Algebric Structure

Module 7

Modulo systems

The modulo system is a way of performing arithmetic where numbers wrap around after reaching a certain value — called the modulus.

Addition modulo m **($+_m$)**

let m be a positive integer. For any two positive integers a and b

a $+_m$ b = a + b if a + b < m

a $+_m$ b = (a+b%m) r if a + b >= m where r is the remainder obtained by dividing (a+b) with m.

Ex. 14 $+_6$ 8 = 22 % 6 = 4

Ex. 9 $+_{12}$ 3= 12 % 12 = 0

Multiplication modulo p **(□$_p$)**

let p be a positive integer. For any two positive integers a and b

a x□$_p$ b = a x b if a x b < p

a x □$_p$ b = r if a x b □ p where r is the remainder obtained by dividing (axb) with p.

Ex. 3 x_5 4 = 2 , 5 x_5 4 = 0 , 2 x_5 2 = 4

Ex. : Show that the set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

Solution: The composition table of G is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

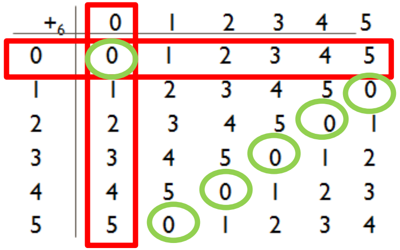
1. **Closure property**: Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Contd.,

2. Associativity: The binary operation $+_6$ is associative in G.

for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

$2 +_6 (3 +_6 4) = 2 +_6 1 = 3$



$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

3. Identity : 0 is the identity element.

4. . Inverse: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.

Hence, (G, $+_6$) is an abelian group.

Ex. : Show that the set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

Solution: The composition table of G is

$\square_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

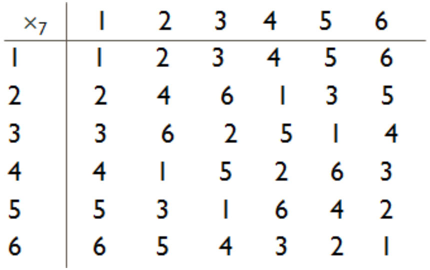
1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $\square_7$.

Contd.,

2. Associativity: The binary operation □$_7$ is associative in G.

for ex. (2 □$_7$ 3) □$_7$ 4 = 6 □$_7$ 4 = 3 and

2 □$_7$ (3 □$_7$ 4) = 2 □$_7$ 5 = 3



$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

3. Identity : 1 is the identity element.

4. . Inverse: From the composition table, we see that the inverse elements of 1, 2, 3, 4. 5 ,6 are 1, 4, 5, 2, 3, 6 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation □$_7$ is commutative.

Hence, (G, □$_7$) is an abelian group.

Ex. : Let Z4 i.e. G = {0, 1, 2, 3}
(i)Prepare its composition table with respect to ‘x4’
(ii) Is it a group ?

Let G = { 0, 1, 2, 3,}

(i) Composition table with respect to ‘X4’

X4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) (a) The set G is closed under the operation X4 because all elements belongs to composition table are belong to set G.

(b) Now check for associativity for any a, b, c ∈ G

X4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- (a X4 b) X4 C = a X4 (b X4 C)

Let a = 1, b = 2, c = 3

(1 X4 2) X4 3 = 1 X4 (2 X4 3)

2 X4 3 = 1 X4 2

2 = 2

'X4' is an associative operation.

(c) For any element a in set A

1 X4 a = a X4 1 = a that is

0 X4 1 = 1 X4 0 = 0

1 X4 1 = 1 X4 1 = 1

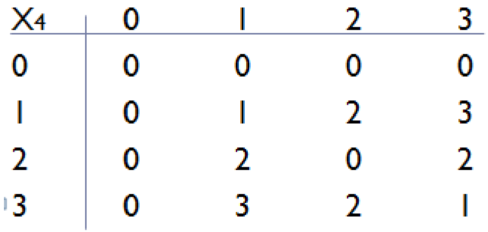
2 X4 1 = 1 X4 2 = 2

3 X4 1 = 1 X4 3 = 3

∴ '1' is identity element.

- Inverse of 1 is 1
- Inverse of 3 is 3
- 0 and 2 do not have inverse.

- SO, (G, ×4) is not a group.



X_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Order of an Element

- In mathematics, particularly in **group theory**,
  the **order of an element ‘a’** is the **smallest positive integer n** such that:

$$a^{n} = e \pmod{m}$$

- where
- e is the **identity element** (for multiplication mod m, $e = 1$; for addition mod m, $e = 0$)
- a^n means a multiplied by itself n times under the operation.
- m is the modulus.

- a^n =e , a*a*a… =e

For ex set (S,*) ,addition modulo 4 ($+_4$) ,

- 1^1= 1
- 1^2=1 $+_4$ 1 = 2
- 1^3= 1 $+_4$ 1$+_4$ +1 =3

Example

- The order of a in G is denoted by O(a).

Let G={1,-1,i,-i} be a multiplicative group. Find order of an every element.

Solution:

e=1(multiplication) and O(e) = 1

$1^1=1$ => O(1)=1

$(-1)^1=-1$, $(-1)^2=1$ => O(-1)=2

$(i)^1=i$, $(i)^2=-1$, $(i)^3=-i$,$(i)^4 =1$, => O(i)=4

$(-i)^1=-i$, $(-i)^2=-1$ ($(-i)^2=(-i)x(-i)= 1x\ i^2 =-1$),$(i)^3 =(-i^2\ x\ -i)=i$, $(-i)^4 =1$ => O(-i)=4

- $A=\{1,3,5,7\}$,X8

Solution:

$1^1=1$ => $O(1) =1$

$3^1=3$, $3^2=1$ =>$O(3)=2$

$5^1=5$, $5^2=1$ =>$O(5)=2$

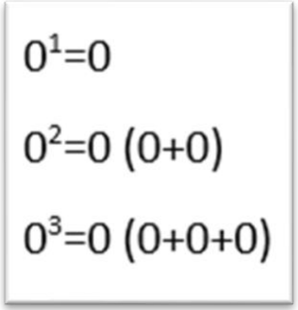
$7^1=5$, $7^2=6$ =>$O(7)=2$

Cyclic group

- A **cyclic group** is a group that can be generated by a single element.
- Every element of a cyclic group is a power of some specific element which is called a **generator**.
- **A group (G,*) is said o be cyclic group if it contains at least one generator element.**
- A cyclic group can be generated by a generator ‘g’, such that every other element of the group can be written as a power of the generator ‘g’.
- {g,g2,g3,…},*

Example

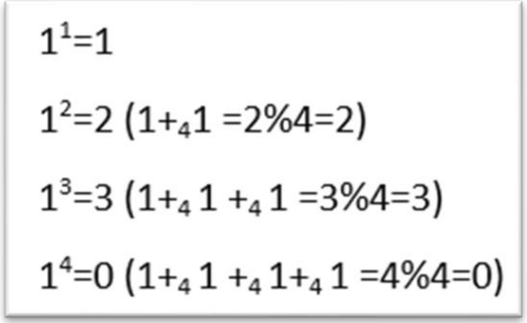
- $\{0,1,2,3\},+_4$



$0^1=0$

$0^2=0$ $(0+0)$

$0^3=0$ $(0+0+0)$

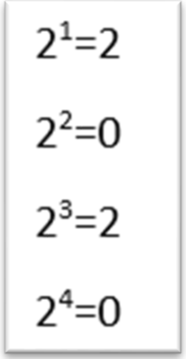


$1^1=1$

$1^2=2$ $(1+_4 1 = 2\%4=2)$

$1^3=3$ $(1+_4 1 +_4 1 = 3\%4=3)$

$1^4=0$ $(1+_4 1 +_4 1 +_4 1 = 4\%4=0)$

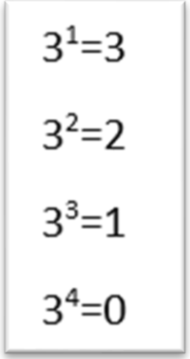


$2^1=2$

$2^2=0$

$2^3=2$

$2^4=0$



$3^1=3$

$3^2=2$

$3^3=1$

$3^4=0$

- $\{1,3,5,7\},x_8$

Subgroup

Let (A, *) be a group and B be a subset of A, (B, *) is said to be a **subgroup** of A if (B, *) is also a group by itself. Suppose we want to check whether (B, *) is a subgroup for a given subset B of A. We note that

1.We should test whether * is a closed operation on B.

2.* is known to be an associative operation.

3. The identity of (A, *) must be in B as the identity of (B, *)

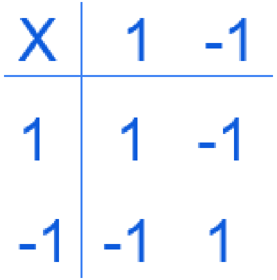
4.Since the inverse of every element in A is unique for every element b in B, we must check that its inverse is also in B.

Example

Let G={1,-1,i,-i} be a multiplicative group and H={1.-1} where H subset of G, then show that it is a subgroup of G.

Sol: composition table

1. Closure
2. Associative
3. Identity element
4. Inverse element:



X	1	-1
1	1	-1
-1	-1	1

1 =1

-1=-1

Coset

- In group theory, a coset is a subset formed by multiplying all elements of a subgroup by a fixed element of the group.

- Let (G, *) be a group and let H be a subgroup of G.
- If a ∈ G then we can form two types of cosets:

1.Left coset:

- aH={a * h | h∈H}

2.Right coset:

- Ha={h *a | h∈H}

Coset

Let H be a subgroup of a group (G, *). For a $\in$ G define

$$Ha \quad = \quad \{h * a \mid h \in H\}$$

then Ha is called a **right coset** of H in G.

$$aH \quad = \quad \{a * h \mid h \in H\}$$

is called a **left coset** of H in G.

a is called as the representative element of the coset aH or Ha.

If a $\in$ H,

then Ha = aH = H.

Hence the right cosets of H in G partition G into disjoint subsets.

Likewise the left cosets of H in G yield a portion of G into disjoint subsets.

Example

- Let G=(Z,+)={…-3,-2.-1,0,1,2,3,…} be a group.
- H=(3Z,+)={,,,-6,-3,0,3,6,…} be its subgroup.

Find all right cosets of H in G.

Sol: H *a , here *=+, hence H+a

H+0 ={…-6,-3,0,3,6,…}

H+1 ={..-5,-2,1,4,7,…}

H+2 ={..-4,-1,2,5,8,…}

H+3 ={,,,-3,0,3,6,…} =H

H+4={…-2,1,4,7,…}= H+1

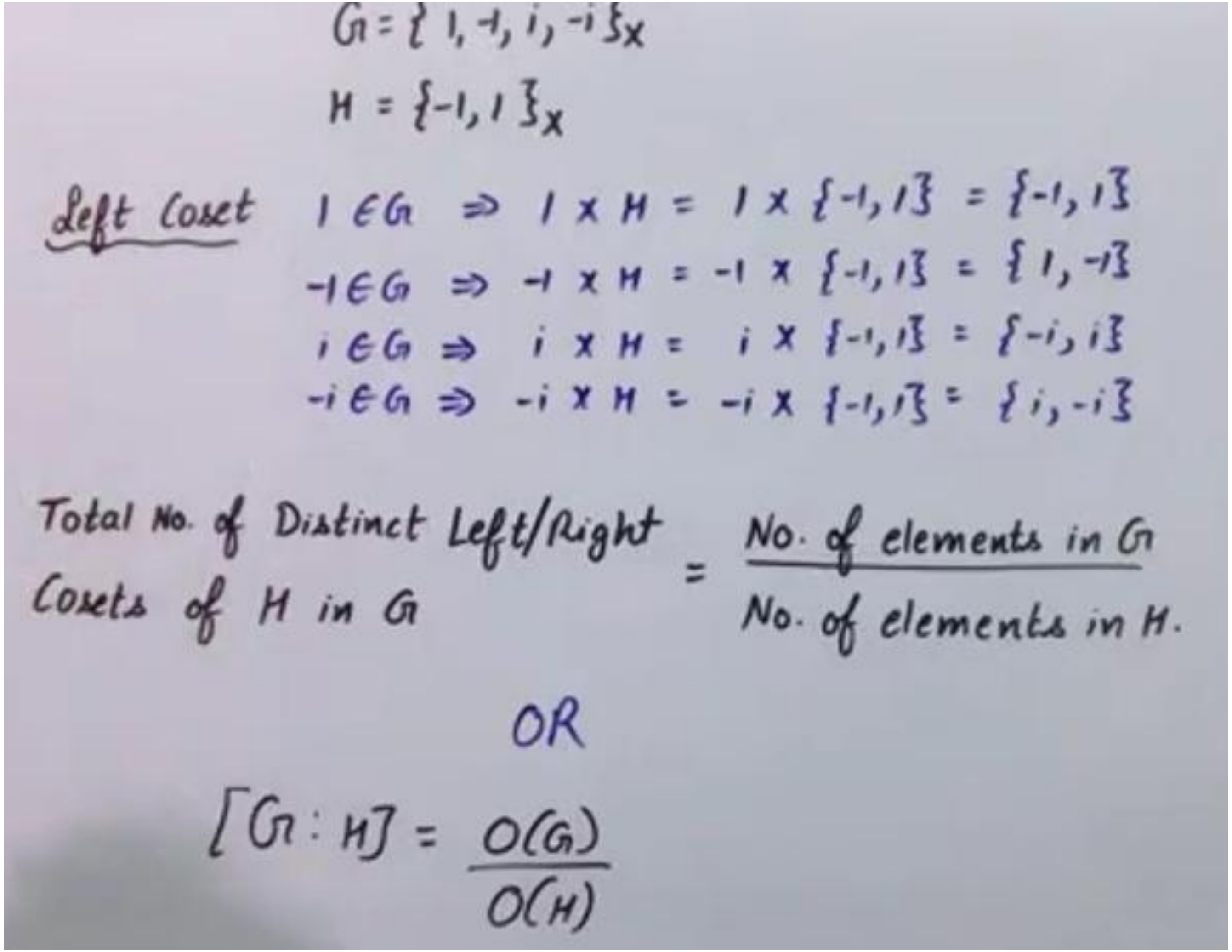
H+5 ={..,-1,2,5,8,…}=H+2

Right coset =3 , H, H+1, H+2

H+6 =H

H+7=H+1

H+8 =H+2



$G = \{1, -1, i, -i\}_{\times}$

$H = \{-1, 1\}_{\times}$

Left Coset

$1 \in G \Rightarrow 1 \times H = 1 \times \{-1, 1\} = \{-1, 1\}$

$-1 \in G \Rightarrow -1 \times H = -1 \times \{-1, 1\} = \{1, -1\}$

$i \in G \Rightarrow i \times H = i \times \{-1, 1\} = \{-i, i\}$

$-i \in G \Rightarrow -i \times H = -i \times \{-1, 1\} = \{i, -i\}$

Total No. of Distinct Left/Right Cosets of H in G = $\dfrac{\text{No. of elements in } G}{\text{No. of elements in } H.}$

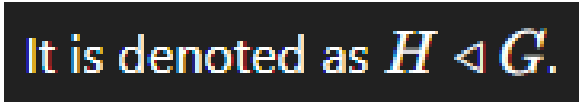
OR

$$[G : H] = \frac{O(G)}{O(H)}$$

Normal Subgroup

A subgroup H of G is said to be a **normal subgroup** of G if for every a ∈ G, aH = Ha.

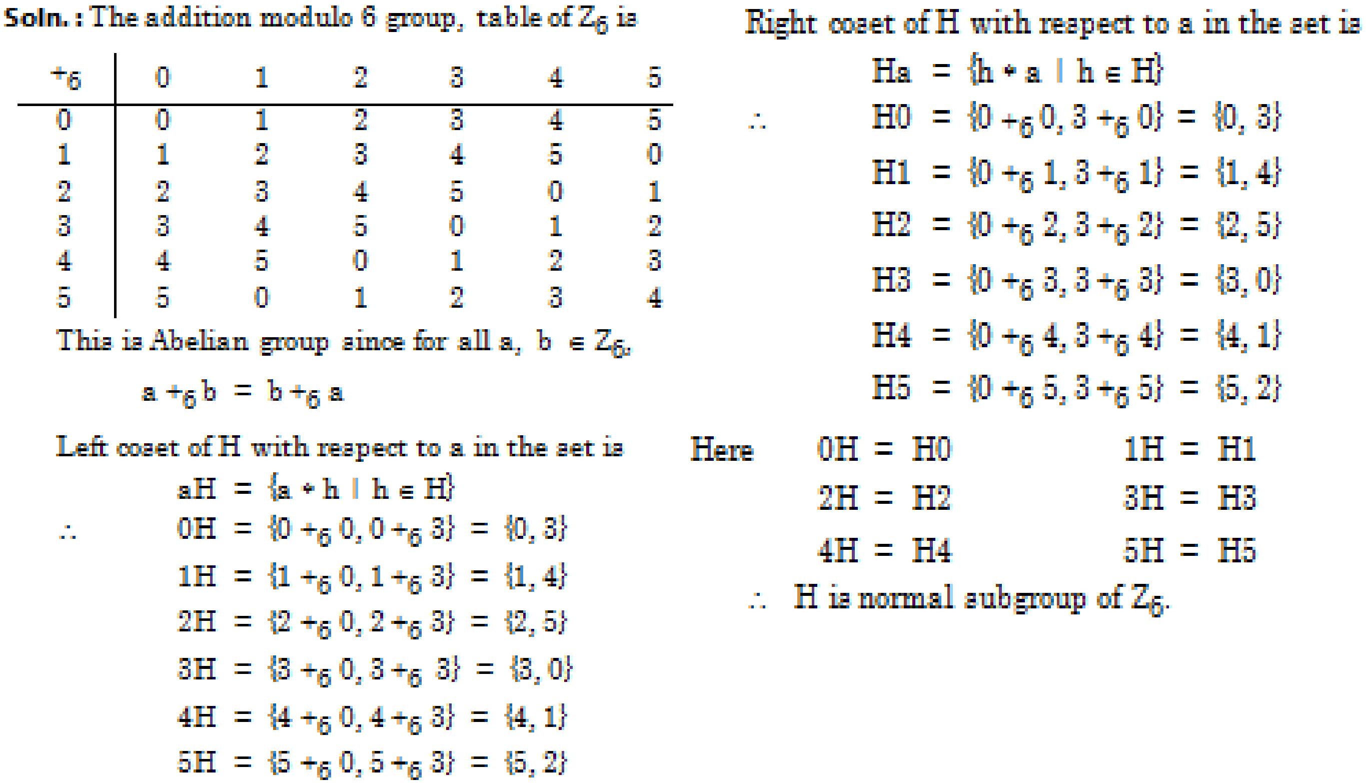
A subgroup of an Abelian group is normal.



It is denoted as $H \triangleleft G$.

- Another equivalent definition says:
- $H\ is\ normal\ in\ G \iff aHa^{-1} = H\ for\ all\ a \in G$

Ex. 1 : Let H = $\{[0]_6, [3]_6\}$. Find the left and right cosets in group Z_6. Is H a normal subgroup of group Z_6.



Soln. : The addition modulo 6 group, table of Z_6 is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

This is Abelian group since for all a, b $\in Z_6$,

$$a +_6 b = b +_6 a$$

Left coset of H with respect to a in the set is

$$aH = \{a * h \mid h \in H\}$$

$$\therefore \quad 0H = \{0 +_6 0, 0 +_6 3\} = \{0, 3\}$$

$$1H = \{1 +_6 0, 1 +_6 3\} = \{1, 4\}$$

$$2H = \{2 +_6 0, 2 +_6 3\} = \{2, 5\}$$

$$3H = \{3 +_6 0, 3 +_6 3\} = \{3, 0\}$$

$$4H = \{4 +_6 0, 4 +_6 3\} = \{4, 1\}$$

$$5H = \{5 +_6 0, 5 +_6 3\} = \{5, 2\}$$

Right coset of H with respect to a in the set is

$$Ha = \{h * a \mid h \in H\}$$

$$\therefore \quad H0 = \{0 +_6 0, 3 +_6 0\} = \{0, 3\}$$

$$H1 = \{0 +_6 1, 3 +_6 1\} = \{1, 4\}$$

$$H2 = \{0 +_6 2, 3 +_6 2\} = \{2, 5\}$$

$$H3 = \{0 +_6 3, 3 +_6 3\} = \{3, 0\}$$

$$H4 = \{0 +_6 4, 3 +_6 4\} = \{4, 1\}$$

$$H5 = \{0 +_6 5, 3 +_6 5\} = \{5, 2\}$$

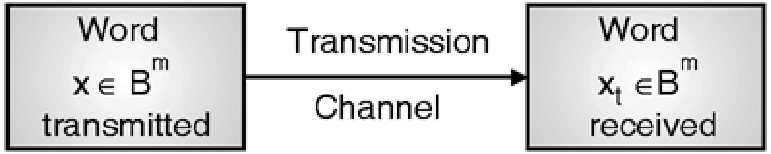
Here $0H = H0 \qquad 1H = H1$

$2H = H2 \qquad 3H = H3$

$4H = H4 \qquad 5H = H5$

$\therefore$ H is normal subgroup of Z_6.

Groups and Coding

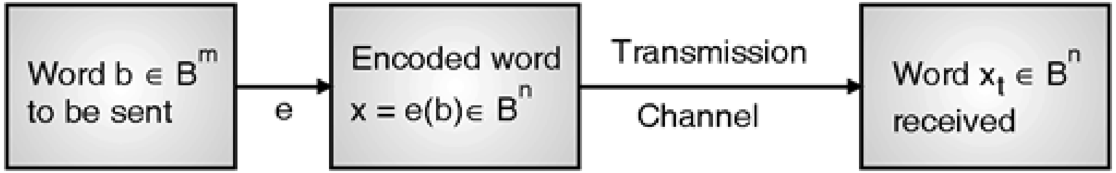


Word $x \in B^m$ transmitted

Transmission Channel

Word $x_t \in B^m$ received

- We first choose an integer n > m and a one to one function e : Bm -> Bn. The function e is called as (m, n) **encoding function**, and we view it as a means of representing every word in Bm as a word in Bn. If b ∊ Bm, then e (b) is called the **code word** representing b.



Word $b \in B^m$ to be sent

e

Encoded word $x = e(b) \in B^n$

Transmission Channel

Word $x_t \in B^n$ received

- We now transmit the code words by means of a transmission **channel**. Then each code word x = e(b) is received as the word xt in Bn.

Groups and Coding

- Encoding function e to be one to one so that different words in Bm will be assigned different code words.

- If the **transmission channel is noiseless**, then xt = x for all x in Bn. In this case x = e(b) is received for each b $\in$ Bm and since **e** is a known function, b may be identified.

- In general, errors in transmission do occur. We will say that the code word x = e(b) has been transmitted with k or fewer errors if x and xt differ in at least 1 but no more than k positions.

Weight

- If x ∈ Bn, then the number of 1's in x is called the **weight** of x and is denoted by |X|.

Find the weight of each of the following words in B5:

(a) x = 01000 (b) x = 11100

(c) x = 00000 (d) x = 11111

Soln. :

(a) x = 1

(b) x = 3

(c) x = 0

(d) x = 5

Hamming Distance

Let x and y be words in Bm. The **hamming distance** $d(x, y)$ between x and y is the weight, of $x \oplus y$. Thus the distance between $x = x1\ x2 \ldots xm$ and $y = y1\ y2 \ldots ym$ is the number of values of i such that $xi \neq yi$, that is, the number of positions in which x and y differ.

Ex. Find the distance between x and y.

(a) $x = 110110$, $y = 000101$ (b) $x = 001100$, $y = 010110$

(c) $x = 1100010$, $y = 1010011$ (d) $x = 0100100$, $y = 0011010$

Soln. :

(a) $x \oplus y = 110011$ so $|x \oplus y| = 4$

(b) $x \oplus y = 011010$ so $|x \oplus y| = 3$

(c) $x \oplus y = 0110001$ so $|x \oplus y| = 3$

(d) $x \oplus y = 0111110$ so $|x \oplus y| = 5$

Minimum Distance

The **minimum distance** of an encoding function e : Bm → Bn is the minimum of the distances between all distinct pairs of code words that is,

$$min\{d(e(x), e(y))|\ x, y \in B_m\}$$

Let x = (10001), y = (01000),

and z = (10101)

The distances are d (x, y) = 3, d (x, z) = 1, and d (y, z) = 4. Therefore, the minimum distance between the words x, y, z is 1.

Minimum distance is also called as '*Hamming distance*'.

With the help of weight and minimum distance as described above, a combination of errors can be detected and corrected.

Theorems

The minimum weight of all non zero words in a group code is equal to its minimum distance

A code can **detect** all combinations of k or fewer iff the minimum distance between any two code words is at least **k + 1**

A code can **correct** all combinations of k or fewer errors iff the minimum distance between any two code words is at least **2 k + 1**

Ex. 1 : Consider the (2, 4) encoding function. How many errors will be detect ?

e (00) = 0000   e (10) = 0110
e (01) = 1011   e (11) = 1100

Soln: We first find distances between pairs of code words

d (0000, 0110) = 2

d (0000, 1011) = 3

d (0000, 1100) = 2

d (0110, 1011) = 3

d (0110, 1100) = 2

d (1011, 1100) = 3

A code can **detect** all combinations of k or fewer iff the minimum distance between any two code words is at least **k + 1**

Minimum distance : 2

K+1=2, so k=1

The code will detect 1 or fewer errors

Ex. 2 : Consider the encoding function e : B2 -> B6 defined as follows :

e (00) = 001000 e (01) = 010100
e (10) = 100010 e (11) = 110001

How many errors it can detect and correct.

Soln. : We first find the distances between pairs of code words.

d (001000, 010100) = 3

d (001000, 100010) = 3

d (001000, 110001) = 4

d (010100, 100010) = 4

d (010100, 110001) = 3

d (100010, 110001) = 3

The code will detect k or fewer errors if and only if its minimum distance is at least k + 1. Since the minimum distance is 3, we have 3 ≥ k + 1 or k ≤ 2. The code will detect two or fewer errors.

The code will correct k or fewer errors if and only if its minimum distance is at least 2 k + 1. Since the minimum distance is 3 we have 3 ≥ 2 k + 1 or k ≤ 1. The code will correct 1 or fewer errors.

Group Codes

- An (m,n) encoding function $e: B^m \rightarrow B^n$ is called a group code

if e(B^m) = {e(b)|b ∈ B^m}=Ran (e) is a subgroup of B^n

Recall from the definition of subgroup that N is a subgroup of B^n if ;

(a) the identity of B^n is in N.

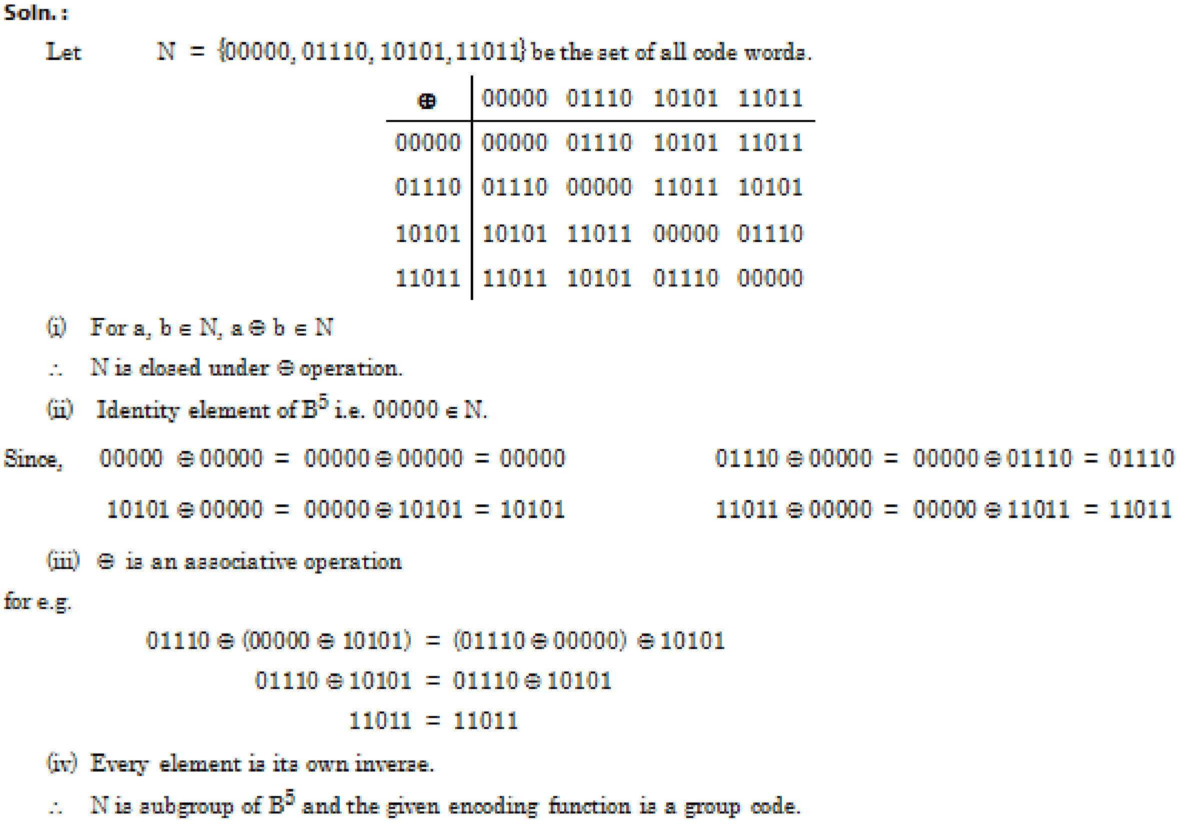
(b) if x and y belong to N, then x $\oplus$ y ∈ N and

(c) if x is in N, then its inverse is in N.

Property (c) need not be checked, since every element in B^n is its own inverse. Moreover, since B^n is Abelian, every subgroup of B^n is a normal subgroup.

$\oplus$

Ex. 1 : Show that the (2, 5) encoding function e : B2 → B5 defined by e (00) = 00000 e (10) = 10101 e (01) = 01110 e (11) = 11011 is a group code.



Soln. :

Let $N = \{00000, 01110, 10101, 11011\}$ be the set of all code words.

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

(i) For $a, b \in N$, $a \oplus b \in N$

∴ N is closed under $\oplus$ operation.

(ii) Identity element of B^5 i.e. $00000 \in N$.

Since, $00000 \oplus 00000 = 00000 \oplus 00000 = 00000$ $\quad$ $01110 \oplus 00000 = 00000 \oplus 01110 = 01110$

$10101 \oplus 00000 = 00000 \oplus 10101 = 10101$ $\quad$ $11011 \oplus 00000 = 00000 \oplus 11011 = 11011$

(iii) $\oplus$ is an associative operation

for e.g.

$$\begin{aligned} 01110 \oplus (00000 \oplus 10101) &= (01110 \oplus 00000) \oplus 10101 \\ 01110 \oplus 10101 &= 01110 \oplus 10101 \\ 11011 &= 11011 \end{aligned}$$

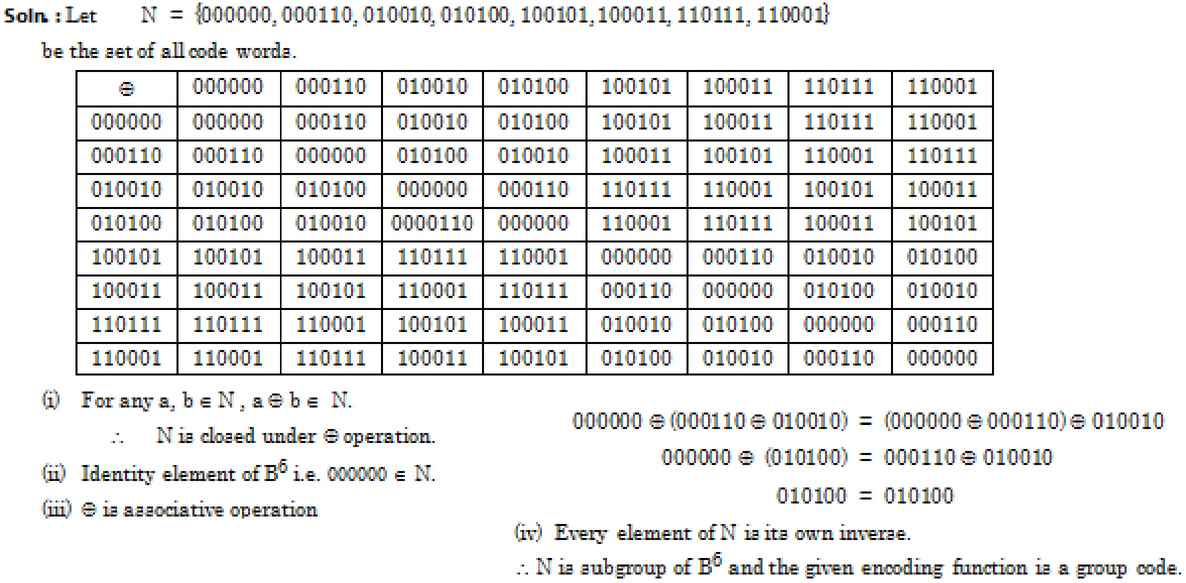
(iv) Every element is its own inverse.

∴ N is subgroup of B^5 and the given encoding function is a group code.

Example 2 : Consider (3, 6) encoding function 'e' as follows.

e (000) = 000000 e (001) = 000110 e (010) = 010010
e (011) = 010100
e (100) = 100101 e (101) = 100011 e (110) = 110111
e (111) = 110001

Show that the encoding function e is a group code.



Soln. : Let N = {000000, 000110, 010010, 010100, 100101, 100011, 110111, 110001}

be the set of all code words.

⊕	000000	000110	010010	010100	100101	100011	110111	110001
000000	000000	000110	010010	010100	100101	100011	110111	110001
000110	000110	000000	010100	010010	100011	100101	110001	110111
010010	010010	010100	000000	000110	110111	110001	100101	100011
010100	010100	010010	0000110	000000	110001	110111	100011	100101
100101	100101	100011	110111	110001	000000	000110	010010	010100
100011	100011	100101	110001	110111	000110	000000	010100	010010
110111	110111	110001	100101	100011	010010	010100	000000	000110
110001	110001	110111	100011	100101	010100	010010	000110	000000

(i) For any a, b ∈ N , a ⊕ b ∈ N.

∴ N is closed under ⊕ operation.

(ii) Identity element of B^6 i.e. 000000 ∈ N.

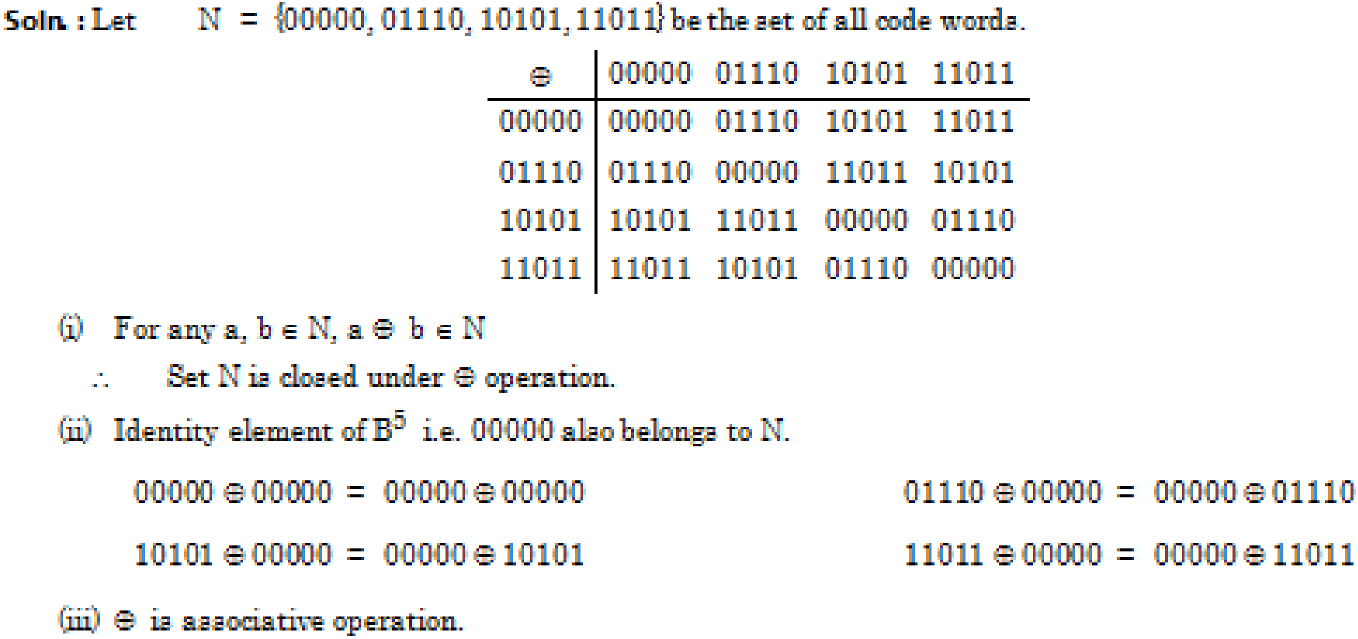
(iii) ⊕ is associative operation

$$000000 \oplus (000110 \oplus 010010) = (000000 \oplus 000110) \oplus 010010$$
$$000000 \oplus (010100) = 000110 \oplus 010010$$
$$010100 = 010100$$

(iv) Every element of N is its own inverse.

∴ N is subgroup of B^6 and the given encoding function is a group code.

Ex. 3 : Show that the (2, 5) encoding function e : B2 ® B5 defined by
e (00) = 00000 e (01) = 01110 e (10) = 10101 e
(11) = 11011
is a group code. How many errors will it detect and correct?



Soln. : Let $N = \{00000, 01110, 10101, 11011\}$ be the set of all code words.

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

(i) For any $a, b \in N$, $a \oplus b \in N$

$\therefore$ Set N is closed under $\oplus$ operation.

(ii) Identity element of B^5 i.e. 00000 also belongs to N.

$00000 \oplus 00000 = 00000 \oplus 00000$ $\qquad$ $01110 \oplus 00000 = 00000 \oplus 01110$

$10101 \oplus 00000 = 00000 \oplus 10101$ $\qquad$ $11011 \oplus 00000 = 00000 \oplus 11011$

(iii) $\oplus$ is associative operation.

(iv) Each element of N is its own inverse.

$00000 \oplus 00000 = 00000 \oplus 00000 = 00000$ $\qquad$ $01110 \oplus 01110 = 01110 \oplus 01110 = 00000$

$10101 \oplus 10101 = 10101 \oplus 10101 = 00000$ $\qquad$ $11011 \oplus 11011 = 11011 \oplus 11011 = 00000$

$\therefore$ N is subgroup of B^5 and the given encoding function is a group code.

$d(00000, 01110) = 3$ $\qquad$ $d(00000, 10101) = 3$

$d(00000, 11011) = 4$ $\qquad$ $d(01110, 10101) = 4$

$d(01110, 11011) = 3$ $\qquad$ $d(10101, 11011) = 3$

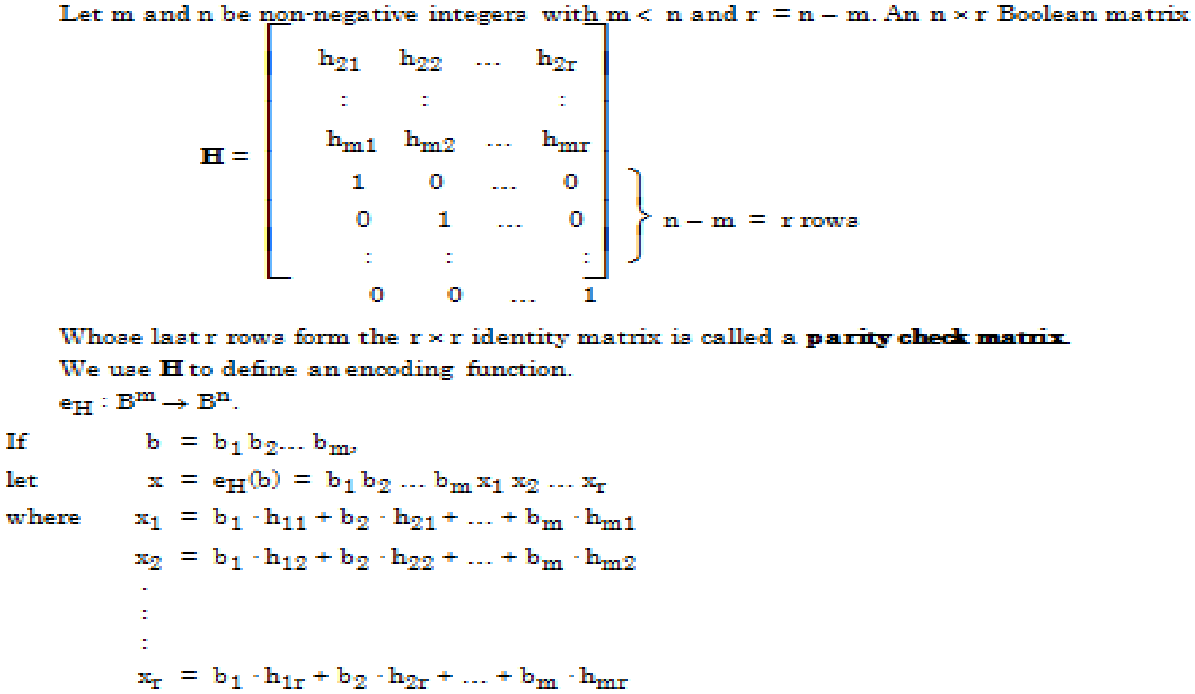
$\therefore$ Minimum distance is 3.

The code will detect k or fewer errors if and only if its minimum distance is atleast $k + 1$. Since the minimum distance is 3, we have $3 \geq k + 1$ or $k \leq 2$. The code will detect 2 or fewer errors.

The code will correct k or fewer errors if and only if its minimum distance is atleast $2k + 1$. Since the minimum distance is 3 we have $3 \geq 2k + 1$ or $k \leq 1$. So the code will correct 1 or fewer errors.

Parity check matrix

A parity check matrix, usually written as H, is a matrix that helps us check whether a received codeword has an error or not.



Let m and n be non-negative integers with $m < n$ and $r = n - m$. An $n \times r$ Boolean matrix

$$\mathbf{H} = \begin{bmatrix} h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} n - m = r \text{ rows}$$

Whose last r rows form the $r \times r$ identity matrix is called a **parity check matrix**.

We use **H** to define an encoding function.

$e_H : B^m \to B^n$.

If $\quad b = b_1 b_2 \ldots b_m,$

let $\quad x = e_H(b) = b_1 b_2 \ldots b_m x_1 x_2 \ldots x_r$

where

$$x_1 = b_1 \cdot h_{11} + b_2 \cdot h_{21} + \ldots + b_m \cdot h_{m1}$$

$$x_2 = b_1 \cdot h_{12} + b_2 \cdot h_{22} + \ldots + b_m \cdot h_{m2}$$

$$\vdots$$

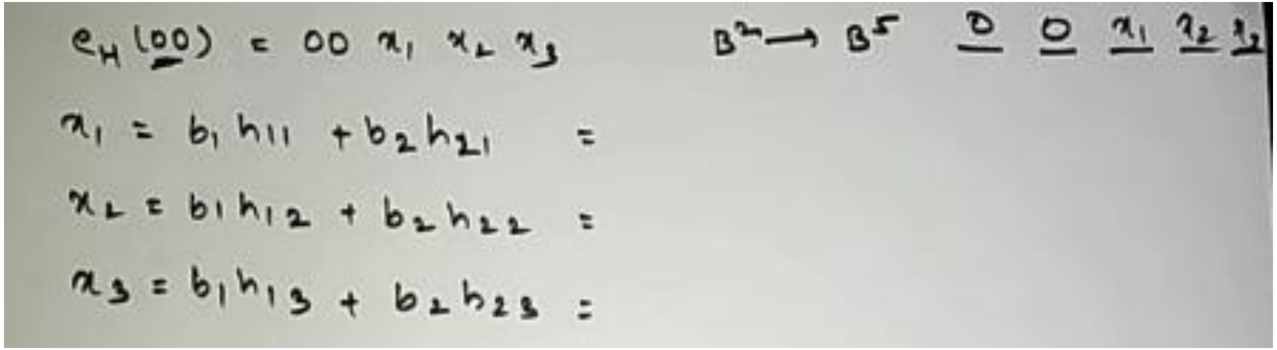
$$x_r = b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \ldots + b_m \cdot h_{mr}$$

snistforum.com

Consider the parity check matrix given by H;

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

Determine the group code $e_H : B^2$□ B^5



$e_H(\underline{00}) = 00\ x_1\ x_2\ x_3$ $\quad B^2 \longrightarrow B^5 \quad \underline{0}\ \underline{0}\ \underline{x_1}\ \underline{x_2}\ \underline{x_2}$

$x_1 = b_1 h_{11} + b_2 h_{21} \quad =$

$x_2 = b_1 h_{12} + b_2 h_{22} \quad =$

$x_3 = b_1 h_{13} + b_2 h_{23} \quad =$

Soln: $B^2 = \{00,01,10,11\}$

Then e(00) = 00 $x_1\ x_2\ x_3 = B^5$

$x_1 = 0 .1 + 0. 0 = 0$

$x_2 = 0 .1 + 0. 1 = 0$

$X_3 = 0 .0 + 0. 1 = 0$

e (00) = 00000

Next e(01) = 01 $x_1\ x_2\ x_3 = B^5$

$x_1 = 0 .1 + 1. 0 = 0$

$x_2 = 0 .1 + 1. 1 = 1$

$X_3 = 0 .0 + 1. 1 = 1$

e (01) = 01011

Next e(10) = 10 x_1 x_2 x_3 = B ^{5}

x_1 = 1 .**1** + 0. **0** **=** 1

x_2 = 1 .**1** + 0. **1** **=** 1

X_3 = 1 .**0** + 0. **1** **=** 0

e (10) = 10110

Next e(11) = 11 x_1 x_2 x_3 = B ^{5}

x_1 = 1 .**1** + 1. **0** **=** 1

x_2 = 1 .**1** + 1. **1** **=** 0

X_3 = 1 .**0** + 1. **1** **=** 1

e (11) = 11101

e_H : B^2□ B ^{5} is as above for e (00) , e (01), e (10) ,e (11)

Problem 1

Consider the parity check matrix given by H;

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

Determine the group code e_H : B^2□ B^5

Soln: B^2 = {00,01,10,11}

Then e(00) = 00 x_1 x_2 x_3 = B
5

x_1 = 0 .**0** + 0. **0** **=** 0

x_2 = 0 .**1** + 0. **1** **=** 0

X_3 = 0 .**1** + 0. **1** **=** 0

e (00) = 00000

Next e(01) = 01 x_1 x_2 x_3 = B^5

x_1 = 0 .**0** + 1. **0** **=** 0

x_2 = 0 .**1** + 1. **1** **=** 1

X_3 = 0 .**1** + 1. **1** **=** 1

e (01) = 01011

Next e(10) = 10 x_1 x_2 x_3 = B^5

x_1 = 1 .**0** + 0. **0** **=** 0

x_2 = 1 .**1** + 0. **1** **=** 1

X_3 = 1 .**1** + 0. **1** **=** 1

e (10) = 10011

Next e(11) = 11 x_1 x_2 x_3 = B^5

x_1 = 1 .**0** + 1. **0** **=** 0

x_2 = 1 .**1** + 1. **1** **=** 0

X_3 = 1 .**1** + 1. **1** **=** 0

e (11) = 11000

e (00) = 00000

e (01) = 01011

e (00) = 10011

e (00) = 11000

Problem 2

Consider the parity check matrix given by H;

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

Determine the group code e_H : B^3□ B^6

e (000) = 000000

e (001) = 001111

e (010) = 010011

e (011) = 011100

e (100) = 100100

e (101) = 101011

e (110) = 110111

e (111) = 111000