8

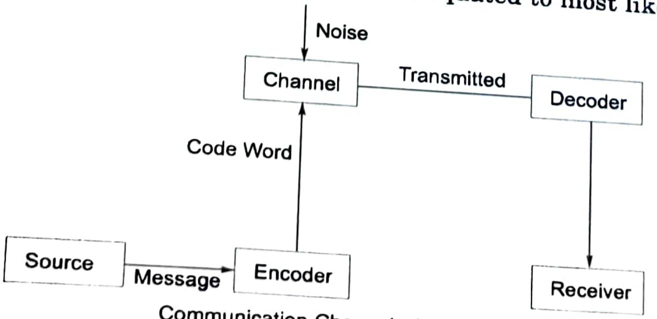
Codes and Group Codes

■ 8.0 INTRODUCTION

When we want to send a message to someone, we send it through some communication channel. This transmission of message over a channel entails some chances of undesirable interference in the channel sometimes deliberate and sometimes due to random defects in the channel. This leads to coding problem. The coding problem is to represent distinct messages by distinct sequence of letters from a given alphabet set.

For example, in a Morse code we represent a message by dots and dashes. Similarly over alphabet can be {0, 1} *i.e.*, binary alphabet.

When a message is to be transmitted, then the message is first given by the source to the encoder, the encoder converts the message into the code word. The encoded message is then sent through the channel, where noise may occur and change the message. When this message arrives at the decoder at the receivers end, it is equated to most likely code word.



Communication Channel with Noise

■ 8.1 TERMINOLOGIES

We will use the following terms in our discussion.

Word: A word is the sequence of letters drawn from the alphabet set.

Code: Code is the collection of words to represent a distinct message.

Code word: A word represented by a code is called the code word.

Block Code: A code consisting of words that are of same length is called Block code. One of the advantages of using the Block Code is its ability to correct errors.

■ 8.2 ERROR CORRECTION

When we transmit a message from the source to the destination, due to the presence of noise in the communication channel the message may get altered, *i.e.*, some of the 1's transmitted may be received as 0's and some of the 0's may be received as 1's. So the received message is no more is the transmitted message. Now we would want to recover the transmitted message from the received message. This is called error correction.

■ 8.3 GROUP CODES

Let A be the set of all binary sequence of length n. Let us define a binary operation ⊕ in A such that X, Y ∈ A implies (X ⊕ Y) ∈ A *i.e.*, a sequence of length n. Where

$$(X \oplus Y) = \begin{cases} 1 & \text{if X, Y differs in position} \\ 0 & \text{if X, Y are same in position} \end{cases}$$

The set A together with the binary operation ⊕, *i.e.*, (A, ⊕) forms a group and a subset G of A is called the group code if (G, ⊕) is a subgroup of (A, ⊕).

Let us consider X = 1 0 0 1 0 0 1 and Y = 0 1 0 1 0 0 1. Therefore, we have

$$(X \oplus Y) = 1\,1\,0\,0\,0\,0\,0.$$

■ 8.4 WEIGHT OF CODE WORD

Let A be the set of all binary sequence of length n. Let X be a code word in A, the weight of X denoted by ω(X) is the number of 1's in X.

Let us consider the code words X = 10101 and Y = 00011. The number of 1's present in X are three whereas the number of 1's present in Y are two. So, the weight of X is 3 and the weight of Y is 2.

i.e., $\omega(X) = 3$ and $\omega(Y) = 2.$

■ 8.5 DISTANCE BETWEEN THE CODE WORDS

Let A be the set of all binary sequence of length n. Let X and Y be two code words in A, the distance between X and Y denoted by d (X, Y) and is defined as the weight of ω (X ⊕ Y).

i.e., $d(X, Y) = \omega(X \oplus Y)$

The distance between the two code words gives the number of positions in which they differ.

Let us consider code words X = 01011 and Y = 10101. Now the distance between X and Y is defined as ω (X ⊕ Y). Now

$$\begin{array}{r} X = 01011 \\ Y = 10101 \\ \hline (X \oplus Y) = 11110 \end{array}$$

Therefore, $d(X, Y) = \omega(X \oplus Y) = 4$

3

8.5.1 Theorem

Let A be the set of all binary sequence of length n. The distance between two code words X and Y satisfies the following properties.

(*a*) Commutative law *i.e.*, $d(X, Y) = d(Y, X)$

(*b*) Triangle's inequality *i.e.*, $d(X, Y) \leq d(X, Z) + d(Z, Y)$.

Proof: (*a*) Let A be the set of all binary sequence of length n. Let X and Y be two code words in A.

Therefore, $X \oplus Y = Y \oplus X$

This implies that $\omega(X \oplus Y) = \omega(Y \oplus X)$

Thus, $d(X, Y) = d(Y, X)$

(*b*) Let A be the set of all binary sequence of length n. Let X ,Y and Z be three code words in A.

We know that $\omega(X)$ is the number of 1's in X and $(X \oplus X) = 0$. This implies that
$\omega(U \oplus V) \leq \omega(U) + \omega(V)$ ...(1)

Now, $\omega(X \oplus Y) = \omega(X \oplus Z \oplus Z \oplus Y)$ [$\because$ $(Z \oplus Z) = 0$]

$\leq \omega(X \oplus Z) + \omega(Z \oplus Y)$ [By equation (1)]

Therefore, $d(X, Y) \leq d(X, Z) + d(Z, Y)$.

■ 8.6 ERROR CORRECTION FOR BLOCK CODE

We know that block code is a code consisting of words that are of same length. The advantage of using block code is its ability to correct the errors.

Let G be a Block code, the distance of G is defined as the minimum distance between any pair of distinct code words in G. The ability of Block codes to correct the errors depends on its distance.

Let a word has been transmitted and we received a word Y (say). Now there is a likelihood of received word containing an error. Now we will like to have the transmitted word corresponding to the received word Y.

We can use two methods. *i.e.*, Maximum likelihood decoding criterion and Minimum distance decoding criterion.

8.6.1 Maximum Likelihood Criterion

Let $X_1, X_2, \ldots\ldots \ldots\ldots, X_n$ be the code words in G. One of this is transmitted and we have received the code word Y. The received word may contain error and we are interested to find the word transmitted. Maximum likelihood criterion says that compute the conditional probabilities $P(X_1 | Y), P(X_2 | Y), \ldots P(X_n | Y)$. Where $P(X_i | Y)$ means the probability that X_i is transmitted when the received word is Y. Let

$$P(X_k \mid Y) = \underset{i}{\text{Max}} \{P(X_i|Y)\};\ i = 1, 2, \ldots\ldots\ldots, n$$

Then X_k is the transmitted word.

4

8.6.2 Minimum Distance Decoding Criterion

In the minimum distance decoding criterion we compute d (X_1, Y), d (X_2, Y), d (X_3, Y), ..., d (X_n ,Y). Let us define

$$d(X_k, Y) = \underset{i}{\text{Min}}\{d(X_i, Y)\};\ i = 1, 2, 3, \ldots\ldots\ldots, n$$

Then, X_k is taken as the transmitted word when the received word is y.

■ 8.7 COSETS

Let (G, ⊕) be a group code. Let a word y is received. Then the coset with respect to y denoted by (G ⊕ y) is defined as

$$(G \oplus y) = \{X_i \oplus y \mid X_i \in G, i \in N\}$$

Again $d(X_i , Y) = \omega (X_i \oplus y)$. So the weights of the words in the coset (G ⊕ y) are the distances between the code words in G and y.

The decoding procedure includes the followings:

1. Determine all cosets of G.
2. For each coset, choose the coset leader, *i.e.*, the word of smallest weight.
3. For the received word y, (e ⊕ y) is the transmitted word.

SOLVED EXAMPLES

Example 1 *Let X = 0101011 and Y = 1010101. Find (X ⊕ Y).*

Solution: Given that X = 0101011 and Y = 1010101

Now
$$X = 0101011$$
$$Y = 1010101$$
$$(X \oplus Y) = 1111110$$

Therefore, (X ⊕ Y) = 1111110.

Example 2 *A is a set of all binary sequence of length n. Show that (A, ⊕) forms a group.*

Solution: Given that is aw set of all binary sequence of length n, say for our convenience we take the length to be 5.

Closure Law: Let X = 01011 and Y = 10101

Now $X \oplus Y = 01011 \oplus 10101 = 11110$

This is again a code word of length 5.

Therefore, X, Y ∈ A implies (X ⊕ Y) ∈ A. So, closure law holds.

Associative Law: Let X = 10101, Y = 10000 and Z = 01010

Now $(Y \oplus Z) = 10000 \oplus 01010 = 11010$

Therefore, $X \oplus (Y \oplus Z) = 10101 \oplus 11010 = 01111$

So, $X \oplus (Y \oplus Z) = 01111$ ...(i)

Again $(X \oplus Y) = 10101 \oplus 10000 = 00101$

Therefore, $(X \oplus Y) \oplus Z = 00101 \oplus 01010 = 01111$

So, $(X \oplus Y) \oplus Z = 01111$ ...(*ii*)

Therefore from equations (*i*) and (*ii*) we get $(X \oplus Y) \oplus Z = X \oplus (Y \ominus Z)$. So, associative law holds.

Existence of Identity: A code word with all zeros of specified length will act as the identity element.

Let $X = 10101$ and $Y = e = 00000$ such that

$$X \oplus Y = 10101 \oplus 00000 = 10101 = X$$

Therefore, $(X \oplus Y) = X$

So, $Y = 00000 \in A$ acts as an identity element.

Existence of Inverse: A code word itself is inverse of its own.

Let $X = 10101$ such that $(X \oplus X) = 10101 \oplus 10101 = 00000 = e$. Therefore, $(X \oplus X) = e$. This implies that every code word is its own inverse. So, $(A, \oplus)$ satisfies all the properties of group and hence called group codes.

Example 3 *Illustrate by example distance function satisfies the commutative and triangle's inequality.*

Solution: Commutative Law: Let $X = 101010$ and $Y = 010101$

So, $(X \oplus Y) = 101010 \ominus 010101 = 111111$

Therefore, $d(X, Y) = \omega\,(X \oplus Y) = 6$ ....(*i*)

Again, $(Y \oplus X) = 010101 \ominus 101010 = 111111$

Therefore, $d(Y, X) = \omega\,(Y \oplus X) = 6$ ...(*ii*)

So, from equations (*i*) and (*ii*) it is clear that $d\,(X, Y) = d(Y, X)$.

Triangle's inequality: Let us take $X = 101010$, $Y = 100010$ and $Z = 101000$. Now

$$(X \ominus Y) = 101010 \oplus 100010 = 001000$$
$$(X \ominus Z) = 101010 \oplus 101000 = 000010$$
$$(Z \oplus Y) = 101000 \oplus 100010 = 001010$$

Therefore,

$$d(X, Y) = \omega\,(X \oplus Y) = 1$$
$$d(X, Z) = \omega\,(X \oplus Z) = 1$$
$$d(Z, Y) = \omega\,(Z \ominus Y) = 2$$

Thus, we have $d(X, Z) + d(Z, Y) = 1 + 2 = 3 \geq d\,(X, Y) = 1$

i.e., $d\,(X, Y) \leq d(X, Z) + d(Z, Y)$

Example 4 *In the minimum distance criterion, a code of distance (2t + 1) can correct t or fewer transmission errors.*

Solution: Let X be the transmitted word and Y be the received word.

Now if t or less number of errors has occurred during the transmission we will have

$$d(X, Y) \leq t \qquad \text{...}(i)$$

Now since the distance is $(2t + 1)$, so for any code word X_1 we have

$$d(X, X_1) \geq 2\,t + 1 \qquad \text{...}(ii)$$

Since the distance means the minimum distance between any pairs of distinct code words. Again from triangle's inequality we have

$$d\,(X, X_1) \leq d\,(X, Y) + d\,(Y, X_1)$$

$$\Rightarrow \quad 2t + 1 \leq d(X, X_1) \leq t + d\,(Y, X_1)$$

$\Rightarrow$ $$2t + 1 \leq t + d\,(Y, X_1)$$

$\Rightarrow$ $$d(Y, X_1) \geq (t + 1) \qquad \ldots(iii)$$

So, we have $d(X, Y) \leq t$ and $d(Y, X_1) \geq (t + 1)$

From the minimum distance decoding criterion X will be selected as the transmitted word.

EXERCISES

1. Let X and Y be two code words. Find $(X \oplus Y)$ in each of the following cases.
   (*a*) X = 11111 and Y = 11111
   (*b*) X = 11111 and Y = 00000
   (*c*) X = 1010101 and Y = 0101010
   (*d*) X = 00101101 and Y = 11101100
   (*e*) X = 1100110 and Y = 0011101
2. Find the weight of the following code words.
   (*a*) X = 11111 (*b*) X = 11111
   (*c*) X = 1010101 (*d*) X = 00101101
   (*e*) X = 1100110
3. Find the distance between the code words in each of the following cases.
   (*a*) X = 10011 and Y = 00000
   (*b*) X = 01101 and Y = 10110
   (*c*) X = 0011101 and Y = 0101010
   (*d*) X = 11101101 and Y = 10011101
   (*e*) X = 1100110 and Y = 1110110
4. Illustrate by example distance function satisfies the associative law and triangle's inequality.
5. Illustrate by example $(A, \oplus)$ forms a group, where A is a set of all binary sequence of length 7.