Error-correcting codes are used to reduce errors when data is transmitted in noisy communication channels, like a telephone line, a satellite communication link, etc. The objective of error-correcting codes is to add a certain amount of redundancy to the message, so that even if some errors occur during transmission, we have high probability to recover the original message.

Definition 0.1. A ***q-ary code*** is a given set of sequences of symbols where each symbol is chosen from a set $F_q = \{\lambda_1, \lambda_2, \ldots, \lambda_q\}$ of q distinct elements. The set F_q is called the ***alphabet***.

In particular, the 2-ary codes are called *binary codes*.

Definition 0.2. A code in which every codeword is of fixed length n is called ***block code of length n***.

We will deal with such codes only, so from now on, 'code' will mean 'block code'. A code C with M codewords of length n is often written as $M \times n$ array. For example, the *binary repitition code* of length 3 is $\begin{bmatrix}000\\111\end{bmatrix}$.

The elements of the set $(F_q)^n$ are called *words* or *vectors* and if C is a q-ary code of length n then $C \subseteq (F_q)^n$.

$$(F_q)^n = \{\mathbf{a} \mid \mathbf{a} = a_1 a_2 \cdots a_n,\ a_i \in F_q\}$$

Definition 0.3 (**Hamming distance**)**.** The ***distance*** between two vectors $\mathbf{x}$ and $\mathbf{y}$ of $(F_q)^n$, denoted by $d(\mathbf{x}, \mathbf{y})$, is the number of places in which they differ.

Theorem 0.4. The Hamming distance satisfies:

(i) $d(\mathbf{x}, \mathbf{y}) = 0 \iff \mathbf{x} = \mathbf{y}$.
(ii) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})\ \forall\ \mathbf{x}, \mathbf{y} \in (F_q)^n$.
(iii) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{y}, \mathbf{z})\ \forall\ \mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$. (Triangle inequality)

Proof. First two statements are trivial. In third, we note that $d(\mathbf{x}, \mathbf{y})$ is the minimum number of changes required to change $\mathbf{x}$ to $\mathbf{y}$, but we can also do this change by first changing $\mathbf{x}$ to $\mathbf{z}$ in $d(\mathbf{x}, \mathbf{z})$ changes and then from $\mathbf{z}$ to $\mathbf{y}$ in $d(\mathbf{z}, \mathbf{y})$ changes. Thus, $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{y}, \mathbf{z})$. □

Suppose a codeword $\mathbf{x}$ is being transmitted, and we receive a distorted vector $\mathbf{y}$. If we decode it as $\mathbf{x}'$ such that $d(\mathbf{y}, \mathbf{x}')$ is minimum, then this decoding scheme is called ***nearest neighbour decoding***.

Definition 0.5. A transmitting channel is said to be ***q-ary symmetric channel*** if

1. Each symbol transmitted has the same probability $p(< \frac{1}{2})$ of being recieved in error.
2. If a symbol is received with error, then all $q - 1$ errors are equally likely.

Theorem 0.6. For a binary symmetric channel, *nearest neighbour decoding* is the *maximum likelihood decoding*, i.e. *nearest neighbour decoding* gives the highest probability of error detection in these types of channels.

Proof. The probability that codeword has errors at given i positions is $p^i(1-p)^{n-i}$, which decreases as i increases (as $p < \frac{1}{2}$), hence the least distant word is the most probable of being the original word. □

Definition 0.7. For a code C, we define ***minimum distance***, denoted by $d(C)$, as the smallest of all the distances between different codewords of C, i.e.

$$d(C) = \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}$$

Theorem 0.8.

(i) A code C can detect upto s errors if $d(C) \geq s + 1$.

(ii) A code C can correct upto t errors if $d(C) \geq 2t + 1$.

Proof.

(i) Suppose $d(C) \geq s + 1$. Now if the recieved codeword has less than or equal to s errors, it will be a different codeword than any present in C. Hence, the error will be detected.

(ii) Suppose $d(C) \geq 2t+1$. Let the original codeword be $\mathbf{x}$ and received one be $\mathbf{y}$ with $d(\mathbf{x}, \mathbf{y}) \leq t$. Let $\mathbf{x}$' be any codeword in C other than $\mathbf{x}$, then by triangle inequality,

$$d(\mathbf{x}, \mathbf{x}') \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{x}', \mathbf{y}) \geq 2t+1$$

$$d(\mathbf{x}', \mathbf{y}) \geq t+1$$

Therefore, $\mathbf{x}$ is the nearest neighbour to $\mathbf{y}$, and nearest neighbour decoding corrects the error.

□

Corollary 0.8.1. If code C has minimum distance d then it can be used either:

(i) to detect upto $d-1$ errors; or

(ii) to correct upto $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors in any coedword.

($\lfloor x \rfloor$ denotes the greatest integer leass than or equal to x)

Proof. Simple rearrangment of terms in the Theorem 0.8 will give the result. □

Notation: A (n, M, d)-*code* is a code with M words of length n, having minimum distance d.