`

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited “A” Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – I–DISCRETE MATHEMATICS – SMT1304

`

UNIT I- LOGIC

Statements and Notations,Connectives,Negation,Conjunction,Disjunction, statement, Formulae and TruthTables ,Conditional and Bi-conditional,Well–formed Formulae, Tautologies, EquivalenceofFormulae,DualityLaw, Tautological Implications.

Definition: Propositional Logic

A proposition is a collection of declarative statements that has either a truth value "true” or a truth value "false". A propositional consists of propositional variables and connectives. We denote the propositional variables by capital letters (A, B, C etc). The connectives connect the propositional variables.

Some examples of Propositions are given below:

- "Man is Mortal", it returns truth value“TRUE” as T.
- "12 + 9 = 3 − 2", it returns truth

value “FALSE” as F.

The following is not a Proposition

- "A is less than 2". It is because unless we give a specific value of A, we cannot say whether the statement is true orfalse.

Connectives

In propositional logic generally we use five connectives which are OR $(\vee)$, AND $(\wedge)$, Negation/ NOT (¬), Conditional or Implication / if-then (→), Bi conditional or If and only if $(\leftrightarrow)$.

Negation (¬) − The negation of a proposition A (written as ¬A) is false when A is true and is true when A is false.

The truth table is as follows –

A	**¬A**
True	False

False	True

AND (∧) − The AND operation of two propositions A and B (written as A ∧ B) is true if both the propositional variable A and B is true.

The truth table is as follows −

A	**B**	**A∧ B**
True	True	False
True	False	False
False	True	False
False	False	True

OR (∨)− The OR operation of two propositions A and B (written as A ∨ B) is true if at least any of the propositional variable A or B is true.

The truth table is as follows −

A	**B**	**A ∨ B**
T	T	T
T	F	T
F	T	T
F	F	F

Implication / if-then (→) − An implication A→B is False if A is true and B is false. The rest cases are true.

The truth table is as follows −

A	B	A → B
True	True	True
True	False	False
False	True	True
False	False	True

If and only if (↔)− A ↔B is bi-conditional logical connective which is true when p and q are both false or both are true.

The truth table is as follows −

A	B	A ↔ B
True	True	True
True	False	False
False	True	False
False	False	True

Well Formed Formulas(WFFs)

The well formed formulas(WFFs) or statement formulas or logic formulas are defined recursively (or inductively) as below.

1. Propositional variables p,q,r,… and propositional constants F,T are well formed formulas. They are known as primitive WFFs.

2. If P and Q are WFFs then $\neg P, \neg Q, P \wedge Q, P \vee Q, P \to Q \; and \; P \leftrightarrow Q$ are also WFFs.
3. All WFFs are obtained by the above procedures applied a finite number of times.
   For example, the following are WFFs
   $p,\ p \wedge q,\ p \to q,\ p \wedge (q \to r) \equiv (p \wedge q) \to r, (p \to q) \to (q \to p)$

Note: In order to avoid excessive use of parenthesis, we adopt an order of precedence for logical Operators.

$\neg, \wedge, \vee, \to \; and \; \leftrightarrow$

Tautologies

A Tautology is a formula which is always true for every value of its propositional variables.

Example − Prove [(A → B) ∧ A] → B is a tautology

The truth table is as follows −

A	B	A → B	(A → B) ∧ A	[(A → B) ∧ A] → B
True	True	True	True	True
True	False	False	False	True
False	True	True	False	True
False	False	True	False	True

As we can see every value of [(A → B) ∧ A] → B is “True”, it is a tautology.

Contradictions

A Contradiction is a formula which is always false for every value of its propositional variables.

Example − Prove (A VB) ∧ [(¬A) ∧ (¬B)] is a contradiction

The truth table is as follows −

A	B	A ∨ B	¬A	¬B	(¬A) ∧ (¬B)	(A V B) ∧ [(¬A) ∧ (¬B)]
True	True	True	False	False	False	False
True	False	True	False	True	False	False
False	True	True	True	False	False	False
False	False	False	True	True	True	False

As we can see every value of (A ∨ B) ∧ [(¬A) ∧ (¬B)] is “False”, it is a Contradiction.

Contingency

A Contingency is a formula which has both some true and some false values for every value of its propositional variables.

Example − Prove (A ∨ B) ∧ (¬A) a contingency

The truth table is as follows −

A	B	A ∨ B	¬A	(A ∨ B) ∧ (¬A)
True	True	True	False	False
True	False	True	False	False
False	True	True	True	True
False	False	False	True	False

As we can see every value of (A ∨ B) ∧ (¬A) has both “True” and “False”, it is a contingency.

Propositional Equivalences

Two statements X and Y are logically equivalent if any of the following two conditions −

- The truth tables of each statement have the same truthvalues.
- The bi-conditional statement X ↔Y is a tautology.

Example−Prove¬(A ∨ B)and[(¬A) ∧ (¬B)]areequivalent

Testing by 1st method (Matching truth table)

A	**B**	**A ∨ B**	**¬ (A ∨ B)**	**¬A**	**¬B**	**[(¬A) ∧ (¬B)]**
True	True	True	False	False	False	False
True	False	True	False	False	True	False
False	True	True	False	True	False	False
False	False	False	True	True	True	True

Here, we can see the truth values of ¬ (A ∨ B) and [(¬A) ∧ (¬B)] are same, hence the statements are equivalent.

Testing by 2nd method (Bi-conditionality)

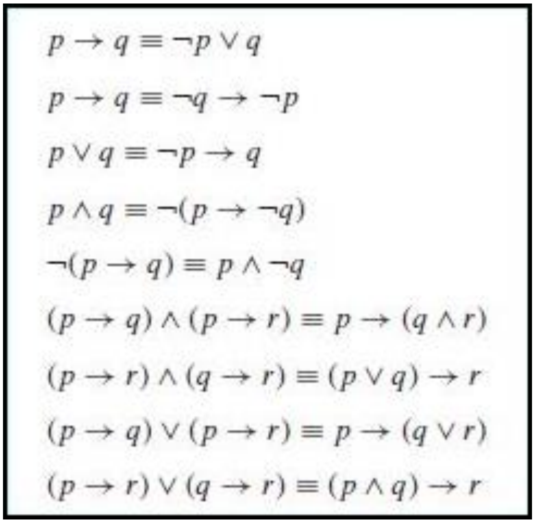
A	**B**	**¬ (A ∨ B)**	**[(¬A) ∧ (¬B)]**	**[¬ (A ∨ B)]↔ [(¬A) ∧ (¬B)]**
True	True	False	False	True
True	False	False	False	True
False	True	False	False	True
False	False	True	True	True

As [¬ (A ∨ B)] ↔ [(¬A) ∧ (¬B)] is a tautology, the statements are equivalent.

Laws of Propositional Logic:

S.No	Name of Laws	Primal Form	Dual Form
1	Idempotent Law	$p \vee p \equiv p$	$p \wedge p \equiv p$
2	Identity Law	$p \vee F \equiv p$	$p \wedge T \equiv p$
3	Dominant Law	$p \vee T \equiv T$	$p \wedge F \equiv F$
4	Complement Law	$p \vee \neg p \equiv T$	$p \wedge \neg p \equiv F$
5	Commutative Law	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
6	Associative Law	$p \vee (q \vee r) \equiv (p \vee q) \vee r$	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
7	Distributive Law	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \wedge (p \wedge r)$
8	Absorption Law	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
9	De Morgan's Law	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
10	Double Negation Law	$\neg(\neg p) \equiv p$	-

Logical Equivalences involving Conditional Statements



$p \to q \equiv \neg p \vee q$

$p \to q \equiv \neg q \to \neg p$

$p \vee q \equiv \neg p \to q$

$p \wedge q \equiv \neg(p \to \neg q)$

$\neg(p \to q) \equiv p \wedge \neg q$

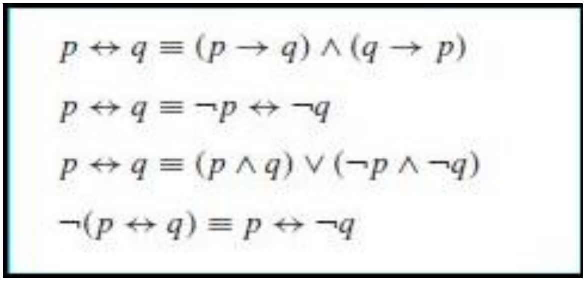
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

Logical Equivalences involving Biconditional Statements



$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Inverse, Converse, and Contra-positive

A conditional statement has two parts − **Hypothesis** and **Conclusion**.

Example of Conditional Statement − “If you do your homework, you will not be punished.” Here, "you do your homework" is the hypothesis and "you will not be punished" is the conclusion.

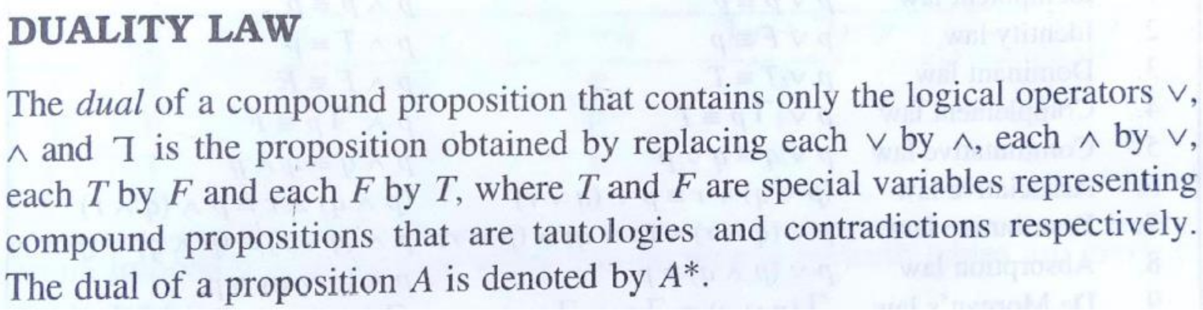
Inverse –An inverse of the conditional statement is the negation of both the hypothesis and the conclusion. If the statement is “If p, then q”, the inverse will be “If not p, then not q”. The inverse of “If you do your homework, you will not be punished” is “If you do not do your homework, you will be punished.”

Converse−The converse of the conditional statement is computed by interchanging the hypothesis and the conclusion. If the statement is “If p, then q”, the inverse willbe “If *q*, then*p*”. The converse of "If you do your homework, you will not be punished" is "If you will not be punished, you do not do your homework”.

Contra-positive –The contra-positive of the conditional is computed by interchanging the hypothesis and the conclusion of the inverse statement. If the statement is “If p, then q”, the inverse will be “If not *q*, then not *p*”. The Contra-positive of "If you do your homework, you will not be punished” is "If you will be punished, you do yourhomework”.

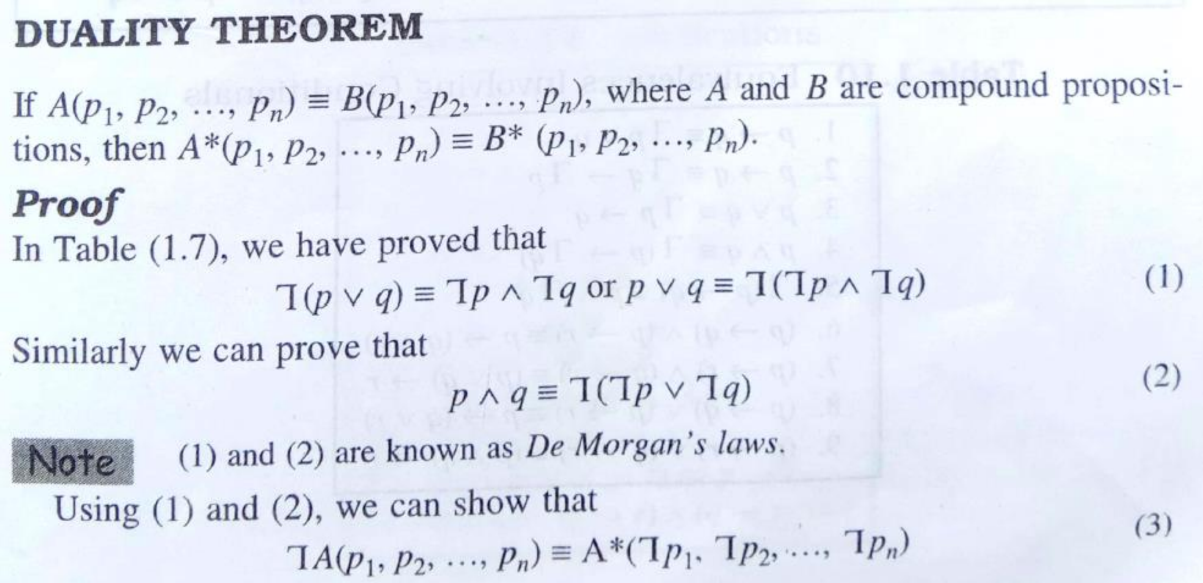
Duality Principle

Duality principle set states that for any true statement, the dual statement obtained by interchanging unions into intersections (and vice versa) and interchanging Universal set into Null set (and vice versa) is also true. If dual of any statement is the statement itself, it is said **self-dual**statement.



DUALITY LAW

The *dual* of a compound proposition that contains only the logical operators ∨, ∧ and ¬ is the proposition obtained by replacing each ∨ by ∧, each ∧ by ∨, each *T* by *F* and each *F* by *T*, where *T* and *F* are special variables representing compound propositions that are tautologies and contradictions respectively. The dual of a proposition *A* is denoted by *A**.



DUALITY THEOREM

If $A(p_1, p_2, \ldots, p_n) \equiv B(p_1, p_2, \ldots, p_n)$, where A and B are compound propositions, then $A^*(p_1, p_2, \ldots, p_n) \equiv B^*(p_1, p_2, \ldots, p_n)$.

Proof

In Table (1.7), we have proved that

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \text{ or } p \vee q \equiv \neg(\neg p \wedge \neg q) \qquad (1)$$

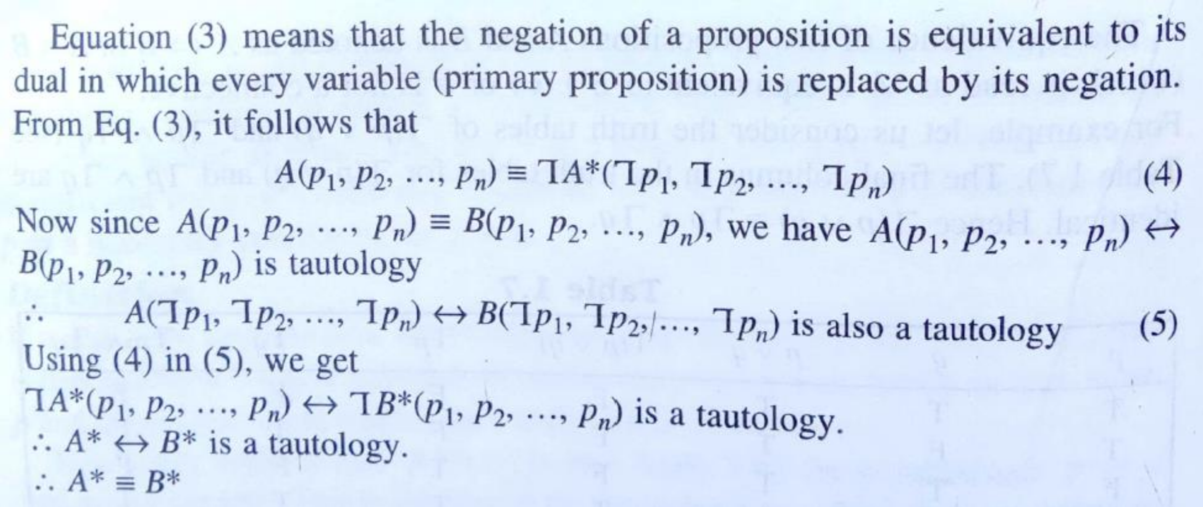
Similarly we can prove that

$$p \wedge q \equiv \neg(\neg p \vee \neg q) \qquad (2)$$

Note (1) and (2) are known as *De Morgan's laws.*

Using (1) and (2), we can show that

$$\neg A(p_1, p_2, \ldots, p_n) \equiv A^*(\neg p_1. \neg p_2, \ldots, \neg p_n) \qquad (3)$$



Equation (3) means that the negation of a proposition is equivalent to its dual in which every variable (primary proposition) is replaced by its negation. From Eq. (3), it follows that

$$A(p_1, p_2, \ldots, p_n) \equiv \neg A^*(\neg p_1, \neg p_2, \ldots, \neg p_n) \qquad (4)$$

Now since $A(p_1, p_2, \ldots, p_n) \equiv B(p_1, p_2, \ldots, p_n)$, we have $A(p_1, p_2, \ldots, p_n) \leftrightarrow B(p_1, p_2, \ldots, p_n)$ is tautology

$\therefore \quad A(\neg p_1, \neg p_2, \ldots, \neg p_n) \leftrightarrow B(\neg p_1, \neg p_2, \ldots, \neg p_n)$ is also a tautology (5)

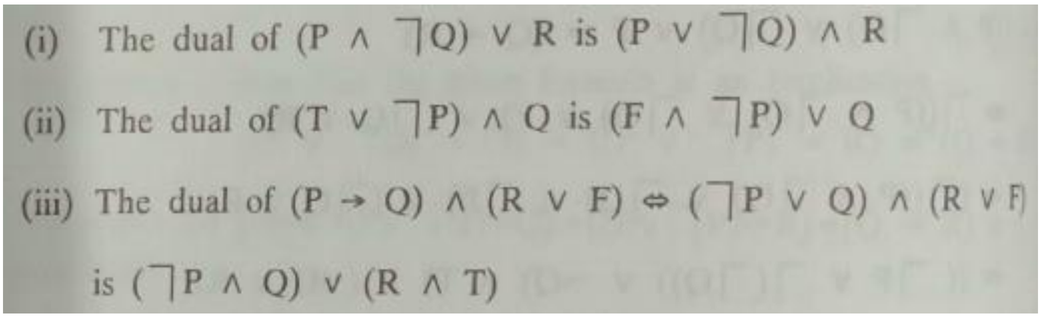
Using (4) in (5), we get

$\neg A^*(p_1, p_2, \ldots, p_n) \leftrightarrow \neg B^*(p_1, p_2, \ldots, p_n)$ is a tautology.

$\therefore A^* \leftrightarrow B^*$ is a tautology.

$\therefore A^* \equiv B^*$

Examples

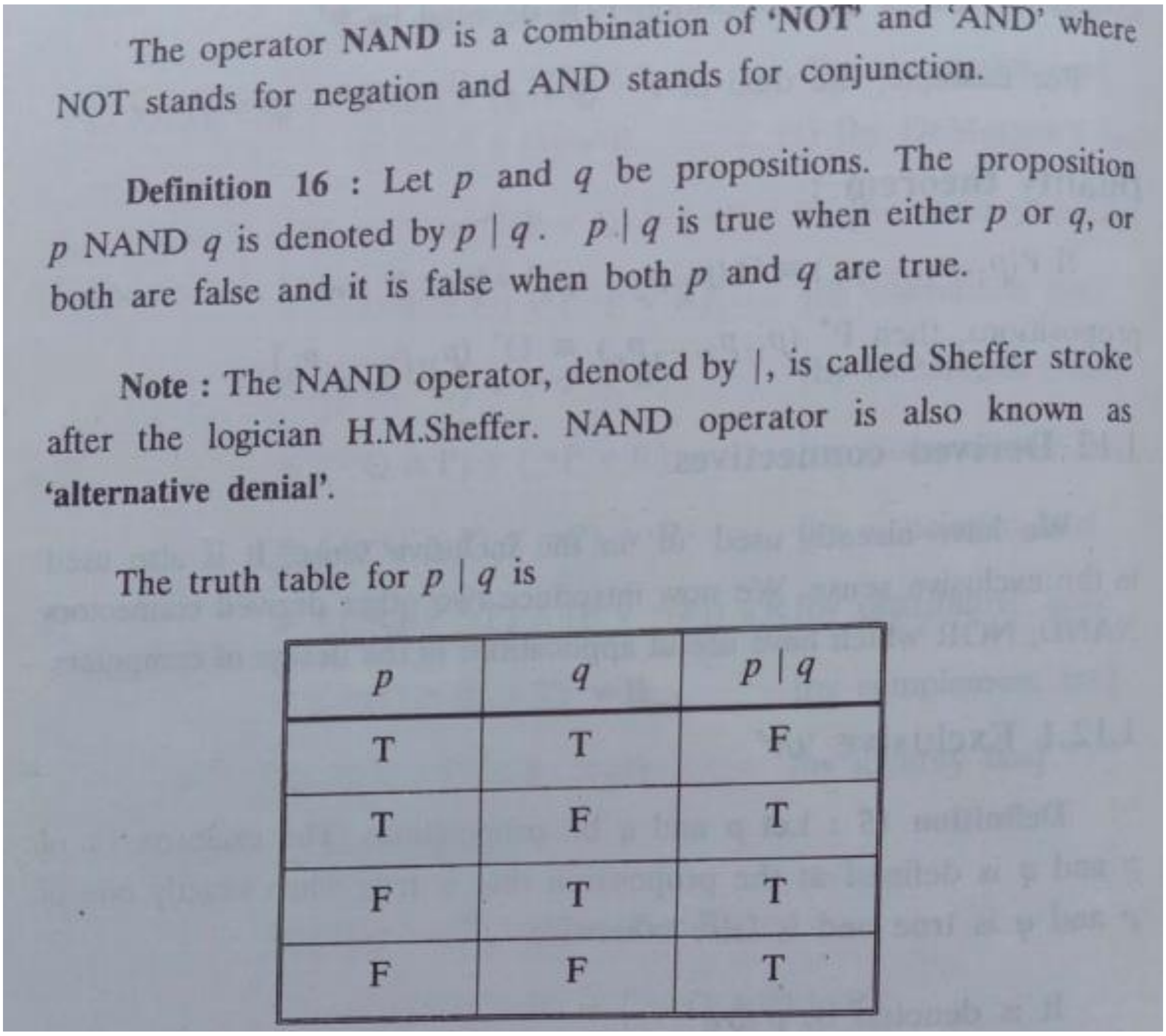


(i) The dual of $(P \wedge \neg Q) \vee R$ is $(P \vee \neg Q) \wedge R$

(ii) The dual of $(T \vee \neg P) \wedge Q$ is $(F \wedge \neg P) \vee Q$

(iii) The dual of $(P \rightarrow Q) \wedge (R \vee F) \Leftrightarrow (\neg P \vee Q) \wedge (R \vee F)$ is $(\neg P \wedge Q) \vee (R \wedge T)$

NAND OPERATOR



The operator **NAND** is a combination of **'NOT'** and 'AND' where NOT stands for negation and AND stands for conjunction.

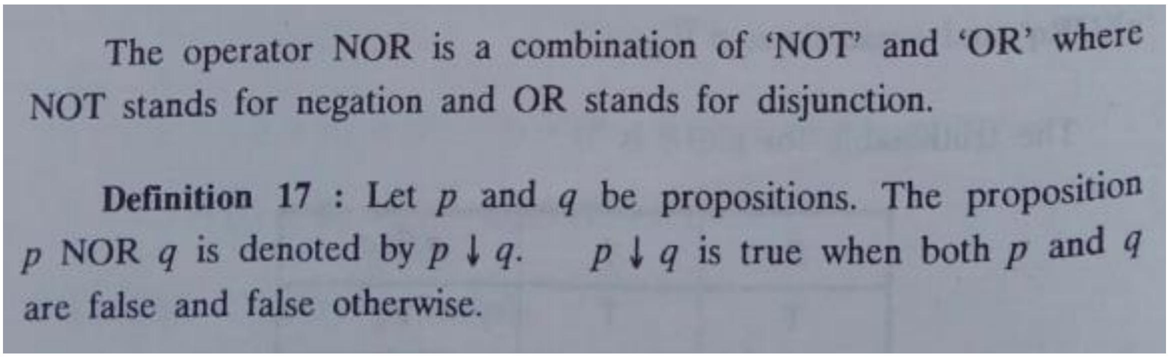
Definition 16 : Let p and q be propositions. The proposition p NAND q is denoted by $p \mid q$. $p \mid q$ is true when either p or q, or both are false and it is false when both p and q are true.

Note : The NAND operator, denoted by |, is called Sheffer stroke after the logician H.M.Sheffer. NAND operator is also known as **'alternative denial'**.

The truth table for $p \mid q$ is

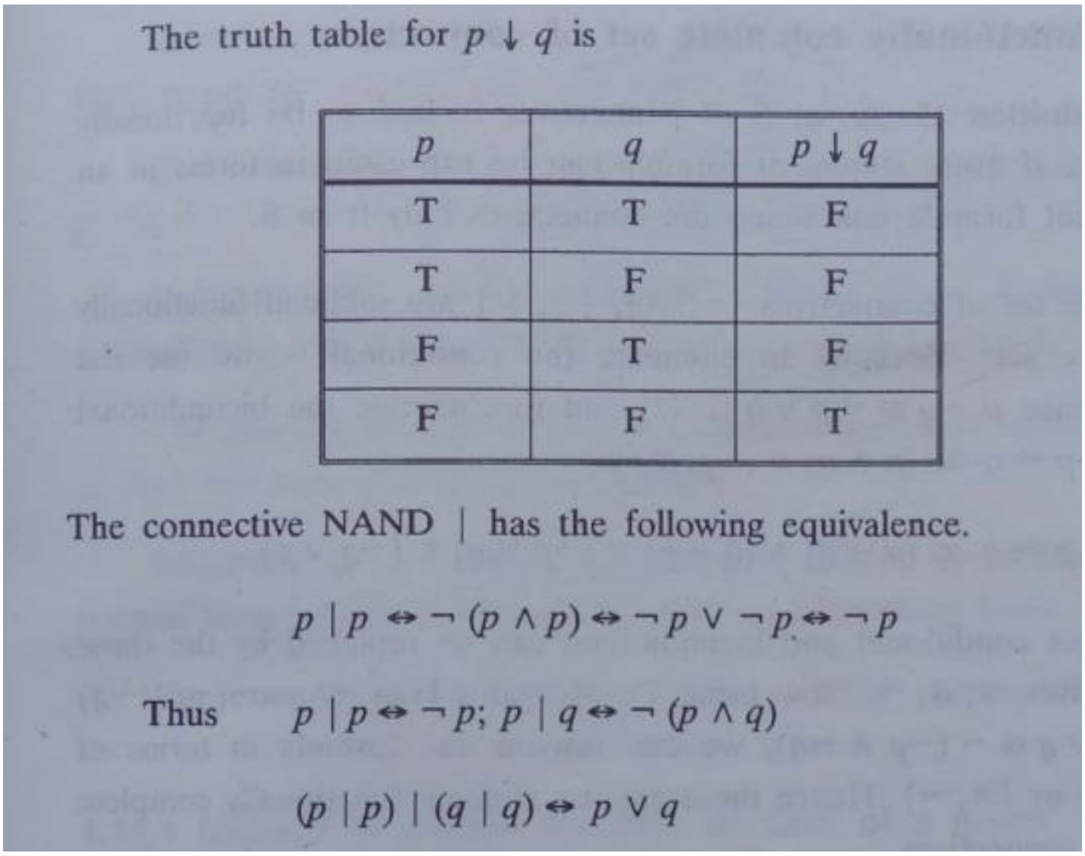
p	q	$p \mid q$
T	T	F
T	F	T
F	T	T
F	F	T

NOR OPERATOR



The operator NOR is a combination of 'NOT' and 'OR' where NOT stands for negation and OR stands for disjunction.

Definition 17 : Let p and q be propositions. The proposition p NOR q is denoted by $p \downarrow q$. $p \downarrow q$ is true when both p and q are false and false otherwise.



The truth table for $p \downarrow q$ is

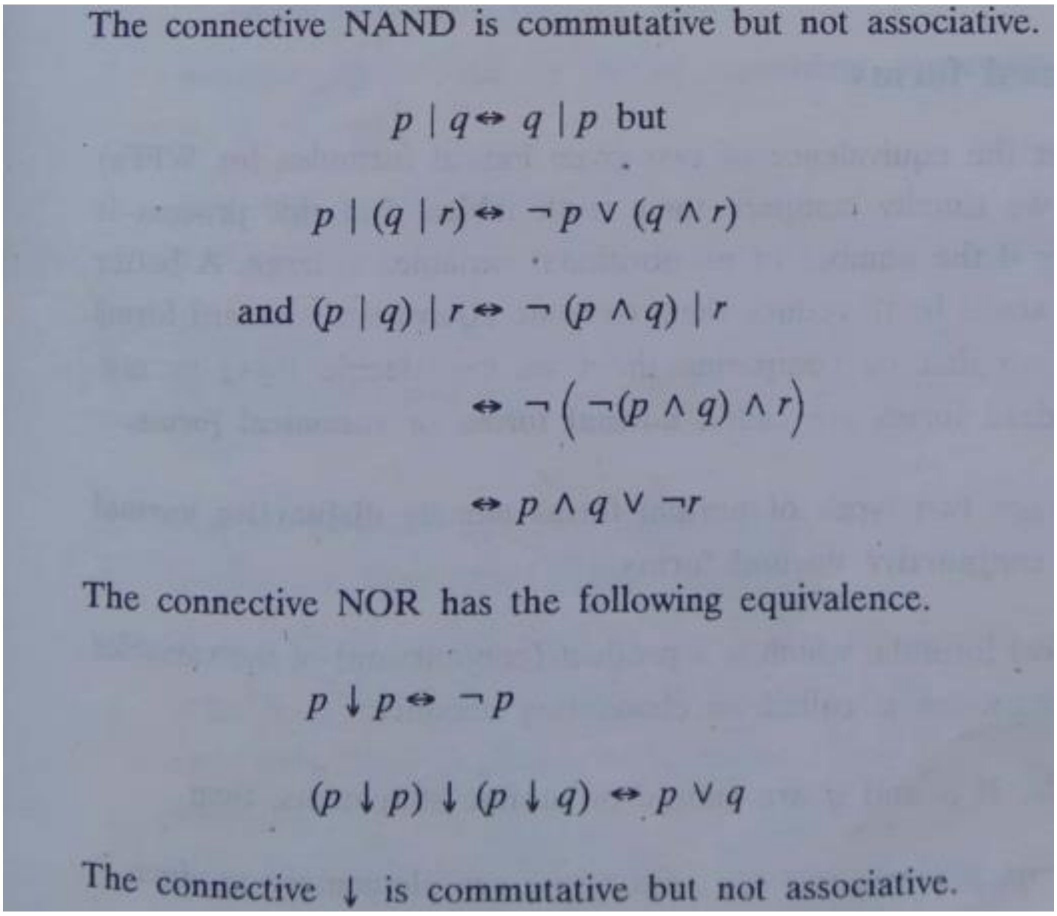
p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

The connective NAND | has the following equivalence.

$$p \mid p \Leftrightarrow \neg (p \wedge p) \Leftrightarrow \neg p \vee \neg p \Leftrightarrow \neg p$$

Thus $p \mid p \Leftrightarrow \neg p; \; p \mid q \Leftrightarrow \neg (p \wedge q)$

$$(p \mid p) \mid (q \mid q) \Leftrightarrow p \vee q$$



The connective NAND is commutative but not associative.

$$p \mid q \Leftrightarrow q \mid p \text{ but}$$

$$p \mid (q \mid r) \Leftrightarrow \neg p \vee (q \wedge r)$$

$$\text{and } (p \mid q) \mid r \Leftrightarrow \neg (p \wedge q) \mid r$$

$$\Leftrightarrow \neg \left(\neg(p \wedge q) \wedge r \right)$$

$$\Leftrightarrow p \wedge q \vee \neg r$$

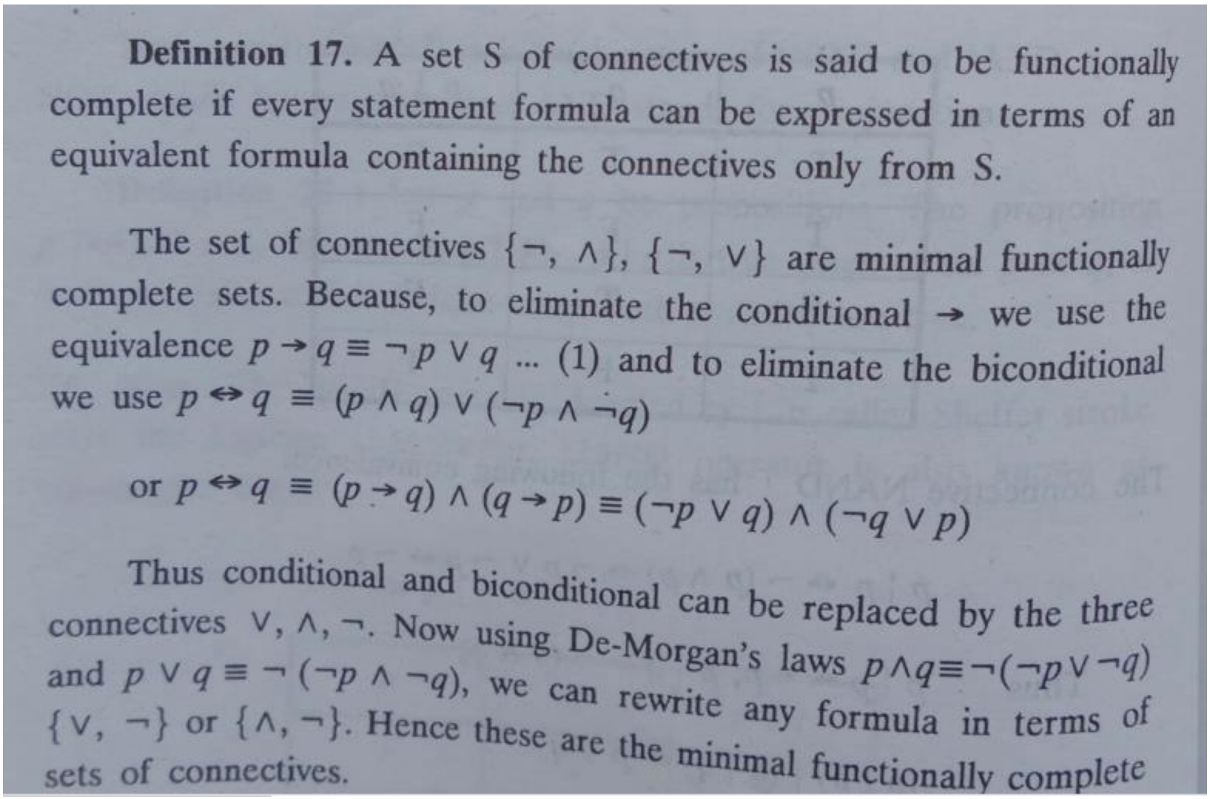
The connective NOR has the following equivalence.

$$p \downarrow p \Leftrightarrow \neg p$$

$$(p \downarrow p) \downarrow (p \downarrow q) \Leftrightarrow p \vee q$$

The connective ↓ is commutative but not associative.

Functionally Complete set of Connectives



Definition 17. A set S of connectives is said to be functionally complete if every statement formula can be expressed in terms of an equivalent formula containing the connectives only from S.

The set of connectives $\{\neg, \wedge\}$, $\{\neg, \vee\}$ are minimal functionally complete sets. Because, to eliminate the conditional → we use the equivalence $p \rightarrow q \equiv \neg p \vee q$ ... (1) and to eliminate the biconditional we use $p \Leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

or $p \Leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p) \equiv (\neg p \vee q) \wedge (\neg q \vee p)$

Thus conditional and biconditional can be replaced by the three connectives $\vee, \wedge, \neg$. Now using De-Morgan's laws $p \wedge q \equiv \neg(\neg p \vee \neg q)$ and $p \vee q \equiv \neg(\neg p \wedge \neg q)$, we can rewrite any formula in terms of $\{\vee, \neg\}$ or $\{\wedge, \neg\}$. Hence these are the minimal functionally complete sets of connectives.

`

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – II–DISCRETE MATHEMATICS – SMT1304

`

UNIT II- INFERENCE THEORY

Normal Forms, Disjunctive Normal Forms, Conjunctive Normal Forms, Principal Disjunctive Normal Forms, Principal Conjunctive Normal Forms, Rules of Inference, the Predicate Calculus, Predicates, Variables and Quantifiers, Predicate Formula, Free and Bound Variables.

Elementary Product: A product of the variables and their negations in a formula is called an elementary product. If p and q are any two atomic variables, then $p, \neg p \wedge q, \neg q \wedge p, \neg p \wedge \neg q$ are some examples of elementary products.

Elementary Sum: A sum of the variables and their negations in a formula is called an elementary sum. If P and Q are any two atomic variables, then $p, \neg p \vee q, \neg q \vee p, \neg p \vee \neg q$ are some examples of elementary sums.

Normal Forms: We can convert any proposition in two normal forms −

1. Conjunctive Normal Form (CNF) 2.Disjunctive Normal Form (DNF)

Conjunctive Normal Form

A compound statement is in conjunctive normal form if it is obtained by operating AND among variables (negation of variables included) connected with ORs.

Examples: 1. $(p \vee q) \wedge (q \vee r)$

2. $(\neg p \vee q \vee r) \wedge (s \vee r)$

Disjunctive Normal Form

A compound statement is in disjunctive normal form if it is obtained by operating OR among variables (negation of variables included) connected with ANDs.

Example: $(p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge \neg q \wedge \neg r)$

Functionally Complete set

A set of logical operators is called functionally complete if every compound proposition is logically equivalent to a compound proposition involving only this set of logical operators. $\wedge, \vee, \neg$ form a functionally complete set of operators.

Minterms: For two variables p and q there are 4 possible formulas which consist of conjunctions of p,q or it's negation given by
$p \wedge q, \neg p \wedge q, p \wedge \neg q, \neg p \wedge \neg q$

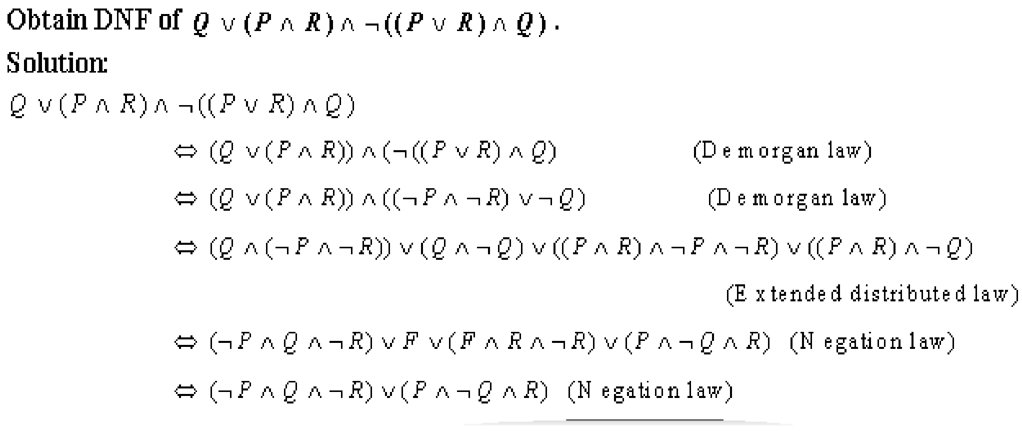
`

Maxterms: For two variables p and q there are 4 possible formulas which consist of disjunctions of p,q or its negation given by
$p \vee q, \neg p \vee q, \; p \vee \neg q, \neg p \vee \neg q$

Principal Disjunctive Normal Form: For a given formula an equivalent formula consisting of disjunctions of minterms only is known as principal disjunctive normal form (PDNF).

Principal Conjunctive Normal Form: For a given formula an equivalent formula consisting of conjunctions of maxterms only is known as principal conjunctive normal form (PCNF).

Problems:



Obtain DNF of $\boldsymbol{Q \vee (P \wedge R) \wedge \neg((P \vee R) \wedge Q)}$ **.**

Solution:

$Q \vee (P \wedge R) \wedge \neg((P \vee R) \wedge Q)$

$\Leftrightarrow (Q \vee (P \wedge R)) \wedge (\neg((P \vee R) \wedge Q)$ (Demorgan law)

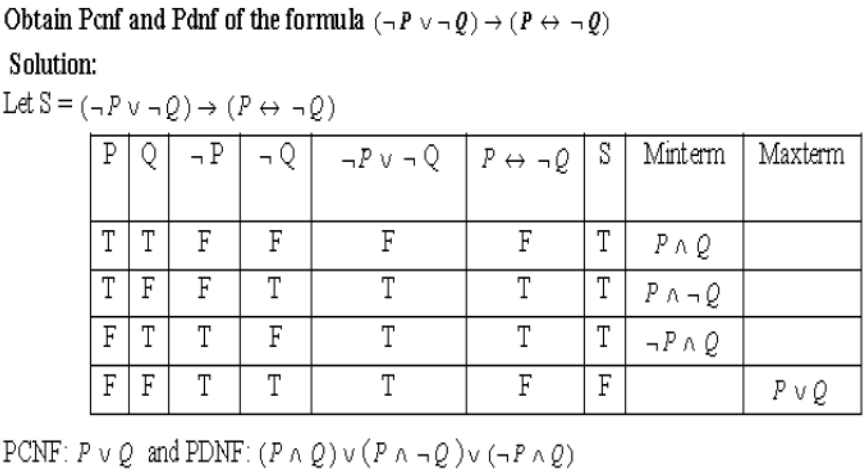
$\Leftrightarrow (Q \vee (P \wedge R)) \wedge ((\neg P \wedge \neg R) \vee \neg Q)$ (Demorgan law)

$\Leftrightarrow (Q \wedge (\neg P \wedge \neg R)) \vee (Q \wedge \neg Q) \vee ((P \wedge R) \wedge \neg P \wedge \neg R) \vee ((P \wedge R) \wedge \neg Q)$

(Extended distributed law)

$\Leftrightarrow (\neg P \wedge Q \wedge \neg R) \vee F \vee (F \wedge R \wedge \neg R) \vee (P \wedge \neg Q \wedge R)$ (Negation law)

$\Leftrightarrow (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R)$ (Negation law)



Obtain Pcnf and Pdnf of the formula $(\neg P \vee \neg Q) \rightarrow (P \leftrightarrow \neg Q)$

Solution:

Let S = $(\neg P \vee \neg Q) \rightarrow (P \leftrightarrow \neg Q)$

P	Q	¬ P	¬ Q	$\neg P \vee \neg Q$	$P \leftrightarrow \neg Q$	S	Minterm	Maxterm
T	T	F	F	F	F	T	$P \wedge Q$	
T	F	F	T	T	T	T	$P \wedge \neg Q$	
F	T	T	F	T	T	T	$\neg P \wedge Q$	
F	F	T	T	T	F	F		$P \vee Q$

PCNF: $P \vee Q$ and PDNF: $(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$

Consistency and Inconsistency of Premises

A set of formular H_1,H_2,....,H_m is said to be **inconsistent** if their conjunction implies Contradiction.
A set of formular H_1,H_2,....,H_m is said to be **consistent** if their conjunction implies Tautology.

Rules of Inference

Rule P: A premise may be introduced at anypoint in the derivation
Rule T: A formula S may be introduced at any point in a derivation if S is tautologically implied by any one or more of the preceedingformula.
Rule CP: If S can be derived from R and set of premises , then R S can be derived from the set ofpremises alone.

Inference Theory

The theory associated with checking the logical validity of the conclusion of the given set of premises by using Equivalence and Implication rule is called **Inference theory**

Direct Method

When a conclusion is derived from a set of premises by using the accepted rules of reasoning is called **direct method**.

Indirect method

While proving some results regarding logical conclusions from the set of premises, we use negation of the conclusion as an additional premise and try to arrive at a contradiction is called **Indirect method**

Rules of Inference

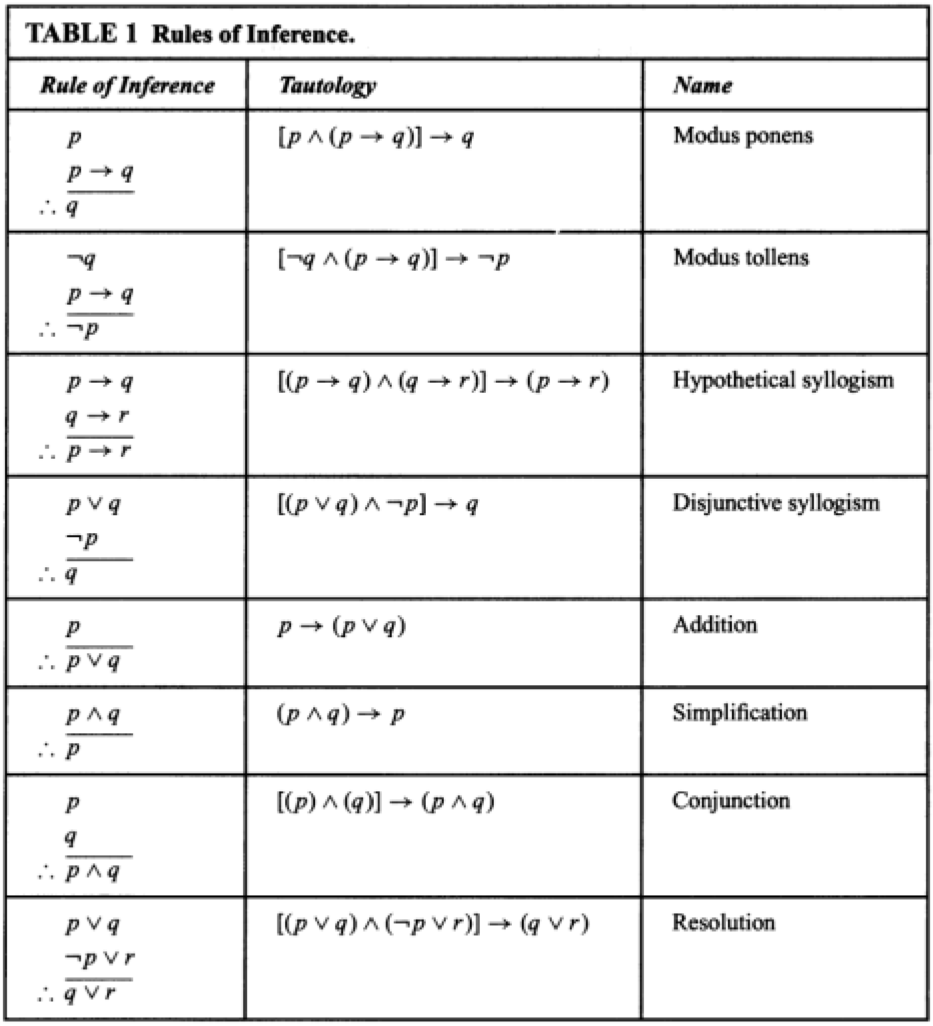


TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $\underline{p \to q}$ $\therefore q$	$[p \land (p \to q)] \to q$	Modus ponens
$\neg q$ $\underline{p \to q}$ $\therefore \neg p$	$[\neg q \land (p \to q)] \to \neg p$	Modus tollens
$p \to q$ $\underline{q \to r}$ $\therefore p \to r$	$[(p \to q) \land (q \to r)] \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\underline{\neg p}$ $\therefore q$	$[(p \lor q) \land \neg p] \to q$	Disjunctive syllogism
$\underline{p}$ $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$\underline{p \land q}$ $\therefore p$	$(p \land q) \to p$	Simplification
p $\underline{q}$ $\therefore p \land q$	$[(p) \land (q)] \to (p \land q)$	Conjunction
$p \lor q$ $\underline{\neg p \lor r}$ $\therefore q \lor r$	$[(p \lor q) \land (\neg p \lor r)] \to (q \lor r)$	Resolution

Rule of inference to build arguments:

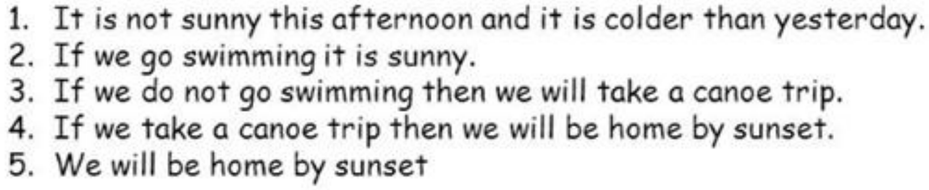
RuleP: A premise may be introduced at point in the derivation

Rule T: A formula S may be introduced in a derivation if S is a tautologically implied by any one or more of the preceeding formulas in the derivation.

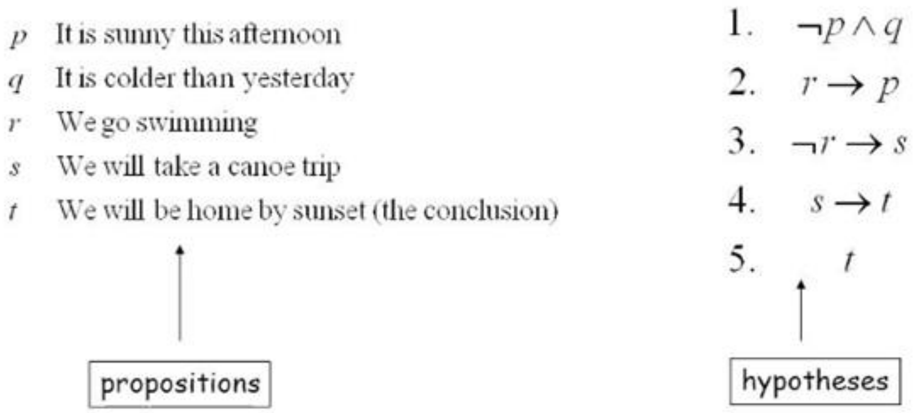
Rule CP: If we can derive S from R and a set of premises, then we can derive $R \to S$ from the set of premises alone. Rule CP is also called deduction theoem.

`

Examples:



1. It is not sunny this afternoon and it is colder than yesterday.
2. If we go swimming it is sunny.
3. If we do not go swimming then we will take a canoe trip.
4. If we take a canoe trip then we will be home by sunset.
5. We will be home by sunset



p	It is sunny this afternoon
q	It is colder than yesterday
r	We go swimming
s	We will take a canoe trip
t	We will be home by sunset (the conclusion)

1. $\neg p \wedge q$
2. $r \rightarrow p$
3. $\neg r \rightarrow s$
4. $s \rightarrow t$
5. t

Example 1.Show that R is logically derived from P → Q, Q → R, and P

Solution.	{1}	(1)	P → Q	Rule P
	{2}	(2)	P	Rule P
	{1, 2}	(3)	Q	Rule (1), (2) and I11
	{4}	(4)	Q → R	Rule P
	{1, 2, 4}	(5)	R	Rule (3), (4) and I11.

Example 2.Show that S V R tautologically implied by (P V Q) ∧ (P → R) ∧ (Q → S).

Solution .	{1}	(1)	P V Q	Rule P
	{1}	(2)	7P → Q	T, (1), E1 and E16
	{3}	(3)	Q → S	P
	{1, 3}	(4)	7P → S	T, (2), (3), and I13
	{1, 3}	(5)	7S → P	T, (4), E13 and E1
	{6}	(6)	P → R	P
	{1, 3, 6}	(7)	7S → R	T, (5), (6), and I13
	{1, 3, 6)	(8)	S V R	T, (7), E16 and E1

Example 3. Show that 7Q, P→ Q => 7P

Solution .			
	{1}	(1) P → Q	Rule P
	{1}	(2) 7P → 7Q	T, and E 18
	{3}	(3) 7Q	P
	{1, 3}	(4) 7P	T, (2), (3), and I11 .

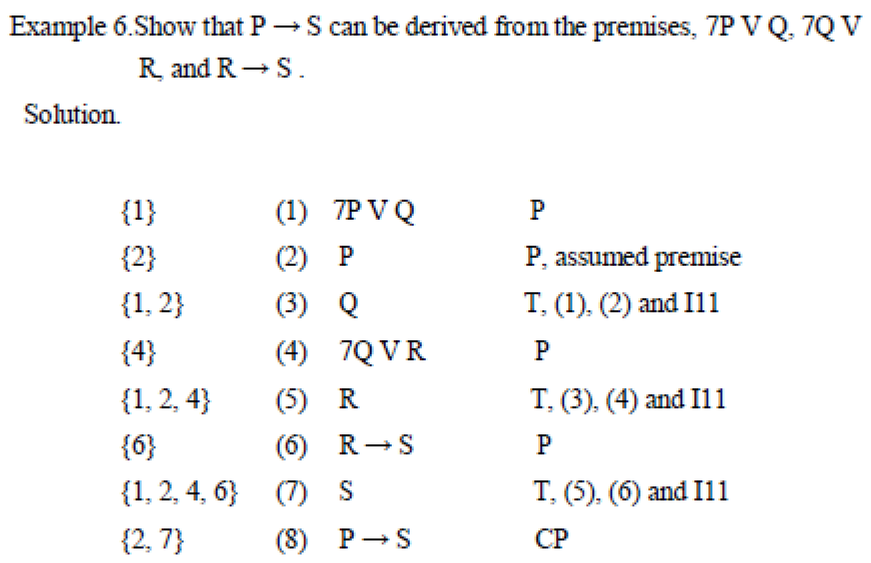
Example 4 .Prove that R ∧ (P V Q) is a valid conclusion from the premises PVQ ,
Q → R, P → M and 7M.

Solution .		
{1}	(1) P → M	P
{2}	(2) 7M	P
{1, 2}	(3) 7P	T, (1), (2), and I12
{4}	(4) P V Q	P
{1, 2 , 4}	(5) Q	T, (3), (4), and I10.
{6}	(6) Q → R	P
{1, 2, 4, 6}	(7) R	T, (5), (6) and I11
{1, 2, 4, 6}	(8) R ∧ (PVQ)	T, (4), (7), and I9.

Example 5 .Show that R → S can be derived from the premises
P → (Q → S), 7R V P , and Q.

Solution.			
	{1}	(1) 7R V P	P
	{2}	(2) R	P, assumed premise
	{1, 2}	(3) P	T, (1), (2), and I10
	{4}	(4) P → (Q → S)	P
	{1, 2, 4}	(5) Q → S	T, (3), (4), and I11
	{6}	(6) Q	P
	{1, 2, 4, 6}	(7) S	T, (5), (6), and I11
	{1, 4, 6}	(8) R → S	CP.

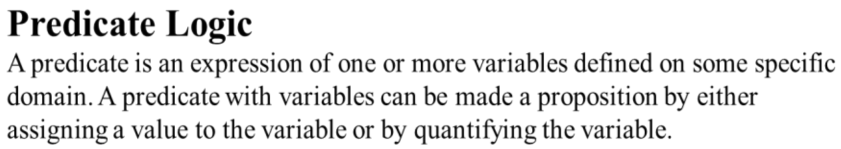
`



Example 6.Show that P → S can be derived from the premises, 7P V Q, 7Q V R, and R → S .

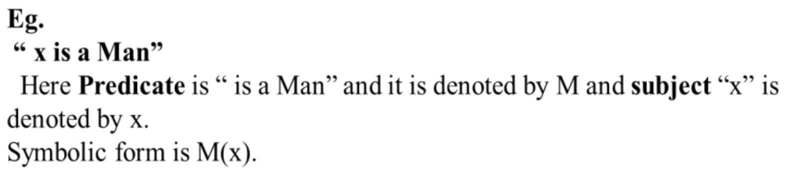
Solution.

{1}	(1)	7P V Q	P
{2}	(2)	P	P, assumed premise
{1, 2}	(3)	Q	T, (1), (2) and I11
{4}	(4)	7Q V R	P
{1, 2, 4}	(5)	R	T, (3), (4) and I11
{6}	(6)	R → S	P
{1, 2, 4, 6}	(7)	S	T, (5), (6) and I11
{2, 7}	(8)	P → S	CP



Predicate Logic

A predicate is an expression of one or more variables defined on some specific domain. A predicate with variables can be made a proposition by either assigning a value to the variable or by quantifying the variable.



Eg.
" x is a Man"
Here **Predicate** is " is a Man" and it is denoted by M and **subject** "x" is denoted by x.
Symbolic form is M(x).

Quantifiers:

The variable of predicates is quantified by quantifiers. There are two types of quantifier in Predicate logic − Universal Quantifier and Existential Quantifier.

Universal Quantifier:

Universal quantifier states that the statements within its scope are true for every value of the specific variable. It is denoted by the symbol ∀.

∀x P(x) is read as for every value of x, P(x) is true.

Example: "Man is mortal" can be transformed into the propositional form ∀x P(x) where P(x) is the predicate which denotes x is mortal and the universe of discourse is all men.

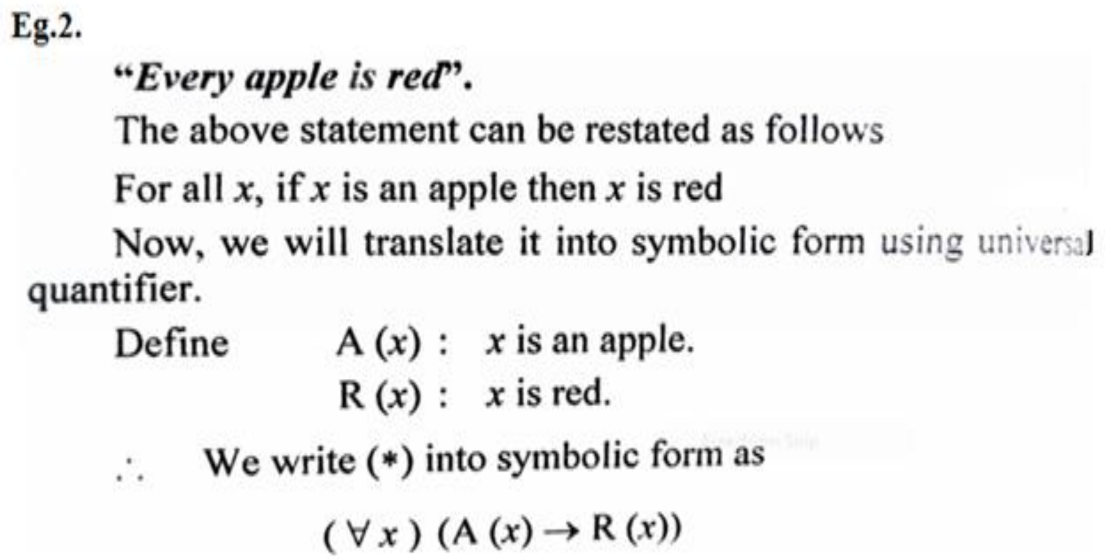
Existential Quantifier:

Existential quantifier states that the statements within its scope are true for some values of the specific variable. It is denoted by the symbol ∃.∃x P(x) is read as for some values of x, P(x) is true.

Example: "Some people are dishonest" can be transformed into the propositional form ∃x P(x) where P(x) is the predicate which denotes x is dishonest and the universe of discourse is some people.

Nested Quantifiers:

If we use a quantifier that appears within the scope of another quantifier, it is called nested quantifier.



Eg.2.

"Every apple is red".

The above statement can be restated as follows

For all x, if x is an apple then x is red

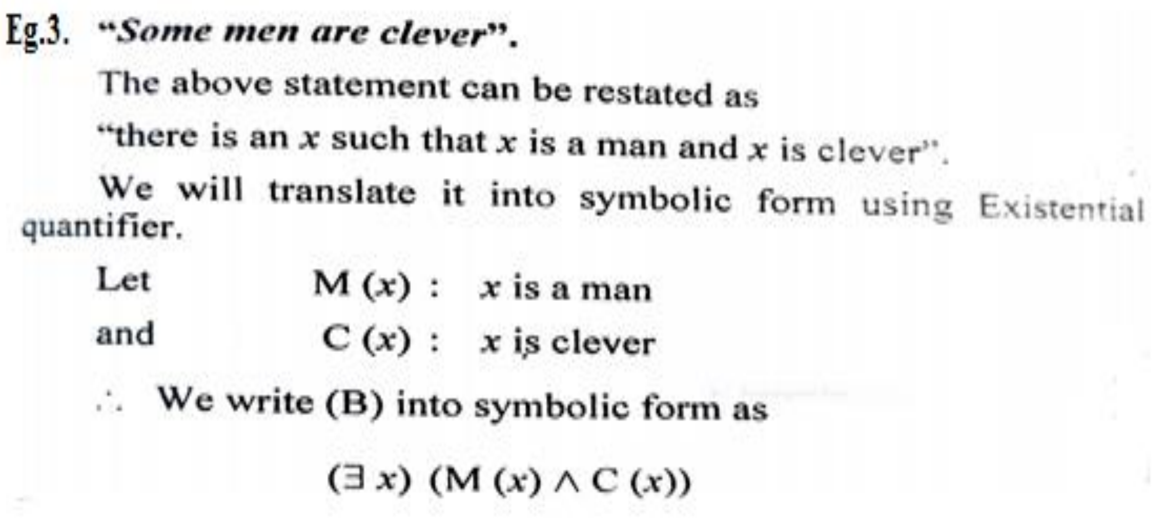
Now, we will translate it into symbolic form using universal quantifier.

Define A (x) : x is an apple.

R (x) : x is red.

∴ We write (∗) into symbolic form as

$$(\forall x)\ (A(x) \rightarrow R(x))$$



Eg.3. ***"Some men are clever".***

The above statement can be restated as

"there is an x such that x is a man and x is clever".

We will translate it into symbolic form using Existential quantifier.

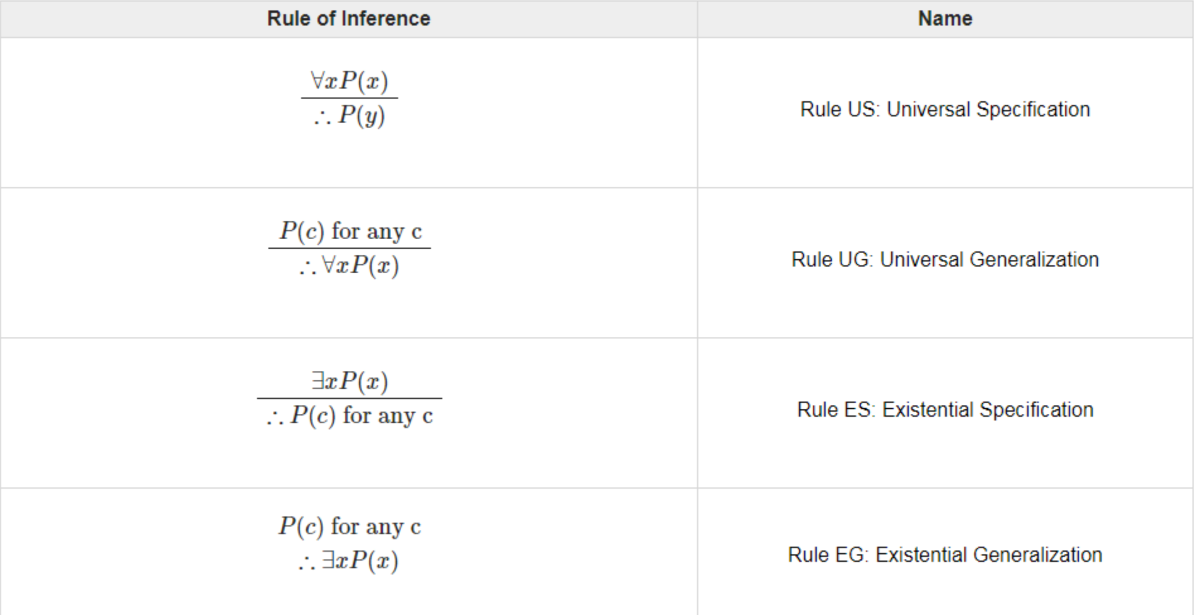
Let M (x) : x is a man

and C (x) : x is clever

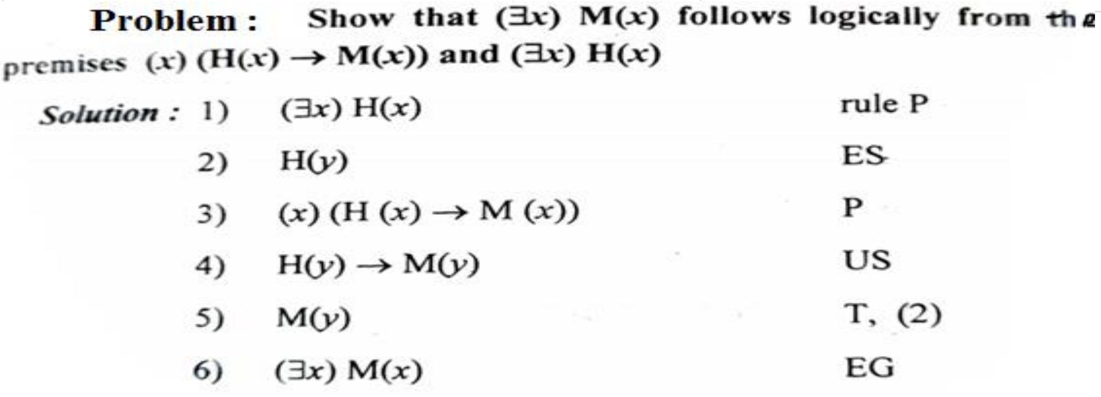
∴ We write (B) into symbolic form as

$$(\exists x)\ (M(x) \wedge C(x))$$

`



Rule of Inference	Name
$\dfrac{\forall x P(x)}{\therefore P(y)}$	Rule US: Universal Specification
$\dfrac{P(c) \text{ for any c}}{\therefore \forall x P(x)}$	Rule UG: Universal Generalization
$\dfrac{\exists x P(x)}{\therefore P(c) \text{ for any c}}$	Rule ES: Existential Specification
$P(c)$ for any c $\therefore \exists x P(x)$	Rule EG: Existential Generalization



Problem : Show that $(\exists x)\ M(x)$ follows logically from the premises $(x)\ (H(x) \rightarrow M(x))$ and $(\exists x)\ H(x)$

Solution :

1)	$(\exists x)\ H(x)$	rule P
2)	$H(y)$	ES
3)	$(x)\ (H\ (x) \rightarrow M\ (x))$	P
4)	$H(y) \rightarrow M(y)$	US
5)	$M(y)$	T, (2)
6)	$(\exists x)\ M(x)$	EG

Symbolize the following statements:

(a) All men are mortal

(b) All the world loves alover

(c) X is the father of
mother of Y (d)No cats
has atail

(e) Some people who trust others are rewarded

Solution:

`

(a) Let $M(x)$: x is a man $H(x)$: x is Mortal
$(\forall x)(M(x) \rightarrow H(x))$

(b) Let $P(x)$: x is a person $L(x)$: x is a lover $R(x,y)$: x loves y
$(x)(P(x) \rightarrow (y)(P(y) \wedge L(y) \rightarrow R(x,y)))$

(c) Let $P(x)$: x is a person $F(x,y)$: x is the father of y
$M(x,y)$: x is the mother of y $(\exists z)(P(z) \wedge F(x,z) \wedge M(z,y))$

(d) Let $C(x)$: x is a cat $T(x)$: x has a tail

$(\forall x)(C(x) \rightarrow \neg T(x))$

(e) Let $P(x)$: x is a person $T(x)$: x trust others $R(x)$: x is rewarded

$(\exists x)(P(x) \wedge T(x) \wedge R(x))$

Use the indirect method to prove that the conclusion $\exists z Q(z)$ follows from the premises $\forall x(P(x) \rightarrow Q(x))$ and $\exists y P(y)$

Solution:

1	$\neg \exists z Q(z)$	P(assumed)
2	$\forall z \neg Q(z)$	T, (1)
3	$\exists y P(y)$	P
4	$P(a)$	ES, (3)
5	$\neg Q(a)$	US, (2)
6	$P(a) \wedge \neg Q(a)$	T, (4),(5)
7	$\neg(P(a) \rightarrow Q(a))$	T, (6)
8	$\forall x(P(x) \rightarrow Q(x))$	P
9	$P(a) \rightarrow Q(a)$	US, (8)
10	$P(a) \rightarrow Q(a) \wedge \neg(P(a) \rightarrow Q(a))$	T,(7),(9) contradiction

Show that $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x) P(x) \wedge (\exists x) Q(x)$

Solution:

1) $(\exists x)(P(x) \wedge Q(x))$	Rule P
2) $P(a) \wedge Q(a)$	ES, 1
3) $P(a)$	Rule T, 2
4) $Q(a)$	Rule T, 2
5) $(\exists x) P(x)$	EG, 3
6) $(\exists x) Q(x)$	EG, 4
7) $(\exists x) P(x) \wedge (\exists x) Q(x)$	Rule T, 5, 6

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT –III–DISCRETE MATHEMATICS – SMT1304

UNIT-III-SEMIGROUPS AND MONOIDS

Semigroups, Monoids, Homomorphism of Semigroups and Monoids, Subsemigroups and Submonoid.

Semigroup: Let S be a non- empty set with a binary operation * defined on it. The algebraic system (S, *) is called a semigroup if * is associative.

(i.e) $a*(b*c)=(a*b)*c \quad \forall a,b,c\in S$

Examples:

1. (2Z, +) and (2Z, .)aresemigroups.
2. If S is the set of all $n\times n$ matrices with real entries, then (S, +) and (S, **.**) are semigroups, where + is matrix addition and . is matrix multiplication.
3. (Z, -) is not a semigroup because ‘ – ‘ is not associative, since $2-(3-4)\neq(2-3)-4$

Monoid:A semigroup(M, *) with identity element **e** is called a monoid. Sometimes a monoid is denoted as (M, *, **e**) indicating the fact that **e** is the identity element.

Examples:

1. $(N,\times)$ia a monoid with identity element**1**. But **(N, +)** is not a monoid, since identity for **+** is **0**, which is not in **N**.
2. The set of non negative integers $S = N\cup\{0\}$ is the monoid under + and $\times$. (i.e) (S, +) and (S, $\times$) are monoids with identity 0 and 1.
3. Let S be the non-empty set and let S^S denote the set of all mappings from S to S. Let **.** denote the composition of functions operation.

   If $f,g\in S^S$, then f and g are functions from $S\to S$. Their composite $(f\circ g)(x)=f(g(x))\,\forall x\in S$. Then $f\circ g$ is a function from $S\to S$ and $f\circ g\in S^S$. We know composition function is associative.

   The identity function $I:S\to S$ defined by $I(x)=x \;\; \forall x\in S$ is the identity element of S^S. For $(I\circ f)(x)=I(f(x))=f(x)\,\forall x\in S$ and $(f\circ I)(x)=f(I(x))=f(x)\,\forall x\in S$

$\therefore\; I\circ f=f\circ I=f \;\; \forall f\in S^S$. $\therefore\; (S^S,\circ)$ is a monoid with identity I.

Sub semigroups: Let (S, *) be a semigroup and let $T\subseteq S$ be a noe-empty subset. If T is closed under *, then (T, *) is called a sub semigroup.

Submonoid: Let (M, *) be monoid and **e** be the identity. If T be a non-empty subset of M and if T is closed under * with$e\in T$, then (T, *) is called a submonoid of (M, *).

Examples:

1. $(N,\times)$ is a semigroup. Let T = 3N then $T\subset S$, if $x,y\in T$ then x = 3r, y = 3s for some positive integers r and s. Now x+y = 3r$\times$3s = 3(3rs) $\in$3N = T. $\therefore$ T is closed under$\times$.

Hence (T, $\times$) is a sub semigroup of (N, $\times$). More generally, if S = mN, where m is a fixed positive integer, then (S, $\times$) is a sub semigroup.

2. For the semigroup (N, +), (2N, +) is a sub semigroup.
3. (Z, +) is monoid with identity 0. If T = the set of all non-negative integers = {0, 1, 2, 3, ...}, then (T, +) is a submonoid with identity 0.

Cyclic Monoid: A monoid (M, *) having identity is said to be cyclic if there exists an element $a \in M$ such that every element $x \in M$ can be written as a^n = e for some $n \in N$. Then 'a' is called a generator of M. Any cyclic monoid is commutative.

Problems:

1. For any commutative monoid (M, *), prove that the set of all idempotent elements of M forms a submonoid.

   Solution: Given (M, *) be a commutative monoid.

   Let e be its identity element.

   Let S be the set of all idempotent elements of M. (i.e) $S = \{x \in M / x * x = x\}$

Since e*e = e, e is an idempotent element of M.

$\therefore$ $e \in S$ and hence S is non-empty.

Let $a, b \in S$ be any two elements. They are idempotent elements.

$\therefore$ a*a = a and b*b = b.

We have to prove a*b is idempotent.

Now (a*b)*(a*b) = a*(b*a)*b [Since * is associative

= a*(a*b)*b [Since * is commutative

= (a*a)*(b*b) [Since * is associative

= a*b

Hence a*b is idempotent and so S is closed under * and $e \in S$.

So (S, *) is a submonoid of (M, *).

2. Show that every finite semigroup has an idempotent element.

Solution: Let (S, *) be a finite semigroup.

Let $a \in S$, then by closure $a, a^2, a^3, a^4, ...$ are all elements of S.

Since S is finite, these elements are not all different. So we have repetitions.

Let $a^m = a^r, where\ r > m$. Let r = m+n.

$\therefore\ a^m = a^r = a^{m+n}$

Then $a^m * a^n = a^{m+n} * a^n \Rightarrow a^{m+n} = a^{m+2n}$

And $a^{m+n} * a^{n} = a^{m+2n} * a^{n} \Rightarrow a^{m+2n} = a^{m+3n}$ and so on.

$\therefore a^{m} = a^{m+n} = a^{m+2n} = a^{m+3n} = ... = a^{m+mn}$

Since $a^{m} = a^{m+mn}$

We have $a^{nm} = a^{nm+mn}$ [Replacing m by nm]

$= a^{nm} * a^{mn}$

This proves that a^{mn} is an idempotent element of S.

$\therefore$ Every finite semigroup has an idempotent element.

3. Show that the set of all invertible elements of a monoid form a group under the same operation as that of the monoid.

Solution: Let (M, *) be a monoid having the identity e.

Let G be the set of all invertible elements of M.

Since $e^{-1} = e$, we have $e \in G$. So G is non- empty. Further inverse is unique.

Let $a, b \in G$, then a and b have inverse. Let a^{-1}, b^{-1} be their inverses.

We have to prove that $a * b \in G$.

S we have to prove that it is invertible.

Now consider $(a *b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1}$

$= a*(e)*a^{-1}$

$= a*a^{-1}$

$= e$

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

$= \quad b^{-1}*(e)*b$

$= b^{-1}*b = e$

$\therefore$ $b^{-1}*a^{-1}$ is the inverse of a*b.

(i.e) a*b is invertible.

Hence $a * b \in G$. So G is closed under *.

Associativity: Since G is a subset of M, associativity is inherited in G.

Identity: $e \in G$ is the identity. Since a*e = e*a = a, $\forall\ a \in G$.

Inverse: Let $a \in G$ be any element. So 'a' is invertible.

$\therefore$ $a*a^{-1} = a^{-1}*a = e \Rightarrow (a^{-1})^{-1} *a^{-1} = a^{-1}*(a^{-1})^{-1} = e$ [Since $(a^{-1})^{-1} = a$

Since a^{-1} is invertible and so $a^{-1} \in G$.

Hence inverse exists for every $a \in S$. So (G,*) is a group.

4. If $\mathbf{Z_6}$ is the set of equivalence classes generated by the equivalence relation "Congruence modulo 6", prove that $\left(Z_6, \times_6\right)$ is a monoid where the operation $\times_6$ on Z_6 is defined as $[j] \times_6 [k] = [(j \times k) \bmod 6]$ for any [j], [k] $\in$ Z_6.

Solution: We know Z_6 = {[0], [1], [2], [3], [4], [5]}. We shall form the composition table.

$\times_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

$\therefore$ Z_6 is closed under $\times_6$.

Associativity: Since $[a] \times_6 [b] \times_6 [c] = [a] \times_6 [bc]$

$$= [a(bc) \bmod 6]$$

$\times_6$ depends on associativity of usual multiplication. $\therefore$ $\times_6$ is associative.

Identity: From the table we find, $[1] \times_6 [a] = [a]$ for all [a] $\in$ Z_6.

$\therefore$ [1] is the identity element. Hence $\left(Z_6, \times_6\right)$ is a monoid.

Homomorphism: Homomorphism is a structure preserving map between two algebraic systems of same type. Homomorphisms of semigroups and monoids are useful in the economical design of sequential machines and in formal languages.

Homomorphism of semigroups: Let (S, *) and (T, **.)** be two semigroups. A mapping $f : S \to T$ is called homomorphism if $f(a * b) = f(a).f(b) \quad \forall a, b \in S$.

The homomorphism of semigroups f is called a monomorphism if f is one-one.

f is called epimorphism if f is onto.

f is called an isomorphism if f is one-one and onto.

If f is an isomorphism of S onto T, we say S is isomorphic to T as semigroups.

Example: Consider the semigroups (N, +) amd (Z_m, $+_m$). Define $f : N \to Z_m$ by $f(a) = [a]$ then $f(a+b) = [a+b] = [a] +_m [b] = f(a) +_m f(b)$.

$\therefore$ f is a semigroup homomorphism.

Monoid Homomorphism: Let (M,*) be a monoid with identity e and (T, .) be a monoid with identity e'. A mapping $f : M \to T$ is called a homomorphism of monoids if $f(a*b) = f(a).f(b) \quad \forall a,b \in M$ and $f(e) = e'$.

The homomorphism of monoids f is called

(i) a monomorphism if f is one-one

(ii) an epimorphism if f is onto

(iii) an isomorphism if f is one-one and onto.

Theorem 1: Let (S,*) be a semigroup and (T, .) be an algebraic system. If $f : S \to T$ is an onto homomorphism, then (T, .) is also a semigroup.

Proof: Given (S,*) is a semigroup and $f : S \to T$ is an onto homomorphism.

(i.e) $f(a*b) = f(a).f(b)$

To prove (T, .) is a semigroup, we have to prove (**.**) is associative.

Let $x, y, z \in T$ be any three elements. Since f is onto, we can find pre images $a, b, c \in S$ such that $f(a) = x,\ f(b) = y,\ f(c) = z$

Now $f[a*(b*c)] = f(a).f(b*c) = f(a).(f(b).f(c)) = x.(y.z)$ and $f[(a*b)*c] = f(a*b).f(c) = (f(a).f(b)).f(c) = (x.y).z$

Since $a*(b*c) = (a*b)*c$, $f[a*(b*c)] = f[(a*b)*c]$.

$\therefore\ x.(y.z) = (x.y).z,\ \forall\ x, y, z \in T$.

Hence (T, .) is a semigroup.

Theorem 2: Let (S, *) and (T, .) be semigroups and $g : S \to T$ be a homomorphism. If $a \in S$ is an idempotent element. Prove that $g(a)$ is an idempotent element of T.

Proof: Given $g : S \to T$ is a homomorphism of semigroups and $a \in S$ is an idempotent element.

$\therefore$ a*a = a $\Rightarrow g(a*a) = g(a) \Rightarrow g(a).g(a) = g(a)$ [Since g is a homomorphism

$\therefore\ g(a)$ is an idempotent element of T.

Theorem 3: If (M, *) is a monoid having identity e and g is an epimorphism from (M, *) to an algebraic system (T, .), then (T, .) is a monoid.

Proof: Given (M, *) is a monoid with identity e.

$\therefore$ (M, *) is a semigroup and $g : M \to T$ is an epimorphism.

(i.e) an onto homomorphism.

$\therefore$ (T, .) is also a semigroup. [By theorem 1

We have to only prove (T, .) has identity.

Let $a \in M$ be any element and $e \in M$ is the identity.

$\therefore\ a * e = a = e * a$

Now $a * e = a \Rightarrow g(a * e) = g(a) \Rightarrow g(a).g(e) = g(a)$ and
$e * a = a \Rightarrow g(e * a) = g(a) \Rightarrow g(e).g(a) = g(a)$

$g(a).g(e) = g(e).g(a) = g(a) \Rightarrow g(e)$ is the identity of (T, .) and hence (T, .) is a monoid.

Theorem 4: Let (S, *) , (T, .) and $(V, \oplus)$ be semigroups and $g : S \to T,\ h : T \to V$ be semigroup homomorphism such that their composite $h \circ g : S \to V$ is defined. Prove that $h \circ g$ is a semigroup homomorphism of (S, *) to $(V, \oplus)$.

Proof: Given $g : S \to T,\ h : T \to V$ are semigroup homomorphisms.

We have to prove $h \circ g : S \to V$ is a homomorphism.

Let $a, b \in S$ be any two elements.

$$\therefore\ (h \circ g)(a * b) = h(g(a * b)) = h(g(a).g(b)) = h(g(a)) \oplus h(g(b))$$

$$= (h.g)(a) \oplus (h.g)(b)$$

$\therefore\ h \circ g$ is a homomorphism of semigroups.

Theorem 5: The set of all semigroup endomorphisms of a semigroup is a semigroup under the operation of composition.

Proof: Let G be the set of all endomorphisms of the semigroup (S,*).

An endomorphism is a homomorph ism of $S \to S$ and so G is the set of all homomorphisms from S to S.

We have to prove (G, .) is a semigroup where **.** is composition of functions.

Let $g_1, g_2 \in G$ be any two elements. (i.e) g_1, g_2 are endomorphisms of S.

$$\therefore\ (g_1 \circ g_2)(a * b) = g_1(g_2(a * b)) = g_1(g_2(a) * g_2(b)) = g_1(g_2(a)) * g_1(g_2(b))$$

$$= (g_1 \circ g_2)(a) * (g_1 \circ g_2)(b)$$

$\therefore\ (g_1 \circ g_2)$ is a homomorphism of $S \to S$ and hence an endomorphism.

$\therefore\ (g_1 \circ g_2) \in G$. Hence G is closed under the operation $(\circ)$.

Next we shall prove that $(\circ)$ is associative.

Let $g_1, g_2, g_3 \in G$ be any three endomorphisms of s.

To prove $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

Now for $a \in S$, we have,

$(g_1 \circ (g_2 \circ g_3))(a) = g_1(a) * (g_2 \circ g_3)(a) = g_1(a) * [g_2(a) * g_3(a)]$ and

$((g_1 \circ g_2) \circ g_3)(a) = (g_1 \circ g_2)(a) * g_3(a) = g_1(a) * [g_2(a) * g_3(a)]$

Since $g_1(a),\ g_2(a),\ g_3(a)$ are elements of S and * is associative, we have

$g_1(a) * [g_2(a) * g_3(a)] = g_1(a) * [g_2(a) * g_3(a)]$

$\therefore\ (g_1 \circ (g_2 \circ g_3))(a) = ((g_1 \circ g_2) \circ g_3)(a),$ for any $a \in S$.

$\Rightarrow g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$. Hence $(\circ)$ is associative and so $(G, \circ)$ is a semigroup.

Theorem 6: Let (S. *) be a semigroup and S^S be the set of all functions from S to S. Then (S^S, .) is a semigroup under composition of functions. Prove that there is a homomorphism $g : S \to S^S$.

Proof: For each $a \in S$, we shall identify a function $f_a : S \to S$, defined by $f_a(x) = a * x\ \forall x \in S$

$\therefore\ f_a \in S^S$

Define $g : S \to S^S$ by $g(a) = f_a\ \forall a \in S$

Let $a, b \in S$ be any two elements, then $a * b \in S$

$\therefore\ g(a * b) = f_{a*b}$

But for any $x \in S,\ f_{a*b}(x) = (a * b) * x = a * (b * x) = f_a(b * x) = f_a(f_b(x)) = (f_a \cdot f_b)(x)$

$\therefore\ f_{a*b} = f_a \cdot f_b$

Hence $g(a * b) = f_{a*b} = f_a \cdot f_b = g(a).g(b)$

$\therefore$ g is a homomorphism of (S, *) into (S^S, **.**).

Theorem 7: Show that monoid homomorphism preserves the property of invertibility.

Proof: Let (M, *) and (M', **.**) be two monoids with identity e and e' respectively.

Let $g : M \to M'$ be a homomorphism.

Let $a \in M$ be an element with inverse a^{-1}.

We have to prove $g(a^{-1}) = [g(a)]^{-1}$. Since a^{-1} is the inverse of a, we have $a * a^{-1} = a^{-1} * a = e$.

Now $a * a^{-1} = e \Rightarrow g(a * a^{-1}) = g(e) = e' \Rightarrow g(a).g(a^{-1}) = e'$

Similarly, $a^{-1} * a = e \Rightarrow g(a^{-1} * a) = g(e) = e' \Rightarrow g(a^{-1}).g(a) = e'$

Hence $g\left(a^{-1}\right)$ is the inverse of $g(a)$

(i.e) $g\left(a^{-1}\right)=\left[g(a)\right]^{-1}$.

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited “A” Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT – IV–DISCRETE MATHEMATICS – SMT1304

UNIT – IV- LATTICES

Lattices as Partially Ordered Set, Properties of Lattices, Lattices as Algebraic Systems, Sublattices, Direct Product and Homomorphism.

Definition: The relation f defined on a nonempty set X is called an anti-symmetric relation if and only if, $\forall$ x, y $\in$ X, the property (x, y) $\in$ f and (y, x) $\in$ f implies that x = y.

It is possible to interpret an anti-symmetric relation using the arrow diagrams of relations.

In this context, a relation is called anti-symmetric if, whenever there is an arrow going from one element to an element different from it, there does not exist an arrow going back from the second element to the first.

Example: Let R1 = $\{(x, y) \in Z + \times Z + \mid x \text{ divides } y\}$ and R2 = $\{(x, y) \in Z \setminus \{0\} \times Z \mid x \text{ divides } y\}$. (a) Show that R1 is an anti-symmetric relation on the set of positive integers. (b) Show that R2 is not an anti-symmetric relation on the set of integers by giving a counter example.

There are two relations which play a prominent role in mathematics. One of them is the equivalence relation, which we have already seen is a relation which is reflexive, symmetric and transitive.

We now introduce the other relation called a partial order.

Definition: A relation f on a nonempty set X is called a partial order if f is reflexive, transitive and anti-symmetric. Here (X, f) is a partially ordered set and is colloquially referred to as a poset.

The relation less than or equal to on the set of real numbers and the relation subset on the set of sets are two fundamental partial orders. These can be thought of as models for the general partial order. It is common practice to use the symbol to denote a partial order.

Further, if (X,) is a poset and x y, then we read this as x is less than or equal to y.

Definition: Let (X,) be a poset. It there exist elements x and y in X, such that either (x, y) $\in$ or (y, x) $\in$ holds, then x and y are said to be comparable. In neither (x, y) nor (y, x) belongs to , then x and y are said to be incomparable.

Example1: Let X = {1, 2, 3, 4, 5}.

(a) The identity relation Id on X is reflexive, transitive and anti-symmetric and is therefore a partial order. However, no two elements of X are comparable.

(b) The relation Id $\cup$ {(1, 2)} is also a partial order on X. Here 1 and 2 are comparable.

(c) The relation = Id$\cup${(1, 2),(2, 1)} is both reflexive and transitive, but not anti-symmetric. Observe that (1, 2), (2, 1) $\in$and 1 6= 2.

(d) The relation Id $\cup$ {(1, 2),(3, 4)} is a partial order on X. Here, 1 and 2 are comparable and so are 3 and 4.

Example: Let X = N. The relation = {(a, b) : a divides b} is a partial order on X.

Example: Let X be a nonempty collection of sets. Here, = $\{(A, B) : A, B \in X, A \subseteq B\}$ is a partial order on X. 4. On R the set = $\{(a, b) : a \leq b\}$ is a partial order. It is called the usual partial order on R.

Definition: Let (X,) be a poset. 1. If any two elements in the poset (X,) are comparable, then is called a linear order and (X,) is called a linearly ordered set.

Often a linear order is also referred to as a total order or a complete order.

A subset, C of X, is called a chain if and only if induces a linear order on C. If C is a finite set, then the length of C is equal to the number of elements if C. If C is not a finite set, then the length of C is said to be infinite.

A subset, A of X, is called an antichain if and only if no two elements of A are comparable. The length of an antichain is defined in precisely the same manner as that of the chain.

The maximum of the lengths of the chains of X is called the height of X and the maximum of the lengths of the antichains of X is called the width of X.

Let X be a nonempty set and let f be a relation on X. Then, recall from Definition, that f is reflexive if (x, x) ∈ f for all x ∈ X; f is transitive if (x, y) ∈ f and (y, z) ∈ f imply (x, z) ∈ f for all x, y, z ∈ X; and f is anti-symmetric if (x, y) ∈ f and x 6= y implies (y, x) ∈/ f, i.e., for all distinct elements x, y of X both (x, y) and (y, x) cannot be in f. Relations which are simultaneously reflexive, transitive and anti-symmetric play an important role in mathematics; and we give a name to such relations. **Definition:** Let X be a nonempty set. A relation f on X is called a partial order if f is reflexive, transitive and anti-symmetric. Let f be a partial order on X and let a, b ∈ X. Then, a and b are said to be comparable (with respect to the partial order f) if either (a, b) ∈ f or (b, a) ∈ f. When a partial order satisfies some other desirable properties, they are given different names. We fix some of these in the following definition.

Definition: Let X be a nonempty set.

1. The pair (X, f) is called a partially ordered set (in short, poset) if f is a partial order on X.

2. A partial order f on X is called a linear order if either (x, y) ∈ f or (y, x) ∈ f for all x, y ∈ X, i.e., when any two elements of X are comparable. A linear order is also called a total order, or a complete order.

3. The poset (X, f) is said to be a linearly ordered set if f is a linear order on X.

4. A linearly ordered subset of a poset is called a chain in the poset. The maximum size of a chain in a poset is called the height of a poset.

5. Let (X, f) be a poset and let A ⊆ X. A is called an anti-chain in the poset if no two elements of A are comparable.

The maximum size of an anti-chain in a poset is called the width of the poset. You may imagine the elements of a linearly ordered set as points on a line. The height of a poset is the maximum of the cardinalities of all chains in the poset. The width of a poset is the maximum of the cardinalities of all anti-chains in the poset.

Examples:

1. The poset in Example1 has height 1 (size of the chain {1}) and width 5 (size of the anti-chain {1, 2, 3, 4, 5}).

2. The poset in Example1 has height 2 (respective chain is $\{1, 2\}$) and width 4 (respective anti-chains are $\{2, 3, 4, 5\}$ and $\{1, 3, 4, 5\}$).

3. The poset in Example1 has height 2 (respective chains are $\{1, 2\}$ and $\{3, 4\}$) and width 3 (a respective anti-chain is $\{1, 3, 5\}$).

4. The usual order (usual $\leq$) in N is a linear/complete/total order. The same holds for the usual order in Z, Q and R.

5. If (X, f) is a finite linearly ordered set then the singleton subsets of X are the only anti-chains.

In this case, the height of X is the number of elements in X and the width of X is 1.

6. The set N with the partial order f defined by "$(a, b) \in f$ if a divides b" is not linearly ordered. However, the set $\{1, 2, 4, 8, 16\}$ is a chain. This is just a linearly ordered subset of the poset.

There are larger chains, for example, $\{2\ k : k = 0, 1, 2, . . .\}$. The set of all primes is an anti-chain here. The poset (N, f) has infinite height and infinite width.

7. The poset $(P(\{1, 2, 3, 4, 5\}), \subseteq)$ is not linearly ordered. However, $\{\emptyset, \{1, 2\}, \{1, 2, 3, 4, 5\}\}$ is a chain in it. Also, $\{\emptyset, \{2\}, \{2, 3\}, \{2, 3, 4\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$ is a chain. The height of this poset is 6.

That is, if f is a partial order on a nonempty set X we write $x \leq y$ to mean that $(x, y) \in f$. Accordingly, the poset (X, f) is written as $(X, \leq)$. Also, instead of writing '(X, f) is a poset' we will often write 'X is a poset with the partial order f'. Following custom, by $x \geq y$ we mean $y \leq x$; by $x < y$ we mean that $x \leq y$ and x 6= y; by $x > y$ we mean $y < x$. Also, we read $x \leq y$ as x is less than or equal to y; $x < y$ as x is less than y; $x \geq y$ as x is greater than or equal to y; and $x > y$ as x is larger than y.

Definition: Let $(\Sigma, \leq)$ be a finite linearly ordered set (like the English alphabet with $a < b < c < \cdots < z$) and let $\Sigma*$ be the collection of all words formed using the elements of Σ. For a = a1a2 · · · an, b = b1b2 · · · bm $\in \Sigma *$ for m, n $\in$ N, define $a \leq b$ if (a) a1 < b1, or (b) ai = bi for i = 1, . . . , k for some k < min{m, n} and ak+1 < bk+1, or (c) ai = bi for i = 1, 2, . . . , n = min{m, n}. Then $(\Sigma* , \leq)$ is a linearly ordered set. This ordering is called the lexicographic or dictionary ordering. Sometimes Σ is called the alphabet and the linearly ordered set $\Sigma*$ is called the dictionary.

A directed graph representation of the poset $(A, \leq)$ with $A = \{1, 2, 3, 9, 18\}$Given a set, X, we can order the subsets of X by the subset relation: $A \subseteq B$, where A, B are any subsets of X.

For example, if $X = \{a, b, c\}$, we have $\{a\} \subseteq \{a, b\}$.

However, note that neither $\{a\}$ is a subset of $\{b, c\}$ nor $\{b, c\}$ is a subset of $\{a\}$.

We say that $\{a\}$ and $\{b, c\}$ are incomparable.

Definition:

A binary relation, $\leq$, on a set, X, is a partial order (or partial ordering) iff it is reflexive, transitive and antisymmetric,

that is: (1) (Reflexivity): $a \leq a$, for all $a \in X$;

(2) (Transitivity): If $a \leq b$ and $b \leq c$, then $a \leq c$, for all $a, b, c \in X$.

(3) (Antisymmetry): If $a \leq b$ and $b \leq a$, then $a = b$, for all $a, b \in X$.

A partial order is a total order (ordering) (or linear order (ordering)) iff for all $a, b \in X$, either $a \leq b$ or $b \leq a$. When neither $a \leq b$ nor $b \leq a$, we say that a and b are incomparable.

A subset, $C \subseteq X$, is a chain iff $\leq$ induces a total order on C (so, for all $a, b \in C$, either $a \leq b$ or

$b \leq a$).

The strict order (ordering), $<$ is the strict order associated with a partial order, $\leq$, then $<$ is transitive and antireflexive, which means that (4) a &< a, for all $a \in X$.

Conversely, let $<$ be a relation on X and assume that $<$ is transitive and anti-reflexive.

If confusion may arise, for example when we are dealing with several posets, we denote the partial order on X by $\leq X$.

The trick is to draw a picture consisting of nodes and oriented edges, where the nodes are all the elements of X and where we draw an oriented edge from a to b iff a is an immediate predecessor of b. Such a diagram is called a Hasse diagram for $(X, \leq)$.

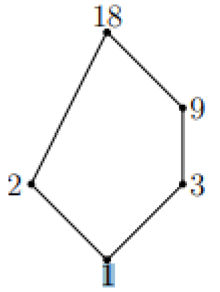
The Hasse diagram of a finite poset $(X, \leq)$ is a picture drawn in the following way:

1. Each element of X is represented by a point and is labeled with the element.

2. If $a \leq b$ then the point labeled a must appear at a lower height than the point labeled b and further the two points are joined by a line.

3. If $a \leq b$ and $b \leq c$ then the line between a and c is removed.

Example: Hasse diagram for the poset $(A, \leq)$ with $A = \{1, 2, 3, 9, 18\}$ and $\leq$ as the 'divides' relation is given below.



Definition:

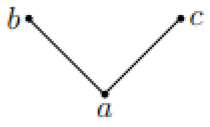
Let $(X, \leq)$ be a poset and let $A \subseteq X$.

1. We say that an element $x \in X$ is an upper bound of A if for each $z \in A$, $z \leq x$; or equivalently, when each element of A is less than or equal to x. An element $y \in X$ is called a lower bound of A if for each $z \in A$, $y \leq z$; or equivalently, when y is less than or equal to each element of A.

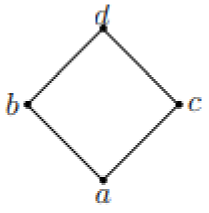
2. An element $x \in A$ is called the maximum of A, if x is an upper bound of A. Thus, maximum of A is an upper bound of A which is contained in A. Such an element is unique provided it exists. In this case, we denote $x = \max\{z : z \in A\}$. Similarly, minimum of A is an element $y \in A$ which is a lower bound of A. If minimum of A exists, then it is unique; and we write $y = \min\{z : z \in A\}$.

3. An element $x \in X$ is called the least upper bound (lub) of A in X if x is an upper bound of A and for each upper bound y of A, we have $x \leq y$; i.e., when x is the minimum (least) element of the set of all upper bounds of A. Similarly, the greatest lower bound (glb) of A is a lower bound of A which is greater than or equal to all upper bounds of A; it is the maximum (largest) of the set of all lower bounds of A.

4. An element $x \in A$ is a maximal element of A if $x \leq z$ for some $z \in A$ implies $x = z$; or equivalently, when no element in A is larger than x. An element $y \in A$ is called a minimal element of A if $z \leq y$ for some $z \in A$ implies $y = z$; or equivalently, when no element in A is less than y. **Example:** Consider the two posets $X = \{a, b, c\}$ and $Y = \{a, b, c, d\}$ described by the following Hasse diagrams:



X



Y

Let A = X. Then,

(a) the maximal elements of A are b and c,

(b) the only minimal element of A is a,

(c) a is the lower bound of A in X,

(d) A has no upper bound in X,

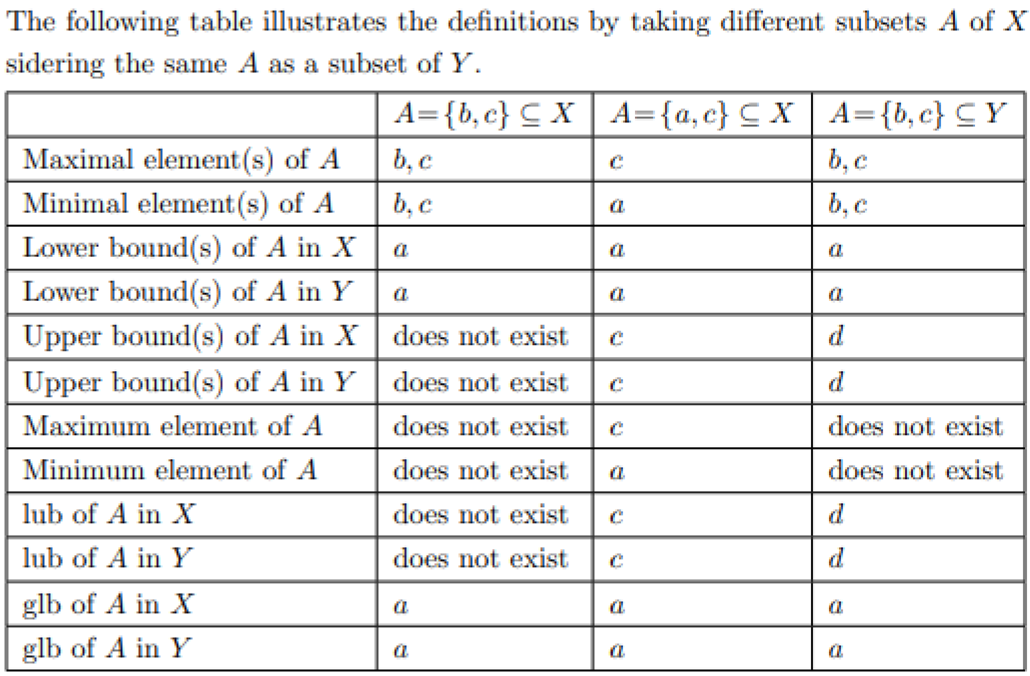
(e) A has no maximum element,

(f) a is the minimum element of A,

(g) no element of X is the lub of A, and

(h) a is the glb of A in X.

Example:



The following table illustrates the definitions by taking different subsets A of X, and also considering the same A as a subset of Y.

	$A = \{b, c\} \subseteq X$	$A = \{a, c\} \subseteq X$	$A = \{b, c\} \subseteq Y$
Maximal element(s) of A	b, c	c	b, c
Minimal element(s) of A	b, c	a	b, c
Lower bound(s) of A in X	a	a	a
Lower bound(s) of A in Y	a	a	a
Upper bound(s) of A in X	does not exist	c	d
Upper bound(s) of A in Y	does not exist	c	d
Maximum element of A	does not exist	c	does not exist
Minimum element of A	does not exist	a	does not exist
lub of A in X	does not exist	c	d
lub of A in Y	does not exist	c	d
glb of A in X	a	a	a
glb of A in Y	a	a	a

Definition: A linear order ≤ on a nonempty set X is said to be a well order if each nonempty subset of X has minimum. We call (X, ≤) a well ordered set to mean that ≤ is a well order on X.

Often we use the phrase ‘X is a well ordered set with the ordering as ≤’ to mean ‘(X, ≤) is a well ordered set’.

Lattice: A poset (L, ≤) is called a lattice if each pair x, y ∈ L has an lub and also a glb. A lub of x, y is also written as x ∨ y (read as ‘x or y’ / ‘join of x and y’) and a glb of x, y as x ∧ y (read as ‘x and y’ / ‘meet of x and y’). A lattice is a poset in which any two elements have a meet and a join.

A complete lattice is a poset in which any subset has a greatest lower bound and a least upper bound.

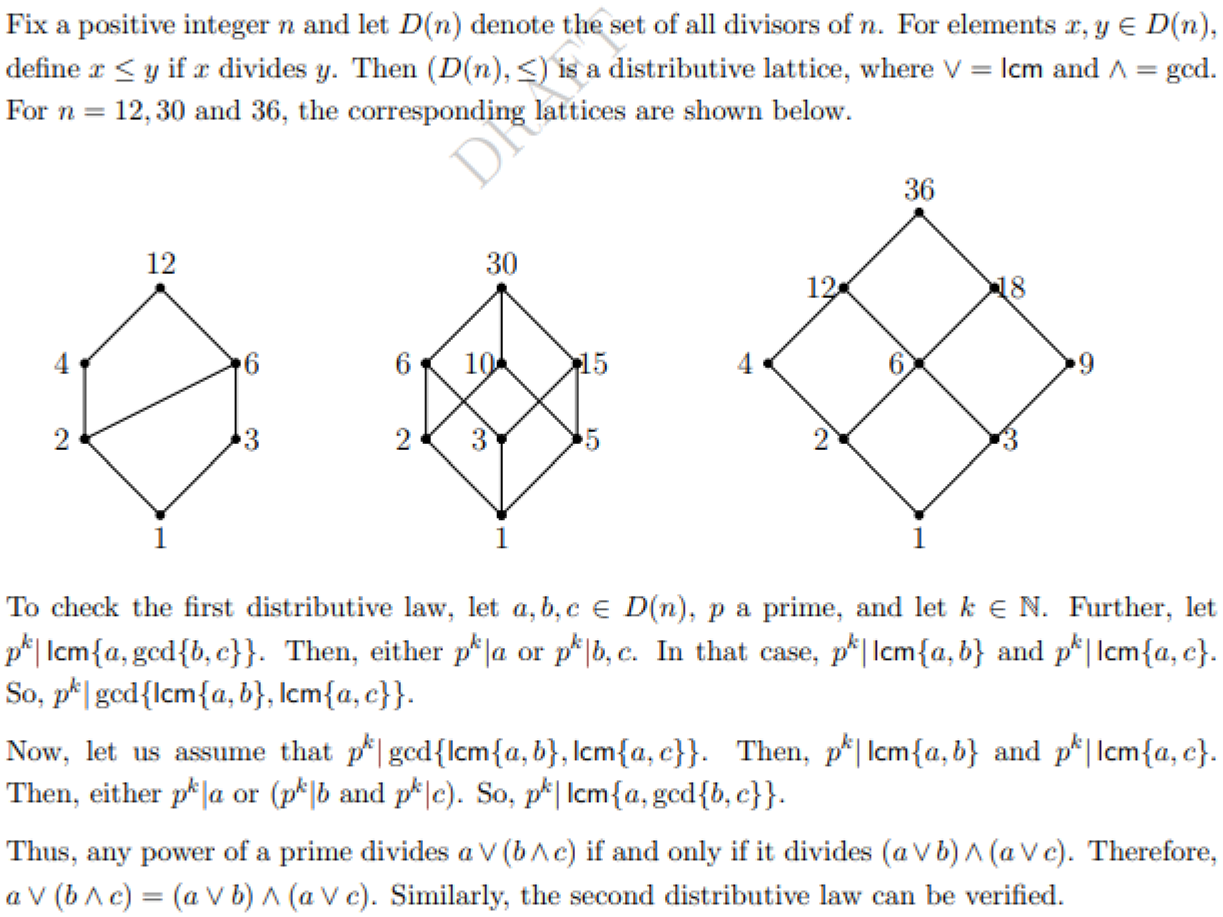
It is easy to show that any finite lattice is a complete lattice and that a finite poset is a lattice iff it has a least element and a greatest element.

The poset N+ under the divisibility ordering is a lattice!

A lattice is called a distributive lattice if for all pairs of elements x, y the following conditions, called distributive laws, are satisfied: x ∨ (y ∧ z) = (x ∨ y) ∧ (x ∨ z), x ∧ (y ∨ z) = (x ∧ y) ∨ (x ∧ z).

Indeed, it turns out that the meet operation corresponds to greatest common divisor and the join operation corresponds to least common multiple.

However, it is not a complete lattice. The power set of any set, X, is a complete lattice under the subset ordering.



Fix a positive integer n and let $D(n)$ denote the set of all divisors of n. For elements $x, y \in D(n)$, define $x \leq y$ if x divides y. Then $(D(n), \leq)$ is a distributive lattice, where $\vee = \mathsf{lcm}$ and $\wedge = \gcd$. For $n = 12, 30$ and 36, the corresponding lattices are shown below.

12
4
6
2
3
1
30
6
10
15
2
3
5
1
36
12
18
4
6
9
2
3
1

To check the first distributive law, let $a, b, c \in D(n)$, p a prime, and let $k \in \mathbb{N}$. Further, let $p^k | \mathsf{lcm}\{a, \gcd\{b, c\}\}$. Then, either $p^k|a$ or $p^k|b, c$. In that case, $p^k | \mathsf{lcm}\{a, b\}$ and $p^k | \mathsf{lcm}\{a, c\}$. So, $p^k | \gcd\{\mathsf{lcm}\{a, b\}, \mathsf{lcm}\{a, c\}\}$.

Now, let us assume that $p^k | \gcd\{\mathsf{lcm}\{a, b\}, \mathsf{lcm}\{a, c\}\}$. Then, $p^k | \mathsf{lcm}\{a, b\}$ and $p^k | \mathsf{lcm}\{a, c\}$. Then, either $p^k|a$ or $(p^k|b$ and $p^k|c)$. So, $p^k | \mathsf{lcm}\{a, \gcd\{b, c\}\}$.

Thus, any power of a prime divides $a \vee (b \wedge c)$ if and only if it divides $(a \vee b) \wedge (a \vee c)$. Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Similarly, the second distributive law can be verified.

Proposition: If X is a lattice, then the following identities hold for all a, b, c ∈ X:

L1 a ∨ b = b ∨ a, a ∧ b = b ∧ a

L2 (a ∨ b) ∨ c = a ∨ (b ∨ c), (a ∧ b) ∧ c = a ∧ (b ∧ c)

L3 a ∨ a = a, a ∧ a = a

L4 (a ∨ b) ∧ a = a, (a ∧ b) ∨ a = a.

Properties (L1) correspond to commutativity,

properties (L2) to associativity,

properties (L3) to idempotence and

properties (L4) to absorption.

Furthermore, for all a, b ∈ X, we have a ≤ b iff a ∨ b = b iff a ∧ b = a, called consistency.

Properties (L1)-(L4) are algebraic properties.

Properties: In a lattice (L, ≤), the following are true:

1. [Idempotence] : a ∨ a = a, a ∧ a = a

2. [Commutativity] : a ∨ b = b ∨ a, a ∧ b = b ∧ a

3. [Associativity] : a ∨ (b ∨ c) = (a ∨ b) ∨ c, a ∧ (b ∧ c) = (a ∧ b) ∧ c

4. $a \leq b \Leftrightarrow a \vee b = b$. Similarly, $a \leq b \Leftrightarrow a \wedge b = a$

5. [Absorption] : $a \vee (a \wedge b) = a = a \wedge (a \vee b)$

6. [Isotonicity] : $b \leq c \Rightarrow a \vee b \leq a \vee c$, $b \leq c \Rightarrow a \wedge b \leq a \wedge c$

7. $a \leq b, c \leq d \Rightarrow a \vee c \leq b \vee d$, $a \leq b, c \leq d \Rightarrow a \wedge c \leq b \wedge d$

8. [Distributive Inequality] : $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$

9. [Modularity] : $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$

Proof. We prove only the first parts of all assertions; the second parts can be proved similarly.

(1) $a \vee a$ is an upper bound of $\{a, a\}$.

Hence $a \vee a \geq a$. On the other hand, a is an upper bound of $\{a, a\}$.

So, $a \vee a$ being the least of all upper bounds of $\{a, a\}$, is less than or equal to a.

Hence $a \vee a = a$.

(2) $a \leq b\vee a$, $b \leq b\vee a$.

So, $b\vee a$ is an upper bound of a, b.

Since $a\vee b$ is the least of all upper bounds of a, b, we have $a \vee b \leq b \vee a$.

Exchanging a and b, we get $b \vee a \leq a \vee b$.

Hence $a \vee b = b \vee a$.

(3) Let $d = a \vee (b \vee c)$.

Then, $d \geq a$, $d \geq b \vee c$ so that $d \geq a$, $d \geq b$ and $d \geq c$. So, $d \geq a \vee b$ and $d \geq c$.

That is, $d \geq (a \vee b) \vee c$. Similarly, $e = (a \vee b) \vee c$ implies $e \geq a \vee (b \vee c)$.

Thus, the first part of the result follows.

(4) Let $a \leq b$. As b is an upper bound of $\{a, b\}$, and $a \vee b$ is the least of all upper bounds of $\{a, b\}$, we have $a \vee b \leq b$.

Also, $a \vee b$ is an upper bound of $\{a, b\}$ and hence $a \vee b \geq b$.

So, we get $a \vee b = b$.

Conversely, let $a \vee b = b$.

As $a \vee b$ is an upper bound of $\{a, b\}$, we have $a \leq a \vee b = b$.

Therefore, $a \leq b \Leftrightarrow a \vee b = b$.

(5) By definition $a \wedge b \leq a$. So, $a \vee (a \wedge b) \leq a \vee a = a$ using (1).

Also, by definition $a \vee (a \wedge b) \geq a$.

Hence, $a \vee (a \wedge b) = a$.

(6) Let b ≤ c. Note that a ∨ c ≥ a and a ∨ c ≥ c ≥ b.

So, a ∨ c is an upper bound of {a, b}.

Thus, a ∨ c ≥ lub{a, b} = a ∨ b.

(7) Using (6), we have a ∨ c ≤ b ∨ c ≤ b ∨ d.

Again, using (6), we get a ∧ c ≤ b ∧ c ≤ b ∧ d.

(8) Note that a ≤ a ∨ b and a ≤ a ∨ c.

Thus, a = a ∧ a ≤ (a ∨ b) ∧ (a ∨ c).

As b ≤ a ∨ b and c ≤ a ∨ c, by (7), we get b ∧ c ≤ (a ∨ b) ∧ (a ∨ c).

So, by definition a ∨ (b ∧ c) ≤ (a ∨ b) ∧ (a ∨ c).

(9) Let a ≤ c. Then, a ∨ c = c and hence by (8), we have a ∨ (b ∧ c) ≤ (a ∨ b) ∧ (a ∨ c) = (a ∨ b) ∧ c. Conversely, let a ∨ (b ∧ c) ≤ (a ∨ b) ∧ c.

Then a ≤ a ∨ (b ∧ c) ≤ (a ∨ b) ∧ c ≤ c.

Theorem:

The direct product of two distributive lattices is a distributive lattice. Proof. Let (a1, b1), (a2, b2), (a3, b3) be elements in the direct product of two distributive lattices. Then [(a1, b1) ∨ (a2, b2)] ∧ (a3, b3) = (a1 ∨ a2, b1 ∨ b2) ∧ (a3, b3) = (a1 ∨ a2) ∧ a3,(b1 ∨ b2) ∧ b3 = (a1 ∧ a3) ∨ (a2 ∧ a3), (b1 ∧ b3) ∨ (b2 ∧ b3) = (a1 ∧ a3),(b1 ∧ b3) ∨ (a2 ∧ a3),(b2 ∧ b3) = = (a1, b1) ∧ (a3, b3) ∨ (a2, b2) ∧ (a3, b3).

This verifies one of the distributive laws. Similarly, the other one can be verified.

Definition: Let (L1, ≤1) and (L2, ≤2) be lattices. A function f : L1 → L2 satisfying f(a∨1b) = f(a)∨2f(b) and f(a∧1b) = f(a)∧2f(b) is called a lattice homomorphism.

Further, if f is a bijection, then it is called a lattice isomorphism.

Definition:

Let (L, ≤) be a lattice. It is called a bounded lattice if there exist elements α, β ∈ L such that for each x ∈ L, we have x ≤ α and β ≤ x. Such an element α is called the largest element of L, and is denoted by 1. The element β ∈ L satisfying β ≤ x for all x ∈ L is called the smallest element of L, and is denoted by 0.

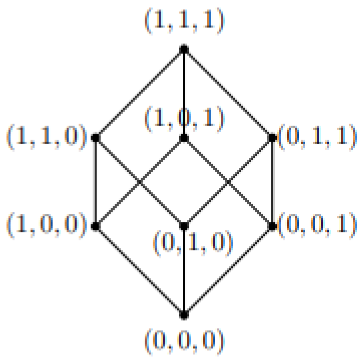
Notice that if a lattice is bounded, then 1 is the lub of the lattice and 0 is the glb of the lattice.

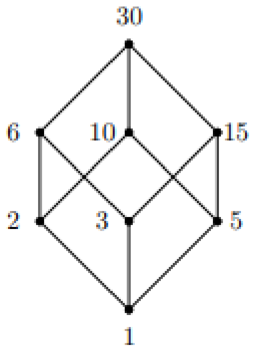
Definition: A lattice (L, ≤) is said to be complete if each nonempty subset of L has lub and glb in L. For A ⊆ L, we write lub of A as ∨A, and glb of A, as ∧A. It follows that each complete lattice is a bounded lattice.

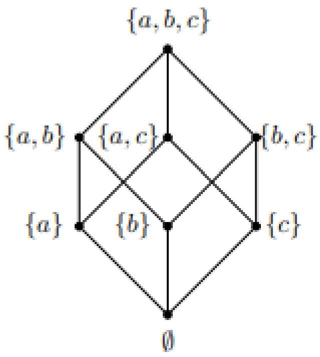
Examples:

1. The set [0, 5] with the usual order is a lattice which is both bounded and complete. So, is the set [0, 1) ∪ [2, 3].
2. The set (0, 5] with the usual order is a lattice which is neither bounded nor complete.

3. The set [0, 1) ∪ (2, 3] with the usual order is a lattice which is bounded but not complete.
4. Every finite lattice is complete, and hence, bounded.
5. The set R with the usual order is a lattice. It is not a complete lattice. Observe that the completeness property of R, i.e., “for every bounded nonempty subset a glb and an lub exist” is different from the completeness in the lattice sense.







Definition: Let (L, ≤) be a bounded lattice. We say that (L, ≤) is a complemented lattice if for each x ∈ L, there exists y ∈ L such that x∨y = 1 and x∧y = 0. Such an element y corresponding to the element x is called a complement of x, and is denoted by ¬x.

Theorem: Let (L, ≤) be a lattice and let a, b, c ∈ L. The following table lists the properties that hold (make sense) in the specified type of lattices.

Properties	**Lattice type**
$\vee, \wedge$ *are idempotent*	*Any lattice*
$\vee, \wedge$ *are commutative*	*Any lattice*
$\vee, \wedge$ *are associative*	*Any lattice*
$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$	*Any lattice*
[Absorption] $a \wedge (a \vee b) = a = a \vee (a \wedge b)$	*Any lattice*
[Isotonicity] $b \leq c \Rightarrow \{a \vee b \leq a \vee c, a \wedge b \leq a \wedge c\}$	*Any lattice*
[Distributive inequalities] $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$	*Any lattice*
[Modular inequality] $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$	*Any lattice*
$\mathbf{0}$ *is unique;* $\mathbf{1}$ *is unique*	*Bounded lattice*
If a is a complement of b, then b is also a complement of a	*Bounded lattice*
$\neg\mathbf{0}$ *is unique and it is* $\mathbf{1}$; $\neg\mathbf{1}$ *is unique and it is* $\mathbf{0}$	*Bounded lattice*
An element a has a unique complement	*Distributive complemented lattice*
[Cancellation] $\{a \vee c = b \vee c,\ a \vee \neg c = b \vee \neg c\} \Rightarrow a = b$ $\{a \wedge c = b \wedge c,\ a \wedge \neg c = b \wedge \neg c\} \Rightarrow a = b$	*Distributive complemented lattice*
[De-Morgan] $\neg(a \vee b) = \neg a \wedge \neg b$ $\neg(a \wedge b) = \neg a \vee \neg b$	*Distributive complemented lattice*
$a \vee \neg b = \mathbf{1} \Leftrightarrow a \vee b = a$ $a \wedge \neg b = \mathbf{0} \Leftrightarrow a \wedge b = a$	*Distributive complemented lattice*

Proof. We will only prove the properties that appear in the last three rows; others are left as exercises.

Cancellation property: $b = b \vee 0 = b \vee (c \wedge \neg c) = (b \vee c) \wedge (b \vee \neg c) = (a \vee c) \wedge (a \vee \neg c) = a \vee (c \wedge \neg c) = a \vee 0 = a$. $b = b \wedge 1 = b \wedge (c \vee \neg c) = (b \wedge c) \vee (b \wedge \neg c) = (a \wedge c) \vee (a \wedge \neg c) = a \wedge (c \vee \neg c) = a \wedge 1 = a$.

De-Morgan’s property: $(a \vee b) \vee (\neg a \wedge \neg b) = (a \vee b \vee \neg a) \wedge (a \vee b \vee \neg b) = 1 \wedge 1 = 1$. $(a \vee b) \wedge (\neg a \wedge \neg b) = (a \wedge \neg a \wedge \neg b) \vee (b \wedge \neg a \wedge \neg b) = 0 \vee 0 = 0$.

$(a \wedge b) \vee (\neg a \vee \neg b) = (a \vee \neg a \vee \neg b) \wedge (b \vee \neg a \vee \neg b) = 1 \wedge 1 = 1$.

$(a \wedge b) \wedge (\neg a \vee \neg b) = (a \wedge b \wedge \neg a) \vee (a \wedge b \wedge \neg b) = 0 \wedge 0 = 0$.

Using Definition, on the first two equalities, we get $\neg(a \vee b) = \neg a \wedge \neg b$; and using it again on the last two equalities, we obtain $\neg(a \wedge b) = (\neg a \vee \neg b)$.

To prove the next assertion, note that if $a \vee \neg b = 1$, then $a = a \vee (b \wedge \neg b) = (a \vee b) \wedge (a \vee \neg b) = (a \vee b) \wedge 1 = a \vee b$.

Conversely, if $a = a \vee b$, then $a \vee \neg b = (a \vee b) \vee \neg b = 1$.

Similarly, the second part is proved.

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT –V–DISCRETE MATHEMATICS – SMT1304

UNIT – V – BOOLEAN ALGEBRA

Boolean Algebra, Basic properties, Sub algebra, Direct Product, and Homomorphism, Boolean Functions.

Definition:

A **Boolean algebra** is a nonempty set S which is closed under the binary operations $\vee$ (called join), $\wedge$ (called meet), and the unary operation $\neg$ (called inverse or complement) satisfying the following properties for all x, y, z $\in$ S:

1. [Commutativity] : $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$.

2. [Distributivity] : $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

3. [Identity elements] : There exist elements 0, 1 $\in$ S such that $x \vee 0 = x$ and $x \wedge 1 = x$.

4. [Inverse] : $x \vee \neg x = 1$ and $x \wedge \neg x = 0$.

When required, we write the Boolean algebra S as $(S, \vee, \wedge, \neg)$ showing the operations explicitly. Notice that the fourth property in the definition above uses the two special elements 0 and 1, whose existence has been asserted in the third property.

This is meaningful when these two elements are uniquely determined by the third property.

Theorem:

Let S be a Boolean algebra. Then the following statements are true:

1. Elements 0 and 1 are unique.

2. Corresponding to each $s \in S$, $\neg s$ is the unique element in S that satisfies the property: $s \vee \neg s = 1$ and $s \wedge \neg s = 0$.

3. For each $s \in S$, $\neg\neg s = s$.

Proof. (1) Let 01, 02 $\in$ S be such that for each $x \in S$, $x \vee 01 = x$ and $x \vee 02 = x$.

Then, in particular, $02 \vee 01 = 02$ and $01 \vee 02 = 01$.

By Commutativity, $02 \vee 01 = 01 \vee 02$.

So, $02 = 01$. That is, 0 is the unique element satisfying the property that for each $x \in S$, $0 \vee x = x$.

A similar argument shows that 1 is the unique element that satisfies the property that for each $x \in S$, $x \wedge 1 = x$.

(2) Let $s \in S$. By definition, $\neg s$ satisfies the required properties.

For the converse, suppose $t, r \in S$ are such that $s \vee t = 1$, $s \wedge t = 0$, $s \vee r = 1$ and $s \wedge r = 0$.

Then $t = t \wedge 1 = t \wedge (s \vee r) = (t \wedge s) \vee (t \wedge r) = 0 \vee (t \wedge r) = (s \wedge r) \vee (t \wedge r) = (s \vee t) \wedge r = 1 \wedge r = r$.
(3) It directly follows from the definition of inverse, due to commutativity.

Examples:

1. Let S be a nonempty set. Then P(S) is a Boolean algebra with $\vee = \cup$, $\wedge = \cap$, $\neg A = Ac$, $0 = \emptyset$ and $1 = S$. This is called the power set Boolean algebra. So, we have Boolean algebras of finite size as well as of uncountable size.

2. Take $D(30) = \{n \in N : n \mid 30\}$ with $a \vee b = \mathrm{lcm}(a, b)$, $a \wedge b = \gcd(a, b)$ and $\neg a = 30\ a$. It is a Boolean algebra with $0 = 1$ and $1 = 30$.

3. Let $B = \{T, F\}$, where $\vee$, $\wedge$ and $\neg$ are the usual connectives. It is a Boolean algebra with $0 = F$ and $1 = T$.

4. Let B be the set of all truth functions involving the variables p1, . . . , pn, with usual operations $\vee$, $\wedge$ and $\neg$. Then B is a Boolean algebra with $0 = \perp$ and $1 = >$. This is called the free Boolean algebra on the generators p1, . . . , pn.

5. The set of all formulas (of finite length) involving variables p1, p2, . . . is a Boolean algebra with usual operations. This is also called the free Boolean algebra on the generators p1, p2, ... Here also $0 = \perp$ and $1 = >$. So, we have a Boolean algebra of denumerable size.

Remark: The rules of Boolean algebra treat $(\vee, 0)$ and $(\wedge, 1)$ equally. Notice that the second parts in the defining conditions of Definition 8.3.1 can be obtained from the corresponding first parts by replacing $\vee$ with $\wedge$, $\wedge$ with $\vee$, 0 with 1, and 1 with 0 simultaneously. Thus, any statement that one can derive from these assumptions has a dual version which is derivable from the same assumptions. This is called the principle of duality.

Theorem: [Laws]

Let S be a Boolean algebra. Then the following laws hold for all $s, t \in S$:

1. [Constants] : $\neg 0 = 1$, $\neg 1 = 0$, $s \vee 1 = 1$, $s \wedge 1 = s$, $s \vee 0 = s$, $s \wedge 0 = 0$.

2. [Idempotence] : $s \vee s = s$, $s \wedge s = s$.

3. [Absorption] : $s \vee (s \wedge t) = s$, $s \wedge (s \vee t) = s$.

4. [Cancellation] : $s \vee t = r \vee t$, $s \vee \neg t = r \vee \neg t \Rightarrow s = r$.

5. [Cancellation] : $s \wedge t = r \wedge t$, $s \wedge \neg t = r \wedge \neg t \Rightarrow s = r$.

6. [Associativity] : $(s \vee t) \vee r = s \vee (t \vee r)$, $(s \wedge t) \wedge r = s \wedge (t \wedge r)$.

Proof. We give the proof of the first part of each item and that of its dual is left for the reader.

(1) $1 = 0 \vee (\neg 0) = \neg 0$.

$s \vee 1 = (s \vee 1) \wedge 1 = (s \vee 1) \wedge (s \vee \neg s) = s \vee (1 \wedge \neg s) = s \vee \neg s = 1$.

$s \vee 0 = s \vee (s \wedge \neg s) = (s \vee s) \wedge (s \vee \neg s) = s \wedge 1 = s$.

(2) $s = s \vee 0 = s \vee (s \wedge \neg s) = (s \vee s) \wedge (s \vee \neg s) = (s \vee s) \wedge 1 = (s \vee s)$.

(3) $s \vee (s \wedge t) = (s \wedge 1) \vee (s \wedge t) = s \wedge (1 \vee t) = s \wedge 1 = s$.

(4) Suppose that $s \vee t = r \vee t$ and $s \vee \neg t = r \vee \neg t$. Then $s = s \vee 0 = s \vee (t \wedge \neg t) = (s \vee t) \wedge (s \vee \neg t) = (r \vee t) \wedge (r \vee \neg t) = r \vee (t \wedge \neg t) = r \vee 0 = r$.

(5) This is the dual of (4) and left as an exercise.

(6) Using distributivity and absorption, we have $s \vee (t \vee r) \wedge \neg s = (s \wedge \neg s) \vee (t \vee r) \wedge \neg s = 0 \vee (t \vee r) \wedge \neg s = (t \vee r) \wedge \neg s = (t \wedge \neg s) \vee (r \wedge \neg s)$.

$(s \vee t) \vee r \wedge \neg s = (s \vee t) \wedge \neg s \vee (r \wedge \neg s) = (s \wedge \neg s) \vee (t \wedge \neg s) \vee (r \wedge \neg s) = (0 \vee (t \wedge \neg s) \vee (r \wedge \neg s) = (t \wedge \neg s) \vee (r \wedge \neg s)$.

Hence, $s \vee (t \vee r) \wedge \neg s = (s \vee t) \vee r \wedge \neg s$.

Also, $(s \vee t) \vee r \wedge s = (s \vee t) \wedge s \vee (r \wedge s) = s \vee (r \wedge s) = s = s \vee (t \vee r) \wedge s$.

Now, apply Cancellation law to obtain the required result.

Isomorphisms between two similar algebraic structures help us in understanding an unfamiliar entity through a familiar one. Boolean algebras are no exceptions.

Definition: Let $(B1, \vee1, \wedge1, \neg1)$ and $(B2, \vee2, \wedge2, \neg2)$ be two Boolean algebras.

A function $f : B1 \to B2$ is a Boolean homomorphism if it preserves 0, 1, $\vee$, $\wedge$, and $\neg$. In such a case, $f(01) = 02$, $f(11) = 12$, $f(a \vee1 b) = f(a) \vee2 f(b)$, $f(a \wedge1 b) = f(a) \wedge2 f(b)$, $f(\neg1a) = \neg2f(a)$.

A Boolean isomorphism is a Boolean homomorphism which is a bijection.

Unless we expect an ambiguity in reading and interpreting the symbols, we will not write the subscripts with the operations explicitly as is done in Definition.

Examples: Recall the notation $[n] = \{1, 2, . . . , n\}$. The function $f : P([4]) \to P([3])$ defined by $f(S) = S \setminus \{4\}$ is a Boolean homomorphism.

We check two of the properties and leave others as exercises. $f(A \vee B) = f(A \cup B) = (A \cup B) \setminus \{4\} = (A \setminus \{4\}) \cup (B \setminus \{4\}) = f(A) \vee f(B)$. $f(1) = f([4]) = [4] \setminus \{4\} = [3] = 1$.

Theorem: Let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. Define the relation $\leq$ on B by $a \leq b$ if and only if $a \wedge b = a$ for all $a, b \in B$. Then $(B, \leq)$ is a distributive complemented lattice in which $\text{lub}\{a, b\} = a \vee b$ and $\text{glb}\{a, b\} = a \wedge b$ for all $a, b \in B$.

Proof: We first verify that $(B, \leq)$ is a partial order.

Reflexive: $s \leq s$ if and only if $s \wedge s = s$, which is true.

Antisymmetry: Let $s \leq t$ and $t \leq s$. Then we have $s = s \wedge t = t$.

Transitive: Let $s \leq t$ and $t \leq r$. Then $s \wedge t = s$ and $t \wedge r = t$.

Using associativity, $s \wedge r = (s \wedge t) \wedge r = s \wedge (t \wedge r) = s \wedge t = s$;

consequently, $s \leq r$. Now, we show that $a \vee b = \text{lub}\{a, b\}$.

Since B is a Boolean algebra, using absorption, we get $(a \vee b) \wedge a = a$ and hence $a \leq a \vee b$. Similarly, $b \leq a \vee b$.

So, $a \vee b$ is an upper bound for $\{a, b\}$. Now, let x be any upper bound for $\{a, b\}$.

Then, by distributive property, $(a \vee b) \wedge x = (a \wedge x) \vee (b \wedge x) = a \vee b$.

So, $a \vee b \leq x$. Thus, $a \vee b$ is the lub of $\{a, b\}$.

Analogous arguments show that $a \wedge b = \text{glb}\{a, b\}$.

Since for all $a, b \in B$, $a \vee b$ and $a \wedge b$ are in B, we see that $\text{lub}\{a, b\}$ and $\text{glb}\{a, b\}$ exist.

Thus $(B, \leq)$ is a lattice.

Further, if $a \in B$, then $\neg a \in B$. This provides the complement of a in the lattice $(B, \leq)$.

Further, both the distributive properties are already satisfied in B.

Hence $(B, \leq)$ is a distributive complemented lattice.

Definition: Let $(B, \vee, \wedge, \neg)$ be a Boolean algebra. The relation $\leq$ on B given by $a \leq b$ if and only if $a \wedge b = a$ for all $a, b \in B$ is called the induced partial order.

A minimal element of B with respect to the partial order $\leq$, which is different from 0 is called an atom in B.

Examples:

1. In the power set Boolean algebra, singleton sets are the only atoms.

2. In Example atoms of D(30) are 2, 3 and 5.

3. The {F, T} Boolean algebra has only one atom, namely T.

Proposition: Each finite Boolean algebra has at least one atom.

Proof:

Let B be a finite Boolean algebra.

Assume that no element of B is an atom.

Now, $0 < 1$ and 1 is not an atom.

Then there exists $b1 \in B$ such that $0 < b1 < 1$.

Since b1 is not an atom, there exists $b2 \in B$ such that $0 < b2 < b1 < 1$.

By induction it follows that we have a sequence of elements (bi) such that $0 < \cdot \cdot \cdot < bi < bi-1 < \cdot \cdot \cdot < b1 < 1$.

As B is finite, there exist $k > j$ such that $bk = bj$.

We then have $bk < bk-1 < \cdot \cdot \cdot < bj = bk$.

This is impossible. Hence B has at least one atom.

Proposition: Let p and q be atoms in a Boolean algebra B. If $p\ 6= q$, then $p \wedge q = 0$.

Proof:

Suppose that $p \wedge q\ 6= 0$.

We know that $p \wedge q \leq p$.

If $p \wedge q\ 6= p$, then $p \wedge q < p$.

But this is not possible since p is an atom.

So, $p \wedge q = p$. Similarly, $q \wedge p = q$.

By commutativity, $p = p \wedge q = q \wedge p = q$.

Theorem: [Representation] Let B be a finite Boolean algebra. Then there exists a set X such that B is isomorphic to P(X).

Proof: Let X be the set of all atoms of B.

By Proposition, $X\ 6= \emptyset$.

Define $f : B \to P(X)$ by $f(b) = \{x \in B : x \text{ is an atom and } x \leq b\}$ for $b \in B$.

We show that f is the required Boolean isomorphism.

Injection: Suppose b1 6= b2.

Then, either b1 b2 or b2 b1.

Without loss of generality, let b1 b2.

Note that $b1 = b1 \wedge (b2 \vee \neg b2) = (b1 \wedge b2) \vee (b1 \wedge \neg b2)$.

Also, the assumption b1 b2 implies $b1 \wedge b2\ 6= b1$ and hence $b1 \wedge \neg b2\ 6= 0$.

So, there exists an atom $x \leq (b1 \wedge \neg b2)$ and hence $x = x \wedge b1 \wedge \neg b2$.

Then $x \wedge b1 = (x \wedge b1 \wedge \neg b2) \wedge b1 = x \wedge b1 \wedge \neg b2 = x$.

Thus, $x \leq b1$.

Similarly, $x \leq \neg b2$. As $x\ 6= 0$,

we cannot have $x \leq b2$ (for, $x \leq \neg b2$ and $x \leq b2$ imply $x \leq b2 \wedge \neg b2 = 0$).

Thus there is an atom in f(b1) which is not in f(b2).

Therefore, f(b1) 6= f(b2).

Surjection: Let $A = \{x1, \ldots, xk\} \subseteq X$.

Write $a = x1 \vee \cdots \vee xk$ (if $A = \emptyset$, take $a = 0$).

Clearly, $A \subseteq f(a)$. We show that $A = f(a)$. So, let $y \in f(a)$.

Then y is an atom in B and $y = y \wedge a = y \wedge (x1 \vee \cdots \vee xk) = (y \wedge x1) \vee \cdots \vee (y \wedge xk)$.

Since $y\ 6= 0$, by Proposition, $y \wedge xi\ 6= 0$ for some $i \in \{1, 2, \ldots, k\}$.

As xi and y are atoms, we have $y = y \wedge xi = xi$ and hence $y \in A$.

That is, $f(a) \subseteq A$ so that $f(a) = A$.

Thus, f is a surjection. Preserving 0, 1 : Clearly $f(0) = \emptyset$ and $f(1) = X$. Preserving $\vee$, $\wedge$: By definition, $x \in f(b1 \wedge b2) \Leftrightarrow x \leq b1 \wedge b2 \Leftrightarrow x \leq b1$ and $x \leq b2 \Leftrightarrow x \in f(b1)$ and $x \in f(b2) \Leftrightarrow x \in f(b1) \cap f(b2)$.

For the other one, let $x \in f(b1 \vee b2)$. Then, $x = x \wedge (b1 \vee b2) = (x \wedge b1) \vee (x \wedge b2)$.

So, $x \wedge b1$ 6= 0 or $x \wedge b2$ 6= 0.

Without loss of generality, suppose $x \wedge b1$ 6= 0.

As x is an atom, $x \leq b1$ and hence $x \in f(b1) \subseteq f(b1) \cup f(b2)$.

Conversely, let $x \in f(b1) \cup f(b2)$. Without loss of generality, let $x \in f(b1)$.

Thus, $x \leq b1$ and hence $x \leq b1 \vee b2$ which in turn implies that $x \in f(b1 \vee b2)$.

Therefore, $x \in f(b1 \vee b2) \Leftrightarrow x \in f(b1) \cup f(b2)$.

Preserving $\neg$: Let $x \in B$. Then $f(x) \cup f(\neg x) = f(x \vee \neg x) = f(1) = X$ and $f(x) \cap f(\neg x) = f(x \wedge \neg x) = f(0) = \emptyset$.

Thus $f(\neg x) = f(x)$ c .

As immediate consequences of the representation theorem, we obtain the following results.

Corollary: Let B be a finite Boolean algebra.

1. If B has exactly k atoms then B is isomorphic to $P(\{1, 2, . . . , k\})$. Hence, B has exactly 2^k elements.

2. Fix $b \in B$. If $p_1, . . . , p_n$ are the only atoms less than or equal to b, then $b = p_1 \vee \cdot \cdot \cdot \vee p_n$.