}_2$ as

$$x^{15}-1 = (x+1)\left(x^2 + x + 1\right)\left(x^4 + x + 1\right)\left(x^4 + x^3 + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right).$$

Let C be the binary cyclic code of length 15 that has generator polynomial

$$g(x) = (x + 1)\left(x^4 + x + 1\right)$$

i) What is the dimension of C ?

ii) Is $x^{14} + x^{12} + x^8 + x^4 + x + 1$ a codeword in C ?

iii) Determine all cyclic binary $(15, 8)$ codes.

iv) How many cyclic binary codes of length 15 are there?

Q3. Let C be the cyclic code of length 15 that has generator polynomial $g(x) = x^4 + x + 1$.

i) Determine a parity check matrix of C.

ii) Find the minimum distance of C.

iii) What is C ?

iv) What is the dimension of $C^{\perp}$?

*The above questions are taken from the textbook Ch. 5.

Programming Tasks

T1. Use SageMath to verify your answers to the above questions.

T2. Use SageMath to investigate the factorization of $x^{31} - 1$ over $GF(2)$.

T3. From the factorization of $x^{31} - 1$, pick three different generator polynomials $g(x)$ and derive cyclic codes from them. Use SageMath to check the parameters of the obtained codes.