Module 2: Algebraic Structures

Semigroups and Monoids - Groups - Subgroups - Lagrange's Theorem - Homomorphism - Properties - Group Codes.

Binary Operation

Binary Operation

A binary operation $*$ on a set G is a function $* : G \times G \to G$
We denote it as $a * b$ for any $a, b \in G$

- A binary operation $*$ on a set G is associative if for all $a, b, c \in G$,

$$a * (b * c) = (a * b) * c$$

- If $*$ is a binary operation on a set G , then $*$ is commutative if for all $a, b \in G$

$$a * b = b * a$$

Example

- $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ respectively)
- $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ respectively)
- $-$(usual subtraction) is a noncommutative binary operation on $\mathbb{Z}$
- $-$ is not a binary operation on $\mathbb{Z}^+$ (nor $\mathbb{Q}^+, \mathbb{R}^+$) because for $a, b \in \mathbb{Z}^+$ with $a < b, a - b \notin \mathbb{Z}^+$, that is, $-$ does not map $\mathbb{Z}^+ \times \mathbb{Z}^+$ into $\mathbb{Z}^+$

Groups

A group $(G, *)$ is a set G together with a binary operation $*$ such that

- Associative: $(a * b) * c = a * (b * c) \qquad \forall a, b, c \in G$
- Identity: $\exists e \in G$ such that $a * e = a = e * a \quad \forall a \in G$
- Inverse: $\forall a \in G, \quad \exists b \in G$ such that $a * b = e = b * a$

- $(\mathbb{Z}, +)$ is a group - associativity holds, identity is 0, inverse for any a is $-a$
- $(\mathbb{Z}, -)$ is not a group (Check associative property)
- $(\mathbb{Z}, x)$ is not a group (Why?) Inverse doesnot exists
- $(\mathbb{Q}, +)$ is a group

Semigroup and Monoid

- A semigroup is an ordered pair $(S, *)$ where S is a non empty set and $*$ is a binary operation which is associative
- A monoid is a semigroup with an identity element
- The group $(G, *)$ is called abelian (or commutative) if $a * b = b * a$ for all $a, b \in G$.

Example

- The set of natural numbers with $+$ as the binary operation is a semigroup. That is, $\{\mathbb{N}, +\}$
- Let X be any set. Then $\rho(X)$, the power set of X is also a semigroup under the operation of taking union of two sets. (verify!)

Example

- The set of integers, rational numbers, real numbers and the complex numbers are monoids under addition.
- $\{\mathbb{Z}^+, .\}$, the set of positive integers forms a monoid under multiplication.

Order of a Group

Order of a group G is the number of elements of G, denoted by $|G|$. If the order of G is finite, then G is a finite group. Otherwise it is an infinite group

Infinite Group

Examples

1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{C}$ forms an abelian group with usual addition. None of these is a group under usual multiplication because 0 has no multiplicative inverse.
2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ (nonzero elements of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, respectively) are abelian groups under usual multiplication
3. The set $\mathbb{Q}^+$ is a group under the operation $*$ defined by $a * b = \frac{1}{2}ab$ for $a, b \in \mathbb{Q}^+$

Problems

1. Check whether the following is a group or not under the stated binary operation. If so, determine the identity and inverse.

(i) $\{-1, 1\}$ under multiplication

(ii) $\{-1, 1\}$ under addition

(iii) $\{-1, 0, 1\}$ under addition

(iv) $\{10n : n \in \mathbb{Z}\}$ under addition

2. If $*$ is the binary operation on the set R of real numbers defined by $a * b = a + b + 2ab$ then check whether $(R, *)$ is an abelian group.

3. If $*$ is the binary operation on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a, b) * (x, y) = (ax, ay + b)$ then check whether $(R, *)$ is an abelian group.

1. Check whether the following is a group or not under the stated binary operation. If so, determine the identity and inverse.

(i) $\{-1, 1\}$ under multiplication

(ii) $\{-1, 1\}$ under addition

(iii) $\{-1, 0, 1\}$ under addition

(iv) $\{10n : n \in \mathbb{Z}\}$ under addition

2. If $*$ is the binary operation on the set R of real numbers defined by $a * b = a + b + 2ab$ then check whether $(R, *)$ is an abelian group.

3. If $*$ is the binary operation on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a, b) * (x, y) = (ax, ay + b)$ then check whether $(S, *)$ is an abelian group.

Properties of Group

(1) Identity element is unique.

(2) Inverse of each element is unique.

(3) Cancellation laws are true.

Eg: (i) $a * b = a * c \Rightarrow b = c$ } Left cancellation law.

(ii) $b * a = c * a \Rightarrow b = c$ } Right cancellation law.

(4) $(a * b)^{-1} = b^{-1} * a^{-1}$, $\forall\ a, b \in G$.

Modular Addition

Modular addition

For any $n \in \mathbb{N}$, let $(a+b)$ mod n or $a +_n b$ is denoted by the remainder when $a+b$ is divided by n.Define $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$.

Example

Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Now, we construct a cayley table.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$1 + 2(mod4) = 3$

$2 + 2(mod4) = 0$

$2 + 3(mod4) = 1$

$3 + 3(mod4) = 2$

Example

- $\mathbb{Z}_4$ is closed under the addition modulo 4 operation
- Associativity holds; Identity is 0
- Inverse of $0, 1, 2$ and 3 are $0, 3, 2$ and 1 respectively.
- Hence, $(\mathbb{Z}_4, +_4)$ is a group

② $(Z_5, +_5)$ ⇒ Abelian group? ✓

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$Z_5 = \{0, 1, 2, 3, 4\}$

$e = 0$

$Inv(2) = 3$

$Inv(4) = 1$

⇒ $(Z_n, +_n)$ is an abelian group.

Modular Multiplication

Modular multiplication

For any $n \in \mathbb{N}$, let $(a \times b) \bmod n$ or $a \times_n b$ is denoted by the remainder when $a \times b$ is divided by n. Define $\mathbb{Z}_n = \{0, 1, 2, \ldots, (n-1)\}$.

Example

Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- Closure, Associativity holds; Identity is 1; but inverse doesn't exist for 0
- $(\mathbb{Z}_4, \times_4)$ is not a group
- Let $\mathbb{Z}_4^* = \mathbb{Z}_4 \setminus \{0\} = \{1, 2, 3\}$. Check whether $\mathbb{Z}_4^*$ is a group under $\times_4$

- $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ is a group under modular addition for any $n \in \mathbb{N}$. The order of the group $(\mathbb{Z}_n, +_n)$ is n
- $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, 3, \ldots, p-1\}$ for prime p is a group under modular muliplication. The order of this group is $p-1$

Try!!!

Check whether $\mathbb{Z}_8 \setminus \{0\}$ is a group under multiplication modulo 8 or not.

Permutation Group

Permutation

A permutation of a set S is a one to one function π of a set S onto itself. If $\pi(1) = 1\ \pi(2) = 2\ \pi(3) = 3$, then we get the permutation as

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Let $S = \{1,2,3\}$. Then the permutation set is $S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

*	p_1	p_2	p_3	p_4	p_5	p_6
p_1						
p_2						
p_3						
p_4						
p_5						
p_6						

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

*	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3					
p_4	p_4					
p_5	p_5					
p_6	p_6					

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$p_2 * p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = p_3$$

*	p_1	p_2	p_3	p_4	p_5	p_6
p_1	$p_1 = e$	p_2	p_3	p_4	p_5	p_6
p_2	p_2	$p_1 = e$	p_4	p_3	p_6	p_5
p_3	p_3	p_6	p_5	p_2	$p_1 = e$	p_4
p_4	p_4	p_5	p_6	$p_1 = e$	p_2	p_3
p_5	p_5	p_4	$p_1 = e$	p_6	p_3	p_2
p_6	p_6	p_3	p_2	p_5	p_4	$p_1 = e$

$S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$

Note: Here p_1 is the identity element e.

(i) Closure: $a * b \in S_3$, $\forall a, b \in S_3$. ✓

(ii) Associative: $a * (b * c) = (a * b) * c$, $\forall a, b, c \in S_3$.

Eg: $(p_2 * p_4) * p_6 = p_3 * p_6 = p_4 = R.H.S$

$p_2 * (p_4 * p_6) = p_2 * p_3 = p_4 = L.H.S$

$*$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3	p_6	p_5	p_2	p_1	p_4
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_1	p_6	p_3	p_2
p_6	p_6	p_3	p_2	p_5	p_4	p_1

(iii) Identity: $a * e = a$, $\forall a \in S_3$.

Here, $\boxed{e = p_1}$

(iv) Inverse: $a * a^{-1} = e$, $\forall a, a^{-1} \in S_3$.

$(p_1)^{-1} = p_1$; $(p_2)^{-1} = p_2$; $(p_3)^{-1} = p_5$; $(p_4)^{-1} = p_4$.

$(p_5)^{-1} = p_3$ and $(p_6)^{-1} = p_6$. $\therefore$ Inverse exists.

Problem: If the permutations of the elements of {1,2,3,4,5} are given by $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{bmatrix}$, then find $\alpha\beta, \alpha^2$ and solve the equation $\alpha X = \beta$.

Sol:-

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix} \qquad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{bmatrix}$$

Now,

$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{bmatrix}$$

$$\alpha^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$$

To find α^{-1}:

(1) Interchange the rows of α.

(2) Rearrange the elements of the first row.

$$\alpha X = \beta \Rightarrow \boxed{X = \alpha^{-1}\beta} \quad \text{— (1)}$$

Now, $\alpha^{-1} = \begin{bmatrix} 2 & 3 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$ * Interchanged the rows of α.

$$\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}$$

Rearranged the elements of the first row

Now,

$$(1) \Rightarrow X = \alpha^{-1}\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{bmatrix}$$

$$X = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{bmatrix}.$$

Homomorphism

Let $(G, *)$ and $(H, \diamond)$ be groups. Then $\phi : G \to H$ is a group homomorphism if $\forall x, y \in G$ such that

$$\phi(x * y) = \phi(x) \diamond \phi(y)$$

Problem

1. If $\phi : (\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ defined by $\phi(x) = \exp(x)$, then prove that ϕ is a group homomorphism.

Solution: Consider $x, y \in \mathbb{R}$. Since $\mathbb{R}$ is a group, $x + y \in \mathbb{R}$. Then

$\phi(x + y) = \exp(x + y)$ (by definition)

$= \exp(x) \exp(y)$

$= \phi(x) \times \phi(y)$

Hence ϕ is a homomorphism.

Problems

2. $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ defined by $f(x) = 2x$ is a homomorphism.

3. $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined by $\phi(x) = cx$ for $c \in \mathbb{R}$. ϕ is a homomorphism.

4. $f : (\mathbb{Z}^2, +) \to (\mathbb{R}, \times)$ defined by $f(m, n) = a^m b^n$ where $a, b \in \mathbb{R}$. Then f is a homomorphism.

Subgroup

Subgroup

Let $(G, *)$ be a group and $H \neq \emptyset \subseteq G$ such that

- for $a, b \in H, a * b \in H$
- $e \in H$, where e is the identity of G
- for any $a \in H$, $a^{-1} \in H$

then $(H, *)$ is called a subgroup of $(G, *)$

$(\{e\}, *), (G, *)$ are trivial subgroups of $(G, *)$. All other subgroups are termed as nontrivial or proper.

Example

(i) $H = \{1, -1\}$ is a subgroup of $G = \{1, -1, i, -i\}$ under usual multiplication

(ii) $(\mathbb{Z}, +)$ is subgroup of $(\mathbb{Q}, +)$ which is a subgroup of $(\mathbb{R}, +)$ which is a subgroup of $(\mathbb{C}, +)$

Theorem

A non empty subset H of a group $(G, *)$ is a subgroup if and only if for $a, b \in H$, $a * b^{-1} \in H$

Lagrange's Theorem

The order of a subgroup H of a finte group G is a divisor of the order of the group G.

Example

(i) $H = \{1, -1\}$ is a subgroup of $G = \{1, -1, i, -i\}$ under usual multiplication

Example

If $|G| = 14$, then the only possible orders for a subgroup are 1,2,7 and 14.

Cosets

Let $(G, *)$ be a group and $(H, *)$ be a subgroup of G.
For $g \in G$, the left H-coset is

$$g * H = \{g * h : \ h \in H\}$$

The right H-coset is

$$H * g = \{h * g : \ h \in H\}$$

Example

Consider the subgroup $(2\mathbb{Z}, +)$ of the group $(\mathbb{Z}, +)$.

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$$

$$2\mathbb{Z} = \{\ldots, -2, 0, 2, \ldots\}$$

The left cosets of $2\mathbb{Z}$ in $\mathbb{Z}$ are

$$0 + 2\mathbb{Z} = \{\ldots, -2, 0, 2, \ldots\}$$

$$1 + 2\mathbb{Z} = \{\ldots, -1, 1, 3, \ldots\}$$

Note that $\mathbb{Z} = (0 + 2\mathbb{Z}) \cup (1 + 2\mathbb{Z})$

Problem 1

List the cosets of the subgroup $\{-1, 1\}$ of $\{1, -1, i, -i\}$ under usual multiplication.

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

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

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

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

are the left cosets of $\{1, -1\}$

Note that $\{1, -1, i, -i\} = (1 \times \{1, -1\}) \cup (i \times \{1, -1\})$

Problems

2. Find all the left cosets of $H = \{0, 3\}$ of $(\mathbb{Z}_6, +_6)$

3. List the elements of all left cosets of $< 9 >$ in U_{28} with multiplication modulo 28.

4. If G is the additive group of integers and H is a subgroup of G obtained by multiplying each element of G by 3, Find the distinct of H in G

Units Modulo n

THEOREM

For a given integer $n > 1$, let m be an integer such that $1 \leq m < n$ and $\gcd(n, m) = 1$. Then the set of all such integers m forms a group, denoted $U(n)$, called the units mod n.

Units Modulo n

One more example: $U(10)$

$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\gcd(10, m) = 1$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Lagrange's Theorem

The order of a subgroup H of a finte group G is a divisor of the order of the group G.

The number of different right cosets of H in G is called the index of H in G and is denoted by $[G : H]$.
Note that $[G : H] = \frac{|G|}{|H|}$

Properties of Cosets

- Any two left cosets have same number of elements
- $g_1 * H$ and $g_2 * H$ are either equal or disjoint for $g_1, g_2 \in G$
- $g \in g * H$ for any $g \in H$
- A coset $g * H$ is a subgroup of G iff $g \in H$

(*) Index of H in G = No. of distinct cosets

Kernal of Homomorphism:

If $f: G \to G'$ is a group homomorphism from $(G, *)$ to (G', Δ), then the set of elements of G, which are mapped into e', the identity element of G', is called the *kernel of the homomorphism* f and denoted by $\ker(f)$.

Problem 1:

If G is the multiplicative group of all $(n \times n)$ non-singular matrices whose elements are real numbers and G' is the multiplicative group of all non-zero real numbers, show that the mapping $f: G \to G'$, where $f(A) = |A|$, for all $A \in G$ is a homomorphism. Find also the kernel of f.

Solution: Let $A, B \in G$

Now, $f(AB) = |AB|$

$= |A| \cdot |B|$

$= f(A) \cdot f(B)$

$\therefore$ f is a homomorphism from G to G'.

The identity of $G' = 1$

$\therefore$ The elements of G whose images under f is 1 from the kernal of f.

Thus, the set of all matrices whose determinant values are equal to 1 from the kernal of f.

Question 2:

Let R and C are additive groups of real and complex numbers respectively and if the mapping $f: C \to R$ is defined by $f(x + iy) = x$, show that f is a homomorphism. Find also the kernel of f.

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. **1**

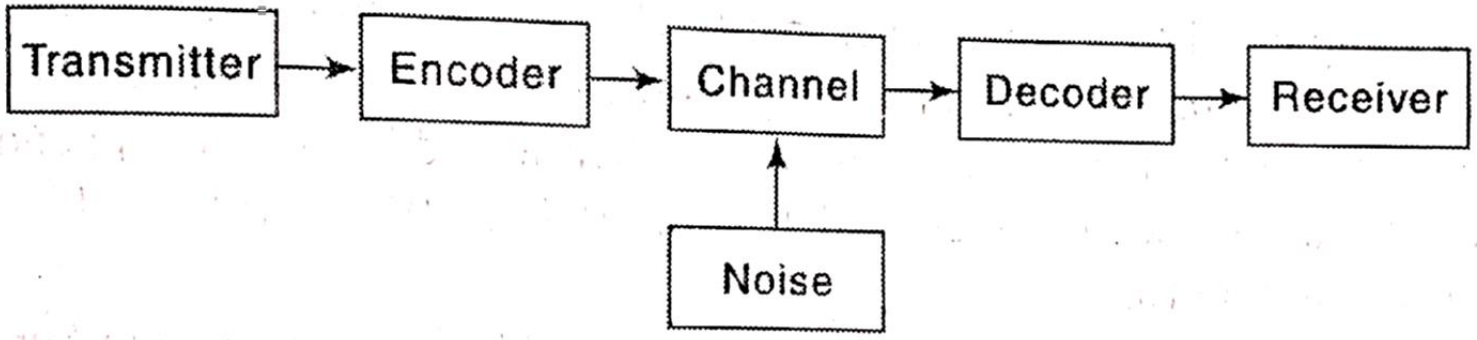

Fig.1

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*.

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.

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.

Generator Matrix (G)

Definition

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 $[I_m|\mathrm{A}]$, 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 belongs to B^m, then $e(w) = wG$ and the code (the set of code words) $\mathrm{C} = e(B^m) \subseteq B^n$, where w is a $(1 \times m)$ vector.

Parity Check Matrix (H)

(*) $H = [A^T \mid I_{n-m}]$

(*) $e : B^m \longrightarrow B^n$, let $m=2, n=5$

Eg: If $A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ then $A^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$

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

A^T $\quad I_{n-m} = I_3$

Problem 1:

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

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

Sol:-

$$H = [A^T \mid I_{n-m}]$$

Now

$$\Rightarrow H = \left[\begin{matrix} 0 & 0 \\ 1 & 1 \\ 1 & 1 \end{matrix}\right]_{A^T} \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} = [A^T \mid I_{n-m}].$$

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

$$A^T = \begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{then} \quad A = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Now, Generated matrix, $G = [I_m \mid A] = [I_2 \mid A]$

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

I_2 A

Now, $B^2 = \{00, 01, 10, 11\}$ and $e(w) = w \cdot G$

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

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

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

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

$\therefore$ The code words generated by H are 00000, 01011, 10011 and 11000.

α

Problem 2:

Find the code words generated by the parity check matrix

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

When the encoding function is $e: B^3 \rightarrow B^6$.

Decoding using Parity check matrix (H):

(*) Let $x \in C$ → set of encoded words.

Case (i): $H \cdot x^T = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

Then there is no error in the code word $-x$.

Case (iii): $H \cdot r^T = i^{th}$ column of H

$\Rightarrow$ Then there is a single error in 'r' and that error occurs at the i^{th} position of 'r'.

Eg: $r = [1\ 0\ 1\ 1] \longrightarrow r = [0\ 1\ 0\ 1\ 1]$

i^{th} column = 1^{st} column

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

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

Case (iii): $H \cdot r^T \neq i^{th}$ column of H.

We have more than one error in the code word 'r'. Then we can't decode the given code uniquely.

Eg: $r = [1\ 1\ 0\ 1\ 0]$

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \neq i^{th} \text{ column of } H.$$

$C : B^2 \to B^5$

$m = 2.$

$n = 5$

Problem 3:

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 $e\colon\ B^3 \to B^6$, 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?

$$(i)\ 110101, \qquad (ii)\ 001111, \qquad (iii)\ 110001, \qquad (iv)\ 111111$$

Problem 4:

Decode each of the following received words corresponding to the encoding function $e\colon\ B^3 \to B^6$ 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 $e(111) = 111\ 001$, assuming that no error or single error has occurred:

$$011110, 110111, 110000, 111000, 011111$$

Problem 3:

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: $B^3 \rightarrow B^6$, 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) 110101, (ii) 001111, (iii) 110001, (iv) 111111

Sol:-

W.K.T, $G = [I_m \mid A_{m\times(n-m)}]$

Given:- $e : B^3 \longrightarrow B^6$.

$m = 3$, $n = 6$

$$G = [I_3 \mid A_{3\times 3}] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

I_3 $A_{3\times 3}$

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \text{then} \quad A^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

W.K.T, Parity check matrix, $H = [A^T \mid I_{n-m}]$

(i.e.) $H = [A^T \mid I_3]$

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

A^T I_3

Decode the encoded message using H:

(i) $y = 110101$

$$H \cdot y^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3\times 6} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}_{6\times 1}$$

Note:
$\oplus \Rightarrow$ Addition modulo 2.

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

Since $H \cdot y^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, the received word contains no error. Hence, the original message for the given encoded word $y = 110101$ is $\underline{110}$.

$C : B^3 \longrightarrow B^6$

(ii) $y = 001111$

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

5th column

$\rightarrow$ case(i) ✗

$\rightarrow$ case(ii) ✓

Since, $H \cdot y^T = 5^{th}$ Column of H, there is an error in the 5^{th} position of $y = 0\,0\,1\,1\,1\,1$.
$\hookrightarrow 5^{th}$ position

$\therefore$ The corrected, $y = 0\,0\,1\,1\,0\,1$.

$\Rightarrow$ The original message is $0\,0\,1$.

(iii) $y = 1\,1\,0\,0\,0\,1$

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

$\hookrightarrow 4^{th}$ column

Since, $H \cdot r^T = 4^{th}$ Column of H, there is an error in the 4^{th} position of $r = 1\,1\,0\,0\,0\,1$ ⟶ 4^{th} position

$\therefore$ The corrected, $r = 1\,1\,0\,1\,0\,1$.

$\Rightarrow$ The original message is $1\,1\,0$.

(iv) $r = 1\,1\,1\,1\,1\,1$

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

Since, $H \cdot y^T \neq$ any column of H, the received message can't be decoded uniquely.

Here, only three received messages are decoded uniquely out of four received messages.

Problem 4:

Given 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 $e(111) = 111\ 001$. Find the parity check matrix and use it to decode the following received words $011110, 110111, 110000, 111000, 011111$ and hence, to find the original message. Are all the words decoded uniquely?

Steps:

1. Find the matrix A using the encoding function.
2. Then form the parity check matrix H.
3. Now decode the received words using the parity check matrix H

Problem 4:

Given 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 $e(111) = 111\ 001$. Find the parity check matrix and use it to decode the following received words $011110, 110111, 110000, 111000, 011111$ and hence, to find the original message. Are all the words decoded uniquely?

Sol:-

Parity check matrix: $H = [A^T \mid I_{n-m}]$.

Given: $e : B^3 \longrightarrow B^6$

$m = 3$ and $n = 6$

Thus, $H = [A^T \mid I_3]$.

Here we need to find the matrix A using the encoding function.

W.K.T, $G = [I_m \mid A_{m\times(n-m)}]$.

$G = [I_3 \mid A_{3\times3}]$.

Given: $\Rightarrow e(010) = 010101$

W.K.T. $e(w) = w \cdot G$.

Let, $w = 010$

$e(010) = [0\ 1\ 0]$ I_3 A

$$\begin{bmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & b_1 & b_2 & b_3 \\ 0 & 0 & 1 & c_1 & c_2 & c_3 \end{bmatrix}$$

$$[0\ 1\ 0\ 1\ 0\ 1] = [0\ 1\ 0] \cdot \begin{bmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & b_1 & b_2 & b_3 \\ 0 & 0 & 1 & c_1 & c_2 & c_3 \end{bmatrix}$$

We choose $w = 010$ to get the constants b1, b2 and b3.

$$[0\ 1\ 0\ 1\ 0\ 1] = [0\ 1\ 0\ b_1\ b_2\ b_3]$$

$$\Rightarrow \boxed{b_1 = 1,\quad b_2 = 0,\quad b_3 = 1}$$

We choose $w = 100$ to get the constants a1, a2 and a3.

NOW

$$e(w) = w \cdot G.$$

$$e(100) = [1\ 0\ 0] \begin{bmatrix} 1 & 0 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & c_1 & c_2 & c_3 \end{bmatrix}$$

$$[1\ 0\ 0\ 1\ 1\ 1] = [1\ 0\ 0\ a_1\ a_2\ a_3]$$

$$\Rightarrow \boxed{a_1 = 1,\quad a_2 = 1,\quad a_3 = 1}$$

We choose $w = 001$ to get the constants c1, c2 and c3.

Now, $e(001) = [0\ 0\ 1]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & c_1 & c_2 & c_3 \end{bmatrix}$

$[0\ 0\ 1\ 0\ 1\ 1] = [0\ 0\ 1\ c_1\ c_2\ c_3]$

$\Rightarrow \boxed{c_1 = 0,\ c_2 = 1,\ c_3 = 1}$

Now $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ then $A^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

Now, Parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

Decoding the following codes using H:

011110, 110111, 110000, 111000, 011111

Do it by your self. . .!

Decoding using Decoding Table

Theorem on Detection

Theorem on Detection:

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

Eg: $S = \{000, 111\}$.

Min. dist of $S = 3 = 2+1 = k+1$

Detection = 2 errors

Theorem on Correction

Theorem on Correction:

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

Eg: $S = \{000, 111\}$

$2k+1$

Min. Dist. of $S = 3 = 2(1) + 1$

Correction = 1 error

Decoding using Decoding Table

1. $e : B^3 \longrightarrow B^6$
2. $B^3 = \{000, 001, 010, 100, 101, 110, 111\}$.
3. Generator matrix, G.
4. $e(w) = w \cdot G$, $w \in B^3$.
5. Code words = {the set of encoded words}.
6. Decoding table [code words $\rightarrow 1^{st}$ Row.
   coset leaders $\rightarrow 1^{st}$ column]

Problem

(1) Construct the decoding table given by the generator matrix

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

Decode the following received words using the decoding table obtained.

(i) 101111

(ii) 011010

(iii) 101110

(iv) 111111

Sol:

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{3\times 6}$$

Encoding function, $e : B^3 \longrightarrow B^6$

$B^3 = \{000, 001, 010, 100, 101, 110, 011, 111\}$.

W.K.T, $e(w) = w \cdot G$

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

$$e(010) = [0\ 1\ 0] \cdot \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 1\ 0\ 1\ 0\ 1]$$

$e(001) = [0\ 0\ 1] \cdot G = [0\ 0\ 1\ 0\ 1\ 1]$

$e(011) = [0\ 1\ 1] \cdot G = [0\ 1\ 1\ 1\ 1\ 0]$

$e(101) = [1\ 0\ 1] \cdot G = [1\ 0\ 1\ 1\ 0\ 0]$

$e(110) = [1\ 1\ 0] \cdot G = [1\ 1\ 0\ 0\ 1\ 0]$

$e(111) = [1\ 1\ 1] \cdot G = [1\ 1\ 1\ 0\ 0\ 1]$.

Code words = {000000, 001011, 010101, 100111, 011110, 101100, 110010, 111001}

Min. distance = 3

(*) Minimum distance of the code words = 3

(*) Theorem on correction:

If Min. dist = $2k+1$

then at most k-errors can be corrected.

(*) $2k+1 = 3 \Rightarrow 2(1)+1 = 3$

$\Rightarrow \boxed{k = 1}$

Here, only one error can be corrected in the given code words.

Decoding Table: 1st Row = code words
1st column = coset leaders

(i) 101111, (ii) 011010, (iii) 101110, (iv) 111111

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

Decoding Table: 1st Row = code words
1st column = coset leaders

(i) 101111

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

Decoding using Decoding table:-

(i) 101111

(*) 101111 appears in the 4th row and 4th column. Thus there is an error at the 3rd position of 101111. Hence, the corrected encoded code is 100111. Therefore, the original message is 100.

Decoding Table: 1st Row = code words
1st column = coset leaders

(ii) 011010

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

(ii) 011010

(*) 011010 appears in the 5th row and 5th column. Thus there is an error at the 4th position of 011010.

Hence, the corrected encoded code is 011110. Therefore, the original message is 011.

Decoding Table: 1st Row = code words
1st column = coset leaders

(iii) 101110

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

(iii) $r = 01110$

(*) 101110 appears in the 6^{th} row and 6^{th} column. Thus there is an error at the 5^{th} position of 101110.

Hence, the corrected encoded code is 101100. Therefore, the original message is 101.

Decoding Table: 1st Row = code words
1st column = coset leaders

(iv) 111111

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

Two errors. Hence not possible to correct uniquely.

(iv) 111111

⊗ 111111 appears in the 8th row. Thus it has two errors.

By the Theorem on correction, we can't correct more than one error uniquely.

Thank You