Problem 13.1.

Consider the Binary Symmetric Channel (BSC) with cross-over probability ϵ, as seen in class. We assume $\epsilon < 0.5$.

1. Calculate the error probability if we send k bits without any coding at all across this channel. Here, "error probability" means the probability of getting one or more of the k bits wrong.
2. Show that if we instead use a $(2^m - 1, 2^m - m - 1)$ binary Hamming code, then the resulting error probability after decoding is no worse than (i.e., upper bounded by)

$$P_e^{\text{with Hamming code}} \leq 1 - (1-\epsilon)^{2^m-1} - (2^m - 1)\epsilon(1-\epsilon)^{2^m-2}$$

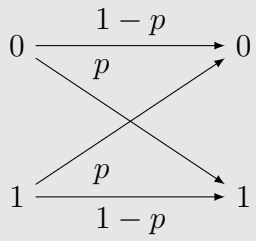
3. Compare the two. For transmission over the BSC, is it sometimes worth using the Hamming code instead of uncoded transmission? Ignore the fact that the Hamming code requires more channel uses than uncoded transmission.

Problem 13.2.

Consider the following binary linear code with $k = 3$ and $n = 5$. The code maps any binary information vector (u_1, u_2, u_3) to its codeword $(x_1, x_2, \ldots, x_5)$ according to the following rule:

$$x_1 = u_1$$
$$x_2 = u_2$$
$$x_3 = u_3$$
$$x_4 = u_1 \oplus u_2$$
$$x_5 = u_1 \oplus u_3$$

1. Find the generator matrix of the code.
2. Find a parity-check matrix for the code.
3. Find the minimum distance of the code.
4. What is the maximum number of errors that can always be corrected when this code is used?
5. Suppose that we want to transmit the information vector $u = (1, 1, 1)$. Let y be the codeword that u is mapped to by the code. What is y?
6. Suppose that codeword y is transmitted and an error of weight 1 occurred. Is it possible that for a particular error of weight 1, a minimum-distance decoder is able to correctly decode the received word back into u?
7. Codeword y is sent through a Binary Symmetric Channel (BSC) with cross-over probability $p = 0.1$, where a BSC is defined as in the figure:



What is the probability that the message is decoded correctly, given that at most one channel cross-over has occurred? (Assume that if a received word is at the same distance from two different codewords, then the minimum-distance decoder declares a decoding error.)

Problem 13.3.

Consider an (n, k) linear MDS code $\mathcal{C}$ defined over a field $\mathbb{F}_q$.

1. Argue that two different codewords of $\mathcal{C}$ cannot agree in k positions.
2. If you fix any k positions (not necessarily consecutive) of a codeword, and write down all the k-tuples that you obtain by reading out, for each codeword, the symbols at those k positions, how many different k-tuples do you get?
3. Show that one can fix any k positions in a word, and for any k-tuple of information symbols, there is a codeword in $\mathcal{C}$ that has those k information symbols in the chosen positions.
4. Argue that any k positions of a codeword can be used as the positions where we insert the k information symbols.
5. Suppose that we are given a codeword $\vec{x}$ with $n - k + e$ erasures, with $e \geq 0$. How many codewords of $\mathcal{C}$ are consistent with $\vec{x}$?

Problem 13.4.

We are sending codewords over an erasure channel and would like to guarantee that the decoder can recover the channel input codeword with a specified probability. Specifically, each channel input symbol is erased by the channel with probability 0.1, our code is an MDS linear code of $k = 3$ and yet unspecified n, and we would like to choose n so that with probability $1 - 10^{-3}$ or higher the decoder can fill in correctly the erased positions.

1. As a function of n, compute and plot the probability that the decoder cannot fill in the erased positions.
2. Determine the block length n of a Reed-Solomon code that we could use to achieve the stated goal.
3. Specify the cardinality of the smallest finite field $\mathbb{F}$ that we could use for the code.

Problem 13.5.

Consider a $(6, 3)$ Reed-Solomon code $\mathcal{C}$ over $\mathbb{F}_7 = (\mathbb{Z}/7\mathbb{Z}, +, \cdot)$. The 6 distinct field elements $\{a_1, a_2, a_3, a_4, a_5, a_6\}$ that characterize the code are chosen as $a_i = 3 - i \bmod 7$, where $i = 1, \ldots, 6$.

1. Find b, c and d, such that $\vec{x} = (0, 1, 1, b, c, d) \in \mathcal{C}$. Is your solution unique?
2. Find the systematic form G_s of a generator matrix for the code $\mathcal{C}$. Is G_s unique?
3. Compute a parity-check matrix H for the code $\mathcal{C}$.
4. What is the minimum distance of $\mathcal{C}$?
5. If we receive the word $(3, ?, ?, 0, 1, ?)$, what is the transmitted codeword?

Problem 13.6.

Consider an RS code $\mathcal{C}$ over $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ with the following parameters: $k = 3$, $n = 5$, $a_i = i$, $i = 1, 2, 3, 4, 5$. For $i = 1, \ldots, k$ let $Q_i(x)$ be the degree $k - 1$ polynomial which is 1 at $x = a_i$ and is 0 at $x = a_j$, $j \neq i$, $1 \leq j \leq k$.

1. Is $\vec{x} = \big(Q_1(a_1), Q_1(a_2), \ldots, Q_1(a_n)\big)$ an element of $\mathcal{C}$?
2. Now, consider the $k \times n$ matrix

$$A = \begin{bmatrix} Q_1(a_1) & Q_1(a_2) & \cdots & Q_1(a_n) \\ Q_2(a_1) & Q_2(a_2) & \cdots & Q_2(a_n) \\ \vdots & & & \\ Q_k(a_1) & Q_k(a_2) & \cdots & Q_k(a_n) \end{bmatrix}.$$

   Evaluate the submatrix that consists of the first k columns of A.
3. Is A a generator matrix for the code $\mathcal{C}$?

Problem 13.7.

Consider the field $\mathbb{F}_4 = (\{0, 1, a, b\}, +, \cdot)$ studied in class.

1. Find a polynomial $P(x)$ of degree at most 3 such that $P(0) = b$ and $P(1) = P(a) = P(b) = 0$.
2. Is $P(x)$ unique?
