Introduction to Coding Theory - Spring 2025
Assignment 1
Submission Deadline: 23 Jan

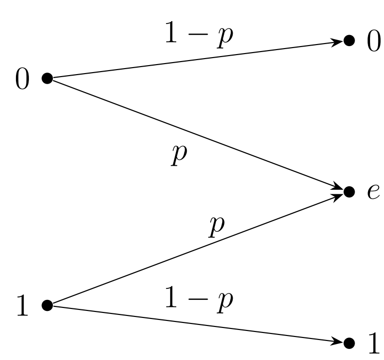
1. Let $V_2(n,t) = \left\{\underline{y} \in \mathbb{F}_2^n : w_H(\underline{y}) \leq t\right\}$. Show that for an (n, M, d) code

$$M \leq \frac{2^n}{V_2(n, t_c)}$$

   Prove that Hamming codes achieve this bound with equality.

2. Show that when one adds an overall parity bit to each codeword of an (n, M, d) code over $\{0, 1\}$, where d is odd, an $(n + 1, M, d + 1)$ code is obtained(where overall parity bit is defined as XOR of all n bits).

3. Binary Erasure channel(BEC) is defined below



   A codeword of the code $\{00000, 01010, 10101, 11111\}$ is selected uniformly at random and transmitted through a BEC with a probability of erasure p = 0.2. A Maximum aposteriori probability (MAP) decoder $\mathcal{D}$ is applied to the received word. Compute the decoding error probability P_{err} of $\mathcal{D}$.

   MAP Decoder: if $\mathbf{y}$ is the received vector, then MAP decoder is defined as:

$$\hat{\mathbf{c}}_{\text{MAP}} = \arg\max_{\mathbf{c}\in\mathcal{C}} P(\mathbf{c} \mid \mathbf{y})$$

4. Let $\mathbf{x_{bin}} = (x_1, x_2, \ldots, x_n)$ be a binary vector where $\mathbf{x_{bin}} \in \{0,1\}^n$, and $\mathbf{x_{bip}} = (x_1, x_2, \ldots, x_n)$ be the corresponding bipolar vector where $\mathbf{x_{bip}} \in \{-1,+1\}^n$. The mapping from binary to bipolar for each component is given by

$$x_{\text{bip}} = 1 - 2x_{\text{bin}}$$

using above mapping we can convert a binary vector $\mathbf{x}$ in bipolar form, now show that if $\mathbf{x}$, $\mathbf{y}$ is n length bipolar vector, the Euclidean distance between the points $\mathbf{x}$ and $\mathbf{y}$ satisfies

$$\sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} = \sqrt{2d_H(\mathbf{x}, \mathbf{y})}$$

where $d_H(\mathbf{x}, \mathbf{y})$ is the hamming distance between point $\mathbf{x}$ and $\mathbf{y}$.

5. Adi and Pragya are playing a game. Pragya has selected a number $x \in \{1, 2, ..., M\}$ that Adi needs to guess. Adi is allowed to ask n questions of the form "Does $x \in S$?", and Pragya answers with "Yes" or "No". The caveat is that Pragya can lie. However, she is allowed to lie at most k times to keep things fair. Prove that if

$$M > \frac{2^n}{\sum_{i=0}^{k}\binom{n}{i}}$$

then Pragya can come up with a strategy to win the game.

6. **Memoryless q-ary Symmetric Channel** As a modification of the memoryless Binary Symmetric Channel (BSC), consider the following definition of the memoryless q-ary symmetric channel (or, the q-SC). Let the input and output symbols be drawn from the set $\mathcal{Q} = \{0, 1, 2, \ldots, q-1\}$, where $q > 1$. Then, the conditional probability of the output symbol y_j, given the input symbol x_j, is given by:

$$P(y_j \mid x_j) = \begin{cases} 1 - p, & \text{if } y_j = x_j, \\ \frac{p}{q-1}, & \text{if } y_j \neq x_j, \end{cases}$$

where $j \in [n]$ and $p \in [0, 1]$.Show that Maximum Likelihood (ML) decoding of an n-length received word is equivalent to minimum distance decoding when $p \leq 1 - \frac{1}{q}$.

7. Let $\mathbf{x}$ and $\mathbf{y}$ be two n length binary vectors. Prove that the Hamming distance between these vectors is less than or equal to the sum of their Hamming weights:

$$d_H(\mathbf{x}, \mathbf{y}) \leq w_H(\mathbf{x}) + w_H(\mathbf{y})$$

Also, determine under what conditions this inequality becomes an equality, $d_H(\mathbf{x}, \mathbf{y})$ is hamming distance between $\mathbf{x}$, $\mathbf{y}$ and $w_H(.)$ is hamming weight of vector.