CODING THEORY

Introduction

The process of communication involves transmitting some information carrying signal (message) that is conveyed by a sender to a receiver. 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

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. A *decoder* is a device which transforms the encoded message into their original form that can be understood by the receiver. 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. The model of a typical data communication system with noise is given in Fig. 5.4.

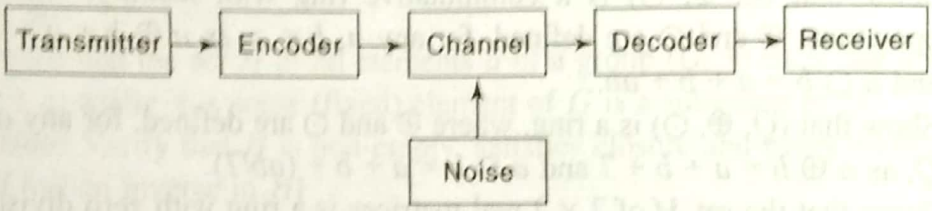

Fig. 5.4

The input message which consists of a sequence of letters, characters or symbols from a specified set (called alphabet) will be transformed by the encoder into a string of characters or symbols of another alphabet in a one-to-one fashion. In our discussion, we will deal with only a binary channel in which the encoder will transform an input message into a binary string consisting of the symbols 0 and 1. Decoding is only the inverse operation of encoding.

GROUP CODE

Definition

If $B = \{0, 1\}$, then $B^n = \{x_1, x_2, \ldots x_n | x_i \in B, i = 1, 2, 3, \ldots n\}$ is a group under the binary operation of addition modulo 2, denoted by $\oplus$. This group $(B^n, \oplus)$ is called a *group code*.

Let us now prove that $(B^n, \oplus)$ is a group.

If $x_1 x_2 \ldots x_n \equiv (x_1, x_2 \ldots x_n)$ and $y_1 y_2, \ldots, y_n \equiv (y_1, y_2 \ldots, y_n) \in B^n$, then

$x_1 x_2 \ldots x_n \oplus y_1, y_2 \ldots y_n = (x_1 +_2 y_1, x_2 +_2 y_2 \ldots, x_n +_2 y_n) \in, B^n$

since $x_i +_2 y_i = 1$ or 0, as $0 +_2 0 = 0$, $0 +_2 1 = 1$, $1 +_2 0 = 1$ and $1 +_2 1 = 1$.

Note The operation $+_2$ is also called binary addition.

$(0, 0, 0, \ldots, 0)$ is the identity element of B^n. Also the inverse of $x_1x_2 \ldots x_n$ is itself.

Hence, $(B^n, \oplus)$ is a group—it is abelian.

In general, any code which is a group under the operation $\oplus$ is called a group code.

HAMMING CODES

The codes obtained by introducing additional digits called *parity digits* to the digits in the original message are called Hamming codes. If the original message is a binary string of length m, the Hamming encoded message is string of length n, $(n > m)$. Of the n digits, m digits are used to represent the information part of the message and the remaining $(n - m)$ digits are used for the detection and correction of errors in the message received.

In Hamming's single-error detecting code of length n, the first $(n - 1)$ digits contain the information part of the message and the last digit is made either 0 or 1. If the digit introduced in the last position gives an even number/odd number of 1's in the encoded word of length n, the extra digit is called an *even/odd parity check*.

For example, when a single even parity check is appended, the words 000, 001, 010, 011, 100, 101, 110 and 111 become 0000, 0011, 0101, 0110, 1001, 1010, 1100 and 1111. On the other hand, when an odd parity is appended to each of the above words, they will become 0001, 0010, 0100, 0111, 1000, 1011, 1101 and 1110.

We note that a single mistake in a word, say, 0000 produces another word 0001 or 0010 or 0100 or 1000. None of these words appear in the set of 8 words transmitted. Hence, it is an indication that an error has occurred in transmission. However, it is not possible to correct the error, as, for example, 0001 might have been got from any of the words 0000, 0011, 0101, 1001 due to a single error.

An error correcting method based on parity checks that helps the detection of positions of erroneous digits, as developed by Hamming will be discussed later.

Definitions

1. The number of 1's in the binary string $x \in B^2$ is called the weight of x and is denoted by $|x|$.
2. If x and y represent the binary strings $x_1\, x_2\, x_3 \ldots x_n$ and $y_1\, y_2\, y_3 \ldots y_n$, the number of positions in the strings for which $x_i \neq y_i$ is called the *Hamming distance* between x and y and denoted by $H(x, y)$.

   Obviously $H(x, y)$ = weight of $x \oplus y$

$$= \sum_{i=1}^{n} (x_i +_2 y_i).$$

For example, if $x = 11010$ and $y = 10101$, then

$$H(x, y) = |x \oplus y| = |01111| = 4$$

3. The minimum distance of a code (a set of encoded words) is the minimum of the Hamming distances between all pairs of encoded words in that code.

   For example, if $x = 10110$, $y = 11110$ and $z = 10011$, then $H(x, y) = 1$, $H(y, z) = 3$ and $H(z, x) = 2$ and so the minimum distance between these code words = 1.

Note The term 'code' used above is sometime called an *(m, n) encoding function*, which is a one-to-one function e: $B^m \to B^n$ (where $n > m$). If $b \in B^m$ is the original word, them $e(b)$ is the code word or encoded word representing b.

Theorem

A code [an(m, n) encoding function] can detect at the most k errors if and only if the minimum distance between any two code words is at least $(k + 1)$.

Proof

A set (combination) of errors in various digit positions cannot be detected if and only if the set transforms a code word x into another code word y.

Since, the minimum distance between any two code words is at least $(k + 1)$, a set of at least $(k + 1)$ errors would be required to change the code word x into the code word y.

Hence, if the code word x is transformed to the word y due to at least $(k + 1)$ errors, almost k errors can be detected.

Example

Let 000 and 111 be the encoded words, viz., two values of the encoding function.

These two code words differ in 3 digits, viz. the distance between them is 3.

If one error occurs during transmission, the word 000 would have become 100 or 010 or 001, whereas the word 111 would have been received as 011 or 101 or 110. The two sets of received words are disjoint.

Hence, if any of the above six words is received due to one error, it is easily found out which encoded word has get altered and in which digit position the error has occurred and hence, the error is corrected. On the other hand if two errors occur during transmission, the word 000 would have been received as 110 or 011 or 101, whereas the word 111 would have been received as 001 or 100 or 010. If an error in a single digit is corrected in any of the received words 110, 011 and 101, the corrected word would be 111, which is not the transmitted word.

Similarly if a single error correction is made in any of the received words 001, 100 and 010, the corrected word would be 000, which is not the transmitted word. Hence error correction is not possible.

Theorem

A code can correct a set of at the most k errors if and only if the minimum distance between any two code words is at least $(2k + 1)$.

Proof

Let the code correct at the most k errors.

Then we have to prove that the minimum distance between any two code words is at least $2k + 1$.

If possible, let there be at least one pair of code words, say x and y such that $H(x, y) < 2k + 1$.

By the previous theorem, $H(x, y) \geq k + 1$, as otherwise the k errors cannot even be detected.

$$\therefore \quad k + 1 \leq H(x, y) \leq 2k \tag{1}$$

Let x' be another word which differs from x in exactly k digits, which form a subset of the set of the digits in which x and y differ i.e.,

$$H(x, x') = k \tag{2}$$

Since, $H(x, x'), + H(x', y) \geq H(x, y)$, we have from (1) and (2), $H(x', y) \leq k$.

$\therefore$ By the previous theorem, the code can detect at the most $(k - 1)$ errors.

Thus, we get a contradiction.

$$\therefore \quad H(x, y) \geq 2k + 1.$$

Converse: Let us assume that $H(x, y) \geq 2k + 1$.

Let x be a code word and x' be a received erroneous word with at most k errors. If a decoding rule correctly decodes x' as x, then x' is nearer to x than any other word y.

Since, $H(x, x') + H(x', y) \geq H(x, y)$, we get

$H(x', y) \geq k + 1 \quad [\because H(x, y) \geq 2k + 1$ and $H(x, x') \leq k]$

This means that every code word y is farther away form x' than x.

Hence x' can be correctly decoded.

Example

Let us consider the encoded words 000 and 111. These words differ in 3 digits. So zero or one error can be corrected.

If zero or one error occurs during transmission, 000 would have become any one of 000, 100, 010 and 001 and 111 would have become any one of 111, 011, 101 and 110. These two sets of received words are disjoint. So whatever be the words received, the single or no error can be easily detected and corrected.

Basic Notions of Error Correction using Matrices

When $m, n \in Z^+$ and $m < n$, the encoding function e: $B^m \to B^n$, where $B \equiv (0, 1)$ is given by a $m \times n$ matrix G over B. This matrix G is called the *generator matrix* for the code and is of the form $[I_m | A]$, where I_m is the $m \times m$ unit matrix and A is an $m \times (n - m)$ matrix to be chosen suitably. If w is a message $\in B^m$, then $e(w) = wG$ and the code (the set of code words) $C = e(B^m) \subseteq B^n$, where w is a $(1 \times m)$ vector. For example, if the message $w \in B^2$, we may assume G

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Note Now row of A has only zeros or only 1.

The words that belong to B^2 are 00, 10, 01 and 11. Then the code words corresponding to the above message words are respectively

$$e(00) = [0\ 0]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [00\ 000]$$

$$e(10) = [1\ 0]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [10\ 110]$$

$$e(01) = [0\ 1]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [01\ 011]$$

$$e(11) = [1\ 1]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [111\ 01]$$

Note While getting wG, the modulo 2 arithmetic is to be used.

Clearly $C = e(B^2) \subseteq B^5$.

We observe that we can get back the message word from the corresponding code word by dropping the last $3(= n - m)$ digits.

For all $w = x_1\, x_2 \in B^2$

$$e(w) = x_1\, x_2\, x_3\, x_4\, x_5 \in B^5 \tag{1}$$

where $x_i \in B$.

Since, $$e(w) = wG = [x_1\ x_2]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix}$$

$$= [x_1, x_2, x_1, x_1 + x_2, x_2] \tag{2}$$

From (1) and (2), we have $x_1 = x_3$, $x_1 + x_2 = x_4$ and $x_2 = x_5$ (3)

Since, $x_i \in B$, by modulo 2 arithmetic $-x_i \pmod 2 = (-x_i + 2x_i) \pmod 2$.

Hence, the equations (3) become

$$\left.\begin{aligned} x_1 \quad\quad + x_3 \quad\quad &= 0\\ x_1 + x_2 \quad\quad + x_4 \quad &= 0\\ x_2 \quad\quad\quad\quad + x_5 &= 0\end{aligned}\right\} \tag{4}$$

i.e., $$\begin{bmatrix}1 & 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\\ x_5\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

i.e., $$H \cdot [e(w)]^T = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix} \tag{5}$$

The $(n - m)$ equations in (3) are called *the parity check equations*.
The matrix H in (5) is called *the parity check matrix*.
We note that H is an $(n - m) \times n$ matrix, whereas G is an $m \times n$ matrix.
Also $H = [A^T | I_{n-m}]$. In the present example

$$A^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } I_{n-m} = I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We also note that H does not contain a column of only 0's and no two columns of H are the same. This is achieved by a careful choice of A. This unique parity check matrix H provides a decoding scheme that corrects a single error in transmission as explained below:

(i) If r is a received word considered as $a(1 \times n)$ matrix and if $H \cdot r^T = [0]$, then we conclude that there is no error in transmission and that r is the code word transmitted. The decoded (original) message then consists of the first m components of r.

In the present example, if $r = [1\ 1\ 1\ 0\ 1]$, then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Hence, r is itself the code word transmitted and the decoded message is 11 (got by taking the first $(m =)2$ components of r).

(ii) If $H \cdot r^T =$ the i^{th} column of H, then we conclude that a single error has occurred during transmission and it has occurred in the i^{th} component of r. Changing the i^{th} component of r, we get the code word c transmitted. As before the first m components of c give the original message.

In the present example if $r = [11\ 011]$, then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Since, $H\ r^T =$ the first column of H, a single error has occurred in the first component of r. Changing the first component of r, we get the code word transmitted as 01011. Taking the first 2 components of the code word, we get 01 as the original message.

(iii) If neither case (i) nor case (ii) occurs then we conclude that more than one transmission error have occurred. Though detection of errors is possible in this case, correction is not possible.

In the present example, if $r = [11\ 010]$, then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Since, $H \cdot r^T \neq$ any column of H, more than one transmission error has occurred.

Since $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ = 1st column of H + 5th column of H,

2 errors have occurred in transmission, one in the first component and the other in the fifth component of r. Changing these components in r, the code word transmitted may be assumed as 01 011 and hence the original message may be taken as 01.

Also $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ = the 2nd column of H + the 3rd column of H.

Hence, 2 errors might have occurred, one in the 2nd component and the other in the 3rd component of r. Changing these components in r, the code word transmitted may be assumed as 10110 and hence, the original message may be taken as 10. Thus, there is an ambiguity as to which message has been encoded and transmitted. In other words, the correction of errors is not possible, even though errors have been detected.

We note that the minimum distance between any pair of code words is 3 in the present example. Hence, according to the two previous theorems, atmost 2 errors can be detected and atmost 1 error can be corrected. We have verified the same in the examples considered above.

ERROR CORRECTION IN GROUP CODES

We have already introduced a group code, that is any code which is a group under the binary operation of addition modulo 2, denoted by $\oplus$. In general when the code words form a group, it is easier to find the minimum distance between code words, using the following theorem.

Theorem

In a group code, the minimum distance between distinct code words is the minimum weight of the non zero code words in it.

Proof

Let a, b, c be 3 members of a group code C, such that $a \neq b$, $H(a, b)$ is minimum and c is a non zero element with minimum weight.

Now $a \oplus b \in C$, by closure property in the group C.

As already seen, $H(a, b) = \text{Wt}(a \oplus b)$

Since the weight of c is minimum, we have

$$H(a, b) \geq \text{Wt}(c) \tag{1}$$

Also $\text{Wt}(c) = H(c, 0)$, where 0 is the identity element of c.

Now $H(c, 0) \geq H(a, b)$, since, $H(a, b)$ is the minimum

i.e., $$\text{Wt}(c) \geq H(a, b) \tag{2}$$

From (1) and (2), it follows that $H(a, b) = \text{Wt}(c)$.

The parity check matrix H defined in the previous section satisfies

$$H \cdot [e(w)]^T = [0],$$

where $e(w)$ is a code word and [0] is a column matrix consisting of 0's. Conversely, if $x = [x_1, x_2 \ldots x_n]$ satisfies

$H \cdot [x]^T = [0]$, where H is an $(n - m) \times n$ matrix, $[x]$ is a $1 \times n$ row matrix and [0] is an $(n - m) \times 1$ column matrix, then x is a code word.

The following two theorems will show that H always defines a group code and the minimum weight of the code can be obtained from H.

Theorem

If H is a parity check matrix with $n - m$ rows and n columns, then the set C of code words $x = (x_1\ x_2 \ldots x_n)$ such that $C = \{x | H \cdot [x]^T = [0], \text{ modulo } 2\}$ is a group code under the operation $\oplus$.

Proof

Since, $$[H]_{n-m \times n} \cdot [0]^T_{n \times 1} = [0]_{m-n \times 1},\ [0]_{1 \times n} \in C.$$

If $x, y, \in C$, then $H \cdot [x]^T = [0]$ and $H \cdot [y]^T = [0]$

$\therefore$ $$H \cdot [x^T \oplus y^T] = [0]$$

i.e., $$H[x \oplus y]^T = [0]$$

$\therefore$ $x \oplus y \in C$ satisfies the closure property.

Similarly the associativitly is satisfied by $\oplus$.

Since $(x \oplus x)^T = [0]$ or $x \oplus x = [0]^T$, every element x in C is its own inverse.

Hence, $[C, \oplus]$ is a group code.

Theorem

The parity check matrix H generates a code word of weight q if and only if there exists a set of q columns of H such that their k-tuple sum (mod 2) is a zero column, where $k = n - m$.

Proof

In the code word x generated by H let the components $x_{i1}, x_{i2}, \ldots x_{iq}$ be 1 each and the remaining components be 0 each.

Note The components $x_{i1}, x_{i2}, \ldots, x_{in}$ of x are the same as the components $x_1, x_2, \ldots, x_n$ written in a different order.

Now the weight of the code word x is q.

Since $H \cdot [x]^T = [0]$, we get

$$h_{i1} \oplus h_{i2} \oplus \ldots \oplus h_{iq} = 0, \text{ where}$$

$h_{i1}, h_{i2}, \ldots, h_{iq}$ are the elements of any row of H corresponding to the positions of $x_{i1}\ x_{i2}, \ldots, x_{iq}$ in x.

As the above result is true for all the $k = n - m$ rows for H, the result follows:

Conversely, let us assume that there is a set of q distinct columns of H such that $h_{i1} \oplus h_{i2} \oplus \cdots \oplus h_{iq} = 0$ for all the rows (where $h_{i1}, h_{i2}, \ldots, h_{iq}$ are the elements of any row in the q columns). Then we can chosen $x = [x_{i1}, x_{i2}, \ldots, x_{in}]$ such that $x_{i1}, x_{i2}, \ldots, x_{iq}$ are 1 each and the remaining components are 0 each.

Then x will satisfy the equation

$$H[x]^T = [0]$$

This means that x is a code word of weight q generated by H.

Example

Let us consider the example considered in the previous section on "error correction using parity check matrix".

In that example, we established that

$$H \cdot [x]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Now it is obvious that the sum of the 1st, 2nd, 3rd and 5th columns of H(mod 2) is the zero column.

The weight of the corresponding code word [1 1 1 0 1] is 4, that verifies the above theorem.

STEP BY STEP PROCEDURE FOR DECODING GROUP CODES

Step 1

We list in a row all the code words in C, starting with the identity.

Thus, we have $c_1(=0)\ c_2\ c_3 \ldots\ c_{2^m}$

For clarity, we shall write the corresponding step with respect to the problem discussed in the previous section, in which $m = 2$

i.e., 0 0 0 0 0 1 0 1 1 0 0 1 0 1 1 1 1 1 0 1

Step 2

We select some word $y_j \in B^n$ but not in C having minimum weight and construct a new row or coset $y_j \oplus c_i$ for all i such that $1 \le i \le 2^m$.

Thus, we have

$$y_j \oplus c_1 \; y_j \oplus c_2 \; y_j \oplus c_3 \ldots y_j \oplus c_{2^m}$$

i.e., $$y_2 \quad y_2 \oplus c_2 \; y_2 \oplus c_3 \ldots y_2 \oplus c_{2^m}$$

In the example, if $y_2 = 10000$, then the second row would be

$$1\,0\,0\,0\,0 \quad 0\,0\,1\,1\,0 \quad 1\,1\,0\,1\,1 \quad 0\,1\,1\,0\,1$$

Step 3

We now form the third row by selecting some $y_k \in B^n$ which is not in the preceding two rows and which has the minimum weight and proceeding as in step 2.

Thus we have

$$y_3 \quad y_3 \oplus c_2 \; y_3 \oplus c_3 \ldots y_3 \oplus c_{2^m}$$

In the example, if $y_3 = 0\,1\,0\,0\,0$, then the third row would be

$$0\,1\,0\,0\,0 \quad 1\,1\,1\,1\,0 \quad 0\,0\,0\,1\,1 \quad 1\,0\,1\,0\,1$$

Step 4

This process is continued until all the elements in B^n are entered in the table. The complete decoding Table 5.12 will be of the form.

Table 5.12

$c_1 (= 0)$	c_2	c_3	...	c_{2^m}
y_2	$y_2 \oplus c_2$	$y_2 \oplus c_3$	...	$y_2 \oplus c_{2^m}$
y_3	$y_3 \oplus c_2$	$y_3 \oplus c_3$	...	$y_3 \oplus c_{2^m}$
...	...	...	...	...
$y_{2^{n-m}}$	$y_{2^{n-m}} \oplus c_2$	$y_{2^{n-m}} \oplus c_3$	...	$y_{2^{n-m}} \oplus c_{2^m}$

For the example in consideration, the complete decoding table is given in Table 5.13.

Table 5.13

0 0 0 0 0	1 0 1 1 0	0 1 0 1 1	1 1 1 0 1
1 0 0 0 0	0 0 1 1 0	1 1 0 1 1	0 1 1 0 1
0 1 0 0 0	1 1 1 1 0	0 0 0 1 1	1 0 1 0 1
0 0 1 0 0	1 0 0 1 0	0 1 1 1 1	1 1 0 0 1
0 0 0 1 0	1 0 1 0 0	0 1 0 0 1	1 1 1 1 1
0 0 0 0 1	1 0 1 1 1	0 1 0 1 0	1 1 1 0 0
1 1 0 0 0	0 1 1 1 0	1 0 0 1 1	0 0 1 0 1
1 0 0 0 1	0 0 1 1 1	1 1 0 1 0	0 1 1 0 0

Note The elements in the first row of the decoding table are the code words, whereas the elements in the first column are the *coset leaders*, which represent the errors that occur during transmission.

Step 5

Once the decoding table is constructed, the decoding of any received word r is done as follows. First we identify the column of the decoding table in which r occurs. If the weight of the coset leader corresponding to r is 1, then the decoded word (viz. the coded word transmitted) is the element at the top of the column in which r occurs.

In the current example, if the received word is 11011, we note that it lies in the 3rd column and 2nd row of the table. Since, the weight of the coset leader in the 2nd row is 1, the decoded word is 01011 that lies at the top of the 3rd column. The corresponding message transmitted is 01.

Note If, by chance the received word happens to lie at the top of any column (or in the first row) of the decoding table, no error has occurred during transmission and the received word itself is the coded word transmitted.

Step 6

If the weight of the coset leader corresponding to the received word r is 2, the decoding cannot be done, viz., the coded word transmitted cannot be determined uniquely, as two coded words might have been received as the same word r due to 2 errors during transmission, as explained below with respect to the current example.

If the received word is 1 1 0 1 0, the weight of the corresponding coset leader is 2 and hence, the top element in the 3rd column, namely, 0 1 0 1 1 cannot be taken as the code word transmitted for the following reason.

After filling up the first 7 rows of the decoding table, the words belonging to B^5 with weight 2 and not included in the table are 10001 and 01100. We have constructed the 8th row by taking coset leader as 10001. Instead had we taken 0 1 1 0 0 as the coset leader of the 8th row, it would have become

0 1 1 0 0 1 1 0 1 0 0 0 1 1 1 1 0 0 0 1

Now as per the alternative 8th row of the decoding table, the received word 1 1 0 1 0 occurs in the record column. The top element in that column is 1 0 1 1 0 and this too can be taken as the code word transmitted. Thus if 2 errors occur during transmission, they can be detected but not corrected.

WORKED EXAMPLES 5(C)

Example 5.1 A binary symmetric channel has probability $p = 0.05$ of incorrect transmission. If the code word $c = 011\ 011\ 101$ is transmitted, what is the probability that (a) we receive $r = 011\ 111\ 101$? (b) we receive $r = 111\ 011\ 100$? (c) a single error occurs? (d) a double error occurs? (e) a triple error occurs?

(a) The received word $r = 011\ 111\ 101$ differs from the transmitted word $c = 011\ 011\ 101$ only in the fourth position.

The probability of occurrence of this specific error

$= P$(1 error and 8 non-errors)

$= 0.05 \times (0.95)^8 = 0.0332.$

(b) The received word r = 111 011 100 differs from the transmitted word c = 011 011 101 only in the first and ninth positions.

The probability of occurrence of these specific error

$= P$(2 errors and 7 non-errors)

$= (0.05)^2 \times (0.95)^7 = 0.0017.$

(c) P(1 error in any one position and 8 non-errors in the remaining positions)

= "$nC_1 \cdot p^r \cdot q^{n-1}$", by Bernoulli's theorem in Probability theory

$9C_1 \times (0.05)^1 \times (0.95)^8 = 0.2985$

(d) P(2 errors in any two positions and 7 non-errors in the remaining positions)

$= 9C_2 \times (0.05)^2 \times (0.95)^7 = 0.0629.$

(e) P(3 errors in any three positions and 6 non-errors in the remaining positions)

$= 9C_3 \times (0.05)^3 \times (0.95)^6 = 0.0077$

Example 5.2 The (9, 3) three times repetition code has the encoding function $e = B^3 \to B^9$, where $B = (0, 1)$.

(a) If d: $B^9 \to B^3$ is the corresponding decoding function, apply 'd' to decode the received words (i) 111 101 100, (ii) 000 100 011; (iii) 010 011 111 by using the majority rule.

(b) Find three different received words r for which $d(r) = 000$

(a) *Triple repetition code* means that when we encode a word $w = B^m$, all the m elements of w are repeated three times so as to produce $e(w) \in B^{3m}$.

To decode any received word by the *majority rule* we examine the 1st, 4th and 7th positions and note down the element (0 or 1) which appear more times. This process is continued with 2nd, 5th and 8th positions, 3rd, 6th and 9th positions and so on and finally with m^{th}, $(2m)^{th}$ and $(3m)^{th}$ positions. The m elements thus noted down are written in the order to give the original word.

(i) The received word is 111 101 100.

Among the elements in the 1st, 4th and 7th positions, 1 appears all the three times. Hence 1 is taken as the first element of the original word.

Among the elements in the 2nd, 5th and 8th positions, 0 appears twice. Hence 0 is taken as the second element of the original word. Among the elements in the 3rd, 6th and 9th positions, 1 appears twice. Hence 1 is taken as the third element of the original word.

$\therefore \quad d(111\ 101\ 100) = 101$

(ii) Similarly $d(000\ 100\ 011) = 000$

(iii) $d(010\ 011\ 111) = 011$

(b) Since $d(r) = 000$, 0 must appear more times in the 1st, 4th and 7th positions and similarly in the 2nd, 5th and 8th positions and in the 3rd, 6th and 9th positions.

One set of such three words is:

100 000 000, 000 010 000, 000 000 001.

Example 5.3 Find the code words generated by the encoding function $e: B^2 \to B^5$ with respect to the parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Note In our discussion, if the encoding function is $e: B^m \to B^n$, the generator matrix was assumed as an $m \times n$ matrix $G = [I_m|A]$ and the parity check matrix was assumed as an $(n - m) \times m$ matrix $H = [A^T|I_{n-m}]$ and as such there was less number of rows and more number of columns in H. We shall stick to our notation. As per our notation, what is given in this problem is not H, but H^T. However some authors use this notation to denote the parity check matrix.

Rewriting the given matrix as per our notation, we have

$$H = \left[\begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T|I_{n-m}]$$

Here $n = 5$ and $m = 2$.

Hence, the generator matrix G is given by

$$G = [I_m|A] = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Now $B^2 \equiv \{0\ 0, 0\ 1, 1\ 0, 1\ 1\}$ and $e(w) = w\ G$

$$\therefore \quad e(0\ 0) = [0\ 0]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 0\ 0\ 0\ 0]$$

$$\therefore \quad e(0\ 1) = [0\ 1]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 1\ 0\ 1\ 1]$$

$$\therefore \quad e(1\ 0) = [1\ 0]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [1\ 0\ 0\ 1\ 1]$$

$$\therefore \quad e(1\ 1) = [1\ 1]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [1\ 1\ 0\ 0\ 0]$$

Hence, the code words generated by H are 0 0 0 0 0, 0 1 0 1 1, 1 0 0 1 1 and 1 1 0 0 0.

Example 5.4 Find the code words generated by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

when the encoding function is e: $B^3 \to B^6$.

Taking $$H = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T | I_{n-m}]$$

as per our notation, the generator matrix

G is given by $$G = [I_m | A] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Now $B^3 = \{0\,0\,0, 0\,0\,1, 0\,1\,0, 1\,0\,0, 0\,1\,1, 1\,0\,1, 1\,1\,0, 1\,1\,1\}$

$\therefore$
$e(0\ 0\ 0) = [0\ 0\ 0] \cdot G = [0\ 0\ 0\ 0\ 0\ 0]$
$e(0\ 0\ 1) = [0\ 0\ 1] \cdot G = [0\ 0\ 1\ 0\ 1\ 1]$
$e(0\ 1\ 0) = [0\ 1\ 0] \cdot G = [0\ 1\ 0\ 1\ 0\ 1]$
$e(1\ 0\ 0) = [1\ 0\ 0] \cdot G = [1\ 0\ 0\ 1\ 1\ 1]$
$e(0\ 1\ 1) = [0\ 1\ 1] \cdot G = [0\ 1\ 1\ 1\ 1\ 0]$
$e(1\ 0\ 1) = [1\ 0\ 1] \cdot G = [1\ 0\ 1\ 1\ 0\ 0]$
$e(1\ 1\ 0) = [1\ 1\ 0] \cdot G = [1\ 1\ 0\ 0\ 1\ 0]$
$e(1\ 1\ 1) = [1\ 1\ 1] \cdot G = [1\ 1\ 1\ 0\ 0\ 1]$

Thus, the code words generated are

0 0 0 0 0 0, 0 0 1 0 1 1, 0 1 0 1 0 1, 1 0 0 1 1 1, 0 1 1 1 1 0,
1 0 1 1 0 0, 1 1 0 0 1 0 and 1 1 1 0 0 1.

Example 5.5 Decode each of the following received words corresponding to the encoding function e: $B^3 \to B^6$ given by $e(000) = 000\ 000$, $e(001) = 001\ 011$, $e(010) = 010\ 101$, $e(100) = 100\ 111$, $e(011) = 011\ 110$, $e(101) = 101\ 100$, $e(110) = 110\ 010$ and $e(111) = 111001$, assuming that no error or signal error has occurred:

0 1 1 1 1 0, 1 1 0 1 1 1, 1 1 0 0 0 0, 1 1 1 0 0 0, 0 1 1 1 1 1.

We note that the minimum distance between the code words (viz., the minimum weight of the non-zero code words) is 3 and hence, atmost 1 error can be corrected that might have occurred in the received words.

(i) The word 0 1 1 1 1 0 is identical with $e(0\ 1\ 1)$. Hence, no error has occurred in this word and the original message is 0 1 1.

(ii) The word 1 1 0 1 1 1 differs from $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 1\ 1$ in the second position only. Correcting this single error, the transmitted word is 1 0 0 1 1 1 and the original message is 1 0 0.

(iii) The word 1 1 0 0 0 0 differs from $e(1\ 1\ 0) = 1\ 1\ 0\ 0\ 1\ 0$ in the fifth position only. Correcting this error, the transmitted word is 1 1 0 0 1 0 and the original message is 1 1 0.

(iv) The word 1 1 1 0 0 0 differs from $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 0\ 1$ in the sixth position only. Correcting this error, the transmitted word is 1 1 1 0 0 1 and the original message is 1 1 1.

(v) The word 0 1 1 1 1 1 differs from $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 1\ 0$ in the sixth position only. Correcting this error, the transmitted word is 0 1 1 1 1 0 and the original message is 0 1 1.

Example 5.6 If x is a specific encoded word that belongs to B^{10} and $S(x, k)$ is the set of all received words corresponding to x with at most k errors, determine $|S(x, 1)|$, $|S(x, 2)|$, $|S(x, 3)|$. If $x \in B^n$, what is $|S(x, k)|$, where $1 \le k \le n$.

$S(x, 1)$ is the set of all received words $\in B^{10}$. Since the position for the single error can be chosen from the 10 positions of x in $10C_1 = 10$ ways. As $S(x, 1)$ includes the word with no error, $S(x, 1)$ contains $1 + 10 = 11$ words.

i.e., $|S(x, 1)| = 11$

Similarly $|S(x, 2)|$ = No. of words with no error, 1 error and 2 errors

$= 1 + 10C_1 + 10C_2$

$= 56.$

$|S(x, 3)|$ = No. of words with no error, 1 error, 2 errors and 3 errors

$= 1 + 10C_1 + 10C_2 + 10C_3$

$= 176.$

In general,

$$|S(x, k)| = 1 + nC_1 + nC_2 + \cdots nC_k = \sum_{i=o}^{k} nC_i$$

Example 5.7 Given the generator matrix $G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, corresponding to the encoding function e: $B^3 \to B^6$, find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message. Are all the words decoded uniquely?

(i) 1 1 0 1 0 1, (ii) 0 0 1 1 1 1, (iii) 1 1 0 0 0 1, (iv) 1 1 1 1 1 1

If we assume that $G = [I_3|A]$, then

$$H = [A^T|I_3] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We compute the *syndrome* of each of the received word by using $H \cdot [r]^T$.

(i) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Since, $H \cdot [e(w)]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, the received word in this case is the transmitted (encoded) word itself. Hence, the original message is 1 1 0.

(ii) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

Since, the syndrome $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is the same as the fifth column of H, the element in the fifth position of r is changed.

$\therefore$ The decoded word is 0 0 1 1 0 1 and the original message is 0 0 1.

(iii) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

Since, the syndrome $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ is the same as the fourth column of H, the fourth component of r is changed to get the decoded word. It is 1 1 0 1 0 1 and the original message is 1 1 0.

(iv) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

Since, the syndrome is not identical with any column of H, the received word cannot be decoded uniquely.

Example 5.8 Construct the decoding table for the group code given by the generator matrix.

$$G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Decode the following received words using the decoding table obtained. Which of the words could not be decoded uniquely?

1 0 1 1 1 1, 0 1 1 0 1 0, 1 0 1 1 1 0, 1 1 1 1 1 1.

Since G is a 3×6 matrix, it corresponds to the encoding function $e: B^3 \to B^6$.

Now, $B^3 = \{0\,0\,0, 0\,0\,1, 0\,1\,0, 1\,0\,0, 0\,1\,1, 1\,0\,1, 1\,1\,0, 1\,1\,1\}$

$e(0\,0\,0) = [0\,0\,0]G = [0\,0\,0\,0\,0\,0]$;

Similarly $e(0\,0\,1) = [0\,0\,1\,0\,1\,1]$; $e(0\,1\,0) = [0\,1\,0\,1\,0\,1]$

$e(1\,0\,0) = [1\,0\,0\,1\,1\,1]$; $e(0\,1\,1) = [0\,1\,1\,1\,1\,0]$;

$e(1\,0\,1) = [1\,0\,1\,1\,0\,0]$; $e(1\,1\,0) = [1\,1\,0\,0\,1\,0]$

and $e(1\,1\,1) = [1\,1\,1\,0\,0\,1]$.

We form the decoding table by making these encoded words as the elements of the first row and the coset leaders as the elements of the first column. The coset leaders with only one 1 have been taken in a certain order and then those with two 1's have been taken. The decoding table is given in Table 5.14.

Table 5.14

Code words→							
000000	001011	010101	100111	011110	101100	110010	111001
100000	101011	110101	000111	111110	001100	010010	011001
010000	011011	000101	110111	001110	111100	100010	101001
001000	000011	011101	101111	010110	100100	111010	110001
000100	001111	010001	100011	011010	101000	110110	111101
000010	001001	010111	100101	011100	101110	110000	111011
000001	001010	010100	100110	011111	101101	110011	111000
011000	010011	001101	111111	000110	110100	101010	100001

↑ Coset leaders

Note The decoding table is not unique as the coset leader of the last row could have been taken as 1 0 0 0 0 1 or 0 0 0 1 1 0.

Decoding of the received words

(i) 101 111 appears in the 4^{th} row and 4^{th} column. The coset leader of the 4^{th} row is 001 000, which contains only one 1,

Since the minimum weight of the code words is 3, atmost one error can be corrected in the received word.

The corrected (received) word, viz., the code word transmitted is the top element of the 4^{th} column. It is 100 111 and hence the original message is 100.

(ii) 0 1 1 0 1 0 appears in the 5^{th} row and 5^{th} column. Hence the corresponding code word transmitted is 0 1 1 1 1 0 and hence the original message is 0 1 1.

(iii) 1 0 1 1 1 0 appears in the 6^{th} row and 6^{th} column. Hence the corresponding code word transmitted is 1 0 1 1 0 0 and hence the original message is 1 0 1.

(iv) 1 1 1 1 1 1 appears in the 8^{th} row, the coset leader of which contains two 1's viz., the received word contains 2 errors. Hence, they cannot be corrected and the code word transmitted cannot be uniquely determined.

EXERCISE 5(C)

Part A: (Short answer questions)

1. What is the main objective of coding theory?
2. What do you mean by encoder and decoder?
3. What is group code?
4. Define Hamming code.
5. Define even and odd parity checks.
6. What is meant by (i) the weight of a code word (ii) the Hamming distance between two code words?
7. If the minimum distance between two code words is (i) 3, (ii) 4 and (iii) 5, how many errors can be detected and how many can be corrected in each case?
8. Define generator matrix corresponding to the encoding function e: $B^m \to B^n$.
9. What are the restrictions on A occurring in the generator matrix $G = [I_m | A]$?
10. How will you use the generator matrix to get the code words corresponding to the given message words?
11. Define the parity check matrix. How is it related to the generator matrix?
12. How will you use the parity check matrix to retrieve the code word from a received word?
13. How will you find the minimum distance between any two code words in a group code?

14. What are the possible weight of the code word x, if

$$H \cdot [x]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} [x]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} ?$$

15. Explain briefly the step by step procedure for constructing the decoding table for group code.
16. How will you make use of the decoding table to get back the code word corresponding to a received word, if it contains a single error?
17. If $x, y, z \in B^n$, prove that (i) $H(x, y) \geq 0$ (ii) $H(x, y) = 0 \Rightarrow x = y$ (iii) $H(x, y) = H(y, x)$.
18. If $x, y, z \in B^n$, prove the triangle inequality $H(x, z) \leq H(x, y) + H(y, z)$ [*Hint:* $H(x, z) = \text{Wt}(x \oplus z) = \text{Wt}\{x \oplus (y \oplus y) \oplus z\} = \text{Wt}\{(x \oplus (y \oplus y) \oplus z)\}$, since $y \oplus y = 0$]
19. If $C \subseteq B^7$, where C is a set of code words and $r = c + e$, where $c \in C$, e is the error pattern and r is the received word, find r, e and c respectively from the following:
    (i) $c = 1\ 0\ 1\ 0\ 1\ 1\ 0$ and $e = 0\ 1\ 0\ 1\ 1\ 0\ 1$
    (ii) $c = 1\ 0\ 1\ 0\ 1\ 1\ 0$ and $r = 1\ 0\ 1\ 1\ 1\ 1\ 1$
    (iii) $e = 0\ 1\ 0\ 1\ 1\ 1\ 1$ and $r = 0\ 0\ 0\ 0\ 1\ 1\ 1$
20. If e: $B^2 \rightarrow B^6$ is given by $e(0\ 0) = 0\ 0\ 0\ 0\ 0\ 0$, $e(1\ 0) = 1\ 0\ 1\ 0\ 1\ 0$, $e(0\ 1) = 0\ 1\ 0\ 1\ 0\ 1$ amd $e(1\ 1) = 1\ 1\ 1\ 1\ 1\ 1$, list the elements in $S(1\ 0\ 1\ 0\ 1\ 0, 1)$ and $S(1\ 1\ 1\ 1\ 1\ 1, 1)$, where $S(x, k)$ is the set of all received words corresponding to x with at most k errors.
21. For each of the following encoding fucntions, find the minimum distance between the code words. State also the error-detecting and error-correcting capabilities of each code:
    (i) $e(0\ 0) = 0\ 0\ 0\ 0$, $e(1\ 0) = 0\ 1\ 1\ 0$, $e(0\ 1) = 1\ 0\ 1\ 1$, $e(1\ 1) = 1\ 1\ 0\ 0$
    (ii) $e(0\ 0) = 0\ 0\ 0\ 0\ 1$, $e(1\ 0) = 1\ 0\ 1\ 0\ 0$, $e(0\ 1) = 0\ 1\ 0\ 1\ 0$, $e(1\ 1) = 1\ 1\ 1\ 1\ 1$
    (iii) $e(0\ 0) = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$; $e(1\ 0) = 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0$, $e(0\ 1) = 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1$; $e(1\ 1) = 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1$.
    (iv) $e(0\ 0\ 0) = 0\ 0\ 0\ 1\ 1\ 1$; $e(0\ 0\ 1) = 0\ 0\ 1\ 0\ 0\ 1$; $e(0\ 1\ 0) = 0\ 1\ 0\ 0\ 1\ 0$; $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 0\ 0$; $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 0\ 0$; $e(1\ 0\ 1) = 1\ 0\ 1\ 0\ 1\ 0$; $e(1\ 1\ 0) = 1\ 1\ 0\ 0\ 0\ 1$, $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 0\ 0$.
    (v) $e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$; $e(0\ 0\ 1) = 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0$; $e(0\ 1\ 0) = 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1$; $e(1\ 0\ 0) = 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0$; $e(0\ 1\ 1) = 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1$; $e(1\ 0\ 1) = 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1$, $e(1\ 1\ 0) = 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0$; $e(1\ 1\ 1) = 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1$.

Part B

22. A binary symmetric channel has probability $p = 0.001$ of incorrect transmission. If the code word 110 101 101 is transmitted, what is the probability (i) of correct transmission (ii) of making atmost one error in transmission (iii) of making atmost 2 errors in transmission?

23. The (24, 8) triple repetition code has the encoding function $e: B^8 \to B^{24}$, where $B \equiv (0, 1)$. If $d: B^{24} \to B^8$ is the corresponding decoding function, apply d to decode the received word 1 0 1 1 0 1 1 0, by using the majority rule.

24. Find the code words generated by the parity check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$, when the encoding function is $e: B^2 \to B^5$.

25. Find the code words generated by the parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$, when the encoding function is $e: B^3 \to B^6$.

26. Prove that the code words generated by the parity check matrix $H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ with respect to the encoding function $e: B^4 \to B^7$ form a group code.

27. If the encoding function $e: B^3 \to B^8$ is given by
$e(0\,0\,0) = 0\,0\,0\,0\,0\,0\,0\,0$, $e(0\,0\,1) = 0\,0\,1\,1\,0\,0\,1\,0$,
$e(0\,1\,0) = 0\,1\,0\,1\,1\,1\,0\,0$, $e(1\,0\,0) = 1\,0\,0\,0\,0\,1\,0\,1$;
$e(0\,1\,1) = 0\,1\,1\,0\,1\,1\,1\,0$, $e(1\,0\,1) = 1\,0\,1\,1\,0\,1\,1\,1$,
$e(1\,1\,0) = 1\,1\,0\,1\,1\,0\,0\,1$, and $e(111) = 11101011$,
find the corresponding parity check matrix.

28. Decide each of the following received words corresponding to the encoding function $e: B^3 \to B^6$ given by $e(0\,0\,0) = 0\,0\,0\,0\,0\,0$, $e(0\,0\,1) = 0\,0\,1\,1\,0\,1$, $e(0\,1\,0) = 0\,1\,0\,0\,1\,1$, $e(1\,0\,0) = 1\,0\,0\,1\,1\,0$, $e(0\,1\,1) = 0\,1\,1\,1\,1\,0$, $e(1\,0\,1) = 1\,0\,1\,0\,1\,1$, $e(1\,1\,0) = 1\,1\,0\,1\,0\,1$ and $e(1\,1\,1) = 1\,1\,1\,0\,0\,0$, assuming that no error or single error has occurred:
1 0 0 1 0 1, 1 0 1 1 0 1, 0 1 1 0 1 0, 1 1 1 0 1 0, 1 0 0 0 1 0.

29. Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$, corresponding to the encoding function $e: B^4 \to B^7$, find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message:
1 1 0 0 0 0 1, 1 1 1 0 1 1 1, 0 0 1 0 0 0 1, 0 0 1 1 1 0 0.

30. Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ corresponding to the encoding function $e: B^3 \to B^6$, find the corresponding parity check matrix and use it to decode the following received words and hence to find the original message:

1 1 1 1 0 1, 1 0 0 1 0 0, 1 1 1 1 0 0, 0 1 0 1 0 0

31. Repeat problem (30) with $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$, $e: B^2 \to B^6$ and received words 0 0 0 1 0 0, 0 1 1 1 0 1, 1 1 1 0 1 0 and 1 0 1 0 1 1.

32. Repeat problem (30) with $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, $e: B^3 \to B^8$ and received words 1 0 1 1 0 1 0 1, 1 0 0 1 1 0 0 1, 0 0 0 1 0 1 0 0, 0 0 1 1 0 0 1 1.

33. Construct the decoding table for the group code given by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Use the decoding table to decode the following received words:
1 1 1 1 0, 1 1 1 0 1, 1 1 0 1 1, 1 0 1 0 1, 1 0 0 1 1, 1 1 1 1 1 and 0 1 1 0 0.

34. Construct the decoding table for the group code given by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

Use the decoding table to decode the following received words:
0 0 0 1 1 0, 0 0 0 0 1 1, 0 0 0 1 0 1, 1 1 0 0 0 1, 1 0 1 0 0 1 and 0 1 1 1 1 1.

35. Construct the decoding table for the group code generated by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Use the decoding table to decode the following received words:
1 1 1 0 0 0, 1 1 0 0 0 0, 1 0 1 0 0 0, 1 0 1 1 1 1, 0 0 1 1 1 0 and 1 1 0 1 0 1.

Exercise 5(c)

7. (i) 2, 1 (ii) 2, 1 (iii) 4, 2
14. 3 or 4
19. (i) 1111011 (ii) 0001001 (iii) 0101000
20. (i) {101010, 001010, 111010, 100010, 101110, 10100, 101011}
    (ii) {111111, 011111, 101111, 110111, 111011, 111101, 111110}
21. (i) 2; can detect atmost 1 error; cannot correct any error.
    (ii) 3; can detect atmost 2 errors; can correct atmost 1 error;
    (iii) 5; can detect atmost 4 errors and can correct atmost 2 erros;
    (iv) 2; can detect atmost 1 error and cannot correct any error.
    (v) 3; can detect 2 errors and can correct 1 error;
22. (i) 0.991036 (ii) 0.999964 (iii) 0.999999
23. 10110111
24. $e(00) = 00000$, $e(01) = 01011$, $e(10) = 10110$, $e(11) = 11101$;
25. $e(000) = 000000$, $e(001) = 001011$, $e(010) = 010101$, $e(100) = 100110$; $e(011) = 011110$, $e(101) = 101101$, $e(110) = 110011$, $e(111) = 111000$.
27. $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$
28. 110101, 001101, 011110, 111000, 100110;
29. 1100, 1110, 0010, 0011
30. 101, 010, 100, could not be decoded.
31. 00, 01, 10, 10;
32. 011, 101, 110, 111.
33. **Table 5.15**

00000	01110	10011	11101
00001	01111	10010	11100
00010	01100	10001	11111
00100	01010	10111	11001
01000	00110	11011	10101
10000	11110	00011	01101
11000	10110	01011	00101
10100	11010	00111	01001

01110, 11101, 10011, 10011, 10011, 11101, 11101 and 01110
Massages are: 01, 11, 10, 10, 10, 11, 11, and 01,