Learners' Space 2025 – Coding Theory
Week 1 Assignment

Aryan Prakash & Nirav Bhattad, MnP Club, IIT Bombay

June 2025

1. In an Huffman code instance, show that if there is a character with frequency greater than $\frac{2}{5}$, then there is a codeword of length 1. Further, show that if all frequencies are less than $\frac{1}{3}$ then there is no codeword of length 1.

2. A distance function on Σ^n (i.e. $d : \Sigma^n \times \Sigma^n \to \mathbb{R}$) is called a metric if the following conditions are satisfied for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \Sigma^n$:

    1. $d(\mathbf{x}, \mathbf{y}) \geqslant 0$
    2. $d(\mathbf{x}, \mathbf{y}) = 0$ iff $\mathbf{x} = \mathbf{y}$
    3. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$
    4. $d(\mathbf{x}, \mathbf{z}) \leqslant d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$

    Prove that the Hamming Distance is a metric.

3. Complete the proof of Theorem 4.11 in the handout – C_H has a distance of 3.

4. Prove the Generalized Hamming Bound, i.e., for every $(n, k, d)_q$ code, we have

$$k \leqslant n - \log_q \left(\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right)$$

5. Show that there is no binary code of block length 4 that achieves the Hamming Bound.

6. If $S \subseteq \mathbb{F}_q^n$ is a linear subspace, then prove that:

    1. $|S| = q^k$ for some $k \geqslant 0$. The parameter k is called the *dimension* of S.
    2. there exists at least one set of linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in S$ called basis elements such that every $\mathbf{x} \in S$ can be expressed as

    $$\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_k\mathbf{v}_k$$

    where $a_i \in \mathbb{F}_q$ for $1 \leqslant i \leqslant k$. In other words, there exists a full rank $k \times n$ matrix G (also known as a *generator matrix*) with entries from $\mathbb{F}_q$ such that every $\mathbf{x} \in S$ satisfies

    $$\mathbf{x} = (a_1, a_2, \ldots, a_k) \cdot G$$

    where

    $$G = \begin{pmatrix} \longleftarrow \mathbf{v}_1 \longrightarrow \\ \longleftarrow \mathbf{v}_2 \longrightarrow \\ \vdots \\ \longleftarrow \mathbf{v}_k \longrightarrow \end{pmatrix}.$$

3. there exists a full rank $(n-k) \times n$ matrix H (called a *parity check matrix*) such that for every $\mathbf{x} \in S$,

$$H\mathbf{x}^T = 0.$$

4. G and H are orthogonal, that is,

$$GH^T = 0.$$

7. Prove that for any $\mathbf{u}, \mathbf{v} \in \{0,1\}^n$, $\Delta(\mathbf{u}, \mathbf{v}) = \mathrm{wt}(\mathbf{u} \oplus \mathbf{v})$, where $\oplus$ is the Bitwise XOR operation