Dr. Khushboo Verma

B.Tech-IV SEM

Discrete Mathematical Structure-AS-404

Defn: The basic unit of information called message, is a finite sequence of character's from a finite alphabet. A sequence of symbols form an alphabet is also called as word.

Code: A code is a collection of words that are to be used to represent distinct message. A word in a code is called code word.

Let us assume that the alphabet is the binary alphabet $\{0;1\}$. Then we have 2^n different binary word of length n.

Example: for $n = 3$, Binary words $= \{000, 001, 011, 100, 101, 110, 111\}$

A (m,n) code for a binary message is a tuple (B^m, B^n, E, D)

where, B^m : set of all Binary m-tuples

B^n : " " " n-tuples $(n > m)$

$E : B^m \to B^n$: Encoding func

$D : R \to B^m$: Decoding func $(R \subseteq B^n)$.

If $b \in B^m \Rightarrow E(b)$ is called code word representing b.

Let $X \subseteq B^m$, $X \neq \phi$ (nonempty) then X is called set of message words and $E(X)$ is called set of code words

Let X' be the set of received words after transmission. then $D(X')$ is called set of decoded words.

Error-Detecting Code & Error correcting Code :—

Codes are classified into error-detecting code whose purpose is to simply detect the presence of errors.

Error-detecting code in which an attempt is to made to correct errors which occurs because of noise in transmission channel

Let $B3 = \{000, 001, 010, 011, 101, 110, 111\}$

If the word 100 is transmitted and an error is occure in second digit and we get 110, Then there is no way to detect the error because 110 is already member of the set.

Thus if we want to detect error, then error must not be the member of the set.

Example: (1) Let $E: B^m \to B^{m+1}$ is defind by $E(a_1a_2 \cdots a_m) = a_1a_2 \cdots a_{m+1}$

where $a_{m+1} = \begin{cases} 1 & \text{if 1's is odd number} \\ 0 & \text{if 1's is even number.} \end{cases}$

$\Rightarrow$ ~~Eg~~ For $m=3 \Rightarrow B^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Then code words are

$$\Rightarrow \left.\begin{array}{ll} E(000) = 0000 & E(100) = 1001 \\ E(001) = 0011 & E(101) = 1010 \\ E(010) = 0101 & E(110) = 1100 \\ E(011) = 0110 & E(111) = 1111 \end{array}\right\} \text{— ①}$$

If transmissian chanel transmits $E(010) = 0100$ (error)

Because $E(010) = 0101$ (from equ ①)

This is the ~~eg~~ example of error detecting code. (because we can detect this error from the set, as this is not the member of the set).

Example (2): Let $E: B^m \to B^{3m}$ s.t.

for $m=3$ $\qquad E(a_1a_2 \cdots a_m) = \underline{a_1a_2 \cdots a_m}\ \underline{a_1a_2 \cdots a_m}\ a_1a_2 \cdots a_m$

$$\Rightarrow \begin{array}{ll} E(000) = 000\ 000\ 000 & E(100) = 100\ 100\ 100 \\ E(001) = 001\ 001\ 001 & E(101) = 101\ 101\ 101 \\ E(010) = 010\ 010\ 010 & E(110) = 110\ 110\ 110 \\ E(011) = 011\ 011\ 011 & E(111) = 111\ 111\ 111 \end{array}$$

Suppose $E(101) = 101\,\underline{100}\,101$ This is the error and also be corrected. In this code we get two error but can correct only one error. This is the example of error correcting code.

<u>Hamming distance</u> and <u>Weight</u>: Let A be the set of all Binary sequence of length n

If $x \in A$ then Hamming weight $w(x)$ is defind by the number of 1's in x and denoted by $w(x)$

Example: $\quad x = 1100 \Rightarrow w(1100) = 2$

$\qquad\qquad\quad x = 1011 \Rightarrow w(1011) = 3$

For $x, y \in A$, Hamming distance $d(x,y)$ between x and y is defined by the number of possitions where the code word have different symbols.

Example: $\quad x = 1100,\ y = 1011 \Rightarrow d(x,y) = 3$

$\qquad\qquad\quad x = 1010,\ y = 0100 \Rightarrow d(x,y) = 3$

Remark: If $x = x_1x_2 \cdots x_n$ $y = y_1y_2 \cdots y_n$ then number of i's for which $x_i \neq y_i$ is called Hamming distance.

propr: of distance func:

$d(x,y) = d(y,x)$

$d(x,y) \geq 0$

$d(x,y) = 0$ if $x = y$

$d(x,y) \leq d(x,z) + d(z,y)$

Theorem ①: A code (B^m, B^n, E, D) can detect K or fewer error if and only if the minimum distance between any two distinct code words is atleast $K+1$.

Proof: Suppose that the min distance between any two code words is atleast $K+1$.

we have to show: we can detect K or fewer error.

let w be the code word which is transmitted and received as w' then

$$d(w, w') \geq K+1$$

$\Rightarrow$ w' is transmitted with $K+1$ or more error.

$\Rightarrow$ any number of errors fewer than $K+1$ will not be in a Code.

$\Rightarrow$ E can detect K or fewer errors.

Converse: let the min distance between two code words w and y be $d(w,y) \leq K$

$\Rightarrow$ $d(w,w') \leq K$

if $w' = y$ $\Rightarrow$ then less than K errors have been committed and have not been detected

which is contradiction.

$\Rightarrow$ min distance is $(K+1)$

Theorem ②: A code (B^m, B^n, E, D) can correct K or fewer errors if and only if the minimum distance between any two distinct code word is atleast $2K+1$.

Proof: Assume that the min. distance between any two distinct code is atleast $2K+1$. Let w be any code word and we receive w' with K or less error then

$$d(w,w') \leq K \quad \text{—(I)} \qquad d(w,c) \geq 2K+1 \quad \text{—(II)}$$

Let c be any code word $\Rightarrow d(w,c) \leq d(w,w') + d(w',c)$

$$d(w,c) \leq d(w',c) + K$$

$\Rightarrow$
$$d(w',c) + K \geq 2K+1$$

$\Rightarrow$
$$d(w',c) \geq K+1$$

$\Rightarrow$ distance between any code word to w' is always greater than the distance between w and w'.

$\Rightarrow$ w' can be detected and also corrected.

Conversely: assume that the min distance between any pair of code w and c is atleast $2K$ (if possible)

i.e. $d(wc) \leq 2K$

Since code correct K or less error

$\Rightarrow$ we detect K errors

$\Rightarrow$ by precious theorem, $d(w,c) \geq K+1$

$\Rightarrow$ $K+1 \leq d(w,c) \leq 2K$

Let w be any worde which is transmitted, with K error and we get w' so that

$d(ww') = K$.

$\Rightarrow$ also assume ~~let~~ $d(w,x) = K$, where x be another code.

$\Rightarrow$ $d(w',x) \leq 2K-K \Rightarrow d(w',x) \leq K$

$\Rightarrow$ w' is at least as close to x as it is to w

$\Rightarrow$ w cannot be cannot be correctly decoded.

$\Rightarrow$ Code is not been able to correct K errors.

which is contradiction.

Example: Consider $(4,2)$-Encoding fun^c. How many errors will detect ?!

$(4,2)$-Encoding fun^c $\Rightarrow$ $m=4, n=2$

$\Rightarrow$ $e(00) = 0000$ $\quad e(10) = 0110$

$e(01) = 1011$ $\quad e(11) = 1100$

Solution: let $x_1 = 0000$, $x_2 = 0110$, $x_3 = 1011$, $x_4 = 1100$

$\Rightarrow$ $d(x_1 x_2) = 2$ $\quad d(x_1 x_3) = 3$, $\quad d(x_1 x_4) = 2$

$d(x_2, x_3) = 3$ $\quad d(x_2 x_4) = 2$ $\quad d(x_3 x_4) = 3$

$\Rightarrow$ min distance $= 2$

$\Rightarrow$ $2 \geq K+1 \Rightarrow \boxed{K \leq 1} \Rightarrow$ code can detect 1 or fewer error.

Group (Linear) code: It is easy to show that $(B^m, +)$ and $(B^n, +)$ are commutative groups under component wise $+_2$ (addition modulo 2) of words. (as every element of B^m and B^n has its own inverse and zero is the identity)

Let $E : B^m \to B^n$ be an encoding fun^C. The code $C = E(B^m)$ is called group code if C is a subgroup of B^n.
By def^n of subgroup, C, the subset of B^n, consist all code word is a subgroup of B^n if
(I) The identity element of B^n is in C.
(II) if $x, y \in C \Rightarrow x+y \in C$.
(III) if x in $C \Rightarrow$ inverse also in C (obvious).

Example: Show that $(5, 2)$ - encoding fun^C $e : B^2 \to B^5$ defined by

$e(00) = 00000$ $e(01) = 01110$
$e(10) = 10101$ $e(11) = 11011$ is a group code.

Soln: To prove the encoding fun^C group code, we have to show that $C = \{00000, 01110, 10101, 11011\}$ is a subgroup of B^5.

Composition table

+	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

$\Rightarrow$ (I) Closure : $\forall x, y \in C \Rightarrow x+y \in C$
(II) identity: $(00000) \in B^5$ is also belong to C.
(III) Inverse : From the composition table it is clear that every element is its own inverse.
$\Rightarrow$ C is subgroup of B^5 $\Rightarrow$ Encoding fun^C is group code.

Parity-check and Generator Matrix :

For (n, m) code $(m<n)$, the encoding function $E : B^m \to B^n$ is given by $m \times n$ matrix G. The matrix G is called the generator matrix (Encoded matrix) for the code.

$$\boxed{G = [I_m | A]_{m \times n}}$$ where A : $m \times (n-m)$ matrix
I_m : $m \times m$ identity matrix

Let G be generator matrix $(m \times n)$ and $E_G : B^m \to B^n$ Encoding fu^c^ defined by.

$$\boxed{E_G(\bar{a}) = \bar{b} = \bar{a} G.} \quad \forall \bar{a} \in B^m.$$

$$\text{if } G = \{e_{ij}\} \Rightarrow \bar{b} = \sum a_i e_{ij} \pmod 2$$

if $G = [I_m | A]_{m \times n}$, where I_m : Identity matrix of $m \times m$ & A is $(m \times (n-m))$ matrix, then parity check matrix is defined by

$$\boxed{H = [A^T | I_{n-m}]_{(n-m) \times n}}.$$

Remark :- Code word c is valid code if $cH^T = 0$ or $Hc^T = 0$

Example :- If parity check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

(i) find Generator matrix G
(ii) Find the code word for data (101).

Soln :

$$H = [A^T | I_{n-m}]_{n-m \times n}$$

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

$$\Rightarrow \quad A^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Rightarrow \quad A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

as $\quad G = [I_m | A]_{m \times n} = [I_3 | A]$

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

Now, $$E(101) = [101] \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= \left[\frac{1+0+0}{+2} \quad \frac{0+0+0}{+2} \quad \frac{0+0+1}{+2} \quad \frac{1+0+1}{+2} \quad \frac{1+0+1}{+2} \right] = [101010]$$

Example(2): find Generator matrix ~~whose~~ of Encoding fun^c $E: B^3 \to B^5$ w.r.to parity check matrix.

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

Soln: as $E: B^2 \to B^5 \Rightarrow m = 2, n = 5$

$\Rightarrow$

$$H = [\quad]_{n-m \times n} = [\quad]_{5-2 \times 5} = [\quad]_{3\times 5}$$

$\Rightarrow$ standard form of H is, $H = [A^T | I_3]_{3\times 5}$

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

Now $G = [I_m | A]_{m\times n} = [I_2 | A]_{2\times 5}$

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

Example-(3) the parity check matrix for a 6-bit linear code is

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

The words $\overset{(a)}{(111001)}$ and $\underset{(b)}{(101011)}$ are received. Use the matrix to decide whether or not the words are likely to have been correctly transmitted.

if words are correctly transmitted $\Rightarrow H \cdot a^T = 0$

If $Ha^T \neq 0 \Rightarrow$ There is an error.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1+1+0+0+0+0}{+_2} \\ \frac{0+1+1+0+0+0}{+_2} \\ \frac{0+0+1+0+0+1}{+_2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\Rightarrow$ [111001] correctly transmitted

Similarly for (101011)

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

$\Rightarrow$ [101011] is not correctly transmitted.

Scanned with CamScanner

Remark: Let H is a parity check matrix and r is the received word

Then compute Hr^T:

(I) if $Hr^T = 0 \Rightarrow r$ transmitted correctly

(II) If $Hr^T \neq 0 \Rightarrow r$ is not " "

In this case locate the column h^i of H s.t. $Hr^T = h^i$ and change the ith bit of r'.

Now ~~Hr^T~~ $Hr'^T = 0 \Rightarrow r'$ is correct code

if $Hr'^T \neq 0 \Rightarrow \exists$ error more than two bit which can not be decode.

Example: If $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$, Let the word $r = 110110$ is received and only one error occure then what is the correct code:

$$Hr^T = \begin{bmatrix} 1 & \boxed{1} & 0 & 1 & 0 & 1 \\ 1 & \boxed{1} & 0 & 0 & 1 & 0 \\ 1 & \boxed{0} & 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Identical

$\Rightarrow$ error in the second bit of $r \Rightarrow$ Change the II^{nd} bit of r.

$\Rightarrow$ new $r = [100110]$

Hamming Code: when the parity check matrix for a Hamming Code is written in the Lexicographical order (increasing) for the column of H, the column h^i is binary representation of i.

If z is the received word containing one error Then Hz^T represent ith binary number. in which error occurs

Algorithm: (1). Arranges the column ~~h~~ of parity check matrix H in order of increasing value.

(2). Determine the Syndrome $S = Hy^T$

(3) if $S = 0 \Rightarrow y$ is correct codeword

(4) if $S \neq 0 \Rightarrow S$ gives the binary representation of the error position.

(5) correct the error position ~~of~~ ~~y~~. in Y.

Coset Decoding: A Group Canbe decoded by using the group Structure of C together with the coset in B^n. This method is called Coset decoding.

Algorithm:

(1). List of all the code of the group code C in a first row beginning with identity (000..0)

(2). Choose a word x of B^n where x does not appear any where in the table and has min weight.

Now list the element to left coset $x+C$ as the next row appearing below a for every $a \in C$. The code word of min weight in a coset (if it is Unique) is called the coset leader. If there are several identical code word, then chose arbitrarily on of them as a coset leader.

(3). repeat step 2 untill all element of B^n are exhausted.

Once the decoding table is completed for each received word r

(4). Identify the column in which r occurs. If weight of the coset leader corresponding to r is 1 then the top most entry of this colum in which r occur is the decoded words

(5). If the weight of the coset leader corresponding to the received word r is 2, then the coded word cannot be determine uniquely.

Example: Construct a decoding table for the group given by the generator matrix
$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$
Use the table to decode the following receive message.

11101 11011 11111 11010

Soln: Step-I: Find C

as $$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{2\times 5} = \left[I_2 | A \right]_{m\times n} \Rightarrow m=2$$

$\Rightarrow$ $E: B^2 \to B^5$ $\Rightarrow$ Total element $2^m = 2^2 = 4$

$\Rightarrow$ This code contain 4 element (messages)

(i.e. (00, 01, 10, 11).

	Element of B^2	set of code word C
0 0	(00) G	00000
1 0	(10) G	10110
0 1	(01) G	01011
1 1	(11) G	11101

Now we develop standard array for decoding :-

C	00000	10110	01011	$\boxed{11101}$
10000+C	10000	00110	$\boxed{11011}$	01101
01000+C	01000	11110	00011	10101
00100+C	00100	10010	01111	11001
00010+C	00010	10100	01001	$\boxed{11111}$
00001+C	00001	10111	01010	11100

for $r_1 = 11101$
This is the member of IVth colum also it is top most entry
$\Rightarrow$ respective code word is $c_1 = 11101$ w.r.to $w_1 = 11$

for $r_2 = 11011$ This the member of IIIrd colum
$\Rightarrow$ Top most entry of IIIrd colum $c_2 = 01011$ w.r.to $w_2 = 01$
asd$(r_2, c_2) = 1$

$r_3 = 11111$
This is member of IVth column
$\Rightarrow$ Top most entry of IVth column $c_3 = 11101$ w.r.to $w_3 = 11$.
asd$(r_3 c_3) = 1$

as $r_4 = 11010$ is not appear yet, add anothe raw in standard array.

11000 + C	11000	01110	10011	00101
01100 + C	01100	$\boxed{11010}$	00111	10001

$r_4 = 11010$ is appeared in IInd colum whose top most entry is $10110 = c_4$ w.r.to $\boxed{w_4 = 10}$ but in this case
$d(r_4, c_4) = 2$
$\Rightarrow$ w_4 is not unique code to represent r_4.

10001+C	10001	00111	$\boxed{11010}$ IIIrd	01100

$r_4 = 11010$ w.r.to. IIIrd colum $\Rightarrow \boxed{w_4 = 01}$
$\Rightarrow$ Two representation for r_4.

(*b*) The symmetric generator matrix G can be derived from H writing H as $H = [A^T \mid I_{n-m}]$ $= [A^T \mid I_3]$ noting that $G = [I_4 \mid A]$ as given below :

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

Note that the generator can also be deduced from $G.H^T = 0$.

(*c*) For code word y_1 the syndrome is equal to

$$S_1 = Hy_1^T = [1\ 1\ 0]^T$$

which corresponds to second column of H. Hence the corrected code word is 1100001 and the transmitted message is 1100.

For code word y_2 the syndrome is equal to

$$S_2 = Hy_2^T = [0\ 0\ 0]^T$$

Hence code word is correct.

Problem Set 19.1

1. Find the Hamming distance between x and y
   (*a*) $x = 1101, y = 1000$ (*b*) $x = 1010101, y = 1100100$
   (*c*) $x = 0010111, y = 0101011$
2. Find the Hamming weight of the given words
   (*a*) 1010101 (*b*) 1110011
   (*c*) 1001101
3. Consign the encoding function $E : B^2 \to B^5$ defined by

   $E(0\ 0) = 00000$
   $E(1\ 0) = 10110$
   $E(0\ 1) = 01101$
   $E(1\ 1) = 11011$

   Find the minimum Hamming distance. How many error will E defect and correct?
4. Find the minimum Hamming distance of the following code,
   0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111
   State the number of errors which can be detected and corrected.
5. Let $E : B^3 \to B^9$ be the encoding function for the code (9, 3) triple repetition code. If $D : B^9 \to B^3$ be the corresponding decoding function, apply D to decode the received words (*i*) 111101100 (*ii*) 000100011.
6. Consider the encoding function $E : B^2 \to B^6$ defined by

   $E(0\ 0) = 000000$
   $E(1\ 0) = 101010$
   $E(0\ 1) = 010101$
   $E(1\ 1) = 111111$

   Find the minimum hamming distance between the code words. Find the no of errors which can be detected and corrected.
7. Use the parity check matrix

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

   to test the words (*a*) 1001111 (*b*) 0111001 (*c*) 0101100

8. For each of the following encoding function, find the minimum distance between the code wor
Discuss the error detecting and error correcting capabilities of each code.

(*a*) $E : B^2 \to B^5$

$E(0\ 0) = 00001$ $\quad E(1\ 0) = 10100$

$E(0\ 1) = 01010$ $\quad E(1\ 1) = 11111$

(*b*) $E : B^3 \to B^9$

$E(000) = 000111$ $\quad E(001) = 001001$

$E(010) = 010010$ $\quad E(011) = 011100$

$E(100) = 100100$ $\quad E(101) = 101010$

$E(110) = 110001$ $\quad E(111) = 111000$

9. For the following generator matrix, find how many errors the corresponding code can detect and h
many errors it can correct.

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

10. Write the complete coset decoding table for the code given by the generator matrix

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

From the table, decode the following received words.

001111, 101010, 011110

11. Find all the codewords of the code determined by the check matrix.

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

12. At a binary channel coding code words are constructed from two information symbols b_1 and b_2 a
three parity check symbols (c_1, c_2 and c_3). The generator matrix is as follows :

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

(*a*) Determine the code words of the code, their weights and their Hamming distances.

(*b*) Determine the parity check matrix H.

(*c*) Determine the syndrome for the following error patterns :

(01000), (00101), (10010), and (11111).

(*d*). A code word (11010) is generated, which is distorted with the following error pattern : (1001
Determine the received code word and which correction will be applied. Explain the decision.

13. A binary code is constructed by adding three parity check symbols to three information symb
(denoted by b_1, b_2 and b_3). For these code symbols

$$x_1 = b_1,$$
$$x_2 = b_2,$$
$$x_3 = b_3,$$
$$x_4 = b_2 + b_3,$$
$$x_5 = b_1 + b_3,$$
$$x_6 = b_1 + b_2.$$

(*a*) Determine the code words of this code.

(*b*) Determine the control or parity check matrix H.

(*c*) Determine the generator matrix G.

(*d*) Determine the Hamming distance of the code.

(*e*) How many errors can this code detect and how many errors can it correct?

14. A binary code has the following parity check matrix.

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

(*a*) Use the matrix to correct the following message :

1101100001100100001 00

(*b*) If the digits of any codeword are numbered x_1 to x_2, then the first line of the parity check matrix could be written as $x_1 + x_2 = 0$ Mod (2).

Write down three more equations based on the parity check matrix.

(*c*) Using your answer to part *b*, or by any other method, find the other five valid codewords in this code.

15. 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 $E: B^2 \to B^5$.

16. 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 $E: B^3 \to B^6$.

17. Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$, find the corresponding parity check matrix.

18. Given the generator matrix

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

Corresponding to the encoding function $E: B^2 \to B^6$, find the corresponding parity check matrix H and use to decode the received words

000100, 011101, 111010, 101011

and hence find the original message.

19. 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:

11110, 11101, 10101, 10011, and 01100.

20. 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:
000110, 000101, 110001 and 011111.

ANSWERS

1. (*a*) 2 (*b*) 3 (*c*) 4 **2.** (*a*) 4 (*b*) 5 (*c*) 4
3. 3, detect 2, correct 1 **4.** 2, detect 1, correct 0
5. 101, 000 **6.** 3, detect 2, correct 1
7. (*a*) correct (*b*) correct (*c*) incorrect
8. (*a*) The minimum distance is 2. The code detects all single errors but has no correction capability distance between code words is 3. The code can detect all errors of weight ≤ 2 and can correct all single errors.

   (*b*) The minimum
9. The code can detect one error. The code cannot correct every single error
10.

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

001111 is decoded as 001011; 101010 is decoded as 001011; 111110 is decoded as 011110.

11. 0000, 1110, 0101, 1011
12. (*a*) code words 10111 01101 11010 00000, weights 4 3 3 0

    Hamming distances are
$$\begin{matrix} 0 & 3 & 3 & 4 \\ 3 & 0 & 4 & 3 \\ 3 & 4 & 0 & 3 \\ 4 & 3 & 3 & 0 \end{matrix}$$

    (*b*) $\begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

    (*c*) $S = [\,1\ 0\ 1\,]^T$

    (*d*) The received code word is 01000. From the vectors given in *c*, 01000 has the smallest weight, this vector is then considered as the error vector. Hence, the supposed code word is 000000 which is incorrect in this case.
13. (*a*) There are 8 messages. Their corresponding code words are given as follows :

Message	*Code Words*
000	000 000
001	001 110

010	010 101
011	011 011
100	100 011
101	101 101
110	110 110
111	111 000

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

(*c*) The generator matrix G can be derived from $G.H^T = 0$. The result is

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

(*d*) The smallest Hamming distance between the code words is 3. Thus the Hamming distance d of the code is equal to 3.

(*e*) For Hamming distance $d = 3$, 2 errors can be detected and 1 error can be corrected.

14. (*a*) 11011000011011 0000000

(*b*) $x_2 + x_3 + x_4 = 0$

(*c*) 0000111, 0011100, 0011011, 1110000, 1110111

15. $e(00) = 00000$, $e(01) = 01011$, $e(10) = 10110$, $e(11) = 11101$

16. $e(000) = 000000$, $e(001) = 001011$, $e(010) = 010101$

$e(100) = 100110$, $e(011) = 011110$, $e(101) = 101101$

$e(110) = 110011$, $e(11) = 111000$

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

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

00, 01, 10, 11

19.

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	00001
10100	11010	00111	01001

01110, 11101, 10011, 10011, 11101 and 01110

Messages are 01, 11, 10, 10, 11 and 01

20.

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

100110, 001101, 110101 and 011110.

Messages: 100, 001, 110 and 011.