PROBLEM 1. In this problem we will show that a binary linear code contains 2^k codewords for some k. Suppose C is a binary linear code of block length n, that is, C is a non-empty set of binary sequences of length n with the property that if x and y are in C so is their modulo 2 sum. Consider the following algorithm.

(i) Initialize D to be the set that contains only the all-zero sequence.

(ii) If C does not contain any element not in D stop. Otherwise C contains an element x not in D. Form $D' = \{x + y : y \in D\}$.

(iii) Augment D to $D \cup D'$ where D' is found above, and go to step (ii).

(a) Show that the all-zero sequence is in C so that at the end of step (i) $D \subset C$. Note that initially $|D| = 1$ which is a power of 2.

(b) Show that if D is a linear subset of C and there is an x that is in C but not in D, then D' formed in (ii) is a subset of C. [The phrase "A is a linear subset of B" means that A is a subset of B, and that if $x \in A$ and $y \in A$ then $x + y \in A$.]

(c) Under the assumptions of (b) show that D' is disjoint from D.

(d) Again under the assumptions of (b) show that D' has the same number of elements as D.

(e) Still under the assumptions of (b) show that $D \cup D'$ is a linear subset of C.

(f) Using parts (b), (c), (d) and (e) show that if at the beginning of step (ii) D is a linear subset of C, then at the end of step (iii) D is still a linear subset of C and it has twice as many elements as in the beginning. Conclude that when the algorithm terminates $D = C$ and the number of elements in D is a power of 2.

Note that the above algorithm also gives a generator matrix G for the code: Let $x_1, \dots, x_k$ be the codewords that are picked at the successive stages of step (ii) of the algorithm. It then follows that each codeword in C can be written as a (unique) linear combination of these x_i's. Taking G as the matrix whose rows are the x_i's gives us the generator matrix.

PROBLEM 2. Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are binary linear codes of block-length n. Denote the number of codewords of $\mathcal{C}_i$ by M_i and the minimum distance of $\mathcal{C}_i$ by d_i. For $\mathbf{u} = (u_1, \dots, u_n)$ and $\mathbf{v} = (v_1, \dots, v_n)$ let $\langle \mathbf{u}|\mathbf{v} \rangle$ denote the concatenation of the two sequences, i.e.,

$$\langle \mathbf{u}|\mathbf{v} \rangle = (u_1, \dots, u_n, v_1, \dots, v_n).$$

Let $\mathcal{C}$ denote the binary code of block-length $2n$ obtained from $\mathcal{C}_1$ and $\mathcal{C}_2$ as follows:

$$\mathcal{C} = \{\langle \mathbf{u}|\mathbf{u} \oplus \mathbf{v} \rangle : \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}.$$

(a) Is $\mathcal{C}$ a linear code?

(b) How many codewords does $\mathcal{C}$ have? Carefully justify your answer. What is the rate R of $\mathcal{C}$ in terms of the rates R_1 and R_2 of the codes $\mathcal{C}_1$ and $\mathcal{C}_2$?

(c) Show that the Hamming weight of $\langle \mathbf{u}|\mathbf{u}\oplus\mathbf{v}\rangle$ satisfies

$$w_H(\langle \mathbf{u}|\mathbf{u}\oplus\mathbf{v}\rangle) \geq w_H(\mathbf{v}).$$

(d) Show that the Hamming weight of $\langle \mathbf{u}|\mathbf{u}\oplus\mathbf{v}\rangle$ satisfies

$$w_H(\langle \mathbf{u}|\mathbf{u}\oplus\mathbf{v}\rangle) \geq \begin{cases} w_H(\mathbf{v}) & \text{if } \mathbf{v}\neq\mathbf{0} \\ 2w_H(\mathbf{u}) & \text{else.}\end{cases}$$

(e) Show that the minimum distance d of $\mathcal{C}$ satisfies

$$d \geq \min\{2d_1, d_2\}.$$

(f) Show that $d = \min\{2d_1, d_2\}$.

Problem 3. Suppose the alphabet $\mathcal{X}$ has q elements and it forms a finite field when equipped with the operations $+$ and $\cdot$. Let $\alpha_0,\dots,\alpha_{m-1}$ be m distinct elements of $\mathcal{X}$. We will describe the codewords of a block code $\mathcal{C}$ of length n ($n\geq m$) as follows: a sequence $\mathbf{x} = (x_0,\dots,x_{n-1}) \in \mathcal{X}^n$ is a codeword if and only if

$$x(\alpha_i) = 0 \quad \text{for every } i = 0,\dots,m-1$$

where $x(D) = x_0 + x_1 D + \cdots + x_{n-1}D^{n-1}$.

(a) Show that the code $\mathcal{C}$ is linear.

(b) Let $g(D) = \prod_{i=0}^{m-1}(D-\alpha_i)$. Show that $(x_0,\dots,x_{n-1})$ is a codeword if and only if $x(D) = g(D)h(D)$, for some $h(D)$, and conclude that the code has q^{n-m} codewords.

Suppose now that the α_i are have the form $\alpha_i = \beta^i$, i.e., $\alpha_0 = 1$, $\alpha_1 = \beta$, …, $\alpha_{m-1} = \beta^{m-1}$.

(c) Let A be the $n\times m$ matrix

$$A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \beta & \beta^2 & \dots & \beta^{m-1} \\ 1 & \beta^2 & \beta^4 & \dots & \beta^{2(m-1)} \\ 1 & \beta^3 & \beta^6 & \dots & \beta^{3(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{n-1} & \beta^{2(n-1)} & \dots & \beta^{(n-1)(m-1)} \end{bmatrix}$$

Show that the columns of A are linearly independent.

Hint: Suppose they were dependent so that there is a column vector $\mathbf{u} = [u_0\, u_1\, \dots\, u_{m-1}]^T$ such that $A\mathbf{u} = \mathbf{0}$. How many roots does $u(D)$ have?

(d) Show that the code has minimum distance $d = m+1$.

Hint: Part (c) says that the rank of the matrix A is m.

PROBLEM 4. Consider a linear code defined over the ternary alphabet $\mathbb{F}_3 = \{0, 1, 2\}$ (equipped with modulo-3 addition and multiplication) as follows: $\mathbf{x}$ is a codeword if and only if $H\mathbf{x} = \mathbf{0}$ where

$$H = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 \end{bmatrix}$$

(and all operations are done in modulo-3 arithmetic).

(a) (4 pts) What is the blocklength, the number of codewords, and the rate of this code?

A codeword $\mathbf{x}$ is sent over a channel. It is known that during the transmission either all letters are received correctly, or, one of the letters is changed (to some other element of $\mathbb{F}_3$).

(b) (5 pts) Show that the receiver can detect if a change has happened and correct it if so.

(c) (4 pts) Suppose we are allowed to augment the matrix H by appending to it a fifth column. How will this change the rate of the code?

(d) (4 pts) Which of the following candidate columns (if any) can be appended to H and still preserve the property in (b): $\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]$?

(e) (5 pts) Suppose it is known that during the transmission all letters are received correctly, or one of the letters is changed in the following restricted way: 0 can be replaced by 1 (but not by 2); 1 can be replaced by 2 (not by 0); 2 can be replaced by 0 (not by 1). Redo part (d) for this channel.