NAME: KULVIR SINGH

REG. NO.: 19BCE2074

SLOT : A1

Discrete Mathematics DA-2

# INTRODUCTION TO CODING THEORY

- The process of communication involves transmitting some information carrying signal (message) that is conveyed by a sender to a receiver receiving.
- Even though the sender may like to have his message received by the receiver without any distortion, it is not possible due to a variety of disturbances (noise) to which the communication channel is subjected
- Coding theory deals with minimizing the distortions of the conveyed message due to noise and to retrieve the original message to the optimal extent possible from the corrupted message

# ENCODERS AND DECODERS

∴ ENCODER:

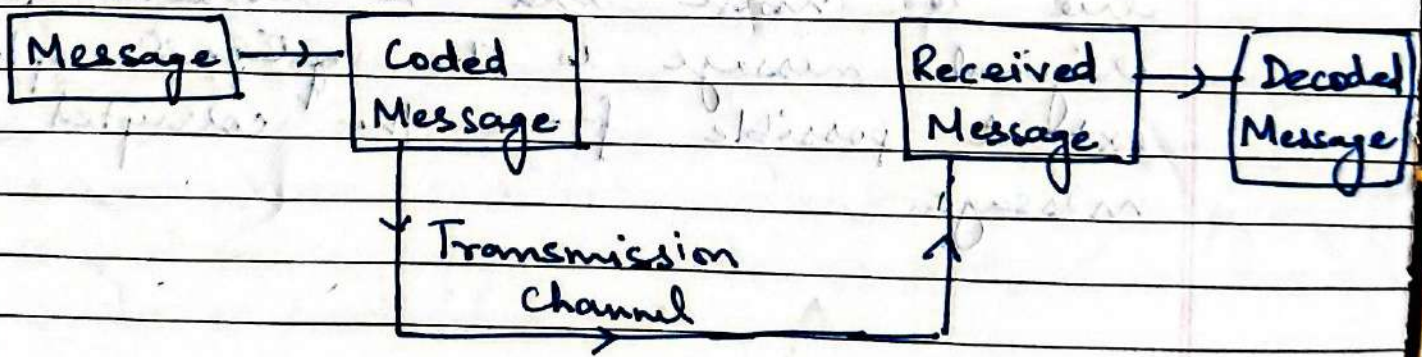
An encoder is a device which transforms the incoming messages in such a way that the presence of noise in the transformed messages is detectable.

∴ DECODER:

A decoder is a device which transforms the encoded message into their original form that can be understood by the receiver.

∴ So, by using a suitable encoder and decoder, it may be possible to detect the distortions in the messages due to noise in the channel and to correct them.

∴ BLOCK DIAGRAM



- The input message can consist of a sequence of letters, characters or symbol of set called alphabet.

- The input message will be transformed by the encoder into a string of characters or symbols of another alphabet in a one-to-one fashion.

- We will discuss a binary channel in which the encoder will transform an input message into a binary string consisting of the symbols 0 and 1.

- Decoding can be seen as the inverse operation of encoding.

# GROUP CODES

**Definition:**

An $(m, n)$ encoding function $e: B^m \longrightarrow B^n$ is called a group code if $e(B^n)$ is a subgroup of $B^n$ (ie, the range of $B^m$ is a subgroup of $B^n$).

**Example:**

The parity check code $e: B^m \longrightarrow B^{m+1}$ is a group code.

**Solution:**

Let $a = a_1 a_2 \ldots a_m$ be any group code in $B^m$.

then $e(b) = a_1 a_2 \ldots a_m a_{m+1} \in B^{m+1}$

where $a_{m+1} = \begin{cases} 0 & \text{if } |x| \text{ even} \\ 1 & \text{if } |x| \text{ odd} \end{cases}$

So, we have

$$a_{m+1} = a_1 + a_2 + \ldots + a_m$$

now,

$$e(a) + e(b) = a_1 a_2 \cdots a_{m+1} \oplus b_1 b_2 \cdots b_{m+1}$$

$$= [a_1 a_2 \cdots a_m (a_1 + a_2 + \cdots + a_m)] \oplus [b_1 b_2 \cdots b_m (b_1 + b_2 + \cdots + b_m)]$$

$$= (a_1 + b_1)(a_2 + b_2)(a_3 + b_3) \cdots (a_m + b_m)(a_1 a_2 + \cdots + a_m + b_1 + b_2 + \cdots + b_m)$$

$$= (a_1 + b_1)(a_2 + b_2) \cdots (a_m + b_m)(a_1 + b_1 + a_2 + b_2 + a_3 + b_3 + \cdots + a_m + b_m)$$

$$= e(a + b)$$

Thus $e(B^m)$ is closed under $\oplus$

Also $\oplus$ is associative under $\oplus$.

Now, 0000.....0 (m factors) is the identity element of $B^m$

Say $c$ = 0000.....0 (m factors)

$\Rightarrow$ $c_{m+1} = 0$

$\therefore$ $e(c) = 00\ldots0$ $(m+1)$ is the identity element in $B^{m+1}$.

And the inverse of any element of $B^{m+1}$ is itself. The inverse of $e(c)$ is also $e(B^m)$. Hence $e(B^m)$ is a subgroup of $B^{m+1}$

$\Rightarrow$ e is a group code

THEOREM:

Let $e: B^m \longrightarrow B^n$ be a group code. Then the minimum distance of e is the minimum weight of a non-zero code word.

PROOF:

Let H be the minimum distance of the group code.

ie, $H = H(x, y)$ for any two distinct words x and y. Let n be the minimum weight of a non-zero code word. So $n = |z|$ for any non-zero code word $z$

Also $x$ and $y$ are code words.

$H = H(x,y) = H(x \oplus y, 0)$

$= |x \oplus y| \geq n$ ..... (1)

Also the distinct code words

$n = |z| = |z \oplus 0| = H(z,0) \geq H$ ..... (2)

From (1) and (2) we get

$n = H$.

Example :

Consider (2,6) encoding function $e : B^2 \to B^6$ defined by:

$e(000) = 000000$, $e(001) = 001100$

$e(010) = 010011$, $e(011) = 011111$

$e(100) = 100101$, $e(101) = 101001$

$e(110) = 110110$, $e(111) = 111010$

Show this encoding function is a group code.

Solution:

To show $e: B^3 \longrightarrow B^6$ is a group code we have to show that

① $e(B^3) = \{e(000), e(001), e(010), e(011), e(100), e(101), e(110), e(111)\}$ is a subgroup of $B^6$ under the operation $\oplus$.

For any $x, y = e(B^3)$ we can see that $x \oplus y$ is closed. Also any element $x, y, z \in e(B^3)$ is associative. And $e(000) = 000000$ is the identity element.

Finally, we can see that the inverse of every element of $e(B^3)$ is itself. Hence the coding function e is a group code.

Date __/__/____

Saathi

## Procedure for generating group codes.

We have seen that the parity check code $(m, m+1)$ is a group code ie,

$$e(a_1, a_2, \ldots a_m) = a_1 a_2 \ldots a_m a_{m+1}$$
$$= a_1 a_2 \ldots a_m (a_1 + a_2 + a_3 + \ldots + a_m)$$
$$= a_1 a_2 \ldots a_m \left( \sum_{i=1}^{m} a_i \right)$$

We can generalize this to an $(M, M+r)$ encoding.
We can add $r$ digits by adding some of the digits to $a_1 a_2 \ldots a_m$.
ie $e(a_1 a_2 \ldots a_m) = a_1 a_n \ldots a_m a_{m+1} \ldots a_{m+r}$

Now we define the parity check matrix and as $(m, m+r)$ encoding procedure.