INF243-Mandatory Assignment 2

***Submission Deadline**: Feb. 27th, 2023*

Instructions for the assignment:

- This assignment has 2 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. For each of the following codes, decide whether it is a linear code. [1 pt]

- $\mathcal{C}_1 = \{w \in \mathbb{F}_2^7 \mid \text{number of 1's is even }\}$
- $\mathcal{C}_2 = \{021, 201, 102, 111, 210, 000, 222, 120\}$ over $\mathbb{F}_3$

Q2. Let q be a prime power and m be a positive integer. Prove that all Hamming codes with parameters

$$\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3\right]_q$$

are perfect. [1 pt]

Q3. The generator matrix for a code $\mathcal{C}$ over $GF(2)$ is given by

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

Determine the systematic generator matrix and parity check matrix of a code equivalent to the code C. [1 pt]

Q4. Suppose the generator and parity check matrix for a binary code $\mathcal{C}$ are given by [3 pts]

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

- Verify that H is a parity check matrix for this generator
- Determine the minimum distances of the codes $\mathcal{C}$ and $\mathcal{C}^\perp$
- List the codewords in the dual code $\mathcal{C}^\perp$
- Form the syndrome decoding table for $\mathcal{C}$
- Decode the received word $\mathbf{r} = [1, 1, 1, 0, 0, 1]$
- Write down an explicit expression for $P(E)$ for this code. Evaluate this when $p = 0.01$

Q5. **Implementation of CRC Encoding and Decoding**. [4 pts]

Write CRC encoder and CRC decoder with the generator polynomial $g(x) = x^{16} + x^{10} + x^8 + x^7 + x^3 + 1$.

- Generate a random file of size 1 MB with message block length of 1024 bytes. Use the file to test your programs (First encode then decode the file, and then compare the decoded file with the original)
- Test your programs further by passing the encoded data through a binary symmetric channel with crossover probabilities of $0.00001, 0.001,$, and 0.1. Are there any blocks of data that have errors that are not detected?