Sample Assignment 2
Minimal Polynomials and Intro to Linear Block Codes

Question 1

Using $p(X)=1+X^2+X^5$ as the primitive polynomial, generate expressions for all elements of GF(32) as functions of 1, α, α^2, α^3, and α^4. Produce an addition table for GF(32) (which will be helpful for question 2).

Question 2

Factor $X^{31}+1$ by finding the minimal polynomials of GF(32) with respect to GF(2). (hint: you need to find the conjugacy classes of each element of GF(32). These are the roots of the minimal polynomials).

Question 3

A binary linear block code is described by the following generator matrix:

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

(a) What are n, k and r of the code?
(b) Find all codewords of the code.
(c) What is the minimum Hamming distance of the code?
(d) Find the parity check matrix H for this code.

Question 4

A systematic nonbinary code uses GF(4) symbols and has the following generator matrix:

$$G = \begin{bmatrix} 1 & 0 & \alpha & 1 & \alpha^2 \\ 0 & 1 & \alpha^2 & \alpha & 1 \end{bmatrix}$$

(a) What is the rate of this code?
(b) Find the parity check matrix H for this code.
(c) What is the minimum distance of this code?