II YEAR – III SEMESTER
COURSE CODE: 7MMA3E1

ELECTIVE COURSE-III (A) – DISCRETE MATHEMATICS

Unit I

Algebraic Systems : Binary Operation – Algebraic Systems – Semigroups and Monoids – Homorphism and Isomophism of Semigroups and Monoids – Properties of Homomorphism – Subsemi groups and Submonoids.

Unit II

Mathematical Induction – Techniques of Proof – Mathematical Induction – Recurrence Relations and Generating Functions – Recurrence – an introduction – Polynomials and their Evaluations Recurrence Relations – Solution of Finite order Homogeneous (Linear) Relations.

Unit III

Solution of Non-homogeneous Relations – Generations Functions – Some Common Recurrence Relations – Primitive Recursive Functions – Recursive and Partial Recursive Fnctions.

Unit IV

Lattices – Lattices – Some Properties of Lattices – New Lattices – Modular and Distributive Lattices.

Unit V

Boolean Algebra – Boolean Algebras – Boolean Polynomials – Karnaugh Map – Switching Circuits

Text Book:

1. Dr. M.K.Venkataraman, Dr. N.Sridharan and Dr. N.Chandra Sekaran, The National Publishing Company, Chennai.

   Chapter IV; Chapter V ,Sections 1 to,9
   Chapter VII -Sections 7.1 to 7.6; Chapter X

Books for Supplementary Reading and Reference:

1. Rudolf Lidl and Gunter Pilz, Applied Abstract Algebra, 2nd Indian Reprint 2006, Springer Verlag, New York.
2. Kenneth H. Rosen, Discrete Mathematics and its Applications, Fourth edition, McGraw Hill Publications.
3. A Gill, Applied Algebra for Computer Science, Prentice Hall Inc., New Jersey.

♣♣♣♣♣♣♣♣♣♣

intersection of the row headed by a_i and the column headed by a_j.

$*$	a_1	a_2	a_3	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$		
a_2				
a_3			$a_3 * a_3$	
⋮				
a_n				

For example, the cayley table for the binary operation multiplication defined on $S = \{0, 1, -1\}$ is given below

$*$	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

Special types of binary operations

1) commutative:

A binary operation $*$ on a set S is said to be commutative if $a * b = b * a$ for all elements $a, b \in S$.

2) Associative:-

A binary operation $*$ on a set S is said to be associative if $a * (b * c) = (a * b) * c$ for all elements $a, b, c \in S$

3) Identity:

A binary operation $*$ on a set S is said to have an identity if there exists

Discrete mathematics

Unit - I

Algebraic systems

Defn: Binary operation

Let S be a non-empty set. A binary operation on S is a rule that assigns to each ordered pair of elements of S, a unique element of S. In other words, a binary operation is a function from $S \times S$ into S

Example: 1

Let $S = N$ be the set of all natural numbers. Then addition and multiplication are binary operations on N as for all $a, b \in N$, $a+b$ and $a \times b \in N$

Subtraction and division are not binary operations on N.

Example: 2

Let $S = \{1, -1, 0\}$. The addition $+$ is not a binary operation on S. Since the sum $1+1 = 2$ is not an element of S. But the multiplication $\times$ is a binary operation on S.

Operation table

When the set S has only a finite number of elements, then the results of applying the binary operation $*$ to its elements may be represented in table known as operation table or cayley table

Suppose $S = \{a_1, a_2, \ldots, a_n\}$. Then the result $a_i * a_j$ is entered at the point of an element e in S such that $a*e=e*a=a$ for all $a \in S$. e is said to be an identity element for the binary operation $*$.

4) Idempotent:

Let $*$ be a binary operation on A. Then an element a in A is idempotent if $a*a=a$

Theorem:

U.Q. 5M An identity element for any binary operation if it exists, is unique.

proof:-

Let S be a nonempty set with a binary operation $*$ on it.

Let e be an identity element for $*$ in S

By definition, $a*e=e*a=a$ for all $a \in S$ — ①

Suppose e' to be another identity element for $*$ in S.

considering e' as an element in S and e as an identity element applying ①.

we get,

$$e'*e=e*e'=e' \quad — ②$$

Similarly considering e as an element in S and e' as an identity element, we get

$$e*e'=e'*e=e \quad — ③$$

combining ② & ③, we have $e'=e*e'=e$

ie) $e'=e$

$\therefore$ The two identity elements are the same.

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

Show that S and T are isomorphic.

Soln:

We define the function $g: S \to T$ such that

$g(0) = 1$, $g(1) = 3$, $g(2) = 9$ and $g(3) = 7$.

Replace the elements in S by their images and the operation + by ×, we then get the following table.

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

Rearranging this table, we get exactly the table for T.

So S and T are isomorphic.

W.E: 7

Let $S = N \times N$, N being the set of positive integers and $*$ be an operation on S given by $(a,b) * (c,d) = (a+c, b+d)$, S.T S is a Semigroup. Define $f: (S,*) \to (Z,+)$ by $f(a,b) = a-b$. S.T f is a homomorphism.

Soln:

Let x, y, z be the ordered pairs $(a,b), (c,d)$ and (e,f) respectively in $N \times N$.

Then $(xy)z = (x*y)*z$

$= [(a,b)*(c,d)]*z$

$= [a+c, b+d) * (e,f)$

Clearly the set F is closed under the operation of composition and the set $\langle F, \circ \rangle$ is an algebraic system. The operation $\circ$ is both commutative and associative. f^0 is the identity element.

$\circ$	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

Consider the set of equivalence class of modulo 4.

$$Z_4 = \{[0], [1], [2], [3]\}$$

Let us define an operation $+_4$ on Z_4 given by $[i] +_4 [j] = [(i+j) \bmod 4]$ for $i, j = 0, 1, 2, 3$

The operation $+_4$ on Z_4 is described

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Clearly the set Z_4 is closed under the operation $+_4$ and the set $\langle Z_4, +_4 \rangle$ is an algebraic system with the operation $+_4$ which is commutative and associative. [0] is the identity element

The two algebraic systems $\langle F, \circ \rangle$ and $\langle Z_4, +_4 \rangle$ are not structurally different. They are only different in the names of the elements and the symbols used for the operations.

We shall now formalise these ideas

Let us now define a mapping

$g : F \to Z_4$ Such that $g(f^j) = [j]$ for $j = 0, 1, 2, 3$

Then for any two elements $a, b \in S$, we have

$$g(a * b) = g(a) \Delta g(b) \quad — ①$$

So, we have $g(a * a) = g(a) \Delta g(a) \quad — ②$

Now, let a be an idempotent element of S.

Then $a * a = a \quad — ③$

Using ③ in ② we get $g(a) = g(a) \Delta g(a) — ④$

Eqn ④ clearly shows that $g(a)$ is an idempotent element of T

So, if a is an idempotent element in S, then its image $g(a)$ is an idempotent element in T

Thm: 6

Let $(S, *)$ and (T, Δ) be monoids with identities e and e' respectively. Let $g: S \to T$ be an onto (semigroup) homomorphism. Then $g(e) = e'$

proof:- Let b be any element of T.

Since g is onto, there is an element a in S such that $g(a) = b$

Now $a = a * e$ (e being the identity element)

$$b = g(a) = g(a * e)$$
$$= g(a) \Delta g(e) \quad (\text{isomorphism of } g)$$
$$= b \Delta g(e) \quad — ①$$

Again $a = e * a$

$$b = g(a) = g(e * a)$$
$$= g(e) \Delta g(a) \quad (\text{isomorphism of } g)$$
$$= g(e) \Delta b \quad — ②$$

combining ① and ② we have

$$b \Delta g(e) = g(e) \Delta b = b$$

This show that $g(e)$ is the identity for T.

$\therefore g(e) = e'$.

Corollary

If $(S, *)$ and (T, Δ) are semigroups such that S has an identity and T does not, then the two semigroups cannot be isomorphic.

Defn:-

Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids. A mapping $g: M \to T$ such that for any two elements $a, b \in M$

$g(a * b) = g(a) \Delta g(b)$ and $g(e_M) = e_T$ is called a monoid homomorphism.

Note:-

If g is onto, $g(a * b) = g(a) \Delta g(b) \Rightarrow g(e_M) = e_T$ by thm 5. If g is not onto $g(e_M)$ need not be e_T. The following example illustrates this.

Ex

Let N be the set of an natural numbers. Define $g: N \to N$ by $g(n) = 2n$, for all n. Then g is a semigroup homomorphism from $(N, +)$ into itself. But $g(1) = 2 \neq 1$.

Thm: 7

S.T the monoid homomorphism preserves the property of invertibility.

proof:-

Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids and let $g: M \to T$ be a monoid homomorphism

If $a \in M$ is invertible, let a^{-1} be the inverse of a in M.

We will now show that $g(a^{-1})$ will be an inverse of $g(a)$ in T.

Step 2: show that g is one-to-one

Step 3: show that g is onto.

Step 4: show that $g(a * b) = g(a) \Delta g(b)$.

2) If $(S, *)$ and (T, Δ) are finite semigroups of and if it is possible to rearrange and relabel the elements of S so that the cayley tables of S and T are identical, then we conclude that $(S, *)$ and (T, Δ) are isomorphic.

3) A semigroup homomorphism preserves associativity. That is,

$$g((a*b)*c) = (g(a) \Delta g(b)) \Delta g(c).$$

W.E:4

Let T be the set of all even integers, show that the semigroups $(Z,+)$ and $(T,+)$ are isomorphic.

soln:-

Step 1: We define the function

$G: Z \to T$ given by $g(a) = 2a$ where $a \in Z$.

Step 2: Suppose $g(a_1) = g(a_2)$ where $a_1, a_2 \in Z$.

Then $2a_1 = 2a_2$ ie. $a_1 = a_2$

Hence mapping by g is one-to-one.

Step 3: Suppose b is an even integer.

Let $a = b/2$, then $a \in Z$ and

$g(a) = g(b/2) = 2 \cdot b/2 = b$

ie) every element b in T has a preimage in Z

So mapping by g is onto.

Step 4: Let a and $b \in Z$

$$g(a+b) = 2(a+b)$$
$$= 2a + 2b$$
$$= g(a) + g(b)$$

Hence $(Z,+)$ and $(T,+)$ are isomorphic semigroups

Then $a = g^{-1}(a')$ and $b = g^{-1}(b')$

Now $g^{-1}(a' \Delta b') = g^{-1}(g(a) \Delta g(b))$

$= g^{-1}(g(a * b))$ since g is an isomorphism

$= (g^{-1} \circ g).(a * b)$

$= a * b$

$= g^{-1}(a') * g^{-1}(b')$

Hence g^{-1} is an isomorphism.

Thm: 4

If g is a homomorphism from a commutative semigroup $(S, *)$ onto a ~~ot~~ semigroup (T, Δ), then (T, Δ) is also commutative.

proof:- Let t_1 and t_2 be any two elements of T. As g is onto, there exists elements s_1 and s_2 in S such that $g(s_1) = t_1$ and $g(s_2) = t_2$.

Now $t_1 \Delta t_2 = g(s_1) \Delta g(s_2)$

$= g(s_1 * s_2)$ as g is homomorphism

$= g(s_2 * s_1)$ as S is commutative under $*$

$= g(s_2) \Delta g(s_1)$ as g is a homomorphism

$= t_2 \Delta t_1$

Hence (T, Δ) is commutative.

Thus isomorphism preserves the property of commutativity.

Thm: 5

The property of idempotency is preserved under a semigroup homomorphism.

proof:- Let g be a semigroup homomorphism from $(S, *)$ to (T, Δ)

$(d * b) * a = c * a$ — (1)

$d * (b * a) = d * b = c$ — (2)

By associative law, $(d * b) * a = d * (b * a)$

$c * a = c$ — (i)

$(d * b) * b = c * b$ — (3)

$d * (b * b) = d * a = d$ — (4)

By associative law, $(d * b) * b = d * (b * b)$

$c * b = d$ — (ii)

$(d * b) * c = c * c$ — (5)

$d * (b * c) = d * c = c$ — (6)

By associative law, $(d * b) * c = d * (b * c)$

$c * c = c$ — (iii)

$(d * b) * d = c * d$ — (7)

$d * (b * d) = d * d = d$ — (8)

By associative law, $(d * b) * d = d * (b * d)$

$c * d = d$ — (iv)

Thus the table is completed with new entries

*	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d	d	c	c	d

W.E:6

Let A be a set with n elements.

a) How many binary operations can be defined on A?

5m 10m

b) How many commutative binary operations can be defined on A?

soln:-

*	a_1	a_2	......	a_n
a_1				
a_2				
⋮				
a_n				

Note:

We can show that a cyclic monoid is commutative. Let $b, c \in M$ and a the generator of a cyclic monoid. We can write $b = a^m, c = a^n$ for some $m, n \in N$. Then $b * c = a^m * a^n = a^{m+n}$ and $c * b = a^n * a^m = a^{n+m}$. So, $b * c = c * b$, for all $b, c \in M$.

Worked exp:

W.E: 1

Let N be the set of positive integers and $*$ the operation of least common multiple(L.C.M) on N. Find whether $(N, *)$ is a commutative semigroup. Is it a monoid? Specify the identity element. Which elements in N have inverse and what are they?

Soln:

Let $a, b, c \in N$.

Let A be the set of all prime numbers which divide atleast one of the numbers a, b, c.

$A = \{p : p$ is a prime number and p divides atleast one of $a, b, c\}$. Then A is a finite set.

Let $A = \{P_1, P_2, \ldots, P_m\}$, we can write

$$a = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_m^{\alpha_m};\ b = P_1^{\beta_1} P_2^{\beta_2} \cdots P_m^{\beta_m} \text{ and}$$

$c = P_1^{\gamma_1} P_2^{\gamma_2} \cdots P_m^{\gamma_m}$ for some non-negative integers $\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_m, \gamma_1, \gamma_2, \ldots, \gamma_m$

Then $a * b = L.C.M(a, b) = P_1^{e_1} P_2^{e_2} \cdots P_m^{e_m}$, where $e_i = \max\{\alpha_i, \beta_i\}$ for all $i = 1, 2, \ldots, m$

As $\max\{\alpha_i, \beta_i\} = \max\{\beta_i, \alpha_i\}$, for all i, we have $a * b = b * a$

As $\max\{\max\{\alpha_i, \beta_i\}, \gamma_i\} = \max\{\alpha_i, \beta_i, \gamma_i\} = \max\{\alpha_i, \max\{\beta_i, \gamma_i\}\}$

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

proceeding thus, we find that

Number of blank spaces in the $(n-1)^{th}$ row $= n-(n-2) = 2$

And number of blank spaces in the n^{th} row $= 1$

Hence total number of blank spaces to be filled

$$= n + (n-1) + (n-2) + \cdots + 2 + 1$$

$$= 1 + 2 + \cdots + n$$

$$= \frac{n(n+1)}{2}$$

Since each space can be filled with any one of the n elements, all the $\frac{n(n+1)}{2}$ blank spaces can be together filled in

$$n \times n \times \cdots \frac{n(n+1)}{2} \text{ times} = n^{n(n+1)/2}$$

So number of commutative binary operations that can be defined on A

$$= n^{n(n+1)/2}$$

Algebraic systems

Defn:

An algebraic system (or simply an algebra) is a mathematical system consisting of a set and one or more n-ary operations on the set. It is denoted by $(S, f_1, f_2, \ldots)$ where S is a non empty set and $f_1, f_2, \ldots$ are operations on S.

Since the operations define a structure on the elements of S, an algebraic system is called an algebraic structure. eg: $(Z, +, \times)$
$(N, +, \times)$

Semigroups and monoids

Defn: Semigroups

A nonempty set S together with an associative binary operation $*$ on it is called a semigroup. The semigroup is denoted by $(S, *)$

Definitions

1) $*$ is left distributive over if and only if for every $a, b, c \in S$,

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

2) $*$ is right distributive over $\odot$, if and only if, for every $a, b, c \in S$

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

3) $*$ is distributive over $\odot$, if $*$ is both right and left distributive over $\odot$

Worked examples

W.E: 1

ST the set operations $\cup, \cap$ (union and intersection) are binary commutative, associative, idempotent and each one is distributive over other.

Soln:-

If A and B are subsets of a universal set U, we know that

$$A \cup B = B \cup A \quad \text{and} \quad A \cap B = B \cap A$$

Hence the operations $\cup$ and $\cap$ are commutative

Also $A \cup (B \cup C) = (A \cup B) \cup C$

And $A \cap (B \cap C) = (A \cap B) \cap C$ for any three sets A, B, C in U

Hence $\cup$ and $\cap$ are associative

We know that $A \cup A = A$ and $A \cap A = A$ for all sets A in U

So $\cup$ and $\cap$ are idempotent

Again we know that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

This shows that union distributes over intersection.

Also $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

ie) intersection distributes over union

From the tables, it is clear that

$$g(f^i \circ f^j) = g(f^k) \text{ where } k = i+j \bmod 4$$

$$= [k] = [i] +_4 [j]$$

$$= g(f^i) +_4 g(f^j), \quad (i, j = 0, 1, 2, 3)$$

This eqn show that the image of g for the argument $f^i \circ f^j$ is the same as the result of the operation $+_4$ applied to the result of the operation $+_4$ applied to the images $f(f^i)$ and $g(f^j)$ of the elements f^i and f^j.

In other words, the mapping g preserves the operations $\circ$ and $+_4$.

This property of the mapping g is shown.

$$\begin{tikzcd} F \times F \arrow[r, "\circ"] \arrow[d, "g \times g"'] & F \arrow[d, "g"] \\ Z_4 \times Z_4 \arrow[r, "+_4"'] & Z_4 \end{tikzcd}$$

We find that the effect of applying the mapping $\circ$ from $F \times F$ to F and applying the mapping g to that result is the same as the effect of the mapping $g \times g$ applied to $F \times F$ to obtain an ordered pair $Z_4 \times Z_4$ and then applying the mapping $+_4$ to this ordered pair.)

Defn:

(Let $(S, *)$ and (T, Δ) be any two semigroups. A mapping $g: S \to T$ such that for any two element $a, b \in S$, $g(a * b) = g(a) \Delta g(b)$ is called a semigroup homomorphism. Suppose g is also one-to-one and onto, then g is called an isomorphism.)

An isomorphism is thus a special kind of homomorphism.

Thus $(S,*)$ is a semigroup, if for any $a,b,c \in S$, $(a*b)*c = a*(b*c)$.

The semigroup $(S,*)$ is said to be commutative, if $*$ is a commutative operation.

Ex:

Let N be the set of positive integers. The $(N,+)$ and $(N,\times)$ are semigroups since addition and multiplication on N are associative. These semigroups are also commutative.

Defn: Monoids

A semigroup $(M,*)$ with an identity element is called a monoid. Thus $(M,*)$ is a monoid, if

1) for any $a,b,c \in S$, $(a*b)*c = a*(b*c)$ and
2) there exists an element $e \in M$ such that for any $x \in M$,

$$x*e = e*x = x$$

Thus a monoid has a unique or a special element called its identity. For this reason, a monoid is represented by $(M,*,e)$ to highlight the fact that e is its identity (e is a 0-ary operation).

Ex:

1) $(Z,+)$ is a commutative semigroup having the number 0 as the identity element. Hence $(Z,+)$ is a monoid.

Defn:

Let $(M,*,e)$ be a monoid and $a \in M$. Then if there exists an element $b \in M$ such that $a*b = b*a = e$, then b is called an <u>inverse of a</u>. In this case a is said to be <u>invertible</u>.

$= [(a+c)+e,\ (b+d)+f]$

$= (a+c+e,\ b+d+f)$ since $a, b, \ldots, f$ are positive integers

$$x(yz) = x * (y * z)$$
$$= (a,b) * [(c,d) * (e,f)]$$
$$= (a,b) * [(c+e), (d+f)]$$
$$= [a+(c+e),\ b+(d+f)]$$
$$= (a+c+e,\ b+d+f)$$

Hence $(xy)z = x(yz)$

So $*$ associative and S is a semigroup.

Now $f(x*y) = f[(a,b) * (c,d)]$

$= f(a+c, b+d)$ by defn of $*$

$= (a+c)-(b+d)$ by defn of f

$= (a-b) + (c-d)$

$= f(a,b) + f(c,d)$

$= f(x) + f(y)$

So f is a homomorphism

properties of homomorphism

Theorem: 3

If g is a semigroup isomorphism from $(S,*)$ to (T,Δ), show that g^{-1} is a isomorphism from (T,Δ) to $(S,*)$

proof:-

g is an isomorphism from $(S,*)$ to (T,Δ).

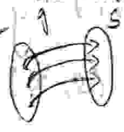
So g is one-to-one onto mapping.

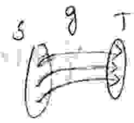
Hence g^{-1} exists and is one-to-one mapping from T to S.

Let a' and b' be any two elements of T.

Since g is onto, we can find elements a and b in S such that

$g(a) = a'$ and $g(b) = b'$





Thus $*$ is associative and $(N, *)$ is a commutative semigroup.

Since $a * 1 = 1 * a = a$ for all $a \in N$, 1 is the identity element for $*$ in N.

Thus $(N, *)$ is a monoid.

Let $a, b \in N$ such that $a * b = 1$.

Then as 1 is the L.C.M of a and b, we have $a \leq 1$, $b \leq 1$.

But as $a, b \in N$, we have $a \geq 1$ and $b \geq 1$.

Thus $a * b = 1$ is possible only when $a = 1 = b$.

And $a = 1$ is the only element which has the inverse with respect to $*$.

W.E: 2

S.T for a finite monoid $(M, *)$, no two rows or columns of the cayley table are identical.

Soln:- As M is a monoid it has an identity element. Denote it by a_1, and the remaining elements of M as $a_2, \ldots, a_n$ (n denotes the number of elements of M). Then the first row of the composition table is $a_1, a_2, \ldots, a_n$, which is also the first column.

Obviously, no two rows (columns) are identical since their first elements are different.

Homomorphism and isomorphism of semigroups and monoids

Let $X = \{1, 2, 3, 4\}$ be a set and a mapping function $f : X \to X$ be given by $f = \{(1,2), (2,3), (3,4), (4,1)\}$.

Form the functions f^2, f^3, f^4. Let us denote f by f^1. Denote the identity function $\{(1,1), (2,2), (3,3), (4,4)\}$ by f^0. Note that $f^4 = f^0$.

Consider the set $F = \{f^0, f^1, f^2, f^3\}$.

a) Let $A = \{a_1, a_2, \dots, a_n\}$ and $*$ be the binary operation.

The operation table contains n rows and n columns. Hence the number of spaces to be filled up $= n \times n = n^2$.

Each space can be filled up with any one of the n elements from A. So there are n ways to fill up each space.

Hence all the n^2 spaces can be together filled in

$$n \times n \times \dots (n^2 \text{ times}) = n^{n^2} \text{ ways.}$$

So number of binary operations that can be defined on $A = n^{n^2}$.

b) For a commutative binary operation, the Cayley table is symmetric.

Hence it is enough if we fill up the spaces on and to the right of the main diagonal.

In this region, the number of spaces in the first row $= n$.

Number of blank spaces in the second row $= (n-1)$

($\because$ the first place need not be filled up, as it is to be filled up by the 2nd element in the first row)

Number of blank spaces in the third row $= (n-2)$.

($\because$ the first two places need not be filled up, as they are to be filled up by the 3rd and 4th elements in the first row).

Suppose $a, b \in S$

Then $g(a+b) = 3^{a+b}$

$= 3^a \cdot 3^b$

$= g(a) \cdot g(b)$

Hence the mapping by g is homomorphism.

Suppose $g(a) = g(b)$. Then $3^a = 3^b$, which implies $a = b$

Hence g is one-to-one. G is not onto since Range g contains no negative numbers.

Hence g is not an isomorphism.

N.E:3 Let R^+ be the set of positive real numbers. S.T the function $g: R^+ \to R$ defined by $g(x) = \log_e x$ is an isomorphism of the semigroup $(R^+, \times)$ to the semigroup $(R, +)$ where $\times$ and $+$ are usual multiplication and addition respectively.

soln:-

Let $x, y \in R$

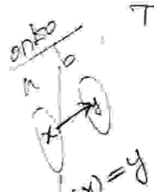
It is given that $g(x) = \log_e x$

$\therefore g(x, y) = \log(xy) = \log x + \log y = g(x) + g(y)$

Hence the function is a homomorphism.

To prove that g is onto take $y \in R$.

They $y = \log_e e^y = g(e^y)$. Note $e^y > 0$



Hence g is onto [for each $y \in R$ $\exists$ $x \in R$ $\ni$: $g(x) = y$.]

Suppose $\log x = \log y$

Then $e^{\log x} = e^{\log y}$

ie) $x = y$

elies between 2 and 3

Hence the mapping is one-to-one

So the function g is an isomorphism.

Note:

1) To show that two semigroups $(S, *)$ and (T, Δ) are isomorphic, we use the following four-step rule.

Step 1: Define a suitable function $g: S \to T$

W.E:5 Let $S=\{x,y,z\}$ and $T=\{a,b,c\}$ be two semigroup with operations $*$ and Δ respectively, as gvn by the following tables.

$*$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

Δ	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

S.T S and T are isomorphic.

soln:- We define the function $g: S \to T$ such that
$g(x)=b$, $g(y)=a$ and $g(z)=c$.

Replace the elements in S by their images and the operation $*$ by Δ, we then get the following table

Δ	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

Rearranging this table, we get exactly the table for T.

So g is an isomorphism between $(S,*)$ and (T,Δ).

W.E!6 Consider the semigroups $(Z_4, +_4)$ $(0,1,2,3)$ (integers modulo 4 under addition) and $(Z_{10}, \times_{10})$ (integers modulo 10 under multiplication). Let $S=\{0,1,2,3\}$ and $T=\{1,3,7,9\}$ be subsets of the above two semigroups respectively, with the following operation tables.

Ex:

The $g: F \to Z_4$ defined by the equation $g(f^i \circ f^j) = g(f^i) + g(f^j)$ is one-to-one and onto and a homomorphism. Hence g is an isomorphism.

Worked examples:

W.E: 1

S.T there exists a homomorphism from the algebraic system $(N, +)$ to the system $(Z_4, +_4)$ where (i) N is the set of natural numbers and (ii) Z_4 is the set of integers modulo 4. Is it an isomorphism?

Soln:-

Let us define $g: N \to Z_4$ by $g(a) = [a(\mathrm{mod}\,4)]$ for all $a \in N$

For $a, b \in N$, let $g(a) = [i]$ and $g(b) = [j]$

Then $g(a+b) = [(i+j)(\mathrm{mod}\,4)]$

$= [i] +_4 [j]$

$= g(a) +_4 g(b)$

$\therefore g$ is a homomorphism.

$f(x) = f(y) \Rightarrow x = y$
$g(7) = g(11)$
$\Rightarrow 7(\mathrm{mod}\,4) = 11(\mathrm{mod}\,4)$
$3 = 3$
$7 \neq 11$

As the mapping defined by g is not one-to-one (for example, $g(7) = g(11)$) it is not isomorphism.

W.E: 2

S.T the mapping g from the algebraic system $(S, +)$ to the system $(T, \times)$ defined by $g(a) = 3^a$, where (i) S is the set of all rational numbers under addition operation $+$ and

ii) T is the set of non-zero real numbers under multiplication operation $\times$ is a homomorphism but not an isomorphism.

Soln:-

Now $g(a) = 3^a$ for any $a \in S$

(Note $g(a) > 0$ for all a in S).

Thm: 2

Let $(M, *, e)$ be a monoid and $a \in M$. If a is invertible, then its inverse is unique.

proof:- Let a be an invertible element in $(M, *, e)$.

Let b' and b'' be elements of M such that

$$a * b' = b' * a = e \quad \text{--- (i)}$$

$$a * b'' = b'' * a = e \quad \text{--- (ii)}$$

now $b' = b' * e$

$= b' * (a * b'')$ from (ii)

$= (b' * a) * b''$ by associative property

$= e * b''$ by (i)

$= b''$

Then $b' = b''$ and hence the inverse of a, if it exists is unique.

Note: If a is invertible in a monoid $(M, *, e)$, then its unique inverse is denoted by a^{-1}.

cyclic monoids

Let $(M, *, e)$ be a monoid and a be any element in M. The powers of a are defined as $a^0 = e$, $a^1 = a$, $a^2 = a * a$, ..., $a^{i+1} = a^i * a$ for $i \in N$

Hence we have $a^{i+j} = a^i * a^j = a^j * a^i$ for all $i, j \in N$

Defn:- A monoid $(M, *, e)$ is said to be cyclic, if there exists an element $a \in M$ such that every element of M can be written as some power of a, that is, a^n for some $n \in N$. In such a case, the cyclic monoid is said to be generated by the element a. The element is called a generator of the cyclic monoid.

$\therefore \; a * a^{-1} = a^{-1} * a = e_M$ (by defn of inverse)

So $g(a * a^{-1}) = g(a^{-1} * a) = g(e_M)$

Hence $g(a) \Delta g(a^{-1}) = g(a^{-1}) \Delta g(a) = g(e_M)$ (since g is a homomorphism)

But $g(e_M) = e_T$ (since g is a monoid homomorphism)

$\therefore g(a) \Delta g(a^{-1}) = g(a^{-1}) \Delta g(a) = e_T$

This means $g(a^{-1})$ is an inverse of $g(a)$ i.e. $g(a)$ is invertible.

Thus the property of invertibility is preserved under monoid homomorphism.

Subsemigroups and submonoids

Let $(S, *)$ be a semigroup and T a subset of S. If the set T is closed under the operation $*$, then $(T, *)$ is said to be a subsemigroup of $(S, *)$.

Similarly, let $(M, *)$ be a monoid with identity e and T a subset of M. If the set T is closed under the operation $*$ and $e \in T$, then $(T, *)$ is said to be a submonoid of $(M, *, e)$.

Ex:

1) For the semigroup $(N, \times)$ where N is the set of all natural numbers, let T be the set of multiples of a positive integer m. Then $(T, \times)$ is a subsemigroup of $(N, \times)$.

W.E:4

Fill in the following table, so that the binary operation $*$ is commutative.

$*$	a	b	c
a	b		
b	c	b	a
c	a		c

soln:-

If the operation is commutative, the rows and columns in the operation table must be identical.

Hence the first row elements must be b c a (as they are the same as the first column elements).

The second ~~row~~ column elements must be c b a (as they are the same as the second row elements)

Now the filled up entries are shown

$*$	a	b	c
a	b	c	a
b	c	b	a
c	a	a	c

W.E:5

– complete the table, so that the binary operation $*$ is associative

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c				
d	d	c	c	d

soln:-

We have to fill up the entries against the row headed by c.

W.E:2
S.T the null set ϕ is the identity element for the operation $\cup$ and the universal set U is the identity element for the operation $\cap$ on $P(U)$, the power set of U.

Soln:- If A is any subset of U, we know that $A \cup \phi = \phi \cup A = A$.

Hence ϕ is the identity element for the operation $\cup$.

Also we know that $A \cap U = U \cap A = A$.

Hence U is the identity element for the operation $\cap$.

W.E:3 The cayley table of a binary operation $*$ on the set $S = \{p, q, r, s\}$ is given

$*$	p	q	r	s
p	p	r	q	s
q	s	p	q	r
r	r	s	q	p
s	s	q	q	r

compute

a) $r * s$ and $s * r$ b) $q * s$ and $s * q$

c) $p * (q * r)$ and $(p * q) * r$ d) Is $*$ commutative, associative?

Soln:-

a) $r * s = p$; $s * r = p$

b) $q * s = r$; $s * q = q$

c) $q * r = q$; $p * (q * r) = p * q = r$

$p * q = r$; $(p * q) * r = r * r = q$.

d) $*$ is not commutative since $q * s \neq s * q$

$*$ is not associative since $p * (q * r) \neq (p * q) * r$

Thm: 8

For any commutative monoid $(M, *)$, the set of idempotent elements of M forms a submonoid.

proof:-

Let S be the set of idempotent elements of M and e be the identity element of M.

As $e * e = e$ by defn, if identity e is an idempotent element in M and $e \in S$.

We shall show that S itself is a monoid with respect to the operation $*$ on M.

Let $a, b \in S$.

The $a * a = a$ and $b * b = b$.

Now $(a * b) * (a * b) = (a * b) * (b * a)$ ($\because (M, *)$ is commutative)

$= a * (b * b) * a$ (associative prop)

$= a * b * a$ (b is idempotent)

$= a * (b * a)$

$= a * (a * b)$ (commutative prop)

$= (a * a) * b$ (associative prop)

$= a * b$ (a is idempotent)

$\therefore$ $(a * b)$ is idempotent of M and so $a * b \in S$.

Thus $a * b \in S$ for all $a, b \in S$.

So S is closed under $*$ and S is a submonoid.

x

Note:

1) Usually a sequence is written as a list. If S is a sequence then it is usually written as a list viz., $s_1, s_2, \ldots, s_n, \ldots$ where $s_n = S(n)$.

2) The domain of a sequence can also be taken as $\{0,1,2,\ldots\}$ or $\{-2,-1,0,1,2,\ldots\}$ or $\{3,4,5,\ldots\}$. Note all these sets are countable, and each set has a least integer say m and all other elements are of the form $m+n$, $n=1,2,\ldots$

Example 1.

The Fibonacci numbers $F_0=1, F_1=1, F_2, \ldots$ is a sequence of integers.

Defn 2

Let S be a sequence of integers. A recurrence relation on S is a formula that relates all but a finite number of terms of S to previous terms of S. That is, there exists a k_0 in the domain of S such that $S(k)$, for $k > k_0$, is expressed in terms of some (possibly all) of the terms of the sequence preceding $S(k)$. The terms, not defined by the formula are said to form the initial conditions (or boundary conditions, or basis) of the sequence.

Note:

The sequence can be defined by the basis and the recurrence relation.

Unit-II

Mathematical induction

Worked example

Prove that for every integer n and every integer $r \le n$, [Ex for dichotomy]

$$^{n}C_r = {}^{(n-1)}C_r + {}^{(n-1)}C_{r-1}$$

Proof:- Let S be a subset of $\{1, 2, \dots, n\}$ of order r.

Then either $n \in S$ or $n \notin S$.

This is our dichotomy.

If $n \notin S$, then S is actually a subset of $\{1, 2, \dots, n-1\}$.

Clearly there are $^{(n-1)}C_r$ subsets of $\{1, 2, \dots, n-1\}$, each of order r, which do not contain n.

If $n \in S$, let $S' = S - \{n\}$ be the set obtained by omitting the element n from the set S.

Then S' is a subset of $\{1, 2, \dots, n-1\}$ of order $r-1$.

There are $^{(n-1)}C_{r-1}$ subsets each of order $(r-1)$ which do not contain n.

With each of these subsets, we can include the element n to obtain $^{(n-1)}C_{r-1}$ subsets of $\{1, 2, \dots, n\}$, each of order r, which contain n.

Hence altogether, there are $^{(n-1)}C_r + {}^{(n-1)}C_{r-1}$ subsets of order r.

This number must be equal to $^{n}C_r$, the number of subsets of order r.

$$\therefore {}^{n}C_r = {}^{(n-1)}C_r + {}^{(n-1)}C_{r-1}$$

equations of higher degree. These eqns can be solved by removing linear factors (got by trial and error). The following rule will be useful in some cases.

If a characteristic polynomial has integral roots then the roots will be factors of the independent term of the polynomial. In such cases the trial and error method can be applied to factors of the independent terms first

Example. 1

Solve the following recurrence relation:

$S(K) - 10\,S(K-1) + 9\,S(K-2) = 0, \quad S(0) = 3, \quad S(1) = 11.$

Sln:

Step 1: The characteristic equation is

$$a^2 - 10a + 9 = 0.$$

Step 2: Its roots are 1, 9. (This can be got by factorization of $a^2 - 10a + 9$ or using the formula $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ for roots of a quadratic equation).

Step 3: As the roots are distinct,

$$S(K) = b_1 \cdot 1^K + b_2 \cdot 9^K = b_1 + b_2 \cdot 9^K.$$

Step 4:

$$3 = S(0) = b_1 + b_2 \cdot 9^0 = b_1 + b_2$$

$$11 = S(1) = b_1 + b_2 \cdot 9^1 = b_1 + 9b_2$$

$b_1 + b_2 = 3$

$\underline{\overset{(-)}{b_1} \overset{(-)}{+} 9b_2 \overset{(-)}{=} 11}$

$-8b_2 = -8$

$b_2 = 1$

$b_1 + 1 = 3$

$b_1 = 3 - 1 = 2$

Solving these equations, we get $b_2 = 1$, $b_1 = 2$.

Hence $S(K) = 2 + 9^K$.

Defn 4

A recurrence relation on a sequence S is a linear recurrence relation with constant coefficients if it is of the form

$$S(K)+C_1 S(K-1)+\ldots+C_n S(K-n)=f(K), K\geq n$$

where $c_1, c_2, \ldots, c_n$ are numbers and f is a function defined for $K\geq n$. Also if $c_n \neq 0$ then the relation is said to be of order n.

Note:

A linear recurrence relation with constant coefficient is simply called a linear relation.

Defn: 5

An nth order linear relation is a homogeneous relation if $f(K)=0$ for all K.

Defn: 6

For a recurrence relation

$S(K)+C_1 S(K-1)+\ldots+C_n S(K-n)=f(K)$, the associated homogeneous relation is

$S(K)+C_1 S(K-1)+\ldots+C_n S(K-n)=0$

Example 6

consider the recurrence relations

i) $D(K)-3D(K-1)=0$

ii) $C(K)-5C(K-1)+6C(K-2)=2K-7$

iii) $S(K)-4S(K-1)-11S(K-2)+30S(K-3)=4^K$

iv) $T(K)=T(\lfloor K/2\rfloor)+5, K\geq 0$ where $\lfloor K/2\rfloor$ is the integral part of $K/2$

soln:

(i) is a homogeneous relation of order 1.

(ii) is a linear relation of order 2 but not homogeneous.

(iii) is a linear, non-homogeneous relation

① − ③ gives $y_n - 4y_{n-1} = B4^n$ — ④

Using ④, $y_{n-1} - 4y_{n-2} = B.4^{n-1}$ — ⑤

From ④ and ⑤ we get

$$y_n - 4y_{n-1} = 4(y_{n-1} - 4y_{n-2})$$

So the required recurrence relation is

$$y_n - 8y_{n-1} + 16y_{n-2} = 0.$$

W.E.3

Find the recurrence relation for the Fibonacci sequence

Soln:

We know that the Fibonacci sequence is defined by $F_n = F_{n-1} + F_{n-2}$.

Hence the recurrence relation for the Fibonacci sequence is $F_n - F_{n-1} - F_{n-2} = 0$ (or) $F(n) - F(n-1) - F(n-2) = 0$.

W.E.4

For the sequence defined by $A(k) = k^2 - k$, $k \geq 0$, obtain the recurrence relation if A is a sequence of integers.

Soln:

$$A(K) = K^2 - K$$

$$\therefore A(K-1) = (K-1)^2 - (K-1)$$

Hence $A(K) - A(K-1) = K^2 - (K-1)^2 - [K - (K-1)]$.

$$A(K) - A(K-1) = 2K - 2.$$

Similarly $A(K-1) - A(K-2) = 2(K-1) - 2 = 2K - 4$

So $[A(K) - A(K-1)] - [A(K-1) - A(K-2)] = 2$

ie) $A(K) - 2A(K-1) - A(K-2) - 4 = 0$ is the recurrence relation for the sequence $A(K)$.

$\therefore$ $a^{k+1} - b^{k-1}$ is divisible by $(a-b)$.

ie., if $p(k)$ is true, $p(k+1)$ is also true.

$\therefore$ By the principle of mathematical induction, $p(n)$ is true for all $n \in N$.

W.E. 3

Prove by mathematical induction that $2^n > n$ for all $n \in N$.

Soln:

Let $p(n) : 2^n - n > 0$

put $n = 1$;

$p(1) = 2^1 - 1 = 2 - 1 = 1 > 0$

So $p(1)$ is true.

Let us assume that $p(k)$ is true.

Here k is a positive integer

ie., $2^k - k$ is positive

Let $2^k - k = m$ — (1)

To prove that $p(k+1)$ also is positive,

consider $2^{k+1} - (k+1)$

Now $2^{k+1} - (k+1) = 2 \cdot 2^k - k - 1$

$= 2 \cdot (k+m) - k - 1$ Substituting for 2^k from (1)

$= k + 2m - 1$

$=$ positive number ($\because$ m is positive)

ie., if $p(k)$ is true, $p(k+1)$ is also true

So by the principle of mathematical induction, $p(n)$ is true.

ie., $2^n - n > 0$

So $2^n > n$ for all $n \in N$.

Solving the eqns,

$$b_1 + b_2 = 4$$
$$2b_1 + 5b_2 = 17,$$

we get, $b_2 = 3$, $b_1 = 1$

Hence $f(n) = 1.2^n + 3.5^n = 2^n + 3\,5^n$

W.E.3 Solve the recurrence relation

$$S(K) - 4S(K-1) - 11S(K-2) + 30\,S(K-3) = 0,$$
$$S(0) = 0,\quad S(1) = -35,\quad S(2) = -85.$$

Soln: The characteristic equation is

$$a^3 - 4a^2 - 11a + 30 = 0$$

As it is a cubic equation, we need to separate a linear factor first.

We check whether the factors of 30, i.e., $\pm 1, \pm 2, \pm 3, \pm 5, \pm 10, \pm 15$ are roots.

± 1 are not roots of the characteristic eqn.

But $a^3 - 4a^2 - 11a + 30 = 0$ is satisfied when $a = 2$.

Hence 2 is a root and $a-2$ is a factor of the characteristic polynomial $a^3 - 4a^2 - 11a + 30$.

By synthetic division,

2	1	-4	-11	30
		2	-4	-30
	1	-2	-15	0

$a^2 - 2a - 15$ is a factor

Roots of $a^2 - 2a - 15 = 0$ are -3 and 5

Hence the roots of the characteristic eqn are $2, -3$ and 5.

Thus $S(K) = b_1 \cdot 2^K + b_2 \cdot (-3)^K + b_3 \cdot 5^K$

As $S(0) = 0$, ~~S(2) = -85~~ $S(1) = -35$ and $S(2) = -85$,

we get

$$0 = S(0) = b_1 \cdot 2^0 + b_2 (-3)^0 + b_3 (5)^0 = b_1 + b_2 + b_3$$

Defn 1 (Recursive defn of a polynomial)

The set $S[X]$ of all polynomials whose coefficients are elements of S is defined (recursively) as follows:

1) any element of S is a polynomial of degree zero.

2) $p(x)x + a$ is a polynomial of degree n when $p(x)$ is a polynomial of degree $n-1$ and $a \in S$.

3) Only those expression obtained by using (1) and (2) finite number of times are polynomials.

Example. 1

consider $F(x) = 5x^3 + 4x^2 + 3x + 2$.

This can be defined using recursive defn as follows:

$F(x) = 5x^3 + 4x^2 + 3x + 2$
$= (5x^2 + 4x + 3)x + 2$
$= ((5x + 4)x + 3)x + 2$

$$F(x) = ((((5)x + 4)x + 3)x + 2)$$

$= ((((5)x+4)x+3)x+2)$

Note:

A polynomial defined recursively is said to be in telescopic form.

The method of writing a polynomial in recursive form (telescoping form) is called Horner's method.

Note:

In computer, multiplication is performed as repeated addition. (ie., $mn = m + m + \ldots + m$ n times)

Hence a reduction in the number of multiplications saves more computer time than reduction in the number of additions.

$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6}$$

$$= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6}$$

$$= \frac{(k+1)(2k^2+7k+6)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$\therefore$ $p(k+1)$ is true

Thus, if $p(k)$ is true, $p(k+1)$ is also true

$\therefore$ By the principle of mathematical induction

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \text{ for all } n \geq 1.$$

W.E:2

Show that $a^n - b^n$ is divisible by $(a-b)$ for all $n \in N$.

Soln:-

Let $p(n) = a^n - b^n$ is divisible by $(a-b)$

put $n=1$.

$p(1) = a^1 - b^1 = a-b$ is divisible by $(a-b)$

$\therefore$ $p(1)$ is true.

Let us assume that $p(k)$ is true ie, $a^k - b^k$ is divisible by $(a-b)$.

Let $a^k - b^k = c(a-b)$

So $a^k = b^k + c(a-b)$ — ①

$$a^{k+1} - b^{k+1} = a^k a - b^k . b$$

$$= a[b^k + c(a-b)] - b^k . b$$

Substituting for a^k from ①

$$= ab^k + ac(a-b) - b^k . b$$

$$= b^k(a-b) + ac(a-b)$$

$$= (a-b)(b^k + ac)$$

Example 2

The Fibonacci sequence is defined by the relation $F_n = F_{n-1} + F_{n-2}$, $F_0 = 1$, $F_1 = 1$ are the initial conditions on the basis. Now any F_n, $(n \geq 2)$ can be obtained by using the basis and repeated application of the recurrence relation.

Example 3

Find the recurrence relation and basis (initial condition) for the sequence $(1, 3, 3^2, \ldots)$

soln:

Take $\{0, 1, 2, \ldots\}$ as the domain of the sequence

Then $a_0 = 1$, $a_1 = 3$, $a_2 = 3^2$.

Hence $a_n = 3a^{n-1}$ is the recurrence relation.

$a_0 = 1$ is the basis.

Example 4

consider D, defined by $D(k) = 5 \cdot 2^k$, $k \geq 0$.

Find the recurrence relation on D.

soln:

For $k \geq 1$, $D(k) = 5\ 2^k$ and $D(k-1) = 5\ 2^{k-1}$

$$\text{So} \quad \frac{D(k)}{D(k-1)} = 2$$

Hence the recurrence relation is $D(k) - 2D(k-1) = 0$, $k \geq 1$

The initial condition is $D(0) = 5$.

Defn: 3

A recurrence relation on a sequence S is of order k if $T(n)$ is expressed as a function of $T(n-1), \ldots, T(n-k)$ and $T(n-k)$ appears in the function.

Example 5

The relation $T(n) = 2(T(n-1))^2 - nT(n-3)$ is a recurrence relation of order 3.

Prove that $\sqrt{2}$ is irrational.

Proof:-

Let us assume that $\sqrt{2}$ is rational (ie. not irrational)

Then $\sqrt{2} = \frac{p}{q}$ where p and q are integers having no common factor.

Then $2 = \frac{p^2}{q^2}$ or $p^2 = 2q^2$

So p^2 is even.

This implies that p is even, since the square of an odd number is odd.

So $p = 2n$ for some integer n.

Then $p^2 = 4n^2$ ie., $2q^2 = 4n^2$ or $q^2 = 2n^2$

Thus q^2 is even.

So q is even.

ie., $q = 2m$ for some integer m

We have now arrived at the result that both p and q are even and have a common factor 2.

This is contrary to our assumption that p and q have no common factor.

Hence our assumption that $\sqrt{2}$ is rational is wrong.

So $\sqrt{2}$ is irrational.

Principle of mathematical induction

Let $p(n)$ be a statement or proposition involving the natural number n.

Then

a) if $p(1)$ is true and

b) if $p(k+1)$ is true on the assumption that $p(k)$ is true.

p is either a prime or a product of prime.
∴ Also, q is either a prime or a product of prime
consequently, pq is a product of prime

Recurrence relations and generating functions

~~Recurrence~~

Example : 1
The Fibonacci numbers can be defined as follows:

$F_0 = 1, \; F_1 = 1, \; F_n = F_{n-1} + F_{n-2}$

Example : 2
^nC_r can be defined as follows:

$^nC_0 = 1, \; ^nC_n = 1,$

$^nC_r = {}^{(n-1)}C_r + {}^{(n-1)}C_{r-1} \quad n > r > 0$

Example : 3
Ackermann's function can be defined as follows:

$A(0, y) = y + 1$

$A(x+1, 0) = A(x, 1)$

$A(x+1, y+1) = A(x, A(x+1, y))$

Note:
The student may verify that $A(4, 0) = 13$

Example:
$F_0 = F_1 = 1$ is the basis for Fibonacci numbers.

$^nC_0 = 1, \; ^nC_n = 1$ is the basis for ^nC_r etc.

Recursion, Iteration and induction

Example : 4
calculate F_4 of the Fibonacci numbers using i) recursion ii) iteration.

So by the principle of mathematical induction $p(n)$ is true for all $n \geq 1$.

W.E:5

Suppose we have stamps of two different denominations, Rs 3 and Rs. 5, show that it is possible to make up exactly any postage of n rupees, where $n \geq 8$ is an integer, using stamps of these two denominations

Soln: Let $p(n)$ be the statement

$p(n)$: It is possible to make up exactly a postage of Rs n using Rs 3 and Rs 5 stamps.

Clearly $p(8)$ is true as one Rs. 3 stamp and one Rs 5 are enough to make up a postage of Rs 8.

Now assume that $p(k)$ is true for some $k \geq 8$

Suppose we make up a postage of Rs k using atleast one Rs. 5 stamp.

Replacing a Rs. 5 stamp by two Rs 3 stamps will yield a way to make up a postage of Rs $(k+1)$. ~~using Rs 3 stamps only.~~

On the other hand, suppose we make up a postage of Rs k using Rs 3 stamps only

Since $k \geq 8$, there must be atleast three Rs 3 stamps.

Replacing three Rs 3 stamps by two Rs 5 stamps will yield a way to make up a postage of Rs $(k+1)$.

Solution of finite order homogeneous (linear) relations

Example 1

Find a closed form expression for the recurrence relation

$$S(K) - 2S(K-1) = 0, \quad S(0) = 5$$

Soln:

$$S(K) = 2S(K-1).$$

As $S(0) = 5$, $S(1) = 2S(0) = 2(5)$

We can prove by induction that $S(K) = 5\,2^K$ for all $K \geq 0$.

Hence $S(K) = 5 \cdot 2^K$ is a closed form expression for S.

Defn 1

The process of finding a closed form expression for the terms of a sequence from its recurrence relation is called solving the relation.

Note:

In example 1, we have solved the relation $S(K) = 2S(K-1)$, $S(0) = 5$.

Defn 2

The characteristic equation of the homogeneous relation of order n.

$$S(K) + c_1 S(K-1) + \dots + c_n S(K-n) = 0$$

is the nth degree equation.

$$a^n + c_1 a^{n-1} + c_2 a^{n-2} + \dots + c_{n-1} a + c_n = 0$$

The left-hand side of this equation is called the characteristic polynomial.

Example 1

Find the characteristic equation of

$J(k) - 4J(k-1) + 4J(k-2) = 0$. order = 2

$a^2 - 4a + 4 = 0$.

Soln:

The characteristic equation is

$$a^2 - 4a + 4 = 0.$$

Algorithm for solving n^{th} order homogeneous recurrence relation

Step 1: Write the characteristic equation of the given homogeneous relation.

Step 2: Find all the roots of the characteristic equation. (They are called characteristic roots)

Step 3: (i) If the roots $a_1, a_2, \ldots, a_n$ are distinct then the general solution of the recurrence relation is

$$S(k) = b_1 a_1^k + b_2 a_2^k + \ldots + b_n a_n^k \quad \text{--- (1)}$$

(ii) If the root a_j is repeated p times, $b_j a_j^k$ is replaced by

$$(c_0 + c_1 k + \ldots + c_{p-1} k^{p-1}) a_j^k$$

(In particular, if a_j is a double root then $b_j a_j^k$ is replaced by $(c_0 + c_1 k) a_j^k$)

Step 4: If n initial conditions are given, obtain n linear eqns in n unknowns $b_1, b_2, \ldots, b_n$ (got in (1)) by replacing LHS of (1) by the given values. If possible, solve these equations.

Note:

We have a general method for solving quadratic equations. But is difficult to solve

Worked examples → we have to find upto general solution

W.E.1

Solve $a(k) - 8a(k-1) + 16a(k-2) = 0$ where

$a(2) = 16$, $a(3) = 80$

soln:-

The characteristic equation is

$$a^2 - 8a + 16 = 0$$

Its roots are $4, 4$.

As the roots are repeated,

$$a(k) = (c_0 + c_1 k) 4^k$$

$$16 = a(2) = (c_0 + 2c_1) 4^2 = 16(c_0 + 2c_1) = 16c_0 + 32c_1$$

$$80 = a(3) = (c_0 + 3c_1) 4^3 = 64c_0 + 192c_1$$

That is, $64c_0 + 192c_1 = 80$ — (1)

$16c_0 + 32c_1 = 16$ — (2)

(1) $- 4 \times$ (2) gives $(192 - 128)c_1 = 80 - 64$.

So $c_1 = 1/4$, $c_0 = 1 - 2c_1 = 1/2$.

Hence $a(k) = \left(\frac{1}{2} + \frac{1}{4}k\right) 4^k$.

W.E.2

Find $f(n)$ if $f(n) = 7f(n-1) - 10f(n-2)$ given that $f(0) = 4$ and $f(1) = 17$.

If initial conditions are given we have to find general soln

soln:-

The relation is

$$f(n) - 7f(n-1) - 10f(n-2) = 0$$

Hence its characteristic equation is

$$a^2 - 7a + 10 = 0$$

Its roots are $2, 5$.

So, $f(n) = b_1 2^n + b_2 . 5^n$

$$4 = f(0) = b_1 . 2^0 + b_2 5^0 = b_1 + b_2$$

$$17 = f(1) = b_1 2^1 + b_2 5^1 = 2b_1 + 5b_2$$

Worked example

W.E.1 Let $p(x) = x^5 + 3x^4 - 15x^3 + x - 10$ in telescopic form.

Soln:- $p(x) = (((((1)x+3)x-15)x+0)x+1)x-10$

W.E.2 Use Horner's method to write $p(x) = x^4+2x^3+3x^2+4x$ in telescoping form. Also mention the number of multiplications and additions / subtractions involved in telescopic form. compare it with usual defn.

Soln:- $p(x) = ((((1)x+2)x+3)x+4)x+0$

We require 4 multiplications and 4 additions

In the usual form we require 7 multiplications and 4 additions (for example

$$p(2) = 1(2^4) + 2(2^3) + 3(2^2) + 4(2) + 0$$

we multiply $4(2)$ (once), 2^2 (once), $3(2^2)$ (once), $2^3 = 2(2^2)$ (once), $2(2^3)$ (once), $2(2^3)$ (once) and $1(2^4)$ (once).

Thus we require 7 multiplications.

Thus by writing a polynomial in telescopic form the number of multiplication is reduced from 7 to 4.

Recurrence relations

Defn: A sequence of integers (also called a discrete function) is a function from N into z (where N is the set of all natural numbers and z is the set of all integers).

are constructed from A have the property p.

3) The elements constructed as in (1) and (2) are the only elements satisfying property p.

programming languages and recursions

A procedure or subroutine is a tool in a programming language which enables a programmer to express just once an algorithm which is used in many places while executing the programme. A procedure that contains a procedure call to itself is known as a recursive procedure.

Recursive procedures are applicable in most of the programming languages like ALGOL etc., and some recent versions of FORTRAN. In some very early versions of FORTRAN, recursive procedure were not allowed.

When a recursive procedure is to be implemented using a computer language, a) each time a procedure calls itself, it must be nearer to a solution.

b) there must be a decision criterion for stopping the computation (this applies to algorithms in general).

polynomials and their evaluations

$$a_0 + a_1 x + a_2 x^2 \text{ as } a_0 + x(a_1 + x(a_2))$$

The advantage is that this way of writing reduces the number of multiplications from three to two.

Thus if $p(k)$ is true for some $k \geq 8$, then $p(k+1)$ is also true.

Thus by the principle of mathematical induction, $p(n)$ is true for all $n \geq 8$.

Principle of strong mathematical induction:

For a given statement involving a natural number n, if we can show that

1 : The statement is true for $n = n_0$ and

2 : The statement is true for $n = k+1$, assuming that the statement is true for all $n_0 \leq n \leq k$,

then we can conclude that the statement is true for all natural numbers $n \geq n_0$.

Example

Any positive integers $n \geq 2$ is either a prime or a product of primes.

To prove this we use the principle of strong mathematical induction

1) Basis of induction : For $n = 2$, since 2 is a prime, the statement is true.

2) Induction step : Assume that the statement is true for any integer n, $2 \leq n \leq k$.

For the integer $k+1$, if $k+1$ is a prime, the statement is true.

If $k+1$ is not a prime, then $k+1$ can be written as pq, for some $2 \leq p \leq k$ and $2 \leq q \leq k$.

According to the induction hypothesis,

We conclude that a statement $p(n)$ is true for all natural numbers n.

Hence to prove that a statement $p(n)$ is true for all natural numbers, we must go through two steps:

First : we must prove that $p(1)$ is true

Second : Assuming that $p(k)$ is true, we must prove that $p(k+1)$ is also true.

The first step is called the basis step of the proof.

The second step is called the induction step of the proof.

Worked examples

W.E.1. prove by induction method, for $n \geq 1$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

Soln:- Let $p(n)$ denote the statement

$$p(n): 1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

Let $n=1$, L.H.S of $p(1) = 1^2 = 1$

$$\text{R.H.S of } p(1) = \frac{1(1+1)(2+1)}{6} = \frac{1\times2\times3}{6} = 1 = \text{L.H.S of } p(1)$$

$\therefore$ $p(1)$ is true

Let us assume that $p(k)$ is true

ie., $p(k) = 1^2+2^2+\cdots+k^2 = \dfrac{k(k+1)(2k+1)}{6}$ is true.

We claim that $p(k+1): 1^2+2^2+\cdots+(k+1)^2 = \dfrac{(k+1)(k+2)(2k+3)}{6}$ is true.

$$\text{Now } 1^2+2^2+\cdots+k^2+(k+1)^2 = (1^2+2^2+\cdots+k^2)+(k+1)^2$$
$$= \frac{k(k+1)(2k+1)}{6}+(k+1)^2 \quad [\because p(k) \text{ is true}]$$

soln:
i) $F_4 = F_3 + F_2 = (F_1+F_2)+F_2 = (F_1 + (F_0+F_1)) + F_0 + F_1$

$= (1+(1+1))+1+1$

$= 5$

ii) $F_2 = F_0 + F_1 = 1+1 = 2$

$F_3 = F_1 + F_2 = 1+2 = 3$

$F_4 = F_2 + F_3 = 2+3 = 5.$

Recursion and iteration

i) Usually iterative computations are faster than recursive computations.

ii) But recursive definition gives more insight into the interpretation of the given function

iii) A recursive programme (programme involving recursion) is more difficult to debug than a corresponding iterative programme.

iv) In general there are many problems involving recursion, for which iterative solutions either do not exist or are not easily found.

Recursion and induction

An inductive definition of a property or set P (having the property) is given as follows:

1) Given a finite set A where elements have the property P.

2) The elements of a set B, all of which

W.E: 4

If $A_1, A_2, \ldots, A_n$ are any n sets, show by mathematical induction that

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i}$$ (Extended De Morgan's law)

($\bar{A}$ denotes complement of A)

soln:-

Let $p(n)$ be the statement that the equality holds for n sets.

Basis step: $p(1)$ is the statement that $\overline{A_1} = \overline{A_1}$ which is obviously true.

Induction step: suppose $p(k)$ is true for any k sets

ie., $\overline{A_1 \cup A_2 \cup \ldots \cup A_k} = \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}$ for any k sets $A_1, A_2, \ldots, A_k$.

Let $A_1, A_2, \ldots, A_{k+1}$ be any $k+1$ sets.

Let $B = A_1 \cup A_2 \cup \ldots A_k$

Then $\bar{B} = \overline{A_1 \cup A_2 \cup \ldots \cup A_k} = \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}$

L.H.S of $p(k+1) = \overline{A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1}}$

$= \overline{(A_1 \cup A_2 \cup \ldots \cup A_k) \cup A_{k+1}}$ (associative property of union)

$= \overline{B \cup A_{k+1}}$

$= \bar{B} \cap \overline{A}_{k+1}$ (by DeMorgan's law for two sets)

$= (\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}) \cap \overline{A}_{k+1}$

$= \left(\bigcap_{j=1}^{k} \overline{A_j}\right) \cap \overline{A}_{k+1}$

$= \bigcap_{j=1}^{k+1} \overline{A_j}$ = R.H.S of $p(k+1)$

ie., if $p(k)$ is true, $p(k+1)$ is also true.

$-35 = S(1) = b_1 \cdot 2^1 + b_2(-3)^1 + b_3(5)^1 = 2b_1 - 3b_2 + 5b_3.$

$-85 = S(2) = b_1 \cdot 2^2 + b_2(-3)^2 + b_3(5)^2 = 4b_1 + 9b_2 + 25b_3$

So we have to solve the eqns,

$$b_1 + b_2 + b_3 = 0 \quad — ①$$

$$2b_1 - 3b_2 + 5b_3 = -35 \quad — ②$$

$$4b_1 + 9b_2 + 25b_3 = -85 \quad — ③$$

~~2×① − ② gives,~~ $\cancel{5b_2 - 3b_3 = 35}$ ~~— ④~~

~~2×② − ③ gives,~~ $\cancel{-15b_2 - 15b_3 = 15}$

$\cancel{b_2 + b_3 = -1}$

$2 \times ① - ② \Rightarrow \quad 2b_1 + 2b_2 + 2b_3 = 0$

$\qquad 2b_1 - 3b_2 + 5b_3 = -35$

$\qquad (-) \quad (+) \quad (-) \quad (+)$

$$5b_2 - 3b_3 = 35 \quad — ④$$

$2 \times ② - ③ \Rightarrow \quad 4b_1 - 6b_2 + 10b_3 = -70$

$\qquad 4b_1 + 9b_2 + 25b_3 = -85$

$\qquad (-) \quad (-) \quad (-) \quad (+)$

$$-15b_2 - 15b_3 = 15$$

$$-b_2 - b_3 = 1$$

$$b_2 + b_3 = -1 \quad — ⑤$$

Solving ④ & ⑤, we get

$④ \Rightarrow \quad 5b_2 - 3b_3 = 35$

$3 \times ⑤ \Rightarrow \quad 3b_2 + 3b_3 = -3$

$$8b_2 = 32$$

$$b_2 = \frac{32}{8}$$

$$b_2 = 4.$$

$⑤ \Rightarrow \quad 4 + b_3 = -1$

$$b_3 = -1 - 4$$

$$b_3 = -5$$

of order 3.

(iv) is a recurrence relation of infinite order. For given any positive integer n, we can find K such that $T(K) = T(K-n)+5$. Just take $K=2n$, then $T(2n) = T(\lfloor \frac{2n}{2} \rfloor)+5 = T(n)+5 = T(2n-n)+5$.

So it is not possible to find a fixed positive integer n such that a relation of the type

$$T(K) + c_1 T(K-1) + \dots + c_n T(K-1) = f(K)$$

holds for all $K \geq n$.

Worked examples

W.E.1 Find the recurrence relation satisfying $y_n = A(3)^n + B(-4)^n$.

Soln:
$$y_n = A\cdot 3^n + B(-4)^n \quad \text{--- (1)}$$
$$y_{n-1} = A\, 3^{n-1} + B(-4)^{n-1} \quad \text{--- (2)}$$
$$3y_{n-1} = A\cdot 3^n + B(3)(-4)^{n-1} \quad \text{--- (3)}$$

(1) − (3) gives $y_n - 3y_{n-1} = B(-4)^{n-1}(-7)$ — (4)

From (4), $y_{n-1} - 3y_{n-2} = B(-4)^{n-2}(-7)$ — (5)

From (4) and (5), $y_n - 3y_{n-1} = -4(y_{n-1} - 3y_{n-2})$

That is, $y_n + y_{n-1} - 12y_{n-2} = 0$, which is the required recurrence relation.

W.E.2 Find the recurrence relation satisfying $y_n = (A+Bn)4^n$.

Soln:
$$y_n = A\cdot 4^n + Bn4^n \quad \text{--- (1)}$$
$$y_{n-1} = A\cdot 4^{n-1} + B(n-1)4^{n-1} \quad \text{--- (2)}$$

From (2), $4y_{n-1} = A\cdot 4^n + B(n-1)\cdot 4^n$ — (3)

Using ①, we get

$$b_1 + 4 - 5 = 0$$
$$b_1 - 1 = 0$$
$$b_1 = 1$$

So $S(k) = 1.2^k + 4.(-3)^k - 5.5^k$.

W.E.4 Write the recurrence relation for Fibonacci numbers and solve it.

Soln: The recurrence relation is

$$F(n) - F(n-1) - F(n-2) = 0$$

The characteristic eqn is

$$a^2 - a - 1 = 0$$

Its roots are

$$\frac{1+\sqrt{5}}{2}, \quad \frac{1-\sqrt{5}}{2}$$

Hence $F(n) = b_1\left(\frac{1+\sqrt{5}}{2}\right)^n + b_2\left(\frac{1-\sqrt{5}}{2}\right)^n$

Also $1 = F(0) = b_1 + b_2$ — ①

$1 = F(1) = b_1\left(\frac{1+\sqrt{5}}{2}\right) + b_2\left(\frac{1-\sqrt{5}}{2}\right)$ — ②

As $b_2 = 1 - b_1$, ② can be written as

$$b_1(1+\sqrt{5}) + (1-\sqrt{5})(1-b_1) = 2$$

ie., $(1+\sqrt{5} - 1+\sqrt{5})b_1 = 1+\sqrt{5}$

So $b_1 = \frac{\sqrt{5}+1}{2\sqrt{5}}$ and $b_2 = 1 - \frac{\sqrt{5}+1}{2\sqrt{5}} = \frac{\sqrt{5}-1}{2\sqrt{5}}$

Hence the recurrence relation for the Fibonacci sequence is

$$F(n) = \left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

6) $s(n) = \frac{1}{n!}$

soln:-

$$G(S;z) = \sum_{n=0}^{\infty} \frac{1}{n!} z^n$$

$$= 1 + \frac{z}{1!} + \frac{z^2}{2!} + \cdots$$

$$G(S;z) = e^z$$

7) $S(K) = \begin{cases} nC_K & \text{for} \quad 0 \le K \le n \\ 0 & \text{for} \quad K > 0 \end{cases}$

soln:-

$$G(S;z) = \sum_{K=0}^{n} nC_K z^K$$

$$= nC_0 + nC_1 z + nC_2 z^2 + \cdots$$

$$G(S;z) = (1+z)^n$$

8) If $p(K) - 6p(K-1) + 5p(K-2) = 0$, $p(0) = 2$, $p(1) = 2$.
what is the generating function of P?

Let $G(P;z)$ be the generating function for P then $G(P;z) = \sum_{n=0}^{\infty} p(n) \cdot z^n$.

We replace the running index k by n.

$$p(n) - 6p(n-1) + 5p(n-2) = 0, \quad n \ge 2$$

Hence,

$$0 = \sum_{n=2}^{\infty} [p(n) - 6p(n-1) + 5p(n-2)] z^n$$

$$= \sum_{n=2}^{\infty} p(n) z^n - 6 \sum_{n=2}^{\infty} p(n-1) z^n + 5 \sum_{n=2}^{\infty} p(n-2) z^n$$

$$= \sum_{n=2}^{\infty} p(n) z^n - 6z \sum_{n=2}^{\infty} p(n-1) z^{n-1} + 5z^2 \sum_{n=2}^{\infty} p(n-2) z^{n-2}$$

$$= [p(2)z^2 + p(3)z^3 + \cdots + p(1)z + p(0) - p(1)z - p(0)]$$

$$-6z[p(1)z + p(2)z^2 + \cdots + p(0) - p(0)] +$$

$$5z^2[p(0) + p(1)z + p(2)z^2 + \cdots]$$

$$= [G(P;z) - 2z - 2] - 6z[G(P;z) - 2] + 5z^2[G(P;z)]$$

Unit - III

sdve - 10m

Solution of non-homogeneous relations.

Problems :

1) Solve $T(K) - 7T(K-1) + 10T(K-2) = 6+8K$ with $T(0)=1$ and $T(1) = 2$.

Soln:-

- Homogeneous equation

The characteristic equation is

$$a^2 - 7a + 10 = 0$$

$d_1 K \quad T(K-2) \quad (K-1)$

$\therefore$ The roots are $2, 5$.

So the general solution is

$$T(K) = b_1 2^K + b_2 5^K$$

particular solution

Take $d_0 + d_1 K$ for $6+8K$

replace $T(K)$, $T(K-1)$, $T(K-2)$ by $d_0 + d_1 K$, $d_0 + d_1(K-1)$, $d_0 + d_1(K-2)$ respectively we get,

$$d_0 + d_1 K - 7(d_0 + d_1(K-1)) + 10(d_0 + d_1(K-2)) = 6+8K$$

ie) $4d_0 - 13d_1 + 4d_1 K = 6+8K$

Equating the corresponding coefficients we get

$$4d_0 - 13d_1 = 6 \ ; \ 4d_1 = 8$$

$$d_1 = 2 \ ; \ 4d_0 - 26 = 6$$

$$4d_0 = 32$$

$$d_0 = 8$$

Hence particular solution is $8+2K$ and the general solution is

$$T(K) = b_1 \cdot 2^K + b_2 \cdot 5^K + 8 + 2K.$$

$$1 = T(0) = b_1 \cdot 2^0 + b_2 \cdot 5^0 + 8 + 0 = b_1 + b_2 + 8$$

$$2 = T(1) = b_1 2^1 + b_2 \cdot 5^1 + 8 + 2 = 2b_1 + 5b_2 + 10$$

ie) $b_1 + b_2 = -7 \rightarrow (1)$

$2b_1 + 5b_2 = -8 \rightarrow (2)$

$(1) \times 2 \Rightarrow 2b_1 + 2b_2 = -14$

$\underline{(-)\ 2b_1 \overset{(-)}{+} 5b_2 = \overset{(+)}{-} 8}$

$-3b_2 = -6$

Eg: 3 (Worst case analysis of binary search algorithm)

In binary search method we divide the file into two halves and search.

Assume that it takes one unit time for locating the middle of the file.

Let $T(n)$ denote the time (worst time) required for searching a file with n records.

Then $T(n) = 1 + T([n/2])$ where $[n/2]$ is the integral part of $n/2$. ($[n/2]$ denotes the size of half the file).

We assume that $T(0) = 0$.

The recurrence relation can be solved easily when $n = 2^k$, $k \geq 0$.

$$T(2^k) = 1 + T([2^k/2]) = 1 + T(2^{k-1})$$

Repeating the calculation, we get

$$T(2^k) = k+1$$

When n is not of the form 2^k we proceed as follows:

Let r be a non-negative integer such that $2^{r-1} \leq n < 2^r$. Then

$N = (a_1 a_2 \ldots a_r)_2$, where R.H.S gives the binary representation of n.

Then $[n/2] = a_1 a_2 \ldots a_{r-1}$. Therefore

$$T(n) = T(a_1 a_2 \ldots a_r) = 1 + T(a_1 a_2 \ldots a_{r-1})$$
$$= 1 + (1 + T(a_1 a_2 \ldots a_{r-2}))$$
$$\vdots$$
$$= (r-1) + T(a_1)$$
$$= (r-1) + T(1)$$

$$T(n) = r.$$

ii) successor function s defined by $s(x) = x+1$

iii) projection function U_i^n defined by
$U_i^n(x_1, x_2, \ldots, x_n) = x_i$

Note:
As $U_1^1(x) = x$ for every x in N, U_1^1 is simply the identity function on N.

Defn: 3
If $f_1, f_2, \ldots, f_k$ are partial functions of n variables and g is a partial function of k variables, then the composition of g with $f_1, f_2, \ldots, f_k$ is a partial function of n variables defined by $g(f_1(x_1, x_2, \ldots, x_n), f_2(x_1, x_2, \ldots, x_n), \ldots, f_k(x_1, x_2, \ldots, x_n))$.

Note:
The composition of g with a single function f, where both f, g are functions of a single variable reduces to the usual composition of two functions.

Eg: 2
Define $f_1(x) = 1+x$ and $g(x) = +\sqrt{x}$

Then $g(f(x)) = \cancel{\sqrt{1+x}}\, g(1+x) = \sqrt{1+x}$

Eg: 3
Let $f_1(x,y) = x+y$, $f_2(x,y) = 2x$, $f_3(x,y) = xy$ and $g(x,y,z) = x+y+z$.

$$g(f_1(x,y), f_2(x,y), f_3(x,y)) = g(x+y, 2x, xy)$$
$$= x+y+2x+xy.$$

Thus the composition of g with f_1, f_2, f_3 is given by a function h defined by
$h(x,y) = x+y+2x+xy$.

Then,

$$G(S;z) = \sum_{n=0}^{\infty} [S(n)] z^n$$

Now, $S(n) - S(n-1) - 2n + 2 = 0$, $n \geq 1$

So

$$\sum_{n=1}^{\infty} [S(n) - S(n-1) - 2n + 2] z^n = 0$$

Hence,

$$0 = \sum_{n=1}^{\infty} S(n) z^n - \sum_{n=1}^{\infty} S(n-1) z^n - 2\sum_{n=1}^{\infty} n z^n + 2\sum_{n=1}^{\infty} z^n$$

$$= [S(1)z + S(2)z^2 + \dots + S(0) - S(0)] - z\left[\sum_{n=1}^{\infty} S(n-1) z^{n-1}\right] - 2\sum_{n=1}^{\infty} n z^n + 2\sum_{n=1}^{\infty} z^n$$

$$= [S(1)z + S(2)z^2 + \dots + S(0) - S(0)] - \cancel{z\left[\sum_{n=1}^{\infty} S(n-1) z^{n-1}\right]}$$
$$z\left[\sum_{n=1}^{\infty} (S(n-1)) z^{n-1}\right] - 2\sum_{n=1}^{\infty} n z^n + 2\left[\sum_{n=0}^{\infty} z^n - 1\right]$$

$$= [S(1)z + S(2)z^2 + \dots + S(0) - S(0)] - z[S(0) + S(1)z + \dots] - 2[z + 2z^2 + \dots] + 2[1 + z + z^2 + z^3 + \dots - 1]$$

$$= [G(S;z) - S(0)] - z[G(S;z)] - 2z\left[\frac{1}{(1-z)^2}\right] + 2\left[\frac{1}{(1-z)} - 1\right]$$

$$= G(S;z) - 3 - zG(S;z) - 2z\left[\frac{1}{(1-z)^2}\right] + 2\left[\frac{1}{(1-z)} - 1\right]$$

$$= (1-z)\, G(S;z) - 3 - 2z\left[\frac{1}{(1-z)^2}\right] + 2\left[\frac{1}{(1-z)} - 1\right]$$

Rewriting we get

$$(1-z)\, G(S;z) = \frac{2z}{(1-z)^2} - \frac{2}{(1-z)} + 5$$

Hence,

$$G(S;z) = \frac{2z}{(1-z)^3} - \frac{2}{(1-z)^2} + \frac{5}{(1-z)}$$

Defn: Generating function

The generating function of a sequence $s_0, s_1, s_2, \ldots$ is the power series

$$G(s; z) = s_0 + s_1 z + s_2 z^2 + \cdots$$

Some common recurrence relations

~~1) Find T(27)~~

Soln:

Ex: 1)

$S(n) = n\, S(n-1)$, $n \geq 1$ and $S(0) = 1$.

Soln:- Given $S(n) = n \cdot S(n-1)$

$$S(1) = 1 \cdot S(0) = 1 \cdot 1 = 1!$$

$$S(2) = 2 \cdot S(1) = 2 \cdot 1 = 2!$$

$$S(3) = 3 \cdot S(2) = 3 \cdot 2 = 6!$$

$$\vdots$$

$$S(n) = n!$$

Eg: 2 $G(k) = 2^k\, G(k-1)$, $k \geq 0$, $G(0) = 1$.

Soln:

$$G(k) = 2^k\, G(k-1)$$

$$= 2^k \cdot 2^{k-1}\, G(k-2)$$

$$= 2^k \cdot 2^{k-1} \cdot 2^{k-2}\, G(k-3)$$

$$\cdots$$

$$= 2^k \cdot 2^{k-1} \cdots 2^1\, G(0)$$

$$= 2^{k + (k-1) + \cdots + 1}$$

$$= 2^{1+2+\cdots+k}$$

$$G(k) = 2^{\frac{k(k+1)}{2}}$$

Defn : 6 A total function f over N is primitive recursive if

a) It is one of the three initial functions or

b) It can be obtained by applying composition and recursion finite number of times to the set of initial functions.

Eg: 5 Show that $f_1(x,y) = x+y$, $x, y \in N$ is primitive recursive.

$2+(2+1) = (2+2)+1$

$2+3 = 4+1$

$5 = 5$

Soln: Now, $x+(y+1) = (x+y)+1$ — ①

Define $f_1(x,0) = x+y = x+0$

$= x = U_1^1(x)$

$f_1(x, y+1) = x+(y+1)$

$f_1(x, y+1) = S(U_3^3(x, y, f_1(x,y)))$

$= S(f_1(x,y))$

$= S(x+y)$ $\quad S(n) = n+1$

$= (x+y)+1$

Worked examples

W.E : 1 Show that $f(x,y) = x*y$ is a primitive recursive function.

Soln: $f(x,0) = x*0 = 0$ — ①

$f(x, y+1) = x*(y+1)$

$= x*y + x$ — ②

$f(x,0) = 0$

$= Z(x)$ — ③

$f(x, y+1) = f_1(U_3^3(x, y, f(x,y)), U_1^3(x, y, f(x,y)))$

$= f_1(f(x,y), x)$

$= f_1(x*y, x)$ $\quad [f_1(x,y) = x+y]$

$= x*y + x$ — ④

$$= G(P;z) - 2z - 2 - 6zG(P;z) + 12z + 5z^2G(P;z)$$

$$= (1-6z+5z^2)\,G(P;z) + 10z - 2$$

$$2 - 10z = (1-6z+5z^2)\,G(P;z)$$

$$G(P;z) = \frac{2-10z}{1-6z+5z^2}$$

4) Using the generating function solve the difference equation $y_{n+2} - y_{n+1} - 6y_n = 0$ given $y_1 = 1$, $y_0 = 2$ 10m

U.Q 10m.

Soln:- Let $G(Y;z)$ be the generating function of the sequence $\{y_n\}$

Then $G(Y;z) = \sum_{n=0}^{\infty} y_n z^n$

As $y_{n+2} - y_{n+1} - 6y_n = 0$, $n \geq 0$

$$\sum_{n=0}^{\infty} (y_{n+2} - y_{n+1} - 6y_n) z^n = 0$$

Hence,

$$0 = \sum_{n=0}^{\infty} y_{n+2} z^n - \sum_{n=0}^{\infty} y_{n+1} z^n - 6\sum_{n=0}^{\infty} y_n z^n$$

$$= \frac{1}{z^2}\left[\sum_{n=0}^{\infty} y_{n+2} z^{n+2}\right] - \frac{1}{z}\left[\sum_{n=0}^{\infty} y_{n+1} z^{n+1}\right] - 6G(Y;z)$$

$$= \frac{1}{z^2}\left[y_2 z^2 + y_3 z^3 + \cdots\right] - \frac{1}{z}\left[y_1 z^1 + y_2 z^2 + \cdots\right] - 6G(Y;z)$$

$$= \frac{1}{z^2}\left[y_2 z^2 + y_3 z^3 + \cdots + y_1(z) + y(0) - y_1(z) - y(0)\right] - \frac{1}{z}\left[y_1 z + y_2 z^2 + \cdots + y(0) - y(0)\right] - 6G(Y;z)$$

$$= \frac{1}{z^2}\left[G(Y;z) - 2 - z\right] - \frac{1}{z}\left[G(Y;z) - 2\right] - 6G(Y;z)$$

Multiplying by z^2, we get

$$G(Y;z) - 2 - z - zG(Y;z) + 2z - 6z^2G(Y;z) = 0$$

Recursive and partial recursive functions

Defn:1

Let $g(x_1, x_2, \ldots, x_n, y)$ be a total function over N. g is a regular function if there exists some $y_0 \in N$ such that $g(x_1, x_2, \ldots, y_0) = 0$ for all values $x_1, x_2, \ldots, x_n$ in N.

Eg:1

$G(x, y) = \min(x, y)$ is a regular function since $g(x, 0) = 0$ for all $x \in N$.

Defn:2

A function $f(x_1, x_2, \ldots, x_n)$ over N is defined from a total function $g(x_1, x_2, \ldots, x_n, y)$ by minimization if

a) $f(x_1, x_2, \ldots, x_n)$ is the least value of all y's such that $g(x_1, x_2, \ldots, x_n, y) = 0$ if it exists. The least value is denoted by $\mu_r(g(x_1, x_2, \ldots, x_n, y) = 0)$

b) $f(x_1, x_2, \ldots, x_n)$ is undefined if there is no y such that $g(x_1, x_2, \ldots, x_n, y) = 0$.

Note:

In general, f is partial, If g is regular then f is total.

Defn:3 A function is recursive if it can be obtained from the initial functions by a finite number of applications of composition, recursion and minimization over regular functions.

Defn:4

A function is partial recursive if it can be obtained from the initial functions by a

$d_0 + d_1 k - 4d_0 - 4d_1 k + 4d_1 + 4d_0 + 4d_1 k - 8d_1 = 3k$

$d_0 + d_1 k + 4d_1 - 8d_1 = 3k$.

$(d_0 - 4d_1) + d_1 k = 3k$

Equating the corresponding coefficients, we get

$d_0 - 4d_1 = 0$; $d_1 = 3$

$d_0 - 4(3) = 0$

$d_0 = 12$

particular soln corresponding to $3k$ is $12 + 3k$.

particular soln for 2^k

Take $dk^2 2^k$.

Replace $S(k)$ by $dk^2 2^k$

$dk^2 2^k - 4[d(k-1)^2 2^{k-1}] + 4[d(k-2)^2 2^{k-2}] = 2^k$

$2^k[dk^2 - 2d(k-1)^2 + d(k-2)^2] = 2^k$

$dk^2 - 2d(k-1)^2 + d(k-2)^2 = 1$

$dk^2 - 2dk^2 + 4dk - 2d + dk^2 - 4dk + 4d = 1$

$2d = 1$

$d = 1/2$

particular soln corresponding to 2^k is $\left(\frac{1}{2}\right)k^2 2^k$

General solution is

$S(k) = (c_0 + c_1 k)2^k + 12 + 3k + \left(\frac{1}{2}\right)k^2 2^k$

$1 = S(0) = 12 + c_0$

$\Rightarrow c_0 = -11$

$1 = S(1) = 12 + 3 + 2(c_0 + c_1 + 1/2)$

ie) $2c_0 + 2c_1 + 16 = 1$

$2(-11) + 2c_1 + 15 = 0$

$2c_1 - 7 = 0$

$2c_1 = 7$

$c_1 = 7/2$

$S(k) = 12 + 3k + [-11 + (7/2)k + k^2(1/2)]2^k$

ie) $S(k) = 12 + 3k + (k^2 + 7k - 22)2^{k-1}$

Note:

1) Defn 3 generalizes the composition of two functions. This concept is useful when a number of outputs become the input for a subsequent steps of a program.

2) If $f_1, f_2, \ldots, f_K, g$ are total then the composition of g with $f_1, f_2, \ldots, f_K$ is total

Defn 4

A function f defined over N is defined by recursion if there exists a constant k, $(k \in N)$, and a function $h(x, y)$ such that

$$f(0) = k, \quad f(n+1) = h(n, f(n)) \quad — (1)$$

Note:

Using (1) and induction, $f(n)$ can be defined for all $n \in N$.

Eg: 4

Define i) $n!$ by recursion

$f(0) = 1$, $f(n+1) = h(n, f(n))$ where $h(x, y) = S(x) * y$

$S(n) = n+1$, $f(n) = n!$

$h(n, f(n)) = S(n) * f(n)$

$= (n+1) n!$

$= (n+1)!$

As $S(x) = x+1$

$$h(n, f(n)) = (n+1) * f(n)$$
$$= (n+1)\, n!$$
$$= (n+1)!$$

Defn: 5 A function f of $n+1$ variables is defined by recursion, if there exists a function g of n variables, and a function h of $n+2$ variables, and f is defined as follows:

$$f(x_1, x_2, \ldots, x_n, 0) = g(x_1, x_2, \ldots, x_n) \quad — (1)$$

$$f(x_1, x_2, \ldots, x_n, y+1) = h(x_1, x_2, \ldots, x_n, y, f(x_1, x_2, \ldots, x_n, y)) \quad — (2)$$

finite number of applications of compositions, recursion and minimization.

It is assumed that we are considering only sets whose elements are natural numbers or sets of n-tuples of the natural numbers.

To each such set A we can define the characteristic function χ_A. The characteristic function χ_A assigns the value 1 for all elements of A and assigns the value 0 for others. For ex if $A = \{2, 4, 8, 16, 32\}$ Then $\chi_A(x) = 1$, if $x = 2, 4, 8, 16$ or 32; and $\chi_A(x) = 0$ for all natural numbers $x \neq 2, 4, 8, 16, 32$.

Defn: 5

A set A is called recursive (partial recursive) if its characteristic function χ_A is recursive (partial recursive)

Worked examples

W.E: 1 Show that $f(x) = x/2$ is partial recursive.

Soln: Let $g(x, y) = |2y - x|$. $2y - x = 0$ for some y only when x is even.

Let $f_1(x) = \mu_y (|2y - x| = 0)$

Then f_1 is defined only for even values of x and is equal to $x/2$.

When x is odd, $f_1(x)$ is not defined.

So f_1 and hence f is partial recursive.

W.E: 2

Let $[\sqrt{x}]$ be the integral part of $\sqrt{2}$.

Show that $[\sqrt{x}]$ is recursive.

$$= [G(F;z) - 1 - z] - z[G(F;z) - 1] - z^2[G(F;z)]$$

$$= G(F;z) - 1 - z - zG(F;z) + z - z^2[G(F;z)]$$

$$= (1 - z - z^2)\, G(F;z) - 1$$

$$1 = (1 - z - z^2)\, G(F;z)$$

$$G(F;z) = \frac{1}{1 - z - z^2}$$

3) Find the generating function for $s(n) = ba^n$.

Soln:-

$$G(S;z) = \sum_{n=0}^{\infty} ba^n . z^n$$

$$= b \sum_{n=0}^{\infty} a^n . z^n$$

$$= b[1 + az + a^2z^2 + \cdots]$$

$$= b[1 - az]^{-1}$$

$$G(S;z) = \frac{b}{1 - az}$$

4) $s(n) = n$

Soln:-

$$G(S;z) = \sum_{n=0}^{\infty} n . z^n$$

$$= z + 2z^2 + \cdots$$

$$= z[1 + 2z + 3z^2 + \cdots]$$

$$= z(1 - z)^{-2}$$

$$G(S;z) = \frac{z}{(1 - z)^2}$$

5) $s(n) = bna^n$

Soln:-

$$G(S;z) = \sum_{n=0}^{\infty} bna^n z^n$$

$$= baz + 2ba^2z^2 + \cdots$$

$$= abz[1 + 2za + 3z^2a^2 + \cdots]$$

$$G(S;z) = \frac{abz}{(1 - az)^2}$$

W.E: 2 Show that $f(x,y) = x^y$ is primitive recursive.

Soln:

$$f(x,0) = x^0 = 1$$

$$f(x,y+1) = x^{y+1} = x^y * x$$

$$= f(x,y) * x$$

Define $f(x,0) = 1$

$$f(x,y+1) = U_1^3(x,y,f(x,y)) * U_3^3(x,y,f(x,y))$$

$$= x * f(x,y).$$

W.E: 3 Show that the following functions over N are primitive recursive

i) constant function over N.

ii) predecessor function.

iii) proper subtraction function

iv) zero test function.

v) odd and even parity function.

Soln:

i) We have to show that $f(x,y) = k$ (constant) is primitive.

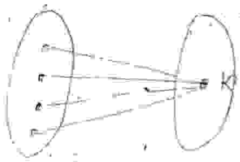
let $f(x) = k$

Define $f(0) = k$

$$f(n+1) = U_2^2(n, f(n))$$

$$= f(n)$$

$$= k$$



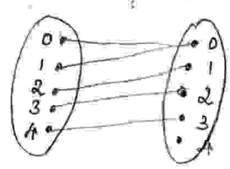
ii) We have to show that $p(x) = x-1$, if $x \neq 0$ and $p(0) = 0$

Define p by $p(0) = 0 = z(0)$

$$p(x+1) = h(x, p(x))$$

$$= U_1^2(x, p(x))$$

$$= x.$$



$p(x) = x-1$

$p(x+1) = x+1-1 = x$

$b_2 = 2$

$b_1 = -7-2$

$b_1 = -9$

$\therefore \quad T(K) = -9 \cdot 2^K + 2 \cdot 5^K + 8 + 2K$.

2) Solve $S(K) - S(K-1) - 6S(K-2) = -30$, $S(0) = 20$, $S(1) = -5$.

Soln:- Characteristic equation is

$a^2 - a - 6 = 0$

$\Rightarrow (a-3)(a+2) = 0$

$\therefore$ roots are $-2, 3$.

RHS = constant replace $S(K), S(K-1), S(K-2)$ by d

General solution is

$S(K) = b_1 (-2)^K + b_2 \cdot 3^K$

R.H.S of recurrence relation is constant.

Take d, replace $S(K), S(K-1), S(K-2)$ by d, we get

$d - d - 6d = -30$

$d = 5$

particular solution is 5

The general solution is

$S(K) = b_1 (-2)^K + b_2 \cdot 3^K + 5$

$20 = S(0) = b_1 + b_2 + 5$

$b_1 + b_2 = 15$

$-5 = S(1) = b_1 (-2)^1 + b_2 \cdot 3^1 + 5$

$= -2b_1 + 3b_2 + 5$

$-2b_1 + 3b_2 = -10$

$b_1 + b_2 = 15 \rightarrow (1)$

$-2b_1 + 3b_2 = -10 \rightarrow (2)$

$(1) \times 2 \Rightarrow \quad 2b_1 + 2b_2 = 30$

$ \quad -2b_1 + 3b_2 = -10$

$5b_2 = 20$

$b_2 = 4$

$b_1 + 4 = 15$

$b_1 = 11$

The solution is

$S(K) = 11(-2)^K + 4 \cdot 3^K + 5$

$= 1 + A(1,4)$

$= 1 + A(0+1, 3+1)$

$= 1 + A(0, A(1,3))$

$= 1 + 1 + A(1,3)$

$= 1 + 1 + A(1+0, 2+0)$

$= 2 + A(0, A(1,2))$

$= 2 + 1 + A(1,2)$ From ①

$= 3 + 4$ from (b)

$A(2,2) = 7$.

e) For proving this we need the result

$A(1,y) = y+2$ — ①

Now $A(1,y) = A(0+1, y-1+1)$

$= A(0, A(1, y-1))$

$= 1 + A(1, y-1)$

$= y-1 + A(1,1)$

$= y-1+3$

$A(1,y) = y+2$.

$A(3,1) = A(2+1, 0+1)$

$= A(2, A(3,0))$

$= A(2, A(2,1))$ by ②

$= A(2,5)$

$= A(1+1, 4+1)$

$= A(1, A(2,4))$

$= 2 + A(2,4)$ From ④

$= 2 + A(1, A(2,3))$

$= 2 + 2 + A(2,3)$

$= 4 + A(1, A(2,2))$

$= 4 + 2 + A(2,2)$ From ④

$= 6 + 7$

$A(3,1) = 13$

3) Solve: $S(K) - 3S(K-1) - 4S(K-2) = 4^K$.

soln:-

characteristic equation is

If $S = ca^K$ one time coincide Take dKa^K

two times coincide Take dK^2a^K

$$a^2 - 3a - 4 = 0$$

$$(a-4)(a+1) = 0$$

$$a = 4, -1$$

$\therefore$ The roots are $-1, 4$

Solution is

$$S(K) = b_1(-1)^K + b_2 \cdot 4^K$$

particular solution

Substitute $dK4^K$ for $S(K)$, $d(K-1)4^{K-1}$ for $S(K-1)$ and $d(K-2)4^{K-2}$ for $S(K-2)$

$$dK4^K - 3d(K-1)4^{K-1} - 4d(K-2)4^{K-2} = 4^K$$

$$4^{K-2}[dK4^2 - 3d(K-1)4 - 4d(K-2)] = 4^2 \cdot 4^{K-2}$$

$$16dK - 12d(K-1) - 4d(K-2) = 16$$

$$16dK - 12dK + 12d - 4dK + 8d = 16$$

$$20d = 16$$

$$d = 16/20 = 4/5 = 0.8$$

particular solution is $(0.8)K4^K$

$\therefore$ The general solution is

$$S(K) = b_1(-1)^K + b_2 4^K + 0.8K4^K.$$

4) Solve: $S(K) - 4S(K-1) + 4S(K-2) = 3K + 2^K$. $S(0) = 1$, $S(1) = 1$

soln:-

characteristic equation is

$$a^2 - 4a + 4 = 0$$

$\therefore$ The roots are $2, 2$

The general solution is

$$S(K) = (c_0 + c_1K)2^K$$

particular solution for $3K$.

Take $d_0 + d_1K$. Replace $S(K)$ by $d_0 + d_1K$, $S(K-1)$ by $d_0 + d_1(K-1)$ and $S(K-2)$ by $d_0 + d_1(K-2)$, we get

$$d_0 + d_1K - 4[d_0 + d_1(K-1)] + 4[d_0 + d_1(K-2)] = 3K$$

Ex:
Find $T(27)$ where $T(n)$ denotes the worst time for binary search of a file with n records.

Soln:-

$$27 = 16+8+2+1$$

$$27 = (11011)_2$$

$$\begin{array}{r|l} 2 & 27 \\ \hline 2 & 13 - 1 \\ \hline 2 & 6 - 1 \\ \hline 2 & 3 - 0 \\ \hline & 1 - 1 \end{array}$$

$$\begin{aligned} T(27) &= 1+T(1101) \\ &= 1+(1+T(110)) \\ &= 1+1+(1+T(11)) \\ &= 1+1+1+(T(11)) \\ &= 1+1+1+1+T(1) \\ &= 1+1+1+1+1 \end{aligned}$$

$$T(27) = 5$$

Primitive recursive functions

Defn:1
A partial function f from X to Y is a rule which assigns to every element of X atmost one element of Y.

Defn : 2
A total function from X to Y is a rule which assigns to every element of X a unique element of Y.

Eg:1
The rule $f(r) = +\sqrt{r}$ is a partial function since $f(r)$ is defined only for non-negative real numbers and not defined for negative numbers

Defn: 2
The initial functions over N are (i) zero function ii) successor function iii) projection function are defined by

i) zero function Z defined by $Z(x) = 0$

iii) Define $p(x,y) = \begin{cases} x-y & \text{if } x \geq y \\ 0 & \text{if } x < y \end{cases}$

$$p(x,0) = x - 0$$
$$= x$$
$$p(x,y+1) = x-(y+1)$$
$$= x-y-1$$
$$= p(x-y)$$

iv) signum $\bar{s}g(0) = S(z(0))$

$$= S(0)$$
$$= 1$$
$$\bar{s}g(x+1) = z(U_2^2(x, \bar{s}g(x)))$$
$$= z(\bar{s}g(x))$$
$$= 0$$

v) $P_r(0) = P_r(2) = \cdots = 0$ and

$P_r(1) = P_r(3) = \cdots = 1$

$$P_r(0) = z(0)$$
$$P_r(x+1) = \bar{s}g(U_2^2(x, P_r(x)))$$
$$= \bar{s}g(P_r(x))$$
$$= 0$$

$\bar{s}g(0) = 1$

$\bar{s}g(1) = 0$

$P_r(3) = \bar{s}g(P_r(2))$

$= \bar{s}g(0)$

$= 1$

N.E: 4

Show that if $f(x,y)$ defines the remainder upon division of y by x, then it is a primitive function.

soln:

We have to show that $f(x,y) = y/_x$ (remainder) is primitive.

$$f(x,0) = 0 = z(x)$$

sgn function

$$f(x,y+1) = S(f(x,y)) * sgn(x - S(f(x,y)))$$
$$sgn(0) = z(0), \quad sgn(x+1) = S(z(U_2^2(x, sgn(x))))$$

Generating functions

1) Find the generating function of the recurrence relation.

$$S(K) = 2S(K-1), \quad S(0) = 1.$$

Soln:-

Let $G(S;z)$ be the generating function of the sequence $\{S(K)\}$

Then $G(S;z) = S(0) + S(1)z + S(2)z^2 + \dots$

$$= S(0) + 2S(0)z + 2^2 S(0)z^2 + \dots$$

$$= 1 + 2z + 2^2 z^2 + \dots$$

$$= \frac{1}{1-2z} \quad \left[\text{Since } \frac{1}{1-x} = 1 + x + x^2 + \dots\right]$$

$S(k) = 2S(k-1)$

$S(1) = 2S(0)$

$S(2) = 2S(1)$

$= 2 \cdot 2S(0)$

$= 2^2 S(0)$

2) Find the generating function of Fibonacci sequence.

Soln:-

$$F(n) = F(n-1) + F(n-2), \quad n \geq 2, \quad F(0) = F(1) = 1$$

Generating function be $G(S;z)$

$$F(n) - F(n-1) - F(n-2) = 0, \quad n \geq 2$$

Hence

$$0 = \sum_{n=2}^{\infty} [F(n) - F(n-1) - F(n-2)] z^n$$

$$= \sum_{n=2}^{\infty} F(n)z^n - \sum_{n=2}^{\infty} F(n-1)z^n - \sum_{n=2}^{\infty} F(n-2)z^n$$

$$= \sum_{n=2}^{\infty} F(n)z^n - z\left[\sum_{n=2}^{\infty} F(n-1)z^{n-1}\right] - z^2\left[\sum_{n=2}^{\infty} F(n-2)z^{n-2}\right]$$

$$= [F(2)z^2 + F(3)z^3 + \dots + F(1)z + F(0) - F(0) - F$$

$$- z[F(1)z + F(2)z^2 + \dots + F(0) - F(0)] - z^2[F(0) + F(1)z + F(2)z^2 + \dots]$$

$$= \left[\sum_{n=0}^{\infty} F(n)z^n - F(0) - F(1)z\right] - z\left[\sum_{n=0}^{\infty} F(n)z^n - F(0)\right] - z^2\left[\sum_{n=0}^{\infty} F(n)z^n\right]$$

W.E : 4

If A denotes Ackermann's function evaluate

a) $A(1,1)$ b) $A(1,2)$ c) $A(2,1)$ d) $A(2,2)$ e) $A(3,1)$ f) $A(3,2)$

soln:- Recall the definition of A from ex 3 and 1

$$A(0,y) = y+1 \quad \text{— ①}$$

$$A(x+1, 0) = A(x,1) \quad \text{— ②}$$

$$A(x+1, y+1) = A(x, A(x+1, y)) \quad \text{— ③}$$

a) $A(1,1) = A(0+1, 0+1)$

$= A(0, A(1,0))$ by ③

$= A(0, A(0,1))$ by ②

$= A(0,2)$ as by ① $A(0,1) = 1+1 = 2$.

$= 2+1$ by ①

Hence $A(1,1) = 3$.

b) $A(1,2) = A(0+1, 1+1)$

$= A(0, A(1,1))$ by ③

$= A(0,3)$ by (a)

$= 3+1$

$A(1,2) = 4$ by ①

c) $A(2,1) = A(1+1, 0+1)$

$= A(1, A(2,0))$

$= A(1, A(1,1))$

$= A(1,3)$

$= A(0+1, 2+1)$

$= A(0, A(1,2))$

$= A(0,4)$

$A(2,1) = 5$.

d) $A(2,2) = A(1+1, 1+1)$

$= A(1, A(2,1))$

$= A(1,5)$

$= A(0+1, 4+1)$

$= A(0, A(1,4))$

Soln: We can note that $(y+1)^2 - x$ is zero for $(y+1)^2 \leq x$ and non-zero for $(y+1)^2 > x$.

Hence $\overline{sg}((y+1)^2 - x)$ is 1 if $(y+1)^2 \leq x$.

Now $[\sqrt{x}]$ is the smallest value of y for which $(y+1)^2 > x$:

Hence $[\sqrt{x}] = \mu_y(\overline{sg}((y+1)^2 - x) = 0)$.

$\overline{sg}(y+1)^2 - x$ is a regular function of x.

As $[\sqrt{x}]$ is got by minimization of a regular function $[\sqrt{x}]$ is recursive.

W.E:3

S.T the set of divisors B of a positive integer n is recursive.

Soln: A set is recursive if its characteristic function is recursive.

Now a number $x \leq n$ is a divisor of n if and only if $|x * i - n| = 0$ for some fixed i, $1 \leq i \leq n$.

Also $|x * i - n|$ is non-zero for all i, $1 \leq i \leq n$, if x is not a divisor of n.

Let χ_B denote the characteristic function of the set of all divisors of n.

Then $\chi_B(x) = \sum_{i=1}^{n} \overline{sg}\,|x * i - n|$

[Note that i is a divisor of $n \Leftrightarrow |x * i - n| = 0$

$\Leftrightarrow \overline{sg}\,|x * i - n| = 1$.

As χ_B is got as a finite sum of primitive recursive functions, it is recursive]

So, $(1-z-6z^2)\, G(Y;z) = 2-z$

Hence,

$$G(Y;z) = \frac{2-z}{1-z-6z^2}$$

To solve the difference equation resolve $G(Y;z)$ into partial fractions

$-6z^2-z+1$

$$1-z-6z^2 = (1-3z)(1+2z)$$

-6

$2 \mid +3$

$-6 \quad 3 \quad -6$

$(-3z+1)(2z+$

Let $\dfrac{2-z}{1-z-6z^2} = \dfrac{A}{1-3z} + \dfrac{B}{1+2z}$

$$2-z = A(1+2z) + B(1-3z)$$

put $z = -1/2$

$$5/2 = 0 + B(5/2)$$

$$B = 1$$

put $z = 1/3$

$$5/3 = 5/3\, A + 0$$

$$A = 1$$

Hence

$$G(Y;z) = \frac{1}{1-3z} + \frac{1}{1+2z}$$

Y_n = co-efficient of z^n in the expansion of $(1-3z)^{-1} + (1+2z)^{-1}$

$$= 3^n + (-1)^n \cdot 2^n$$

$\Big[(1-3z)^{-1} = 1 + 3z + (3z)^2 + \dots + (3z)^n + \dots$

$(1+2z)^{-1} = 1 - 2z + (2z)^2 + \dots + (-1)^n (2z)^n + \dots \Big]$

10) Solve the recurrence relation $s(n) = s(n-1) + 2(n-1)$ with $s(0)=3$, $s(1)=1$ by finding its generating function.

Soln:

Let $G(S;z)$ be the generating function of S.

f) $A(3,2) = A(2+1, 1+1)$

$= A(2, A(3,1))$

$= A(2, 13)$ from (e)

$= A(1, A(2,12))$

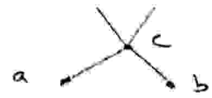
$= 2 + A(2,12)$ by (i)

$= 2 + A(1, A(1,11))$

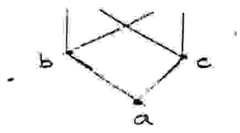
$= 2 + A(1,13)$ by (i)

$= 2 + 2 + 13$ by (i)

$A(3,2) = 17$



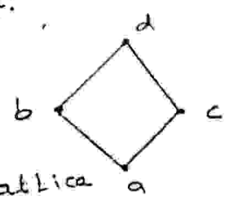
$a \vee f \neq$
$d \wedge f = c$



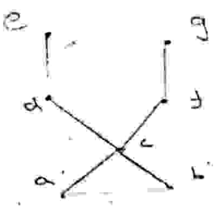
Lattice :-

Defn: A poset $(X, \leq)$ is said to be a lattice if for every $a, b \in X$ both $a \vee b$ & $a \wedge b$ exist.

Ex:



lattice



is not a lattice

Thm: 1

Every chain is a lattice

Pf: Let $(X, \leq)$ be a chain and $a, b \in X$

Then we have either $a \leq b$ or $b \leq a$

case (i)

Assume that $a \leq b$,

clearly, b is an upper bound of a and b., if c is an upper bound of a and b.

we have $a \leq c$ and $b \leq c$. Thus $b \leq c$, for every upper bound of a and b.

hence b is the least upper bound of a and b

ie) $a \vee b = b$

IIIly $a \wedge b = a$

case (ii)

Assume that $b \leq a$

Then Prove that $a \vee b = a$ and $a \wedge b = b$

Thus $a \vee b$ & $a \wedge b$ exist $\forall a, b \in X$.

lattices.

So $n = km$, $n = kln$ this is possible only $kl = 1$

So $k = 1$ and $l = 1$ and $n = m$ thus $\leq$ is anti

Symmetric.

(iii) Let n, m, s be +ve integer such that n divides m, m divides s. then $m = kn$, $s = lm$ for some +ve integer k and l. Now $s = lm \Rightarrow lkn$

n divides s. So $\leq$ is transitive also.

Defn:-

Let $(X, \leq)$ be a poset and $a, b \in X$ if there is an element c in X such that $\underline{a \leq c,\ b \leq c}$. then c is said to be an upper bound for a and b.

LCM

an element c in X is said to be a least upper bound (join) of a and b. if (i) c is an upper bound of a and b $(a \leq c, b \leq c)$

(ii) whenever d is an upper bound of a and b then $c \leq d$. $(a \leq d, b \leq d \Rightarrow c \leq d)$

An element c is said to be a lower bound of a and b then $c \leq a$, $c \leq b$ an element c is said to be a greatest lower bound (meet) of a and b if (i) c is a lower bound of a and b

gcd

(ii) whenever d is a lower bound of a and b $d \leq c$.

Ex:-

In the poset $(D(12), \leq)$ where $\leq$ is the relation "is a divisor of" $2 \vee 3 = 6$, $3 \vee 6 = 6$, $4 \vee 6 = 12$

Let (L, ≤) ...

relation $\leq'$ in L as follows. If $a, b \in L$, $a \leq' b$ if and only if $b \leq a$ in $(L, \leq)$,

Then $\leq'$ is also a partial ordering on L. the partial ordering $\leq'$ is called the reversal of the partial ordering $\leq$. clearly for all $a, b \in L$.

lub $\{a,b\}$ in $(L, \leq') =$ glb $\{a,b\}$ in $(L, \leq)$ and glb $\{a,b\}$ in $(L, \leq') =$ lub $\{a,b\}$ in $(L, \leq)$.

$\therefore (L, \leq')$ is also a lattice. This lattice is called the dual of the lattice $(L, \leq)$.

Ex:-

$a \leq b \Rightarrow a \vee b = b$ is valid. Hence its dual statement $a \geq b \Rightarrow a \wedge b = b$ is valid.

Thm: 4

In any lattice $(L, \leq)$ the operations $\vee$ and $\wedge$ are isotone (ie) if $y \leq z$ in L. then $x \wedge y \leq x \wedge z$ and $x \vee y \leq x \vee z$ for all $x \in L$.

Pf:- Let $x, y, z \in L$ and $y \leq z$

By idempotent law, $x \wedge x = x$. As $y \leq z$, we have $y \wedge z = y$

So $x \wedge y = (x \wedge x) \wedge (y \wedge z)$ $= x \wedge ((x \wedge y) \wedge z)$

$= x \wedge ((y \wedge x) \wedge z)$ commutative

$= x \wedge (y \wedge (x \wedge z))$

$= (x \wedge y) \wedge (x \wedge z)$ using associative law

From $x \wedge y = (x \wedge y) \wedge (x \wedge z)$ and by thm 3. $a \leq b \; a \vee b = b$

Defn:-

Let $(X, \leq)$ be a poset if there is an element $a \in X$ Such that $a \leq x$ $\forall$ $x \in X$ then a is said to be a least element in X.

Defn (An element $b \in X$ such that $x \leq b$ $\forall$ $x \in X$, b is said to be a greatest element in X.) if there is a least element in $(X, \leq)$ Then it is unique

If there is a greatest element in $(X, \leq)$ then it is unique

Defn:- The greatest element if it exists is denoted by 1 and the least element if it exists is denoted by 0.

A Lattice which has both 0 and 1 is called a bounded lattice.

Ex: In the lattice $(P(X), \subseteq)$ where X is a set then null set ϕ is the least element and the set X is greatest element.

Some Properties of Lattices:

Thm: 2

$(L, \leq)$ be a Lattice then L satisfies the following laws: (i) Idempotent Laws $a \wedge a = a$ and $a \vee a = a$ for all $a \in L$ (ii) commutative Law $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$ $\forall$ $a, b \in L$ (iii) associative Law $(a \vee b) \vee c =$

15

UNIT- IV

Defn:- LATTICES

A relation R is said to be an equivalents relation if R is reflexive, symmetric and transitive

Defn:- A Relation R is said to be a partial ordering on A if R is reflexive, antisymmetric and transitive

Defn:- If R is partical ordering on A then (A, R) is called a partially ordered set or a poset usually we write $\leq$ or $\subseteq$ instead of R

Ex: (i) Let x be a set and P(x) be the set of all subsets of x.

$(A, \leq)$

$(A, \subseteq)$

$$(a\wedge b)\wedge c \le a\wedge(b\wedge c) \longrightarrow (3)$$

Now, $a\wedge(b\wedge c)\le a$ and $a\wedge(b\wedge c)\le b\wedge c$.

As $b\wedge c\le b$, by transitivity, $a\wedge(b\wedge c)\le b$.

Since $a\wedge(b\wedge c)\le a$ and $a\wedge(b\wedge c)\le b$, we have

$$a\wedge(b\wedge c)\le(a\wedge b) \qquad \text{As } a\wedge(b\wedge c)\le b\wedge c\le c$$

$$a\wedge(b\wedge c)\le(a\wedge b)\wedge c \longrightarrow (4)$$

From (3) and (4) by antisymmetric property, it follows that $a\wedge(b\wedge c)=(a\wedge b)\wedge c$

IIIly we can prove that $a\vee(b\vee c)=(a\vee b)\vee c$

(iv) Let $a,b\in L$. Then $a\le a$ and $a\le a\vee b$; $a \le a\wedge b$

So $a\le a\wedge(a\vee b)$. on the other hand $a\wedge(a\vee b)\le a$

By antisymmetric

IIIly we have $a=a\vee(a\wedge b)$ $\forall\, a,b\in L$

Thm: 3

Let $(L,\le)$ be a Lattice. For any $a,b \in L$ the following are equivalent. (i) $a\le b$ (ii) $a\vee b=b$ (iii) $a\wedge b=a$

Pf:-

(i) => (ii) Assume $a\le b$. As $a\le b$ and $b\le b$, from the defn/- of $a\vee b$.

we have $a\vee b\le b$ on the other hand $b\le a\vee b$

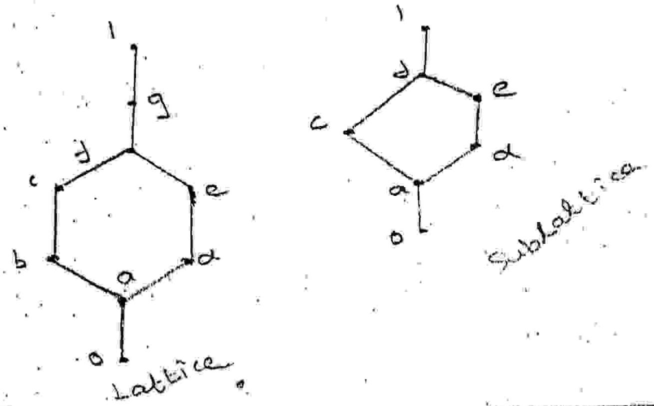
Hence by antisymmetric property of $\le$.

we have $a\vee b=b$

(ii) => (iii) Assume that $a\vee b=b$. Then by absorption law

$$a\wedge b=a\wedge(a\vee b)=a$$

(iii) => (i) Assume that $a\wedge b=a$. Then a is a lower



Defn:- Lattice homomorphism

Let $(L_1, \wedge, \vee)$ and $(L_2, \wedge, \vee)$ $(L_2, \sqcap, \sqcup)$ be Lattices and $f: L_1 \to L_2$ be a map than f is said to be a

(i) meet - homomorphism if $f(x \wedge y) = f(x) \sqcap f(y)$ $\forall\ x, y \in L_1$

(ii) join - homomorphism if $f(x \vee y) = f(x) \sqcup f(y)$ $\forall\ x, y \in L_2$

(iii) (Lattice) homomorphism if it is both meet-homomorphism and Join-homomorphism.

(iv) order-preserving map is $x \leq y$ in $L_1 \Rightarrow f(x) \leq f(y)$ in L_2

(v) order-reversing map if $x \geq y$ in $L_1 \Rightarrow f(x) \geq f(y)$ in L_2

Remark:-

Injective, surjective, and bijective (lattice) homomorphisms are called monomorphisms, epimorphisms and isomorphism respectively.

1-1 homo. onto, homo

Defn:-

Two posets $(P, \leq)$ and $(Q, \leq')$ are called order isomorphic if there is a bijective map $f: P \to Q$ such that $x \leq y$ in P iff $f(x) \leq' f(y)$ in Q

Ex:

Let L_1 and L_2 be the lattices represents by the Hasse diagrams given in the.

Let $f_1, f_2, f_3 : L_1 \to L_2$ be the maps given by we have $x \wedge y \leq x \wedge z$.

Thus if $y \leq z$ then $x \wedge y \leq x \wedge z$.

The dual of this statement is also true. So if $y \geq z$ then $x \vee y \geq x \vee z$. Interchanging the role of y and z in this statement, we get the following true statement

If $z \geq y$, then $x \vee z \geq x \vee y$.

Corollary :-

For any a, b, c, d in a lattice $(L, \leq)$, if $a \leq b$ and $c \leq d$ then $a \vee c \leq b \vee d$ and $a \wedge c \leq b \wedge d$

Pf:

As $a \leq b$, we have $a \vee c \leq b \vee c$. As $c \leq d$ we have $b \vee c \leq b \vee d$. By transitivity of $\leq$,

It follows that $a \vee c \leq b \vee d$.

$|||^{ly}$ we can obtain $a \wedge c \leq b \wedge d$.

Thm: 5

The elements of an arbitrary lattice $(L, \leq)$ satisfy the following inequalities.

(1) Distributive Inequalities :- (i) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

(ii) $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

(2) modular Inequalities :- (iii) $x \leq z \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z$

(iv) $x \geq z \Rightarrow x \wedge (y \vee z) \geq (x \wedge z) \vee z$

Pf:-

As (ii) and (iv) are duals of (i) and (iii) respectively it is enough to prove (i) and (iii) only. First we prove (i)

Let $x, y, z \in L$. As $x \leq x \vee y$ and $x \leq x \vee z$, we have

$x \leq (x \vee y) \wedge (x \vee z)$

of $\hat{glb}$ of x and y, we have $x \wedge y \leq x$ —> (1)

and if $z \leq x$ and $z \leq y$, then

$z \leq x \wedge y$ —> (2)

Now take $x = y = z = a$. As $a \leq a$ from (1) & (2) we have

$a \wedge a \leq a$ and $a \leq a \wedge a$ respectively.

By the antisymmetric property it follows that

$a = a \wedge a$.

|||ly we can prove that $a \vee a = a$.

(ii) Given a and $b \in L$, both $a \wedge b$ and $b \wedge a$ are glb's of a and b.

By the uniqueness of glb of a and b, we have

$a \wedge b = b \wedge a$

|||ly $a \vee b = b \vee a$ a holds good.

(iii) Let $a, b, c \in L$, By the defn we have $(a \wedge b) \wedge c \leq c$

$(a \wedge b) \wedge c \leq (a \wedge b)$ and

By the Defn/- of glb of a and b. we have

$a \wedge b \leq a$ and $a \wedge b \leq b$.

So by transitive property of '$\leq$', we have

$(a \wedge b) \wedge c \leq a$ and $(a \wedge b) \wedge c \leq b$.

As $(a \wedge b) \wedge c \leq b$ and $(a \wedge b) \wedge c \leq c$, we see that

$(a \wedge b) \wedge c$ is a lower bound for b and c.

From the defn of $b \wedge c$, it follows that

$(a \wedge b) \wedge c \leq b \wedge c$

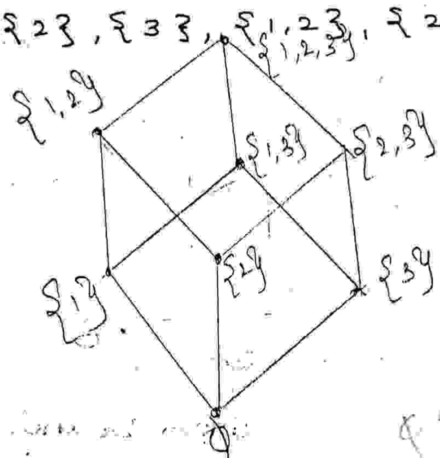
As $(a \ldots$ and $(a \wedge b) \wedge c \leq (b \wedge c)$ from the

Defn of $a \wedge (b \wedge c)$, we have

Ex:-

The Hasse diagram of the poset $(P(X), \subseteq)$ is given below where $X = \{1, 2, 3\}$ and $\subseteq$ is the relation (subset of)

$X = \{\{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{\}\}$



$2 \not\leq 3$

$3 \not\leq 2$

φ is the subset of all sets

Defn:- chain or totally ordered set:-

A partial ordered relation $\leq$ on a set A is called a total order or linear order if for every $a, b \in A$. either $a \leq b$ or $b \leq a$. If $\leq$ is a total order on A. then poset $(A, \leq)$ is called a total ordered set. a chain (or) totally ordered set.

Ex:-

(i) Let N be the set of all natural no/- define relation $\leq$ on N. as follows.

For $m, n \in N$, $m \leq n$ iff m is a divisor of n. (ie) ($m \leq n$ iff $n = mk$ for some +ve integer k)

(ii) As each +ve integer is a divisor of itself $n \leq n$ for $n \in N$. If n and m or +ve integer such that m divides n and n divides m. then $n = km$ and $m = ln$ for some +ve integer k and l

Define a relation $\leq$ on $P(X)$ as follows for $A, B \in P(X)$ $A \leq B$ iff A is a subset of B. as every set is a subset of itself. we have $A \leq A$ for every $A \in P(X)$. So $\leq$ is reflexive

(ii) If $A \neq B$ and $A \leq B$ implies that $B \leq A$ is not true. and hence the relation $\leq$ is anti symmetric.

(iii) Let $A \leq B$ and $B \leq C$ for some A, B, C in P
then A is a subset of B and B is subset of C and so A is a subset of C. (ie) $A \leq C$ Thus $\leq$ is transitive.

As the relation $\leq$ is reflexive, Symmetric transitive it is a partial order relation on P

Hasse diagrams :-

Defn :- A partially ordered finite set $(A, \leq)$ can be graphically represented by a diagram called Hasse diagram of the poset $(A, \leq)$

The elements of A are represented as points in the plane such that is $a, b \in A$ such that and $a \neq b$ then the pt :- b is plotted above the point a. The point b need not be exactly vertically above a, there may be a deviation to the left or right of the vertical line through a

T\ $a < b$ and there is no c in a such that

So $(x \vee y) \wedge (x \vee z)$ is an upper bound ...

hence $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$. Thus (i) is proved

The equality (iii) is a special case of (i)

If $x \leq z$ then $x \vee z = z$ and so from (i) we obtain

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z) = (x \vee y) \wedge z$$

which is the inequality (iii).

Thm: 6

Let L be a non-empty set and $\sqcap$ (meet) and $\vee$ (joint) be two binary operations on L. Such that $\wedge$ and $\vee$ satisfy the following conditions for all $x, y, z \in L$

Commutative Law : $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$.

Associative Law : $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$

Absorption Law : $x \vee (x \wedge y) = x$ and $x \wedge (x \vee y) = x$

If we define $\leq$ on L as $x \leq y$ if and only if $x \wedge y = x$ then $(L, \leq)$ is a Lattice.

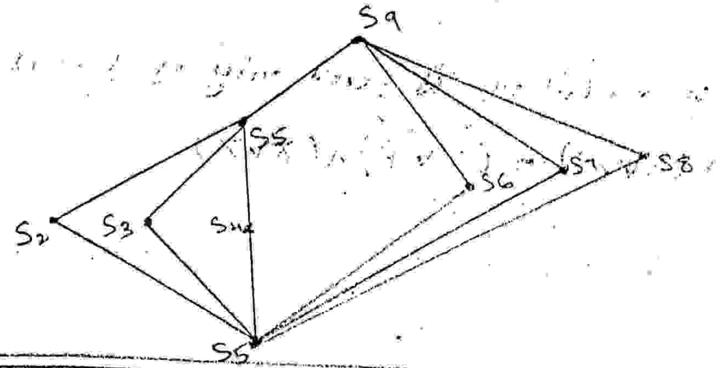
Defn:- New Lattice

A non-empty subset S of a lattice L is called a sublattice of L if S is closed under the operations "join and meet" of L. ie) for all $s_1, s_2 \in S$ the glb $\{s_1, s_2\}$ and lub $\{s_1, s_2\}$ in the lattice L are elements of S.

Ex: 1. Let $(L, \leq)$ be a Lattice if $x \in L$, the set $\{x\}$ is a sublattice of L. If $x, y \in L$ such that $x \leq y$. then the set $[x, y] = \{z \in L / x \leq z \leq y$ in $L\}$ is a sublattice of L.

2. Let $(L_1, \leq)$ and $(L_2, \leq)$ be the lattices represented by the Hasse diagrams given in respectively. The lattice $(L_2, \leq)$ ... lattice of $(L_1, \leq)$ (note $L_2 = L_1 - \{b, g\}$

any groups forms a modular lattice with respect to inclusion.



2. If G is a group, then the set of all normal subgroups of G forms a modular lattice.

Pf:-

If A is a normal subgroup of G, we write $A \triangleleft G$. The set of all normal subgroup is a poset, if the partial ordering is set theoretic inclusion.

If $A, B \triangleleft G$ the $A \cap B \triangleleft G$ and it is the largest subgroup that is contained in both A and B.

So $A \wedge B = A \cap B$. Also $= \{ab / a \in A . b \in B\}$ is a normal subgroup containing both A and B.

If $C \triangleleft G$ and $A \subset C$, $B \subset C$ then $ab \in C$ if $a \in A, b \in B$

So $AB \subset C$ and AB is the smallest normal subgroup of G that contains both A and B.

ie) $A \vee B = AB$. Thus the normal subgroup of G form a Lattice. Let $A, C \triangleleft G$ and $A \leq C$. we need to show that

$(A \vee B) \wedge C \leq A \vee (B \wedge C)$ ie) $(AB) \cup C \leq A(B \wedge C)$

Let $x \in (AB) \cap C$. Then $x = ab$ for some $a \in A\, b \in B$ also $x \in C$..

Soln:- (i) ⇒ (ii) Let $a \wedge b \leq x \leq a \vee b$

Now, $(a \wedge x) \vee (b \wedge x) \vee (a \wedge b) = ((a \wedge x) \vee (b \wedge x)) \vee (a \wedge b)$

$= ((a \vee b) \wedge x) \vee (a \wedge b)$

$= x \vee (a \wedge b)$ as $x \leq a \vee b$

$= x$ as $a \vee b \leq x$

(ii) ⇒ (i) Let $x = (a \wedge x) \vee (b \wedge x) \vee (a \wedge b)$

$x = ((a \wedge x) \vee (b \wedge x)) \vee (a \wedge b)$

$= ((a \wedge b) \wedge x) \vee (a \wedge b)$

From this we get $a \wedge b \leq x$

As $x = ((a \vee b) \wedge x) \vee (a \wedge b)$, we have

$x = ((a \vee b) \vee (a \wedge b)) \wedge (x \vee (a \wedge b))$

$= (a \vee b) \wedge (x \vee (a \wedge b))$

$= (a \vee b) \wedge x$ as $a \wedge b \leq x$.

So we get $a \wedge b \leq x$ and $x \leq a \vee b$

2, Show that a lattice L is distributive if and only if for all a, b, c in L $(a \vee b) \wedge c \leq a \vee (b \wedge c)$

Pf:

(i) If L is distributive, then for all $a, b, c \in L$

$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c) \leq a \vee (b \wedge c)$ as $a \wedge c \leq a$

(ii) conversely, assume that $(a \vee b) \wedge c \leq a \vee (b \wedge c)$ $\forall a, b, c \in L$.

To show that L is distributive it is enough to prove that $(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge a)$ $\forall a, b, c \in L$

Now, $(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge (a \vee c))$ by assumption

$= a \vee ((a \vee c) \wedge b)$

$\leq a \vee (a \vee (c \wedge b))$

$= a \vee (c \wedge b)$, $a \leq a \vee (c \wedge b)$

$= a \vee (b \wedge c)$

So $(a \vee b) \wedge (a \vee c) \leq a \vee (b \wedge c)$, $\forall a, b, c \in L$.

Soln: Let L_1 and L_2 be two distributive lattices.

Let $x, y, z \in L_1 \times L_2$ the ~~dust~~ direct product of L_1 & L_2

Then $x = (a_1, a_2)$, $y = (b_1, b_2)$ and $z = (c_1, c_2)$ for some $a_1, b_1, c_1 \in L_1$ and $a_2, b_2, c_2 \in L_2$

Now
$$
\begin{aligned}
x \vee (y \wedge z) &= (a_1, a_2) \vee ((b_1, b_2) \wedge (c_1, c_2)) \\
&= (a_1, a_2) \vee (b_1 \wedge c_1, \; b_2 \wedge c_2) \\
&= (a_1 \vee (b_1 \wedge c_1), \; a_2 \vee (b_2 \wedge c_2)) \\
&= ((a_1 \vee b_1) \wedge (a_1 \vee c_1), (a_2 \vee b_2) \wedge (a_2 \vee c_2)) \\
&= ((a_1 \vee b_1)(a_2 \vee b_2)) \wedge ((a_1 \vee c_1), (a_2 \vee c_2)) \\
&= ((a_1, a_2) \vee (b_1, b_2)) \wedge ((a_1, a_2) \vee (c_1, c_2)) \\
&= (x \vee y) \wedge (x \vee z)
\end{aligned}
$$

So $\forall \; x, y, z \in L_1 \times L_2$, $x \vee (y \wedge z) = (x \vee z) \wedge (x \vee z)$

Thus if L_1 and L_2 are distributive, then $L_1 \times L_2$ is also distributive

---

Defn:-
A Lattice L with 0 and 1 is called complemented if for each $x \in L$, there is at least one element $y \in L$ such that $x \wedge y = 0$ and $x \vee y = 1$ such an element $y \in L$ is said to be a complement of x.

Thm: 19
If L is a distributed lattice with 0 and 1 then each element $x \in L$ has atmost one complement.

Pf:- Let $x \in L$, If y_1 and $y_2 \in L$ such that $x \wedge y_1 = 0$; $x \vee y_1 = 1$ and $x \wedge y_2 = 0$; $x \vee y_2 = 1$ then

$x \wedge y_1 = x \wedge y_2 = 0$

$$
\begin{aligned}
y_1 &= y_1 \vee (x \wedge y_1) \\
&= y_1 \vee (x \wedge y_2) \\
&= (y_1 \vee x) \wedge (y_1 \vee y_2)
\end{aligned}
$$

the following conditions holds for all x, y, z in L.

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

Ex:- If X is a set then $(P(X), \cap, \cup)$ is a distributive Lattice.

Thm : 14

Every chain is a distributive lattice

Pf:-

Let $(L, \leq)$ be a chain and $a, b, c \in L$. consider the following possible cases.

(i) $a \leq b$ or $a \leq c$ and (ii) $b \leq a$ and $c \leq a$.

In case (i), $a \leq b \vee c$. So $a \wedge (b \vee c) = a$ and $(a \wedge b) \vee (a \wedge c) = a$

In case (ii) $b \vee c \leq a$. So $a \wedge (b \vee c) = b \vee c$ and $(a \wedge b) \vee (a \wedge c) = b \vee c$

Thus for all $a, b, c \in L$. the distributive equation

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

holds and hence L is distributive.

Thm : 15

Every distributive Lattice is modular.

Pf:-

Let $(L, \leq)$ be a distributive Lattice. $x, y, z \in L$. Let $(L, \leq)$ be a distributive lattice. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. Thus if $x \leq z$. we have $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$. So if $x \leq z$. Then $x \vee z = z$ and $x \vee (y \wedge z) = (x \vee y) \wedge z$.

The modular equation is satisfied and L is modular.

Ex: 1 N_5 is not distributive

By thm 14, if a lattice is not modular, then it is not distributive.

In particular the pentagon Lattice N_5 is not distributive

Thus $x \in (A \vee B) \wedge C \Rightarrow x \in A \vee (B \wedge C)$ whenever $A \leq C$

i.e) if $A \leq C$ then $(A \vee B) \wedge C < A \vee (B \wedge C)$

Hence the lattice L is modular.

Thm : 12

A Lattice L is modular if and only if forall $x, y, z \in L$. $x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$

Pf:-

If L is modular, as $x \leq (x \vee z)$, by modular equation we have

$$x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$$

Conversely,

assume that for all $x, y, z \in L$

$$x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z) \longrightarrow (*)$$

If $x \leq z$, then $x \vee z = z$ and $(*)$ becomes

$$x \vee (y \wedge z) = (x \vee y) \wedge z$$

which is the modular equation so the lattice L is modular

Thm:-13

A Lattice L is modular if and only if for all $x, y, z \in L$

$(x \vee (y \wedge z)) \wedge (y \vee z) = (x \wedge (y \vee z)) \vee (y \wedge z)$

Pf:

If L is modular, as $y \wedge z \leq y \vee z$, we have

$$(y \wedge z) \vee (x \wedge (y \vee z)) = ((y \wedge z) \vee x] \wedge (y \vee z)$$
$$= (x \vee (y \wedge z)) \wedge (y \vee z)$$

Conversely,

Assume that the eqn/- (1) is valid for all $x, y, z \in L$

If $y \leq z$ then as $y \wedge z = y$ and $y \vee z = z$ we get

$(x \vee (y \wedge z)) \wedge (y \vee z) = (x \vee y) \wedge z$ and

Thm: 8

Let f be an (order) isomorphism from a poset $(L, \leq)$ onto a poset $(M, \leq')$. If L is a lattice, then M is also a lattice and f is a lattice isomorphism.

Pf:- Let $f: L \to M$ be an order isomorphism.

Assume L to be a Lattice. Let $x, y \in M$. As f is a bijection, there exists a unique $a \in L$.

Such that $f(a) = x$ and a unique $b \in L$ such that $f(b) = y$

Let $c = a \vee b \in I$. Let $z = f(c)$ in M.

As $a \leq c$, $b \leq c$ and f is order preserving, we have $f(a) \leq' f(c)$ and $f(b) \leq' f(c)$ in M.

ie) we have $x \leq' z$ and $y \leq' z$ in M and z is upper bound for $\{x, y\}$ in M.

Let $w \in M$ be an upper bound for $\{x, y\}$ in M. Let d be the unique element in L such that $f(d) = w$

As $x \leq' w$, $y \leq' w$ (ie $f(a) \leq' f(d)$, $f(b) \leq' f(d)$) and f is an order isomorphism, we have $a \leq d$ and $b \leq d$ in L

So $c = a \vee b \leq d$ in L. As $c \leq d$, we have $f(c) \leq' f(d)$ in M

So we get $z \leq' w$ is M Thus we have proved that

(i) z is an upper bound for $\{x\ y\}$ in M and

(ii) where w is an upper bound for $\{x, y\}$ in M then $z \leq' w$. In other words. we have proved that $x \vee y$ exists in M and $x \vee y = z = f(c) = f(a \vee b)$ where $f(b) = x$ and $f(b) = y$.

(iii) $\forall$ $x, y \in M$ the ged $x \wedge y$ exists in M and if $x = f(a)$ and $y = f(b)$ then $x \wedge y = f(a \wedge b)$

... is a lattice and as the bijection $f: L \to M$

So $y_1 = y_1 \vee y_2$.

$|||^{ly}$ $y_2 = y_1 \vee y_2$ Thus $y_1 = y_2$ Thus if $x \in L$ has a complement then its complement is unique.

Thm: 20

Let L be a complement, distributive lattice, For $a, b \in L$ the following are equivalent.

(i) $a \leq b$, (ii) $a \wedge b' = 0$, (iii) $a' \vee b = 1$ (iv) $b' \leq a'$

Pf:- $a \leq b \Rightarrow a \vee b = b$

$\Rightarrow (a \vee b) \wedge b' = 0$ as $b \wedge b' = 0$

$\Rightarrow (a \wedge b') \vee (b \wedge b') = 0$

$\Rightarrow a \wedge b' = 0$ as $b \wedge b' = 0$

Hence (i) $\Rightarrow$ (ii)

$a \wedge b' = 0 \Rightarrow (a \wedge b')' = 1$

$\Rightarrow a' \vee (b')' = 1$

$\Rightarrow a' \vee b = 1$ as b is the complement of b'

Hence (ii) $\Rightarrow$ (iii)

$a' \vee b = 1 \Rightarrow (a' \vee b) \wedge b' = b$

$\Rightarrow (a' \wedge b') \vee (b \wedge b') = b'$

$\Rightarrow a' \wedge b' = b'$ as $b \wedge b' = 0$

$\Rightarrow b' \leq a'$

Hence (iii) $\Rightarrow$ (iv)

$b' \leq a' \Rightarrow a' \wedge b' = b'$

$\Rightarrow a \vee b = b$ taking complement on both sides and using Demorgan's law

$\Rightarrow a \leq b$

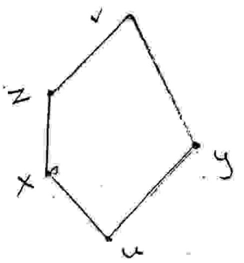
Hence (iv) $\Rightarrow$ (i)

Thus we have Prove

$$\text{(ii)}\ v \geq z \vee y \geq x \vee y \quad = a \vee (b \wedge c) \vee b$$
$$= a \vee ((b \wedge c) \vee b)$$
$$= a \vee b$$
$$= v$$

So $z \vee y = x \vee y = v$

These observation lead to the representation of $S = \{u, x, y, z, v\}$ by a Hasse diagram so the sublattice $S = \{u, x, y, z, v\}$ is isomorphic to N_5



Thus we have proved that if $(L, \leq)$ is not modular, then it has a sublattice isomorphic to N_5.

Ex: 1

The lattice of all subgroups of a group in general not modular For example. we now prove that the lattice of all subgroups of the alternating group A_4 is not modular

The subgroup of A_4 are.

$S_1 = \{(1)\}$, $S_2 = \{(1), (12)(34)\}$, $S_3 = \{(1)\ (13)(24)\}$
$S_4 = \{(1), (14)(23)\}$, $S_5 = \{(1), (12)(34), (14)(23), (13)(24)\}$
$S_6 = \{(1)\ (132)\ (123)\}$, $S_7 = \{(1)\ (134), (143)\}$, $S_8 = \{(1)(234)\ (243)\}$; $S_9 = A_4$

The Hasse diagram for the lattice L of all subgroups of A_4 is given in. The sublattice formed by S_1, S_4, S_5, S_6 and S_9 is isomorphic to N_5 hence by

$f_3(0) = 0$,

Then, (i) f_1 is both meet and join - homomorphism

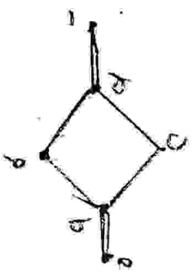
(ii) f_2 is a meet homomorphism but not join homomorphism

($f_2(b \vee c) = f_2(d) = 1$, but $f_2(b) \vee f_2(c) = b \neq 1$)

(iii) f_1 is neither a meet - homomorphism nor a join - homomorphism

Note that all these three maps are order - preserving maps

The map f_3 is an example for an order - preserving map which is neither a meet - homomorphism nor a join - homom.



1. Lattice L_1

2. Lattice L_2

Thm: 7

Every meet - homomorphism (join - homomorphism) is an order preserving map.

Pf:- Let $f : L_1 \to L_2$ be a meet - homomorphism from a lattice $(L_1, \leq_1)$ to a lattice $(L_2, \leq_2)$.

Let $a \leq_1 b$ in L_1. Then $a \wedge b = a$.

As f is a meet homomorphism, we have

$f(a) = f(a \wedge b) = f(a) \wedge f(b)$. Thus $f(a) \wedge f(b) = f(a)$ in L_2.

Hence $f(a) \leq_2 f(b)$ in L_2. Thus $a \leq_1 b$ in $L_1 \Rightarrow f(a) \leq_2 f(b)$ in L_2. and f is an order - preserving map.

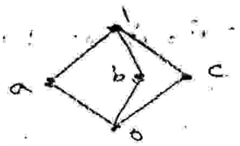
The proof for join - homomorphism is

2. The Lattice given by the Hasse diagram is an example for a modular lattice which is not distributive. This Lattice is denoted by the symbol M_5 and called 'diamond lattice'

In M_5 $a \vee (b \wedge c) = a \vee 0 = a$, while

$(a \vee b) \wedge (a \vee c) = 1 \wedge 1 = 1$.

So M_5 is not distributive. As N_5 is not a sublattice of M_5, M_5 is modular.



we now state a thm/- whose pf/- is left as an exercise

Thm: 16

A Lattice is distributive if and only if $\forall$ $x, y, z \in L$

$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee z) \wedge (y \vee z) \wedge (z \vee x)$

Remark: By thm 16, if a Lattice is not distributive, then we can find elements x, y, z in L such that

$$(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) < (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$$

we have already observed that the diamond lattice is modular, but not distributive.

Can we characterize those modular lattice which are distributive also?

The following theorem answers this quation/-

Thm: 17

A modular Lattice is distributive is and only if none of its sublattices is isomorphic to the diamond lattice M_5.

Pf:- As the diamond Lattice M_5 is not distributive, any Lattices having a subLattice isomorphic to M_5

The next theorem given ... condition for a lattices to be modular.

Thm: 10
A lattice L is modular iff none of its sublattices is isomorphic to the pentagon lattice N_5

Pf:
The Pentagon Lattice is not modular and hence any lattice having a pentagon a sublattice cannot be modular.

To prove the converse, let $(L, \leq)$ be a non modular lattice.

As it is not modular there are elements a, b, c in L such that

$a \leq c$ and $a \vee (b \wedge c) < (a \vee b) \wedge c$

Let $u = b \wedge c$

$x = a \vee (b \wedge c)$,

$y = b$

$z = (a \vee b) \wedge c$ and

$v = a \vee b$

one can verify that these five elements are all distinct.

we have, $u \leq x \leq z \leq v$ and $u \leq y \leq v$

Therefore,

(i) $u \leq x \wedge y \leq z \wedge y$ $= (a \vee b) \wedge c \wedge b$

$= ((a \vee b) \wedge b) \wedge c$

$= b \wedge c = u$

So $x \wedge z = z \wedge y = u$

Thm: 9

~~Let~~ $(L \times M, \wedge, \vee)$ is a ~~lattice~~

$L = x_1, x_2, x_3$ $M = y_1, y_2, y_3$

Pf:-

we now show that $\wedge$ and $\vee$ defined above satisfy commutative laws, associative law, absorption law. As $(L, \wedge, \vee)$ and $(M, \sqcup, \sqcap)$ are lattices the operations $\wedge$ and $\vee$ on L and the operations $\sqcap$ and $\sqcup$ on M satisfy those laws. $L(x_1, y_1), (x_2, y_2)$ and $(x_3, y_3) \in L \times M$

(a) $(x_1, y_1) \vee (x_2, y_2) = (x_1 \vee x_2, y_1 \sqcup y_2)$

$= (x_2 \vee x_1, y_2 \sqcup y_1)$

$= (x_2, y_2) \vee (x_1, y_1)$

III^{ly} $(x_1, y_1) \wedge (x_2, y_2) = (x_2, y_2) \wedge (x_1, y_1)$

(b) $(x_1, y_1) \vee ((x_2, y_2) \vee (x_3, y_3)) = (x_1, y_1) \vee ((x_2 \vee x_3, y_2 \sqcup y_3))$

$= (x_1 \vee (x_2 \vee x_3), y_1 \sqcup (y_2 \sqcup y_3))$

$= ((x_1 \vee x_2) \vee x_3 (y_1 \sqcup y_2) \sqcup y_3)$

$= (x_1 \vee x_2, y_1 \sqcup y_2) \vee (x_3, y_3)$

$= ((x_1, y_1) \vee (x_2, y_2)) \vee (x_3, y_3)$

Similary $(x_1, y_1) \wedge ((x_2, y_2)) \wedge (x_3, y_3)) = ((x_1, y_1) \wedge (x_2, y_2)) \wedge (x_3, y_3)$

(c) $(x_1, y_1) \vee ((x_1, y_1) \wedge (x_2, y_2)) = (x_1, y_1) \vee (x_1 \wedge x_2, y_1 \sqcap y_2)$

$= (x_1 \vee (x_1 \wedge x_2), y_1 \vee (y_1 \sqcap y_2))$

$= (x_1, y_1)$

Simillarly $(x_1, y_1) \vee ((x_1, y_1) \wedge (x_2, y_2)) = (x_1, y_1)$

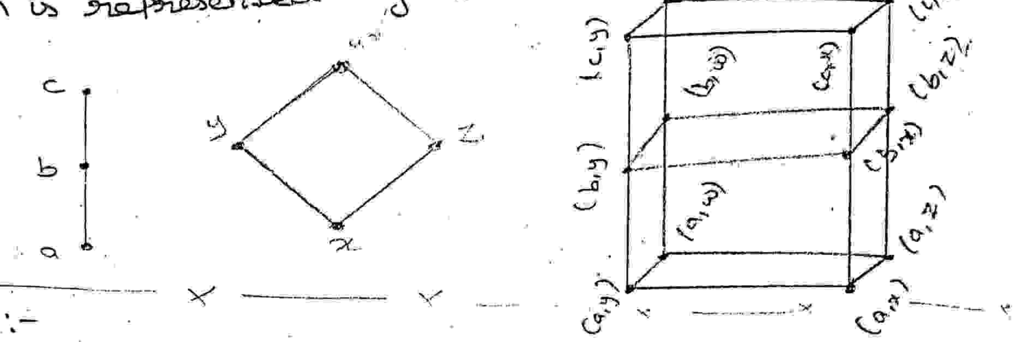
Thus $(L \times M, \wedge, \vee)$ is lattice.

Defn:-

The lattice $(L \times M, \wedge, \vee)$ is called the product lattice of the lattice L and M.

Ex: 1.

If L and M are lattices represented by Hasse diagrams given in respectively, then the direct Product L × M is represented by the Hasse diagram given in



Defn :-

A Lattice L is called modular if $\forall\, x, y, z \in L$

$x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$

Ex :- 1.

Any chain is modular

Let $(L, \leq)$ be a chain. Let $a, b, c \in L$ and $a \leq c$.

As L is a chain either $b \leq c$ (or) $c \leq b$.

Assume that $b \leq c$. Then c is an upper bound of a and b. So $a \vee b \leq c$ and $(a \vee b) \wedge c = a \vee b$. As $b \leq c$, we have $b \wedge c = b$.

So $a \vee (b \vee c) = a \vee b$. Thus is this case we have $(a \vee b) \wedge c = a \vee (b \wedge c)$.

Assume that $c \leq b$. Then by transitive Property of $\leq$, we have $a \leq b$, and $(a \vee b) \wedge c = b \wedge c = c$, while $a \vee (b \wedge c) = a \vee c = c$.

In this case also we have $(a \vee b) \wedge c = a \vee (b \wedge c)$

Thus whenever $a \leq c$, the modular eqn $(a \vee b) \wedge c = a \vee (b \wedge c)$ is satisfied and $(L, \leq)$ is modular lattice.

---

2. The Lattice N_5 is not modular :

In the discussion before the definition of modular

So, by thm 16, we can find x, y, z in L such that

$$(x\wedge y)\vee(y\wedge z)\vee(z\wedge x) < (x\vee y)\wedge(y\vee z)\wedge(z\vee x) \longrightarrow (*)$$

Let $u = (x\wedge y)\vee(y\wedge z)\vee(z\wedge x)$

$v = (x\vee y)\wedge(y\vee z)\wedge(z\vee x)$

$a = u\vee(x\wedge v)$

$b = u\vee(y\wedge v)$ and $c = u\vee(z\wedge v)$

one can verify that these five element u, v, a, b, c form a sublattice which is isomorphic to the diamond lattice.

Thm: 18

Let L be a distributive lattice and $a, b, c \in L$. If $a\wedge b = a\wedge c$ and $a\vee b = a\vee c$ then $b = c$ [This result is known as "cancellation Rule" for distributive lattices]

Pf:- Let $a, b, c \in L$ such that $a\wedge b = a\wedge c$ and $a\vee b = a\vee c$

Now $(a\wedge b)\vee c = (a\vee c)\wedge(b\vee c)$ by the distributive property

$= \cancel{(a\vee b)\wedge(b\vee c)}$ as $a\vee c = a\vee b$

$= (b\vee a)\wedge(b\vee c)$ as $a\vee b = b\vee a$

$= b\vee(a\wedge c)$ distributive property

$= b$ by absorption law

Also $(a\wedge b)\vee c = (a\wedge c)\vee c$ as $a\wedge b = a\wedge c$

$= c$ as absorption law

Thus $b = (a\wedge b)\vee c = c$

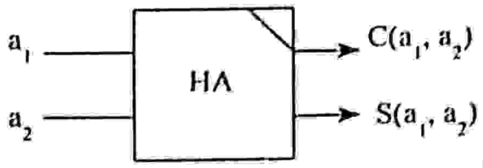
So $a\wedge b = a\wedge c$ and $a\wedge b = a\vee c \Rightarrow b = c$

Worked Examples:-

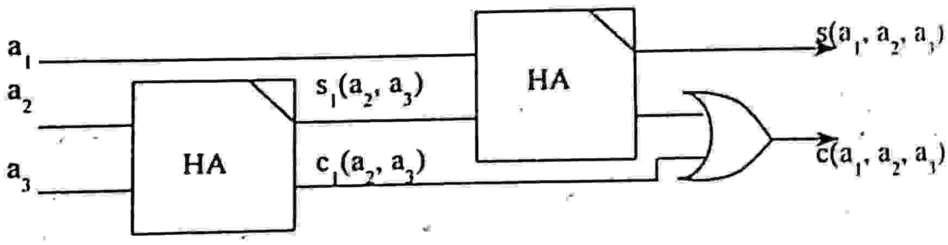
W.E: 1 In a distributive lattice. Prove that the following are equivalent (i) $a\wedge b \le x \le a\vee b$

(ii) $x = (a\wedge x)\vee(b\wedge x)\vee(a\wedge b)$

Symbolically we write



W.E.4. (Full-adder). Let a_1, a_2, a_3 be three one-digit binary numbers. With a and a_3 as inputs we obtain outputs $s_1(a_2, a_3)$ and $c_1(a_2, a_3)$ using a half-adder. The output $s_1(a_2, a_3)$ together with a_1 forms inputs of a second half-adder whose outputs are $s(a_1, a_2, a_3)$ and $c_2(a_1, s(a_2, a_3))$. Hence $s(a_1, a_2, a_3)$ is the final sum. $c_1(a_2, a_3)$ and $c_2(a_1, s_1(a_2, a_3))$ yields $c(a_1, a_2, a_3)$. Hence a full-adder is composed of half-adder of the form



So its circuit is

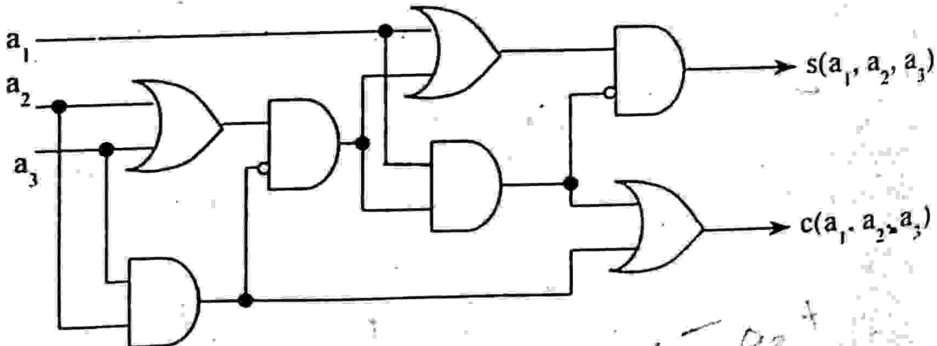


Figure 48.

W.E: 2 Expand the following function in to the Canonical Sum-of-products forms.

$$f(x, y, z) = xy + y\bar{z}$$

Soln:

$$f(x, y, z) = xy + y\bar{z}$$

$$= xy(z + \bar{z}) + (x + \bar{x})y\bar{z}$$

$$= xyz + xy\bar{z} + xy\bar{z} + \bar{x}y\bar{z}$$

$$= xyz + xy\bar{z} + \bar{x}y\bar{z}.$$

— x —.

W.E: 3 Write down the minterm normal form of $f(x_1, x_2) = \bar{x}_1 \vee \bar{x}_2$.

Soln:-

$$f(x_1, x_2) = \bar{x}_1 \vee \bar{x}_2$$

$$= \left(\bar{x}_1 \wedge (x_2 \vee \bar{x}_2)\right) \vee \left(\bar{x}_2 \wedge (x_1 \vee \bar{x}_1)\right)$$

$$= (\bar{x}_1 \wedge x_2) \vee (\bar{x}_1 \wedge \bar{x}_2) \vee (x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge \bar{x}_2)$$

$$= (\bar{x}_1 \wedge x_2) \vee (\bar{x}_1 \wedge \bar{x}_2) \vee (x_1 \wedge \bar{x}_2).$$

— x —.

The given function f $= ((x_1 + x_2) + (x_1 + x_3)) \cdot x_1\bar{x}_2$

$$= (x_1 + x_2 + x_3)\, x_1\bar{x}_2$$

$$= x_1\bar{x}_2 + x_1x_2\bar{x}_2 + x_1\bar{x}_2x_3$$

$$= x_1\bar{x}_2 + x_1\bar{x}_2x_3 \quad \text{as} \quad x_2\bar{x}_2 = 0$$

$$= x_1\bar{x}_2$$

The circuit diagram is given in Figure 50.

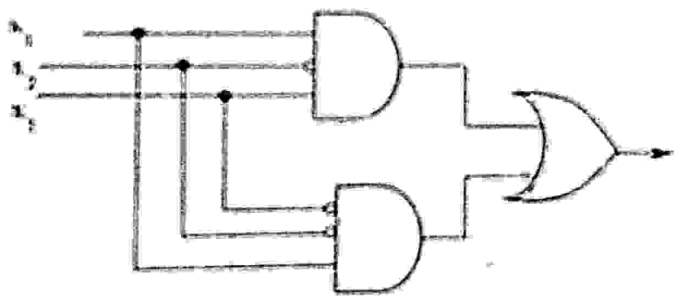


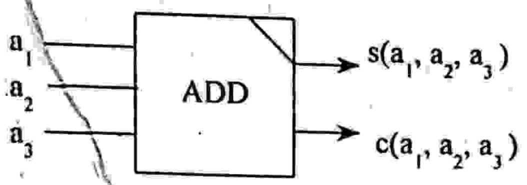
Figure 50

The Table 1 will be helpful when it is required to use only NAND gates (or only NOR gates).

W.E.7. For the formula $(P \wedge Q) \vee (\neg R \wedge \neg P)$ *draw a corresponding circuit using*

(i) NOT, AND and OR gates.
(ii) NAND gates only. *(Nov'97, M.C.A., M.U.)*

A symbolic full-adder is



W.E.5. A voting-machine for three voters has three YES-NO switches. Current is in the circuit precisely when YES has a majority. Draw a contact diagram and the symbolic representation by gates and simplify it.

Solution

Let to each i = 1, 2, 3, x_i = 1 if i votes YES,

0 if i votes NO.

Then $f(a_1, a_2, a_3) = 1$ only when (a_1, a_2, a_3) differs in zero place or in one place with (1, 1, 1).

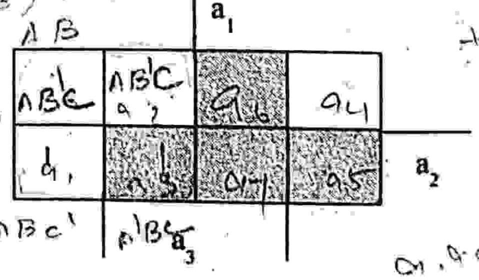
EX-OR

$\bar{A}B + A\bar{B}$ = A

a_1	a_2	a_3	$f(a_1, a_2, a_3)$
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1
0	0	1	0
0	1	0	0
1	0	0	0
0	0	0	0

So $f(a_1, a_2, a_3) = a_1a_2a_3 + a_1a_2\bar{a}_3 + a_1\bar{a}_2a_3 + \bar{a}_1a_2a_3$.

To simplify we use the Karnaugh map.



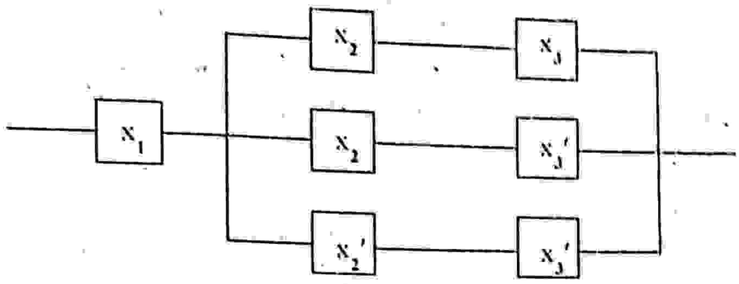
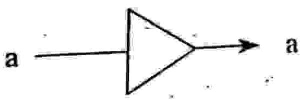
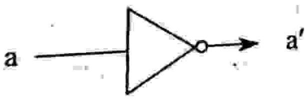
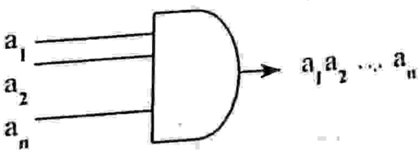


Figure 39.

Nowadays, electrical switches are of less importance than semiconductor elements. These elements are types of electronic blocks which are predominant in the logical design of digital building components of electronic computers. So the switches are represented by so-called *gates*, or combination of gates. The representation using gates is known as the *symbolic representation*.

Definition of some special gates :

	Some Special Gates		***Polynomial***
(1)		identity gate	x
(2)		NOT-gate	x'
(3)		AND-gate	$x_1x_2\ldots x_n$

$= \left(x_1 x_3 x_4 (x_2 + x_2') + x_1 x_3 x_4' (x_2 + x_2')\right) +$

$\left(x_1' x_3 x_4 (x_2 + x_2') + x_1 x_3 x_4 (x_2 + x_2')\right) +$

$\left(x_2 x_3' x_4 (x_1 + x_1') + x_2 x_3 x_4 (x_1 + x_1')\right)$

$= \left(x_1 x_3 x_4 + x_1 x_3 x_4'\right) + \left(x_1' x_3 x_4 + x_1 x_3 x_4\right)$

$+ \left(x_2 x_3' x_4 + x_2 x_3 x_4\right)$

$= x_1 x_3 + x_3 x_4 + x_2 x_4$

— x —

W.E: 2 Simplify $f = x_1' x_2' + x_1 x_3 x_4 + x_1 x_2 x_4' + x_2' x_3$.

Soln:

$x_1' x_2' = x_1' x_2' \left((x_3 \vee x_3')(x_4 \vee x_4')\right)$

$= x_1' x_2' \left(x_3 x_4 \vee x_3 x_4' \vee x_3' x_4 \vee x_3' x_4'\right)$

$= x_1' x_2' x_3 x_4 \vee x_1' x_2' x_3 x_4' \vee x_1' x_2' x_3' x_4 \vee x_1' x_2' x_3' x_4'$

$= m_3 + m_2 + m_1 + m_0$.

$x_1 x_3 x_4 = x_1 x_3 x_4 (x_2 \vee x_2')$

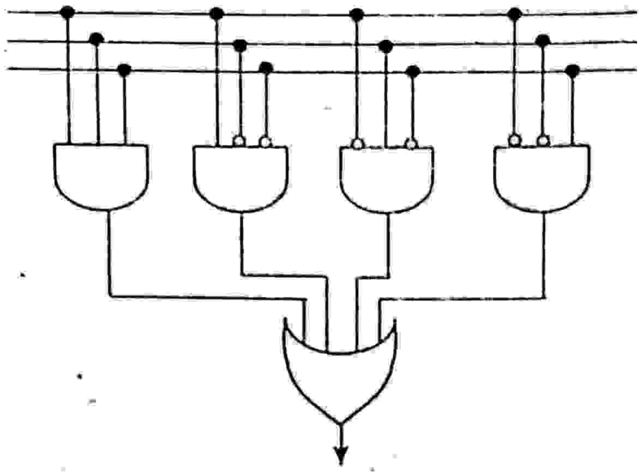
$= x_1 x_2 x_3 x_4 \vee x_1 x_2' x_3 x_4$

$= m_{15} + m_{11}$

From this we can derive the disjunction normal form for the switching circuit p as

$$p = x_1x_2x_3 + x_1x_2'x_3' + x_1'x_2x_3' + x_1'x_2'x_3.$$

The symbolic representation of p is given in Figure 45.



$\bar{p}(a_1, a_2, a_1)$

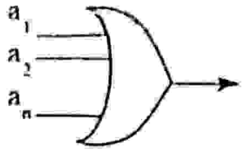
Figure 45.

W.E.3. (Half-adders) Describe the addition of two one-digit binary numbers.

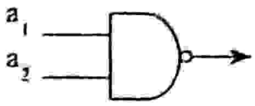
Solution

In order to add two single digit binary numbers a_1 and a_2 we have to consider a carry $C(a_1, a_2)$. $C(a_1, a_2) = 1$ if and only if $a_1 = a_2 = 1$. We have the following table for the sum $\bar{s}(a_1, a_2)$ and $c(a_1, a_2)$.

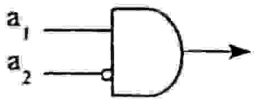
a_1	a_2	$s(a_1, a_2)$	$c(a_1, a_2)$
1	1	0	1
1	0	1	0
0	1	1	0
0	0	0	0

(4) 

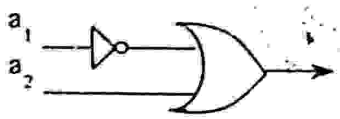
$a_1 + a_2 + \dots + a_n$ OR-gate $x_1 + x_2 + \dots + x_n$

(5) 

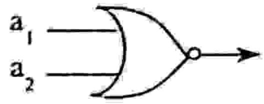
$(a_1a_2)'$ NAND-gate $(x_1x_2)'$

(6) 

a_1a_2' x_1x_2'

(7) 

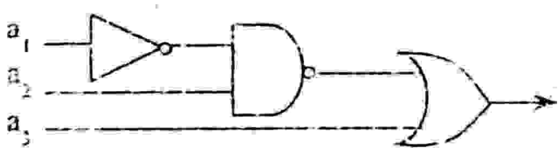
$(a_1' + a_2)$ Subjunction gate $x_1' + x_2$

(8) 

$(a_1 + a_2)'$ NOR-gate $(x_1 + x_2)'$

Examples

1. The symbolic representation of $p = (x_1'x_2)' + x_3$ is given in Figure 40.



$p(a_1,a_2,a_3) = (a_1'a_2)' + a_3$

Figure 40

2 The symbolic representation of the circuit given by
$$p = (x_1 + x_2 + x_3)(x_1' + x_3)(x_1x_3 + x_1'x_2)(x_2' + x_3)$$
is given in Figure 41.

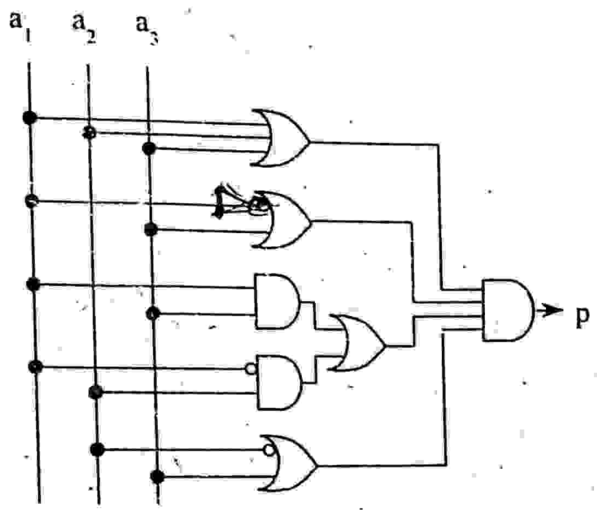


Figure 41.

3. The symbolic representation of $p = (x_1 + x_2 + x_2x_3')(x_1x_2'x_3)$ is given in Figure 42.

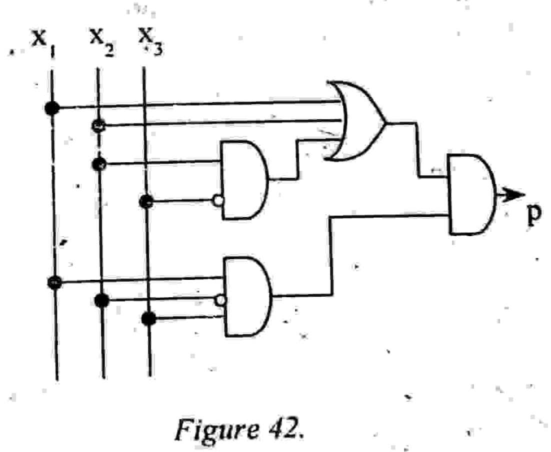
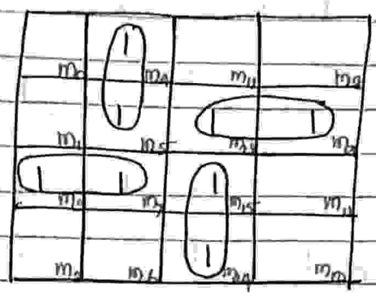


Figure 42.

K-map

Example : 1

A Boolean fn/ is represented by K-map.



Soln:

The gn/ fn/ is $m_3 + m_4 + m_5 + m_7 + m_9 + m_{13} + m_{14} + m_{15}$.

$= (m_3 + m_7) + (m_4 + m_5) + (m_9 + m_{13}) + (m_{14} + m_{15})$

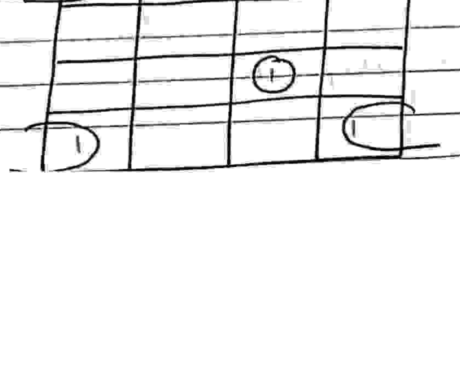
$= (a'b'cd + a'bcd) + (a'bc'd' + a'bc'd) + (ab'c'd + abc'd) + (abcd' + abcd)$

$= acd(b+b') + a'bc'(d+d') + ac'd(b+b') + abc(d+d')$

$= acd + a'bc' + ac'd + abc.$

——— x ———

Example : 3



$$x_2 x_3' x_4 = x_2 x_3' x_4 (x_1 \vee x_1')$$

$$= x_1 x_2 x_3' x_4 \vee x_1' x_2 x_3' x_4$$

$$= m_{13} + m_5$$

$$x_2' x_3 x_4 = x_2' x_3 x_4 (x_1 \vee x_1')$$

$$= x_1 x_2' x_3 x_4 \vee x_1' x_2' x_3 x_4$$

$$= m_{11} + m_3.$$

m_0	m_4	m_{12}	m_8
m_1	m_5 1	m_{13} 1	m_9
m_3 1	m_7 1	m_{15} 1	m_{11} 1
m_2	m_6	m_{14} 1	m_{10} 1

$$f(x_1, x_2, x_3, x_4) = (m_{15} + m_{11} + m_{14} + m_{10}) + (m_3 + m_7 + m_{15} + m_{11})$$

$$+ (m_5 + m_3 + m_7 + m_{15})$$

$$= (x_1 x_2 x_3 x_4 + x_1 x_2' x_3 x_4 + x_1 x_2 x_3 x_4' + x_1 x_2' x_3 x_4')$$

$$+ (x_1' x_2' x_3 x_4 + x_1' x_2 x_3 x_4 + x_1 x_2 x_3 x_4 + x_1 x_2' x_3 x_4)$$

$$+ (x_1' x_2 x_3' x_4 + x_1 x_2 x_3' x_4 + x_1' x_2 x_3 x_4 + x_1 x_2 x_3 x_4)$$

$$= (m_0 + m_1 + m_2 + m_3) + (m_{10} + m_{11} + m_{14} + m_{15})$$

$$+ \quad (m_{12} + m_{14})$$

$$= (x_1'x_2'x_3'x_4' + x_1'x_2'x_3'x_4 + x_1'x_2'x_3x_4' + x_1'x_2'x_3x_4)$$

$$+ (x_1x_2'x_3x_4' + x_1x_2'x_3x_4 + x_1x_2x_3x_4' + x_1x_2x_3x_4)$$

$$+ (x_1x_2x_3'x_4' + x_1x_2x_3x_4')$$

$$= (x_1'x_2'x_3' + x_1'x_2'x_3) + (x_1x_2'x_3 + x_1x_2x_3)$$

$$+ \quad x_1x_2x_4'$$

$$= x_1'x_2' + x_1x_3 + x_1x_2x_4'$$

—— X ——

Then $f(a_1, a_2, a_3) = a_1a_2 + a_1a_3 + a_2a_3$. The symbolic representation is given in Figure 49.

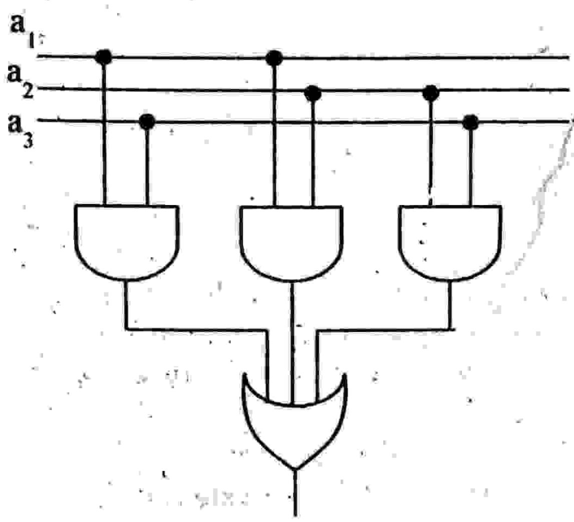


Figure 49.

W.E.6. Consider the Boolean function

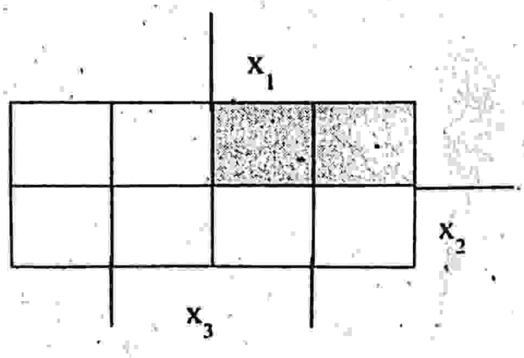
$$f(x_1, x_2, x_3) = ((x_1 + x_2) + (x_1 + x_3)). x_1.\bar{x}_2$$

Simplify this function and draw the circuit gate diagram for it.

(Apr'99, B.E., M.K.U.)

Solution.

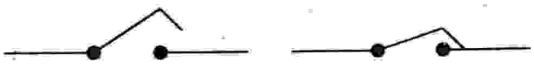
Use Karnaugh map to simplify the given function.



§ 8. SWITCHING CIRCUITS

Electrical switches or contacts can be symbolized in a switching or a circuit diagram or contact sketch :

Such a switch can be bi-stable, either 'open' or 'closed'. Open and closed switches are symbolized as

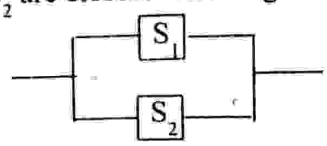


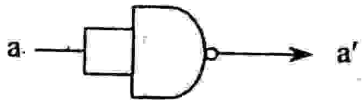
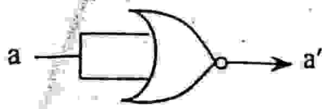
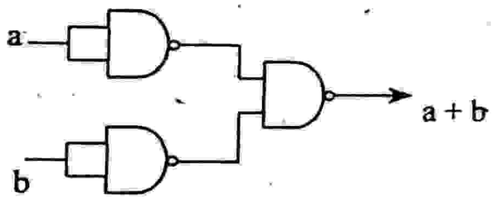
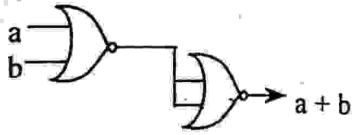
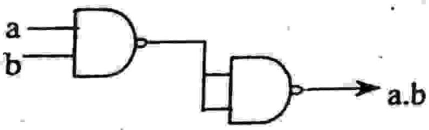
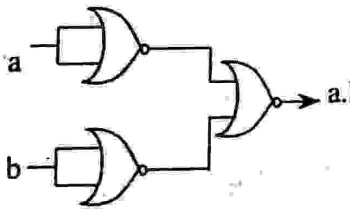
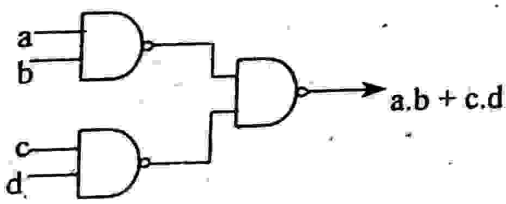
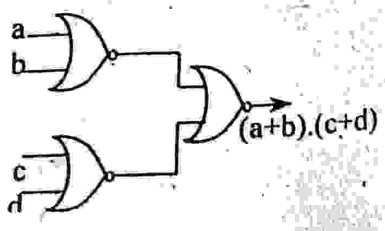
respectively. The basic assumption is that for current to flow through a switch it is necessary that the switch be closed.

If S_1 appears in two separate places in a circuit it means that there are two separate switches linked so as to ensure that they are always either both open or both closed.

S_1' indicates a switch which is the complement of S_1. The switch S_1' is closed if and only if S_1 is open. The diagram

is called series connection and we have current if and only if either or both of S_1 and S_2 are closed. The diagram



	Only NAND Gates	Only NOR Gates
1.		
2.		
3.		
4.		(See Exercises)
5.	(See Exercises)	

4. The Boolean polynomial p for the symbolic representation of the circuit given in Figure 43 is $p = x_1x_2' + x_2x_3$.

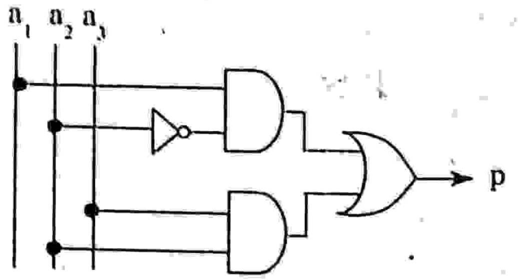


Figure 43.

Worked Examples

W.E.1. A hall light is controlled by two switches, one upstairs and one down stairs. Design a circuit so that the light can be switched on or off from the upstairs or the downstairs.

Solution

A hall light is controlled by two switches x_1 and x_2. They take the value 0 when they are up and 1 when they are down. Let f be the function that determines whether the light is on or off. Suppose f = 0 when the light is off and the light is off when both the switches are up. The function value table is given below :

x_1	x_2	f
0	0	0
0	1	1
1	0	1
1	1	0

So $f(x_1, x_2) = x_1'x_2 + x_1x_2'$. The circuit is given in Figure 44.

W.E.2. In a large room there are electrical switches next to the three doors to operate the central lighting. Each switch has two positions : either on or off. Each switch can switch on or switch off the lights. Determine the switching circuit p, and its symbolic representation.

Boolean Polynomials.

Example 3.

Express the polynomial $P(x_1, x_2, x_3) = x_1 \vee x_2$ in an equivalent Sum-of-Products Canonical form in three Variables x_1, x_2 and x_3.

Soln:

$$x_1 \vee x_2 = \left(x_1 \wedge (x_2 \vee x_2')\right) \vee \left(x_2 \wedge (x_1 \vee x_1')\right)$$

$$= (x_1 \wedge x_2) \vee (x_1 \wedge x_2') \vee (x_2 \wedge x_1) \vee (x_2 \wedge x_1')$$

$$= (x_1 \wedge x_2) \vee (x_1 \wedge x_2') \vee (x_1' \wedge x_2)$$

$$= \left((x_1 \wedge x_2) \wedge (x_3 \vee x_3')\right) \vee \left((x_1 \wedge x_2') \wedge (x_3 \vee x_3')\right) \vee \left((x_1' \wedge x_2) \wedge (x_3 \vee x_3')\right)$$

$$= (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3') \vee (x_1 \wedge x_2' \wedge x_3)$$
$$(x_1 \wedge x_2' \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3) \vee (x_1' \wedge x_2 \wedge x_3')$$

$$= m_2 \vee m_3 \vee m_4 \vee m_5 \vee m_6 \vee m_7.$$

— × —

W.E: 1 Find the PDNF of $P(x_1, x_2, x_3) = (x_2 + x_1 x_3)\overline{((x_1 + x_3)x_2)}$

Soln: $(x_2 + x_1 x_3)\overline{((x_1 + x_3)x_2)} = (x_2 + x_1 x_3)(\overline{x_1}\,\overline{x_3} + \overline{x_2})$

$$= x_2 \overline{x_1}\,\overline{x_3} + x_2 \overline{x_2} + x_1 x_3 \overline{x_1}\,\overline{x_3} + x_1 x_3 \overline{x_2}$$

$$= x_2 \overline{x_1}\,\overline{x_3} + x_1 x_3 \overline{x_2} \quad \text{as} \quad x_2\overline{x_2} = x_1\overline{x_1} = 0$$

$$= \overline{x_1}\, x_2\, \overline{x_3} + x_1 \overline{x_2}\, x_3.$$

— × —

is called parallel connection and we have current if and only if either or both of S_1 and S_2 are closed.

These properties of electrical switches allow the use of Boolean algebras in modeling and simplifying switching circuits. We write $x + y$ and xy for $x \vee y$ and $x \wedge y$ respectively.

Definitions

Let $X_n = \{x_1, x_2, \ldots, x_n\}$. The elements $x_1, x_2, \ldots, x_n$ are called switches. Let $\mathbf{P}_n$ be the set of all Boolean polynomials over $x_1, x_2, \ldots, x_n$.
Each element of $\mathbf{P}_n$ is called switching circuit.
To each x_i, x_i' is called the complementation switch of x_i.
x_ix_j is called the series connection of x_i and x_j.
$x_i + x_j$ is called the parallel connection of x_i and x_j.
To each $p \in \mathbf{P}_n$, the corresponding function $\widetilde{p} : \mathbf{B}^n \rightarrow \mathbf{B}$ is called the switching function of p.

Each switching circuit can be represented by a contact diagram. (We use x_i for the switch S_i.) For example, the circuit $x_1x_2 + x_3(x_1 + x_2)$ can be represented by the contact diagram given in Figure 38.

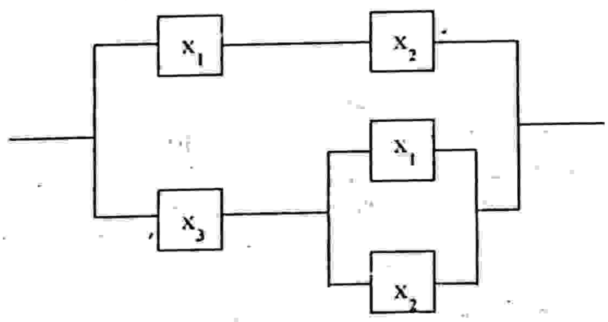


Figure 38. Contact Diagram for $x_1x_2 + x_3(x_1 + x_2)$

Each contact diagram can be represented by a polynomial in $\mathbf{P}_n$. For example the contact diagram given in Figure 39 can be represented by the polynomial $x_1(x_2x_3 + x_2x_3' + x_2'x_3')$.

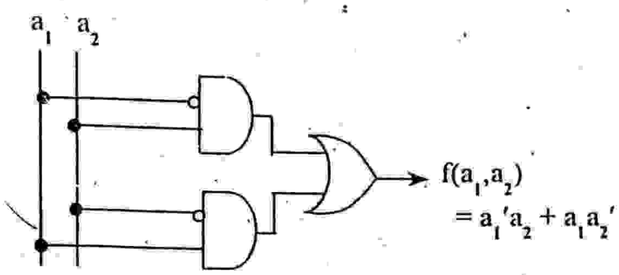


Figure 44.

Solution

We denote the switches by x_1, x_2, x_3 and two possible states of the switches x_i by $a_i \in \{0, 1\}$. The light situation in the room is given by the value

$\tilde{p}(a_1, a_2, a_3)$ = 0 if the light is off and
= 1 if the light is on.

We choose $\tilde{p}(1, 1, 1) = 1$.

If we operate one or all the three switches then the light goes off. i.e., $\tilde{p}(a_1, a_2, a_3) = 0$ if (a_1, a_2, a_3) differs in one or in three places from (1, 1, 1).

If we operate two switches, the light stay on. So $\tilde{p}(a_1, a_2, a_3) = 1$ if (a_1, a_2, a_3) differs in zero place or in two places from (1, 1, 1).

Table

a_1	a_2	a_3	Minterms	$\tilde{p}(a_1, a_2, a_3)$
1	1	1	$x_1x_2x_3$	1
1	1	0	$x_1x_2x_3'$	0
1	0	1	$x_1x_2'x_3$	0
1	0	0	$x_1x_2'x_3'$	1
0	1	1	$x_1'x_2x_3$	0
0	1	0	$x_1'x_2x_3'$	1
0	0	1	$x_1'x_2'x_3$	1
0	0	0	$x_1'x_2'x_3'$	0

$$x_1 x_2 x_4' = x_1 x_2 x_4' \,(x_3 \vee x_3')$$

$$= x_1 x_2 x_3 x_4' \vee x_1 x_2 x_3' x_4'$$

$$= m_{14} + m_{12}$$

$$x_2' x_3 = x_2' x_3 \big((x_1 \vee x_1')(x_4 \vee x_4')\big)$$

$$= x_2' x_3 \,(x_1 x_4 \vee x_1 x_4' \vee x_1' x_4 \vee x_1' x_4')$$

$$= x_1 x_2' x_3 x_4 \vee x_1 x_2' x_3 x_4' \vee x_1' x_2' x_3 x_4$$

$$\vee\, x_1' x_2' x_3 x_4'$$

$$= m_{11} + m_{10} + m_3 + m_2$$

$$f(x_1, x_2, x_3, x_4) = (m_3 + m_2 + m_1 + m_0) + (m_{15} + m_{11})$$

$$+ (m_{14} + m_{12}) + (m_{11} + m_{10} + m_3 + m_2)$$

m_0 1	m_4	m_{12} 1	m_8
m_1 1	m_5	m_{13}	m_9
m_3 1	m_7	m_{15} 1	m_{11} 1
m_2 1	m_6	m_{14} 1	m_{10} 1

$= m_{15} + (m_0 + m_4 + m_{12} + m_8) + (m_2 + m_{10} + m_8 + m_0)$

$= abcd + (a'b'c'd' + a'bc'd' + abc'd' + ab'c'd')$
$+ (a'b'cd' + ab'cd' + ab'c'd' + a'b'c'd')$

$= abcd + (b'c'd'(a+a') + bc'd'(a+a')) +$
$(a'b'd'(c+c') + ab'd'(c+c'))$

$= abcd + c'd' + b'd'$

—— x ——

W.E:1 Simplify the following using K-map.

$f(x_1, x_2, x_3, x_4) = x_1x_3 + x_1'x_3x_4 + x_2x_3'x_4 + x_2'x_3x_4'$

Soln:-

$x_1x_3 = \boxed{x_1x_3\,(x_2 \vee x_2')(x_4 \vee x_4')}$

$= x_1x_3\,(x_2x_4 \vee x_2x_4' \vee x_2'x_4 \vee x_2'x_4')$

$= x_1x_2x_3x_4 + x_1x_2x_3x_4' + x_1x_2'x_3x_4 + x_1x_2'x_3x_4'$
$= m_{15} + m_{14} + m_{11} + m_{10}.$

$x_1'x_3x_4 = x_1'x_3x_4\,(x_2 \vee x_2')$

$= x_1'x_2x_3x_4 \vee x_1'x_2'x_3x_4$

$= m_7 + m_3.$

So S and C have the disjunctive normal forms $x_1x_2' + x_1'x_2$ and x_1x_2, respectively.
The corresponding circuit is given in Figure 46.

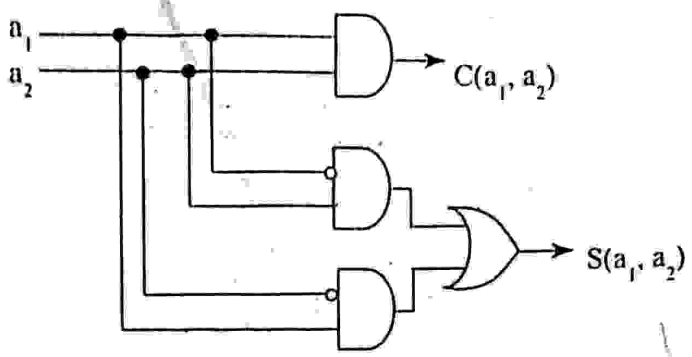


Figure 46.

By modifying S we can obtain a simplex circuit:

$$
\begin{aligned}
S &= x_1x_2' + x_1'x_2 \\
&\sim (x_1' + x_2)' + (x_1 + x_2')' && \text{using } (x \wedge y)' = x' \vee y' \\
&\sim ((x_1' + x_2)(x_1 + x_2'))' && \text{using } x \vee y = (x' \wedge y')' \\
&\sim (x_1'x_1 + x_2x_1 + x_1'x_2' + x_2x_2')' && \text{as } x_1x_1' = x_2x_2' = 0 \\
&\sim (x_1x_2 + x_1'x_2')' \\
&\sim (x_1x_2)'(x_1'x_2')' \\
&\sim C'(x_1 + x_2)
\end{aligned}
$$

This leads to the circuit given in Figure 47.

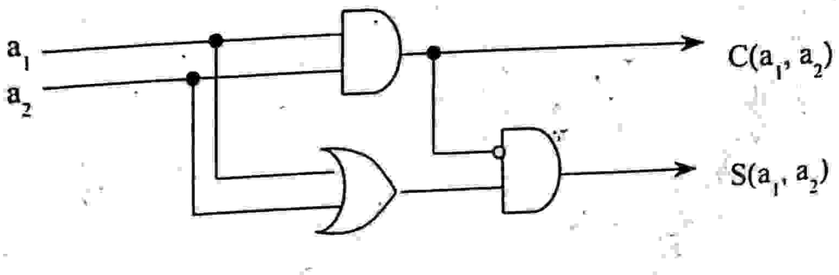


Figure 47.