INF243-Mandatory Assignment 3

***Submission Deadline**: March 20th, 2023*

Instructions for the assignment:

- This assignment has 3 pages and accounts for 10 points for your final grade
- Prepare a PDF file for your answers
  - you can use Latex (see manual at this link) as the text editor which compiles to a nice PDF file
  - you can use MS word as the text editor and convert it to a PDF file
  - you can answer the questions in a hand note, make sure that your hand writing can be easily recognized; you can take photo of your handnote and convert it to a PDF file
- For the implementation assignment, you can use SageMath, Matlab, Python or other languages.
  - make sure to properly comment your source code.
  - Compress your source code as a ZIP file and include it in your submission

Q1. Basics on Finite Fields [0.5+0.5+1 pts]

(i) For an irreducible polynomial $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ with a root α, use it to create a polynomial representation of $GF(2^4)$. Use this representation of $\mathbb{F}_{2^4}$ to show that α is not a primitive element while $\beta = \alpha + 1$ is primitive. (A primitive element w in $\mathbb{F}_{2^4}$ can represent any nonzero element as a^i for certain integer $0 \le i < 2^4 - 2$.)

(ii) Find the minimal polynomial $q(x)$ of $\beta = \alpha + 1$.

(iii) Use the minimal polynomial $q(x)$ to generate $\mathbb{F}_{2^4}$, and create a table such as Table 5.1 (Page 206) in the textbook including the Zech logarithms (Page 211).

Q2. Basics on factorization. [1 pt]

Partition the set $\{1, 2, \ldots, 2^m - 2\}$ into cyclotomic cosets modulo $2^m - 1$ for $m = 3, 4, 5, 6$. Suppose α is a primitive element of $GF(2^5)$ generated by $x^5 + x^2 + 1$. Use your cyclotomic cosets for $m = 5$ to factorize $x^{31} - 1$ into a product of polynomials over $\mathbb{F}_2$.

Q3. BCH codes [1+1 pts]

Let α be a root of the polynomial $f(x) = x^6 + x^4 + x^3 + x + 1$ in $\mathbb{F}_2[x]$, which is used to generate the finite field $\mathbb{F}_{2^6}$.

Suppose a binary BCH code $\mathcal{C}$ of length 63 is defined by the generator polynomial $g(x)$ that has roots

$$\alpha, \alpha^3, \alpha^5, \alpha^6, \alpha^7.$$

(i) What is the BCH bound on the minimum distance of the code $\mathcal{C}$?

(ii) Suppose a message $\mathbf{m}$ has a binary representation as

$$\begin{aligned} \mathbf{m} &= m_0 m_1 \ldots m_{38} \\ &= 000001111100000111110000011111000001010. \end{aligned}$$

Encode this message in the systematic way.

Q4. BCH Decoder (Implementation) [4+1 pts]

Read Section 6.3 and 6.4. Build a decoder for narrow-sense binary BCH codes, which uses

- Peterson's algorithm to obtain error-locator polynomial $\Lambda(x)$; and
- Chien search to find the roots of $\Lambda(x)$.

(i) Thoroughly test your decoder on the binary $(15, 5)$ BCH code with generator polynomial

$$g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$

Your decoder should correct all received words with errors of Hamming weight up to 3.

(ii) For the BCH code defined in Q3, suppose a codeword $\mathbf{c}$ in $\mathcal{C}$ is transmitted and the following word is received:

$$\begin{aligned} \mathbf{r} &= r_0 r_1 \ldots r_{62} \\ &= 010000000000011111000001011011111010101011000001111011010110111. \end{aligned}$$

Assume that this word can be uniquely decoded. Use the syndrome decoding to obtain the codeword.