SINGLETON BOUND

Definition 0.1. *Let $\mathbb{F}_q$ be a finite field with order q, and let n be a positive integer. A **code** C of length n over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$. Each element of C is called a **codeword**.*

Definition 0.2. *For two codewords $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, the **Hamming distance** $\text{HamDist}(x, y)$ is defined as the number of positions in which x and y differ:*

$$\text{HamDist}(x, y) = |\{i \mid x_i \neq y_i,\ 1 \leq i \leq n\}|$$

*The **distance** $d(C)$ of a code C is defined as:*

$$d(C) = \min_{x \neq y \in C} \text{HamDist}(x, y).$$

Definition 0.3. *An **erasure** in a codeword $(c_1, ..., c_n) \in C$ means one symbol c_i is erased and replaced with ?. For example the codeword $(0, 1, 0, 0, 1) \in \mathbb{F}_2^5$ may change to $(0, 1, ?, 0, ?)$ after two erasures. We say that a code C **corrects** e **erasures** if there is an algorithm such that for any codeword $x \in C$, the algorithm can recover x given x with e erasures.*

Lemma 0.4. *A code with distance $d(C)$ can correct e erasures if $d(C) > e$.*

Theorem 0.5 (Singleton Bound). *Suppose $C \subseteq \mathbb{F}_q^n$ is a code of length n over $\mathbb{F}_q$. Then $|C| \leq q^{n-d(C)+1}$.*

Proof. Define the projection map $C \to \mathbb{F}_q^{n-d(C)+1}$ as follows:

$$(c_1, c_2, \ldots, c_n) \mapsto (c_1, c_2, \ldots, c_{n-d(C)+1})$$

Since we are erasing fewer than $d(C)$ bits, this map is one-to-one. The codewords can be uniquely identified by the projection because fewer than $d(C)$ erasures can be corrected.

Thus, the dimension of the code must be less than or equal to the number of possible strings of length $n - d(C) + 1$. Therefore:

$$|C| \leq q^{n-d(C)+1}$$

This completes the proof. □