1. Let $C$ be a binary linear code of blocklength $n$.

   (a) Show that either all codewords have even Hamming weight, or exactly half of the codewords have even Hamming weight.
   
   \[ \text{[Hint: First observe that the codewords of even weight form a subgroup of $C$. What are the cosets of this subgroup in $C$?]} \]

   (b) For any $i \in \{1, 2, \ldots, n\}$, show that either no codeword in $C$ has $i$th coordinate equal to 1, or exactly half the codewords in $C$ have $i$th coordinate equal to 1.

2. Consider the $[5, 2]$ binary linear code with systematic generator matrix

   \[
   G = \begin{bmatrix}
   1 & 0 & 1 & 1 & 0 \\
   0 & 1 & 1 & 0 & 1
   \end{bmatrix}
   \]

   A 2-bit message vector $u = [u_1 \ u_2]$ is encoded as $c = uG = [u_1 \ u_2 \ p_3 \ p_4 \ p_5]$, and transmitted across a memoryless binary symmetric channel with crossover probability $\epsilon$.

   (a) Choose as coset leaders the all-zero word, all words of weight 1, and the words $00011$ and $10001$.

   Construct the standard array, together with the syndromes corresponding to each coset.

   (b) If the standard array as above is used for decoding, what is the probability that the transmitted codeword $c$ is decoded incorrectly?

   (c) If the code is used only for error detection, what is the probability that any channel errors that take place during transmission go undetected?

   (d) If the standard array of part (a) is used for decoding, what is the probability that the first message bit, $m_1$, is decoded incorrectly?

3. An international publishing house is seeking to design a block code of length 10 over $\mathbb{F}_{11}$ to be used as an enhanced International Standard Book Number (ISBN) scheme. Their requirement is that the code, with a suitable choice of decoder, should be able to correct single transposition errors. These are errors in which exactly one pair $(c_i, c_j)$ of coordinates in a codeword $c = (c_1, c_2, \ldots, c_{10})$ gets interchanged; for example, the codeword $(1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ may get transformed to $(1, 2, 6, 4, 5, 3, 7, 8, 9, 10)$. Other kinds of errors may be ignored.

   Consider the linear code $C$ over $\mathbb{F}_{11}$ with parity check matrix $H$ as below:

   \[
   H = \begin{bmatrix}
   1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
   1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2
   \end{bmatrix}
   \]

   (a) Does the code $C$, under syndrome decoding, meet the requirements of the enhanced ISBN scheme?
   
   \[ \text{[Hint: Identify the error patterns $e$ obtainable as $e = y - c$, where $c$ is a codeword, and $y$ is obtained by interchanging some two coordinates of $c$.]} \]
(b) Would your answer to answer to part (a) change if only single transposition errors involving a pair of adjacent digits are required to be corrected? To be precise, the only errors that need be corrected are those in which exactly one pair \((c_i, c_{i+1})\) of adjacent digits in a codeword \(c = (c_1, \ldots, c_{10})\) gets interchanged; for example, the codeword \((1, 2, 3, 4, 5, 6, 7, 8, 9, 10)\) may get transformed to \((1, 2, 3, 4, 6, 5, 7, 8, 9, 10)\). Other kinds of errors may be ignored.

4. Construct the best possible double-error-correcting binary block code (not necessarily linear) of length 7. You must provide a justification for why your construction is the best possible. Here, ‘best possible’ means having the largest number of codewords among all such codes.

5. We wish to have a binary linear code of blocklength 1000 that is 100-error-correcting. Determine the largest value of \(k\) for which such a code of dimension \(k\) is guaranteed to exist by the Gilbert-Varshamov bound.

6. Let \(C\) be an \([n, k]\) linear code over \(\mathbb{F}\), with \(1 \leq k \leq n - 1\).

   (a) Let \(H\) be an \((n - k) \times n\) parity check matrix for \(C\). Show that \(C\) is maximum distance separable (MDS) if and only if every set of \(n - k\) columns of \(H\) is linearly independent.

   (b) Let \(G\) be a \(k \times n\) generator matrix for \(C\). Show that \(C\) is MDS if and only if every set of \(k\) columns of \(G\) is linearly independent.

   \[\text{Hint: For a codeword } c = (c_1c_2 \ldots c_n) \in C \text{ of weight } w > 0, \text{ let } J = \{i : c_i = 0\} \text{ be the subset of coordinates that are } 0 \text{ in } c. \text{ Now, consider the } k \times (n - w) \text{ submatrix } G_J \text{ of } G \text{ formed by the columns indexed by } J. \text{ Since there is a linear combination of rows of } G \text{ that results in } c \text{, the corresponding linear combination of rows of } G_J \text{ results in the } 0 \text{ vector. Thus } \text{rank}(G_J) < k, \text{ implying that any } k \text{ columns of } G_J \text{ are linearly dependent.}\]

   (c) Show that if \(C\) is MDS then \(C^\perp\) is also MDS.