Relations.

Def: Any set of ordered pairs defies a binary relation.

Binary Relation: We shall call a binary relation simply a relation. It some times convenient to express the fact that a particular ordered pair, say $\langle x,y\rangle \in R$, where R is a relation, by writting xRy which may be read as "x is in relation R to y".

Example: A familiar example is the relation "greater than" for real numbers. This relation is denoted by $>$. Each member of any of the ordered pairs in the set is a real number, and if a and b are two real numbers such that $a > b$, then we say that $\langle a,b\rangle \in >$.

ie $> = \{\langle x,y\rangle \mid x,y \text{ are real nos and } x > y\}$.

Another example:

The relation of father to his child can be described by a set, say F of ordered pairs in which the first member is the name of the father and the second the name of his child.

(ie) $F = \{\langle x,y\rangle \mid x \text{ is the father of } y\}$.

Domain and range:

Let S be a binary relation. The set D(S) of all objects x such that for some y, $\langle x,y\rangle \in S$ is called the Domain of S, that is

$$D(S) = \{x \mid (\exists y)(\langle x,y\rangle \in S)\}.$$

Similarly, the set R(S) of all objects y such that for some x, $\langle x, y\rangle \in S$ is called the range of S

(ie) $R(S) = \{ y \mid (\exists x)(\langle x,y\rangle \in S)\}$

Ex:

$S = \{\langle 2,4\rangle, \langle 1,3\rangle, \langle \lambda, 6\rangle, \langle \text{Joan}, H\rangle\}$

$D(S) = \{2, 1, \lambda, \text{Joan}\}$

$R(S) = \{4, 3, 6, H\}$

Cartesian product. defines a relation.

Let X and Y be any two sets. A subset of the cartesian product $X \times Y$ will define a relation. For any such relation C, $D(C) \subseteq X$ and $R(C) \subseteq Y$ and the relation C is said to be from X to Y.

If $Y = X$, then C is any relation from X to X. In this case C is called a relation in X.

Universal Relation. Any relation in X is a subset of $X \times X$, then the set $X \times X$ itself defines a relation in X and is called a Universal relation in X.

3

Void relation: The empty set which is also a subset of $X \times X$ is called a void relation in X.

Relation: A relation has been defined as a set of ordered pairs.

Properties of Binary Relations in a set.

Defn: A binary relation R in a set X is ~~reflex~~ reflexive if for every $x \in X$, xRx that is

$\langle x, x \rangle \in R$ (or)

R is reflexive in $X \iff (x)(x \in X \rightarrow xRx)$

Ex: The relation $\leq$ is reflexive in the set of real numbers.

Defn: A relation R in a set X is symmetric if for every x and y in X, whenever xRy, then yRx. That is

R is symmetric in $X \iff (x)(y)(x \in X \wedge y \in X \wedge xRy \rightarrow yRx)$

Ex: 1. The relation of equality is symmetric in the set of real numbers.

2. The relation of similarity in the set of triangles in a plane is both reflexive and symmetric.

4

Defn: A Relation R in a set X is ~~symmetric~~ Transitive if, for every x, y and z in X, whenever xRy and yRz then xRz. That is

R is transitive in X

$\Longleftrightarrow (x)(y)(z)(x \in X \wedge y \in X \wedge z \in X \wedge xRy \wedge yRz \rightarrow xRz)$.

Ex:

1. The relations $\leq$, $<$ and $\supset$ are transitive in the set of real numbers.

2. The relation of similarity of triangles in a plane is transitive.

Def: A relation R in a set X is irreflexive if for every $x \in X$, $\langle x, x \rangle \notin R$

Ex: The relation $<$ in the set of real numbers is irreflexive.

The relation of proper inclusion in the set of all nonempty subsets of a universal set is irreflexive.

Defn: A relation R in a set X is antisymmetric if, for every x and y in X, whenever xRy and yRx then $x = y$. That is

R is antisymmetric in X iff

$(x)(y)(x \in X \wedge y \in X \wedge xRy \wedge yRx \rightarrow x = y)$.

Ex: Let X be the collection of the subsets of a universal set. The relation of inclusion in X is antisymmetric. and also proper inclusion in X is antisymmetric.

Relation matrix and the graph of a relation

5

Let $X = \{x_1, x_2, \ldots x_m\}$, and $Y = \{y_1, y_2, \ldots y_n\}$, R be a relation from X to Y.
We assume that the elements of X and Y appear in a certain order, then the relation R can be represented by a matrix whose elements 1's and 0's.
This matrix can be written by

$$r_{ij} = \begin{cases} 1 & \text{if } x_i R y_j \\ 0 & \text{if } x_i \not R y_j \end{cases}$$

Where r_{ij} is the element ~~&~~ in the i^{th} row and j^{th} column.
This matrix is called relation matrix.

<u>Ex:</u> ~~Relation~~ ~~Let~~ $X = \{x_1, x_2, x_3\}$ $Y = \{y_1, y_2\}$
the relation R is $R = \{\langle x_1, y_1\rangle, \langle x_2, y_1\rangle, \langle x_3, y_2\rangle,$
$\langle x_2, y_2\rangle\}$

The relation R is given by relation matrix is

$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\begin{array}{c} \begin{array}{cc} y_1 & y_2 \end{array} \\ \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \end{array}$$

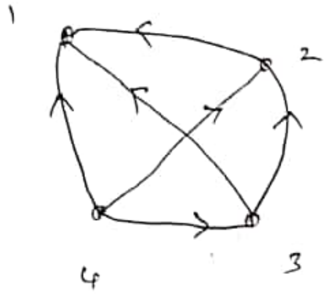
A relation can also be represented pictorially by drawing its graph. Let R be a relation in a set $X = \{x_1, x_2, \ldots x_m\}$. The elements of X are represented by points or circules called nodes. The nodes corresponding to x_i and x_j are labelled x_i and x_j. respectively. This nodes called vertices. If $x_i R x_j$, (i.e) if $\langle x_i, x_j\rangle \in R$, then we connect x_i and x_j by an arc and put an arrow in the direction from x_i and x_j.
when all the nodes corresponding to the the ordered pairs in ~~the~~ R are connected by arcs with proper arrows, we get a graph of the relation.
If $x_i R x_j$ and $x_j R x_i$, then we draw two arcs between x_i and x_j. If ~~~~ $x_i R x_j$ we get an arc which

starts from x_i and return to x_i. Such an arc is called a loop.

Ex: Let $X = \{1,2,3,4\}$ and $R = \{\langle x,y\rangle \mid x > y\}$

Draw the graph of R and also give its matrix.

Soln: $R = \{\langle 4,1\rangle, \langle 4,2\rangle, \langle 4,3\rangle, \langle 3,1\rangle \langle 3,2\rangle \langle 2,1\rangle\}$



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

graph - representation. matrix representation.

partition and covering of a set.

Let S be a given set and $A = \{A_1, A_2, \cdots A_m\}$ where each A_i, $i = 1,2, \cdots m$ is a subset of S and $\bigcup_{i=1}^{m} A_i = S$. Then the set A is called a covering of S and $A_1, A_2, \cdots A_m$ are said to covers S. If the elements of A, which are subsets of S are mutually disjoint, then A is called a partition of S and the sets $A_1, A_2 \cdots A_m$ are called the blocks of the partition.

Ex: Let $S = \{a, b, c\}$

Consider the collection of subsets

$A = \{\{a,b\}, \{b,c\}\}$ $B = \{\{a\}, \{a,c\}\}$ $C = \{\{a\},\{b,c\}\}$

$D = \{\{a,b,c\}\}$, $E = \{\{a\},\{b\},\{c\}\}$.

$F = \{\{a\},\{a,b\},\{a,c\}\}$

The sets A and F are coverings of S and the sets C, D and E are partition of S.

Note: Every partition is also a covering.

Set B is neither a partition nor a covering of S.

Note:

Two partitions ~~sets~~ said to equal if they are equal as sets.

For a finite set, every partition contains only a finite number of blocks.

In the above collection of the subsets:

A has 2 blocks, B has 2 blocks D has 1 block

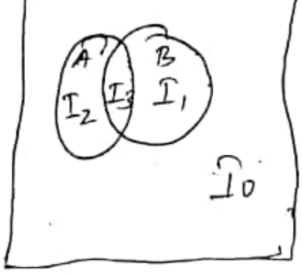
E has 3 blocks.

Ex:- Let A and B be any two subset of E and consider the sets

$I_0 = \sim A \cap \sim B$, $I_1 = \sim A \cap B$ $I_2 = A \cap \sim B$, $I_3 = A \cap B$.

The sets I_0 I_1, I_2 and I_3 are called the complete intersection or the minterms generated by the subsets A and B. I_0, I_1, I_2 and I_3 are mutually disjoint and

$E = I_0 \cup I_1 \cup I_2 \cup I_3 = \bigcup_{j=0}^{3} I_j$



The complete intersection or the minterms are the blocks of the partition of E generated by A and B.

Equivalence Relations. A relation R in a set X is called an equivalence relation if it is (i) reflexive (ii) symmetric and (iii) transitive.

If R is an equivalence relation in a set X, then D(R) the domain of R is X itself.
$\therefore$ R will be called a relation on X.

Ex:

1. Similarity of triangles on the set of triangles.
2. Relation of lines being parallel on a set of lines in a plane.

3. Ex: Let $X = \{1, 2, 3, 4\}$
and $R = \{\langle 1,1\rangle, \langle 1,4\rangle, \langle 4,1\rangle, \langle 4,4\rangle, \langle 2,2\rangle, \langle 2,2\rangle, \langle 2,3\rangle \langle 3,2\rangle, \langle 3,3\rangle\}$

where R - is a equivalence relation -

R - equivalence class generated by $x \in X$.

Let R be an equivalence relation on a set X. For any $x \in X$, the set $[x]_R \subseteq X$ given by

$$[x]_R = \{ y \mid y \in X \wedge xRy \}$$

- is called an R - equivalence class generated by $x \in X$.

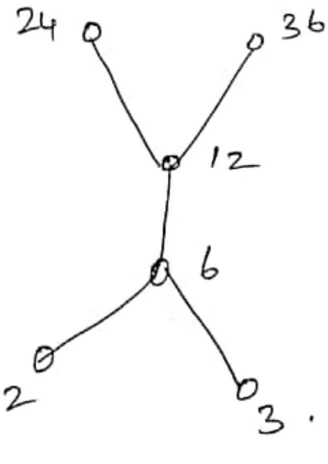
Ex: 1. Let R be the set of real numbers. The relation "less than or equal to" or $\leq$ is a partial ordering on R. The converse of relation $\geq$ is also a partial ordereing on R.

2. Inclusion: Let $\rho(A) = 2^A = X$ be the power set of A, (ie) X is the subsets of A. The relation of inclusion ($\subseteq$) on X is a partial ordering.

Hasse diagram. A partial ordereing $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or partially ordered set diagram of $(P, \leq)$

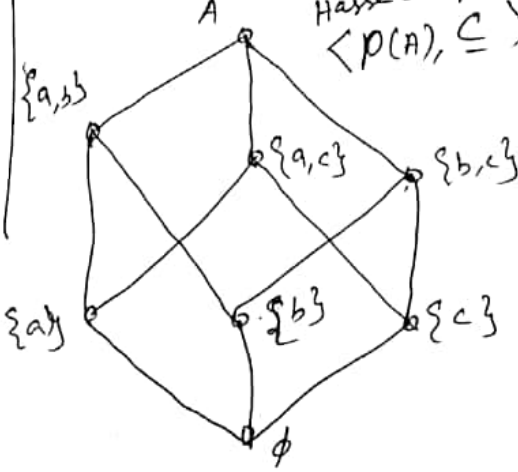
Ex: Let $X = \{2, 3, 6, 12, 24, 36\}$ and the relation $\leq$ be such that $x \leq y$ if x divides y.

The Hasse diagram is



Ex: $A = \{a, b, c\}$

$\rho(A) = \{\{a,b,c\}, \{a,b\}$
$\{a,c\}, \{b,c\}\ \{a\}\ \{b\}$
$\{c\}\ \{\phi\}\}$



Defn: upper bound and lower bound.

Let $\langle P, \leq \rangle$ be a partially set and let $A \subseteq P$. Any element $x \in P$ is an upper bound for A if for all $a \in A$, $a \leq x$. Similarly, any element $x \in P$ is a lowerbound for A if forall $a \in A$, $x \leq a$.

Defn: Supremum and infimum.

Let $\langle P, \leq \rangle$ be a partially ordered set and let $A \subseteq P$. An element $x \in P$ is a least upper bound, or supremum for A if x is an upper bound for A and $x \leq y$ where y is any upper bound for A. Similarly, the greatest lowerbound or infimum for A is an element $x \in P$ such that x is a lower bound and $y \leq x$ for all lowerbounds y.

Defn: well-ordered

A partially ordered set is called well-ordered if every nonempty subset of it has a least member.

Defn function.

Let X and Y be any two sets. A relation f from X to Y is called a function if for every $x \in X$ there is a unique $y \in Y$ such that $\langle x, y \rangle \in f$.

Defn: If $f: X \to Y$ and $A \subseteq X$, then $f \cap (A \times Y)$ is a function from $A \to Y$ called the restriction of f to A and is sometimes as f/A. If g is a restriction of f, then f is called the extension of g.

<u>Compatibility relation:</u> A Relation R in X is said to be a compatibility relation if it is reflexive and symmetric.

<u>Note:</u> All equivalence relations are compatibility relations.

<u>Defn:</u> <u>Composite relations.</u>

Let R be a relation from X to Y and S be a relation from Y to Z. Then a relation written as $R \circ S$ is called a composite relation of R and S where

$$R \circ S = \{ \langle x, z \rangle \mid x \in X \wedge z \in Z \wedge (\exists y)(y \in Y \wedge \langle x, y \rangle \in R \wedge \langle y, z \rangle \in S) \}$$

The operation of obtaining $R \circ S$ from R and S is called composition of relations.

<u>Ex:</u> Let $R = \{ \langle 1,2 \rangle, \langle 3,4 \rangle, \langle 2,2 \rangle \}$

and $S = \{ \langle 4,2 \rangle, \langle 2,5 \rangle, \langle 3,1 \rangle, \langle 1,3 \rangle \}$.

(i) $R \circ S = \{ \langle 1,5 \rangle, \langle 3,2 \rangle, \langle 2,5 \rangle \}$

$S \circ R = \{ \langle 4,2 \rangle, \langle 3,2 \rangle, \langle 1,4 \rangle \}$

$(R \circ S) \circ R = \{ \langle 3,2 \rangle \}$

$R \circ (S \circ R) = \{ \langle 3,2 \rangle \}$

$R \circ R = \{ \langle 1,2 \rangle, \langle 2,2 \rangle \}$

$R \circ R \circ R = \{ \langle 1,2 \rangle, \langle 2,2 \rangle \}$

Defn: Converse Relation:

Given a relation R from X to Y, a relation $\bar{R}$ from Y to X is called the Converse of R, where the ordered pairs of $\bar{R}$ are obtained by interchanging the members in each of the ordered pairs of R. This means, for $x \in X$ and $y \in Y$ that $x R y \Leftrightarrow y \bar{R} x$.

Note: The relation matrix $M_{\bar{R}}$ of $\bar{R}$ can be obtained by simply interchanging the rows and columns of M_R. Such a matrix is called the transpose of M_R.

$$\therefore \; M_{\bar{R}} = \text{transpose of } M_R.$$

Defn: Let X be any finite set and R be a relation in X. The relation $R^+ = R \cup R^2 \cup R^3 \cup \ldots$ in X is called the transitive closure of R in X.

Defn: partial order relation: A binary relation R in a set P is called a partial order relation or a partial ordering in P iff R is reflexive, antisymmetric, and transitive.

Defn: Chain: Let $\langle P, \leq \rangle$ be a partially ordered set. If for every $x, y \in P$, we have either $x \leq y \vee y \leq x$, then $\leq$ is called a simple ordering or linear ordering on P and $\langle P, \leq \rangle$ is called a totally ordered or simply ordered set or a chain.

Unit - 2

MATHEMATICAL LOGIC :-

Proposition:

A number of words making a complete geommentrical structure having a sense and meaning and also meant an assation in logic or mathematics is called a sentence.

A Proposition or statement is a declaration sentence that is either true or palse.

Compound Proposition:

A proposition consisting of only a single point propositional variable or a single propositional Constant is called an Atomic proposition.

A propositive obtained from the combination of two or more propositive by means of single proposition is refered to Molecular or compound Proposition.

Connectives:-

The words and phrase used to form compound proposition are called Connective.

Negation:

If p is any proposition, the negation of is denoted by ~p or ¬p and reads as not p is a proposition which is false when p is true and true when p is false.

Conjuction:

If p and q are two statement then conjuction of p and q is the compound statement denoted by $p \wedge q$ and reads as q" The component statement $p \wedge q$ is true when both p and q are true otherwise it is false.

Disjuction:

If p and q are two statement the disjuction of p and q is the compound statement denoted by $p \vee q$ and read as p' (or) q'. The statement $p \vee q$ is true if atleast one of p (or) q is true, It is false when both p and q are false.

Proposition and Truth Table:-

The truth table for a proposition is either true or false is denoted by T (or) F.

A Truth table is a table that shows the truth value of the compound proposition of all possible cases.

1. Consider the conjuction of two proposition p and q compound statement p and q and either $p \vee q$ (or) $\sim q$ (or) $\sim p \vee q$ (or) $\sim p \wedge q$.

Soln:

Let p and q be two proposition.

The Truth table for $P \vee q$ is

P	q	$P \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

The Truth table for $P \wedge q$ is

P	q	$P \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

The Truth table for $\sim P \vee q$

P	q	$\sim P$	$\sim P \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Logical Equivalence:

If two proposition P and q have the same truth in every possible case: the propositions are called logically equivalent (or) simply equivalent.

To test whether two proposition p and q are logically equivalent the following steps are followed.

* constructed the truth table for p
* construct the truth table for q
* check each combinations of truth values of the proposition is equivalent.

2. using the truth table show that $\sim(p \wedge q) = (\sim p) \vee (\sim q)$

Soln:

(i) Construct the truth table $P = \sim(p \wedge q)$

p	q	$p \wedge q$	$\sim(p \wedge q)$
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

(ii) construct the truth table $Q = (\sim p) \vee (\sim q)$

p	q	$\sim p$	$\sim q$	$(\sim p) \vee (\sim q)$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

$\therefore \sim(p \wedge q) = (\sim p) \vee (\sim q).$

Algebra of Proposition:

Proposition satisfies various laws are listed in the following table which are useful to simplify the expression and all the law of the table occurs in pairs are called dual pairs.

3. using the Proposition and Truth table show that $P \wedge (q \vee q)$

Soln:

P	q	$q \vee q$	$P \wedge (q \vee q)$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	F	F

4. using the proposition and truth table show that $\sim(p \vee q) \vee (\sim p \wedge \sim q)$

p	q	$\sim p$	$\sim q$	$p \vee q$	$\sim(p \vee q)$	$\sim(p \wedge \sim q)$	$\sim(p \vee q) \vee (\sim p \wedge \sim q)$
T	T	F	F	T	F	F	F
T	F	F	T	T	F	F	F
F	T	T	F	T	F	F	F
F	F	T	T	F	T	T	T

5. using the truth table show that

$\sim(p \vee q) = \sim p \wedge \sim q$

soln:

(i) construct the truth table for $P = \sim(p \vee q)$

p	q	$p \vee q$	$\sim(p \vee q)$
T	T	T	F
T	F	T	F
F	T	T	F
F	F	F	T

(ii) construct the truth table for $Q = \sim p \wedge \sim q$

p	q	$\sim p$	$\sim q$	$(\sim p) \wedge (\sim q)$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Conditional statements:

If P and Q are two statement. Then the statement P implies Q read as "If P then. Q" is called a conditional statement. If the statement $P \to Q$ has a truth value F when Q has the truth value F and P the truth value T. otherwise has the truth table T.

Truth Table :

P	Q	P → Q
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional statement :

If P and Q are two statement then the statement $P \rightleftarrows Q$ is called a Biconditional statement

$$P \rightleftarrows Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$$

Truth Table :

$P \rightleftarrows Q$	P	Q	$P \to Q$	$Q \to P$	$(P \to Q) \wedge (Q \to P)$
T	T	T	T	T	T
F	T	F	F	T	F
F	F	T	T	F	F
T	F	F	T	T	T

Tautology :

A statement formula which is true for all the truth values in the final column is called to as a tautology.

8

6. verify whether $(P \vee Q) \rightarrow P$ is a Tautology.

Soln:

P	Q	$P \vee Q$	$P \vee Q \rightarrow P$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	T

contain a false value hence $(P \vee Q) \rightarrow P$ is not a Tautology.

7. Prove that $(P \rightarrow R) \wedge (Q \rightarrow R) \rightarrow (P \vee Q) \rightarrow R$ is Tautology.

P	Q	R	$P \rightarrow R$	$Q \rightarrow R$	$(P \rightarrow R) \wedge (Q \rightarrow R)$	$P \vee Q$	$P \vee Q \rightarrow R$	$(P \rightarrow R) \wedge (Q \rightarrow R) \rightarrow P \vee Q$
T	T	T	T	T	T	T	T	T
T	T	F	F	F	F	T	F	T
T	F	T	T	T	T	T	T	T
T	F	F	F	T	F	T	F	T
F	T	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T	T
F	F	T	T	T	T	F	T	T
F	F	F	T	T	T	F	T	T

(9)

8. Prove that $((P \to Q) \wedge (R \to S)) \wedge ((P \vee R) \to (Q \vee S))$

P	Q	R	S	$P \to Q$	$R \to S$	$P \vee R$	$P \to Q \wedge R \to S$ $P \vee R$	$Q \vee S$	$((P \to Q) \wedge (R \to S)) \wedge [(P \vee R)\ (Q \vee S)]$
T	T	T	T	T	T	T	T	T	T
T	T	T	F	T	F	T	F	T	T
T	T	F	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T	T	T
T	F	T	T	F	T	T	F	T	T
T	F	T	F	F	F	T	F	F	T
T	F	F	T	F	T	T	F	T	T
T	F	F	F	F	T	T	F	F	T
F	T	T	T	T	T	T	T	T	T
F	T	T	F	T	F	T	F	T	T
F	T	F	T	T	T	F	F	T	T
F	T	F	F	T	T	F	F	T	T
F	F	T	T	T	T	T	T	T	T
F	F	T	F	T	F	T	F	F	T
F	F	F	T	T	T	F	F	T	T
F	F	F	F	T	T	F	F	F	T

9. Prove that $((P \to (Q \vee R)) \wedge (\neg Q)) \to (P \to R)$ is a Tautology.

P	Q	R	$Q \vee R$	$P \to (Q \vee R)$	$\sim Q$	$P \to (Q \vee R) \wedge (\sim Q)$	$P \to R$	$P \to (Q \vee R) \wedge \neg Q \to R$
T	T	T	T	T	F	F	T	T
T	T	F	T	T	F	F	F	T
T	F	T	T	T	T	T	T	T
T	F	F	F	F	T	F	F	T
F	T	T	T	T	F	F	T	T
F	T	F	T	T	F	F	T	T
F	F	T	T	T	T	T	T	T
F	F	F	F	T	T	T	T	T

Distributive law:-

~~Use this~~

The truth table which satisfies the following condition is a distributive law.

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee q)$$

Proof:

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

Condition Proposition:

(i) calculate Truth table for

(i) $p \vee \sim q \Rightarrow p$ (ii) $((\sim(p \wedge q) \vee r) \Rightarrow \sim p)$

Soln:

The truth Table of the given compound statement is shown below.

p	q	r	$(p \wedge q)$	$\sim(p \wedge q)$	$\sim(p \wedge q) \vee r$	$\sim p$	$(\sim(p \wedge q) \vee r) \Rightarrow \sim p$
T	T	T	T	F	T	F	F
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	F
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	T
F	T	F	F	T	T	T	T
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

Replacement Process:

Consider the formula $A: P \to (Q \to R)$. The formula $Q \to R$ is a part of the formula A. If we replace $Q \to R$ by an equivalent formula $\neg Q \vee R$ in A. We get the formula $B: P \to (\neg Q \vee R)$ One can easily verify other this process of obtaining B from A is known as the replacement process.

12

Equivalent Formula:-

$P \vee P \Leftrightarrow P$ $\quad$ $P \wedge P \Leftrightarrow P$ $\quad$ Idempotent Law

$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ $(P \wedge Q) \wedge P \Leftrightarrow (P \wedge (Q \wedge R))$ $\quad$ Associative Law

$P \vee Q \Leftrightarrow Q \vee P$ $\quad$ $P \wedge Q \Leftrightarrow Q \wedge P$ $\quad$ Commutative law

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

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

$P \vee R \Leftrightarrow P$ $\quad$ $P \wedge T \Leftrightarrow P$

$P \vee T, F \Leftrightarrow T$ $\quad$ $P \wedge T, F \Leftrightarrow F$ $\quad$ Absorption law

$P \vee \neg P \Leftrightarrow T$ $\quad$ $P \wedge \neg P \Leftrightarrow F$

$P \vee (P \wedge Q) \Leftrightarrow P$ $\quad$ $P \wedge (P \vee Q) \Leftrightarrow P$

$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ $\quad$ De-Morgan's Law.

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

(i) $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$

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

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

$\Leftrightarrow (\neg P \vee \neg Q) \vee R$ (Associative law)

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

$\Leftrightarrow (P \wedge Q) \to R$

(ii) P.T $(P \to Q) \wedge (R \to Q) \Leftrightarrow (P \vee R) \to Q$

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

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

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

$\Leftrightarrow (P \vee R) \to Q$

(iii) Prove that $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge P) \vee (P \wedge Q) \Leftrightarrow R$ 13

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

$\Leftrightarrow ((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$ (Asso & Distributive law)

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

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

$\Leftrightarrow T \wedge R$

$\Leftrightarrow R$ as $T \wedge R \rightarrow R$

(iv) P.T $P \rightarrow (Q \rightarrow P) \Leftrightarrow \neg P \rightarrow (P \rightarrow Q)$

$P \rightarrow (Q \rightarrow P) \Leftrightarrow \neg P \vee (Q \rightarrow P)$

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

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

$\Leftrightarrow T \vee (\neg Q)$

$\Leftrightarrow T$

$\neg P \rightarrow (P \rightarrow Q) \Leftrightarrow \neg(\neg P) \vee (P \rightarrow Q)$

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

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

$\Leftrightarrow T \vee Q$

$\Leftrightarrow T$

So $P \rightarrow (Q \rightarrow P) \Leftrightarrow T \Leftrightarrow \neg P \rightarrow (P \rightarrow Q)$

(v) P.T $(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q$

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

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

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

$\Leftrightarrow (P \vee R) \rightarrow Q$

14

(vi) a) $\neg(P \rightleftarrows Q) \Leftrightarrow (P \vee Q) \wedge \neg(P \wedge Q)$

b) $\neg(P \rightleftarrows Q) \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q)$

a) $\neg(P \rightleftarrows Q) \Leftrightarrow \neg((P \to Q) \wedge (Q \to P))$

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

$\Leftrightarrow \neg[((\neg P \vee Q) \wedge \neg Q) \vee ((\neg P \vee Q) \wedge P)]$

$\Leftrightarrow \neg[(\neg P \wedge Q) \vee (Q \wedge \neg Q) \vee (\neg P \wedge P) \vee (Q \wedge P)]$

$\Leftrightarrow \neg[\neg(P \vee Q) \vee F \vee F \vee (Q \wedge P)]$

$\Leftrightarrow \neg[\neg(P \vee Q) \vee (Q \wedge P)]$

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

b) $\neg(P \rightleftarrows Q) \Leftrightarrow (P \vee Q) \wedge (\neg P \vee \neg Q)$

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

$\Leftrightarrow [(P \wedge \neg P) \vee (P \wedge \neg Q)] \vee [(Q \wedge \neg P) \vee (Q \wedge \neg Q)]$

$\Leftrightarrow F \vee (P \wedge \neg Q) \vee [Q \wedge \neg P] \vee F$ (Ass Law)

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

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

(vii) Show that $[(P \vee Q) \wedge \neg(\neg P \vee (\neg Q \vee \neg R))] \vee (\neg P \wedge \neg Q)$ $\vee (\neg P \wedge \neg R)]$ is a Tautology.

By Demorgan's law we've

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

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

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

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

Also,

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

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

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

$[[(P \vee Q) \wedge (P \vee Q) \wedge (P \vee R)] \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

consequently then given formula is equivalent to $((P \vee Q) \wedge (P \wedge R) \rightarrow \neg((P \vee Q) \wedge (P \vee R))$

which is a substitution instance of $P \vee \neg P$

Normal Forms:

A better method is to transform the statement formulas A and B to same standards from A' and B' ∋. a simple comparison of A' and B' shows whether $A \Leftrightarrow B$. The standard forms are called canonical forms or normal forms.

Elementary product:

A product of variables and their negotations is called an Elementary products.

Elementary sum:

The sum of statement variables and their negotions is called elementary sum.

Disjunctive normal Forms:

A formula which is equivalent to a given formula and which consists of a sum of elementary products is called a disjunctive normal forms of the given formula.

Conjuctive normal Forms:

A formula which is equivalent to a given formula and which consists of a product of elementary sums is called a conjuctive normal forms of the given formula.

Principle Disjunctive normal Form:

A minimum term consists of Conjuction in which each statement variable or its negation but not both appears only ones.

Principle conjuctive normal Form:

A maximum term consist of disjunction in which each variable or its negotation but not both appear by only once

If P and Q are two variable then the maximum term are given by $P \vee Q$, $P \vee \neg Q$, $\neg P \vee Q$, $\neg P \vee \neg Q$.

An equivalent formula consists of conjuctions of maximum term only is known as Principle conjuctive normal Form.

1. obtain DNF, $P \to [(P \to Q) \wedge (\neg(\neg Q \vee \neg P))]$ without using Truth Table.

Soln:

$$P \to [(P \to Q) \wedge \neg(\neg Q \vee \neg P)] \Leftrightarrow \neg P \vee [(P \to Q) \wedge \neg(\neg Q \vee \neg P)]$$

$$\Leftrightarrow \neg P \vee [(\neg P \vee Q) \wedge (Q \wedge P)]$$

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

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

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

$$\Leftrightarrow \neg P \vee F \vee Q \wedge P$$

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

2. Obtain the CNF for the following without using Truth table

(i) $\neg(P \vee Q) \rightleftarrows (P \wedge Q)$

(ii) $[Q \vee (P \wedge R)] \wedge \neg[(P \wedge R) \wedge Q]$

Soln:

(i) $\neg(P \vee Q) \rightleftarrows (P \wedge Q)$

$\Leftrightarrow [\neg(P \vee Q) \rightarrow (P \wedge Q)] \wedge [(P \wedge Q) \rightarrow \neg(P \vee Q)]$

$\Leftrightarrow \neg[\neg(P \vee Q) \vee (P \wedge Q)] \wedge [\neg(P \wedge Q) \vee \neg(P \vee Q)]$

$\Leftrightarrow [(P \vee Q) \vee (P \wedge Q)] \wedge [\neg P \vee \neg Q] \vee (P \wedge \neg Q)$

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

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

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

(ii) $[Q \vee (P \wedge R)] \wedge \neg[(P \vee R) \wedge Q]$

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

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

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

3. Obtain the PDNF for $P \rightarrow [(P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P)]$ without using Truth Table.

Soln:

$\Leftrightarrow \neg P \vee [(P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P)]$

$\Leftrightarrow \neg P \vee [(\neg P \vee Q) \wedge (Q \wedge P)]$

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

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

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

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

1. obtain PCNF for $(\neg P \to R) \wedge (Q \rightleftharpoons R)$ without using Truth Table. 18

Soln:

$[\neg(\neg P) \vee R] \wedge [(Q \to P) \wedge (P \to Q)]$

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

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

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

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

Theory of Inference:

If a conclusion is derived from a set of premises by using certain rules then the process of derivation is called deduction and the Argument and the conclusion is said to be valid Argument and valid conclusion.

Valid conclusion:

Let A and B be two statement formula we say that "B logically follows from A" (or) " B is a valid conclusion " if $A \to B$ is a tautology.

Valid Argument:

we say that a set of permises $\{H_1, H_2, \ldots, H_n\}$ is a valid argument for a valid conclusion if $H_1 \wedge H_2 \wedge \ldots \wedge H_n \to C$ is a Tautology.

1. Determine whether conclusion c follows logically from the hypothesis H_1 and H_2.

(i) $H_1 : P \to Q$, $H_2 : P$, $C = Q$

(ii) $H_1 : P \to Q$, $H_2 : \neg P$; $C = Q$

(iii) $H_1 : \neg Q$, $H_2 : P \to Q$; $C = \neg P$.

Soln:

(i) $H_1 : P \to Q$; $H_2 : P$; $C = Q$

To prove : $H_1 \wedge H_2 \to C$

P	Q	$P \to Q$ H_1	$(P \to Q) \wedge P$ $H_1 \wedge H_2$	$[(P \to Q) \wedge P] \to Q$ $(H_1 \wedge H_2) \to C$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

The given conclusion follows logically from H_1 and H_2.

(ii) $H_1 : P \to Q$; $H_2 : \neg P$; $C = Q$

To prove : $H_1 \wedge H_2 \to C$

P	Q	$P \to Q$	$\neg P$	$(P \to Q) \wedge \neg P$	$[(P \to Q) \wedge \neg P] \to C$
T	T	T	F	F	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	F

(iii) $H_1 : \neg Q$; $H_2 : P \to Q$; $C = \neg P$

To prove : $H_1 \wedge H_2 \to C$

P	Q	$\neg P$	$\neg Q$	$P \to Q$	$\neg P \wedge (P \to Q)$	$\neg P \wedge (P \to Q) \to \neg P$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

The given conclusion follows logically from H_1 and H_2.

2. Demonstrate that S is a valid inference from the premises $P \to \neg Q$, $Q \vee R$, $\neg S \to P$, $\neg R$

Soln:

S.NO	Premises	Rules
1.	$Q \vee R$	Rule P
2	$\neg R$	Rule P
3 (1,2)	Q	Rule T, I_{10}
4.	$P \to \neg Q$	Rule P
5. (3,4)	$\neg P$	Rule T, I_{12}
6.	$\neg S \to P$	Rule P
7. (5,6)	S	Rule T, I_{12}

3. Derive $P \to (Q \to S)$ without using truth table form $P \to (Q \to R)$, $Q \to (R \to S)$

Soln:

S.NO	Premises	Rules
1.	$P \to (Q \to R)$	Rule P
2.	P	Assumed premise
3. (1,2)	$Q \to R$	Rule T, I_{11}
4.	$\neg Q \vee R$	Rule T, E_{16}
5.	$Q \to (R \to S)$	Rule P
6.	$\neg Q \vee (R \to S)$	Rule T, E_{16}
7. (4,6)	$\neg Q \vee (R \vee R \to S)$	Rule T, dist, law
8.	$\neg Q \vee S$	Rule T
9.	$Q \to S$	Rule T
10. (2,9)	$P \to (Q \to S)$	Rule CP

Predicate calculus:-

The logic derived based upon the predicate is ~~so~~ said to be predicate calculus.

Eg:
The statement "x is a student" has two parts. The first part x is a subject and the second part student is a predicate.

If we remove the predicate by P. Then "x is a student" is written as P(x).

Quantifiers:-

Certain statements involve words that indicates quantity such as "all", "some", "none" (or) "one". They answer the question "How many". Since such words indicate quantity they are called qualifiers.

Eg:
(i) Some men are tall
(ii) All birds have wings.

Universal Quantifier:-

The quantifier "all" is the universal quantifier. It is denoted by a symbol $(\forall x)$. This symbol represents the following phrases.

(i) for all x
(ii) for every x
(iii) for each x
(iv) Everything x is such that

Essential Quantifier:

The Quantifier "Some" is an essential quantifier. It is denoted by $(\exists x)$. This symbol represents the following phrases.

(i) for some x

(ii) Some x such that

(iii) There exist an x such that.

1. Write the following statements in symbols form

(i) Something is good.

(ii) Everything is good

(iii) nothing is good

(iv) Something is not good.

Soln:

(i) Something is good implies that there is atleast $x \ni: x$ is good.

It is denoted by $(\exists x)(G(x))$

(ii) Everything is good implies for all x, x is good.

It is denoted by $(\forall x)\ G(x)$

(iii) nothing is good ~~implies~~ that for all x, x is not good.

It is denoted by $(\forall x)(\neg G(x))$.

(iv) Something is not good implies that "there is atleast one $x \ni: x$ is not good".

It is denoted as $(\exists(x))(\neg G(x))$.

2. Write the following statements in symbols form. 2

(i) All monkeys have tails

(ii) No monkeys has a tail

(iii) Some monkeys have tail

(iv) Some monkey have no tail.

Soln:

Let x is a monkey $M(x)$

x has tails $T(x)$

(i) All monkeys have tails for all x, if x is a monkey then it has tail

It is denoted by $(\forall x)(M(x) \rightarrow T(x))$

(ii) No monkey has a tail for all x, if x is monkey it does not have a tail.

It is denoted by $(\forall x)(M(x)) \rightarrow \neg T(M)$

(iii) Some monkey have tail such that x, if $(\exists x)(M(x) \rightarrow T(x))$

(iv) Some monkey have no tail. Such that for x, if $\exists x\,(M(x) \rightarrow \neg(T(x))$

3. Write the following statements in symbol form

(i) All men are good

(ii) No men are good

(iii) Some men are good

(iv) Some men are not good.

Soln:

(i) All men are good, $\forall x$ if x is a man then he is good.

It is denoted by $(\forall x)(M(x) \rightarrow G(x))$

(ii) No men are good $\Rightarrow \forall x$, if x is a man then he is not good.

It is denoted as $(\forall x)(M(x) \rightarrow \neg G(x))$

(iii) Some men are good $\Rightarrow \exists x$, if x is a man then he is good

It is denoted as $(\exists x)(M(x) \rightarrow G(x))$

(iv) Some men are not good $\Rightarrow \exists x$, if x is a man then he is not good.

It is denoted as $(\exists x)(M(x) \rightarrow \sim G(x))$

Theory of Inference: (Predicate calculus)

The eliminate of quantifiers can be done by rules of specification called US and ES.

To predict correct quantifiers we need the rules of generalization is called UG and EG.

Rule US: universal specification:

If a statement is of the form $(\forall x)$ $P(S)$ is true then the universal quantifier can be dropped to obtain $P(t)\ \forall t$.

In symbol: $\dfrac{\forall(x)\ P(x)}{P(t)\ \forall t}$

Rule UG: universal Generalization:

If the statement is of the form $P(t)\ \forall t$, then the ~~statement is of~~ the form universal quantifiers may be introduced to obtain for all x, $\forall x (p(x))$

In symbol : $\dfrac{p(t) \text{ for all } t}{\forall (x)\ p(x)}$

Rule ES : Existential specification:

If $(\exists x) P(x)$ is assumed to be true then there is an t is the universal specifi $\exists$ $p(t)$ is true.

In symbol $\dfrac{(\exists x)\ P(x)}{P(t) \text{ for some } t}$

1. verify the validity of the following Argument,
   (i) Every Living thing is a plant or an animal.
   John's gold fish is alive and it is not a plant.
   All animals have hearts.
   Therefore John's gold fish has a heart.

Soln:

Let $P(x) = x$ is a plant

$A(x) = x$ is an animal

g - John's gold fish

$H(x) = x$ have hearts.

It is an Existential generalisation.

If $p(t)$ is true for some element t in the universe then $(\exists x)$, $P(x)$ is true.

In symbol: $\dfrac{P(t) \text{ for some } t}{(\exists x)(P(x))}$

Then the Inference pattern is

(i) $\forall x \ (P(x) \vee A(x))$

(ii) $\neg P(x)$

(iii) $(\forall x)(A(x) \rightarrow H(x))$

S.NO	Premises	Rules
1.	$(\forall x)(P(x) \vee A(x))$	Rule P
2.	$P(g) \vee A(g)$	Rule T, Rule US
3.	$\neg P(g)$	Rule P
		$P(g) \vee A(g)$, $\neg (P(g)) \to A(g)$
4. (2,3)	$A(g)$	Rule T, I_{10}
		$I_{10} = \neg P\ (P \vee Q) = Q$
5.	$(\forall x)(A(x) \to H(x))$	Rule P
6.	$A(g) \to H(g)$	Rule T, Rule US.
7. (4,6)	$H(g)$	Rule T, I_{11}

Thus this conclusion is valid $A(g)$,

$$A(g) \to H(g) = H(g)$$

2. Prove that $(\forall x)(P(x) \to Q(x))$.
$(\forall(x))\ R(x) \to \neg Q(x) \Rightarrow \forall(x)(R(x) \to \neg P(x))$.

Soln:

S.NO	Premises	Rules
1.	$\forall x (P(x) \to Q(x))$	Rule P.
2.	$P(b) \to Q(b)$	Rule T, Rule US.
3.	$\forall x (R(x) \to \neg Q(x))$	Rule P
4.	$R(b) \to \neg Q(b)$	Rule T, Rule US.
5.	$R(b)$	Assumed premises
6.	$\neg Q(b)$	Rule T, I_6
7. (2,6)	$\neg P(b)$	I_{12} Rule T
8. (5,7)	$R(b) \to \neg P(b)$	Rule CD
9. $\forall$	$\forall x, R(x) \to \neg P(x)$	Rule T, Rule UG

3. Find whether the following arguments are valid or not.

All integers are rationals number.

Some integer are power of 3.

Some Rational number are power of 3.

Soln:

$I(x)$: x is an integer

$R(x)$: x is a Rational number

$P(x)$: x is a power

(i) $(\forall x)\ I(x) \rightarrow R(x)$

(ii) $(\exists x)\ (I(x) \wedge P(x))$

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

S.NO	Premises	Rules
1.	$\forall x\ I(x) \rightarrow R(x)$	Rule P
2.	$I(b) \rightarrow R(b)$	Rule T, Rule US
3.	$\exists(x)(I(x) \wedge P(x))$	Rule P
4.	$I(b) \wedge P(b)$	Rule T, Rule ES
5. (4)	$I(b)$	Rule T
6. (2,5)	$R(b)$	Rule T, I_4
7. (4)	$P(b)$	Rule T
8. (6,7)	$R(b) \wedge P(b)$	Rule T
9.	$\exists(x)(R(x) \wedge P(x))$	Rule ES, Rule T.

29

Implications:

I_1 $P \wedge Q \Rightarrow P$
I_2 $P \wedge Q \Rightarrow Q$ } Simplification

I_3 $P \Rightarrow P \vee Q$
I_4 $Q \Rightarrow P \vee Q$ } Addition

I_5 $\sim P \Rightarrow P \rightarrow Q$

I_6 $Q \Rightarrow P \rightarrow Q$

I_7 $\sim (P \rightarrow Q) \Rightarrow P$

I_8 $\sim (P \rightarrow Q) \Rightarrow \sim Q$

I_9 $P, Q \rightarrow P \wedge Q$

I_{10} $\sim P, P \vee Q \Rightarrow Q$ (DIS Function)

I_{11} $P, P \rightarrow Q \Rightarrow Q$

I_{12} $\sim Q \; P \rightarrow Q \Rightarrow \sim P$

I_{13} $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$

I_{14} $P \vee Q, P \rightarrow R, Q, R \Rightarrow R$

Equivalence;

E_1. $\sim\sim P \Leftrightarrow P$ (double negation)

E_2 $P \wedge Q \Leftrightarrow Q \wedge P$
E_3 $P \vee Q \Leftrightarrow Q \vee P$ } commutative laws

E_4 $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
E_5 $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ } Associative Laws

E_6 $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
E_7 $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ } Distributive Law

E_8 $\sim(P\wedge Q) \Leftrightarrow \sim P\vee\sim Q$ } De Morgan's laws

E_9 $\sim(P\vee Q) \Leftrightarrow \sim P\wedge\sim Q$ }

E_{10} $P\vee P \Leftrightarrow P$

E_{11} $P\wedge P \Leftrightarrow P$

E_{12} $R\vee(P\wedge\sim P) \Leftrightarrow R$

E_{13} $R\wedge(P\vee\sim P) \Leftrightarrow R$

E_{14} $R\vee(P\vee\sim P) \Leftrightarrow T$

E_{15} $R\wedge(P\wedge\sim P) \Leftrightarrow F$

E_{16} $P\rightarrow Q \Leftrightarrow \sim P\vee Q$

E_{17} $\sim(P\rightarrow Q) \Leftrightarrow P\wedge\sim Q$

E_{18} $P\rightarrow Q \Leftrightarrow \sim Q\rightarrow\sim P$

E_{19} $P\rightarrow(Q\rightarrow R) \Leftrightarrow (P\wedge Q)\rightarrow R$

E_{20} $\sim(P\rightleftarrows Q) \Leftrightarrow P\rightleftarrows\sim Q$

E_{21} $P\rightleftarrows Q \Leftrightarrow (P\rightarrow Q)\wedge(Q\rightarrow P)$

E_{22} $P\rightleftarrows Q \Leftrightarrow (P\wedge Q)\vee(\sim P\wedge\sim Q)$

Statement Involving more than one Quantifies:-

If a predicate formulae involves more than one different variable, then more than one quantifies is needed to produce a closed sentence (symbolic sentence).

1. Write the following statement in the symbolic form "Every one who likes fun will enjoy each of these plays.

Soln:

$L(x)$: x likes fun

$P(x)$: x is a play

(13)

$E(x,y)$: x will enjoy y

The statement can be represented as "For each x, if x likes fun and for each y, if y is a play then x enjoys y". in symbolic form

$(\forall x)(\forall y)\left[L(x) \wedge P(y) \rightarrow E(x,y)\right]$

2. Write the symbolic form and negotiate the following statements.

(a) Every one who is healthy can also do all kinds of work

(b) Some people are not admired by everyone

(c) Every one should help his neighbours or his neighbours will not help him.

Soln:

a) The given statement is

"Everyone who is healthy can do all kinds of work".

Let $H(x)$: x is a health person

$W(y)$: y is a kind of work

$D(x,y)$: x can do y.

The statement is

"For all x if x is healthy and for all y, if y is a kind of work, then x can do y".

So a symbolic form is

$(\forall x)(\forall y)\left[H(x) \wedge H(y) \rightarrow D(x,y)\right]$

Its negation is given by

T/V.

$\neg(\forall x)(\forall y)[H(x) \wedge H(y) \rightarrow D(x,y)]$

i.e., $(\exists x)\,\neg(\forall y)[H(x) \wedge H(y) \rightarrow D(x,y)]$

i.e., $(\exists x)(\neg y)[\neg(H(x) \wedge H(y) \rightarrow D(x,y))]$

i.e., $(\exists x)(\exists y)[H(x) \wedge H(y) \wedge \neg D(x,y)]$

i.e., There exist a healthy person and there exist a kind of work such that x cannot do y.

i.e., There is some healthy person who cannot do some kind of work.

b) In the universe of people, let $A(x,y)$: x admires y. Then the given statement is "there is a person who is not admired by some person".

So it is $(\exists y)(\exists x)(\neg A(x,y))$.

Its negation is $\neg\exists y(\exists x)(\neg A(x,y))$

i.e., $(\forall y)\neg(\forall x(\forall (x,y)))$

$\Rightarrow$ Every person is admired by everyone

In the universe, which consists of everything.

Let $P(x)$: x is a person and

$A(x,y)$: x admires y.

Then the given statement is

$(\exists y)(\exists x)(P(x) \wedge P(y)) \rightarrow \neg A(x,y)$

Its negation is

$(\forall y)(\forall x)(A(x,y) \wedge P(x) \wedge P(y))$.

c) In the universe of people. Let

$N(x,y)$: x and y are neighbours

$H(x,y)$: x should help y.

32

$P(x,y)$: x will help y.

The given statement is

For every person x and every person y. If x and y are neighbours, then either x should help y or y will not help x.

So the symbolic form is,

$(\forall x)(\forall y)(N(x,y) \rightarrow (H(x,y) \vee \neg P(y,x)))$

Its negation is

$\neg(\forall x)(\forall y)(N(x,y)) \rightarrow (H(x,y) \vee \neg P(y,x)))$

i.e., $(\exists x)\neg(\forall y)(\neg N(x,y)) \vee H(x,y) \vee \neg P(y,x))$

i.e., $(\exists x)(\exists y)(\neg(N(x,y)) \vee H(x,y) \vee \neg P(y,x))$

i.e., $(\exists x)(\exists y)(N(x,y)) \wedge \neg H(x,y) \wedge P(y,x))$

There are some people who should not help their neighbours but this neighbours will help them.

3. verify the validity of the following Inference. If one person is more successful than another, then he ask worked harder to success. vishu has not worked harder than Anjala. Therefore vishu is not more successful than Anjala.

Soln:

Let the universe consists of all persons

Let $S(x,y)$: x is more successful than y.

$W(x,y)$: x has worked harder than y to deserve success.

a : vishu

b : Anjala

(34)

Then the inference pattern is

$$(\forall x)(\forall y)[S(x,y) \rightarrow W(x,y)]$$

$$\frac{\neg W(a,b)}{\neg W(a,b)}$$

Argument:

1.	(1)	$\neg W(a,b)$	Rule P
2.	(2)	$(\forall x)(\forall y)[S(x,y) \rightarrow W(x,y)]$	Rule P
3.	(2)	$(\forall y)[S(a,y) \rightarrow W(a,y)]$	Rule US(2)
4.	(2)	$S(a,b) \rightarrow W(a,b)$	Rule US(3)
5.	(1,2)	$\neg S(a,b)$	Rule T, (1)(4)

Thus the inference is valid one.

Lattice.

Defn: Lattice: A lattice is a partially ordered set $\langle L, \le \rangle$ in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

Ex: 1. Let S be any set and $\rho(S)$ be its power set. The partially ordered set $\langle \rho(S), \subseteq \rangle$ is a lattice in which the meet and join are the same as the operations $\cap$ and $\cup$ respectively.

Note: S has a single element, the corresponding lattice is a chain containing two elements.

Ex: 2 Let n be a positive integer and S_n be the set of all divisors of n. For example, $n = 6$, $S_6 = \{1,2,3,6\}$, for $n = 24$ $S_{24} = \{1,2,3,4,6,8,12,24\}$. Let D denote the relation of "division", then $\langle S_6, D\rangle$, $\langle S_{24}, D\rangle$ are lattices.

Some properties of Lattices

We ~~shall first~~ list some of the properties of the two binary operations of meet and join denoted by $*$ and $\oplus$ on a lattice $\langle L, \le \rangle$. For any $a, b, c \in L$, we have

(L-1) $a * a = a$ (L-1)' $a \oplus a = a$ (Idempotent)

(L-2) $a * b = b * a$ (L-2)' $a \oplus b = b \oplus a$ (commutative)

(L-3) $(a * b) * c = a * (b * c)$ (L-3)' $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (Associative)

(L-4) $a * (a \oplus b) = a$ (L-4)' $a \oplus (a * b) = a$ (Absorption).

P.T $a * (a \oplus b) = a$.

proof: For any $a \in L$, $a \leq a$ and $a \leq a \oplus b$ by defn of $\oplus$.

Hence $a \leq a * (a \oplus b)$.

On the other hand $a * (a \oplus b) \leq a$ by the defn of $*$

Theorem: Let $\langle L, \leq \rangle$ be a lattice in which $*$ and $\oplus$ denote the operations of meet and Join respectively. For any $a, b \in L$,

$$a \leq b \iff a * b = a \iff a \oplus b = b.$$

proof: Now we prove that $a \leq b \iff a * b = a$.

We assume that $a \leq b$. and also know that $a \leq a$. $\therefore a \leq a * b$.

But from the defn of $a * b$, we have $a * b \leq a$

Hence $a \leq b \Rightarrow a * b = a$.

Next assume that $a * b = a$, but it is only possible if $a \leq b$, that is $a * b = a \Rightarrow a \leq b$.

Combinin these two results we get, $a \leq b \iff a * b = a$.

From $a * b = a$, we have

$$b \oplus (a * b) = b \oplus a = a \oplus b.$$

~~(by Absorption and~~ (by commutative)

but

$$b \oplus (a * b) = b \text{ (by Absorption)}.$$

Hence $a \oplus b = b$, follows from $a * b = a$.

Repeat the similar steps, we show that $a * b = a$ follows from $a \oplus b = b$.

Hence proved.

Theorem: Isotonicity property.

Let $\langle L, \leq \rangle$ be a lattice. For any $a, b, c \in L$, the following are hold.

$$b \leq c \Longrightarrow \begin{cases} a * b \leq a * c \\ a \oplus b \leq a \oplus c. \end{cases}$$

Proof: We know the theorem

$$a \leq b \Longleftrightarrow a * b = a \Longleftrightarrow a \oplus b = b.$$

From this theorem

$$b \leq c \Longleftrightarrow b * c = b.$$

To show $a * b \leq a * c$, we shall show that

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

Note that

$$(a * b) * (a * c) = (a * a) * (b * c) \quad \text{(by Associative and commutative)}$$

$$= a * (b * c) \quad \text{(by Idempotent)}$$

$$= a * b. \quad \text{(by Absorption)}.$$

By the similar manner we prove second result.

Theorem: Distributive Inequlities.

Let $\langle L, \leq \rangle$ be a lattice. For any $a, b, c \in L$, the following distributive inequalities hold.

$$a \oplus (b * c) \leq (a \oplus b) * (a \oplus c).$$

$$a * (b \oplus c) \leq (a * b) \oplus (a * c).$$

proof: By defn, $a \le a \oplus b$ and

$a \le a \oplus c$

$\Rightarrow a \le (a \oplus b) * (a \oplus c)$ — (1)

Again by defn: $b * c \le b \le a \oplus b$

and $b * c \le c \le a \oplus c$

$\Rightarrow b * c \le (a \oplus b) * (a \oplus c)$ — (2)

$\therefore$ from (1) & (2)

$a \oplus (b * c) \le (a \oplus b) * (a \oplus c)$

similarly, by the duality principle

$a * (b \oplus c) \geq (a * b) \oplus (a * c)$.

Theorem

Modualar inequality: Let $\langle L, \le \rangle$ be a ~~Theorem~~ lattice for any $a, b, c \in L$, the following hold

$a \le c \Longleftrightarrow a \oplus (b * c) \le (a \oplus b) * c$.

proof: $a \le c$ iff $a \oplus c = c$

by distributive ~~eq~~ inequality

$a \oplus (b * c) \le (a \oplus b) * (a * c) = (a \oplus b) * c$

$\therefore a \oplus (b * c) \le (a \oplus b) * c$.

Thus $a \le c \Rightarrow a \oplus (b * c) \le (a \oplus b) * c$.

Similarly the converse part can prove.

—

Lattice as Algebraic System

Defn: A lattice is algebric system $\langle L, *, \oplus \rangle$ with two binary operations $*$ and $\oplus$ on L which are (1) Commutative (2) Associative and (3) Absorption laws satisfied.

Sublattice: Let $\langle L, *, \oplus \rangle$ be a lattice and let $S \subseteq L$ be a subset of L. The Algebra $\langle S, *, \oplus \rangle$ is a sublattice of $\langle L, *, \oplus \rangle$ iff S is closed under operations $*$ and $\oplus$.

EX: The Divisors of any positive integer form a Lattice. For ~~any~~ example integer $n = 36$

$\langle S_{36}, D \rangle$ is a lattice.

$\langle S_{12}, D \rangle$ is a Sub lattice.

Direct product

Defn: Let $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ be two lattices. The algebraic system $\langle L \times S, \cdot, + \rangle$ in which the binary operations $+$ and $\cdot$ on $L \times S$ are such that for any $\langle a_1, b_1 \rangle$ and $\langle a_2, b_2 \rangle$ in $L \times S$

$$\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle = \langle a_1 * a_2, \; b_1 \wedge b_2 \rangle$$

$$\langle a_1, b_1 \rangle + \langle a_2, b_2 \rangle = \langle a_1 \oplus a_2; \; b_1 \vee b_2 \rangle$$

is called the direct product of the lattices ⑥
$\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$.

Lattice Homomorphism: Let $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ be two lattices. A mapping $g: L \rightarrow S$ is called a lattice homomorphism from the lattice $\langle L, *, \oplus \rangle$ to $\langle S, \wedge, \vee \rangle$ If for any $a, b \in L$,

$g(a * b) = g(a) \wedge g(b)$ and

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

Some Special Lattices.

Complete lattice A lattice is called complete if each of its nonempty subsets has a least upper bound and a greatest lowerbound.

Ex: Let S be any finite set. Then $\langle \wp(S) \subseteq \rangle$ is a complete lattice.

Note: Every finite lattice is a complete lattice.

Bounded Lattice:

A lattice L, which has both a least element denoted by '0' and a gratest element denoted by '1' is called a bounded lattice.

Example: For the lattice $\langle L, *, \oplus \rangle$ with $L = \{a_1, a_2, \ldots, a_n\}$

$$\underset{i=1}{\overset{n}{*}} a_i = 0 \quad \text{and} \quad \bigoplus_{i=1}^{n} a_i = 1$$

The bounds 0 and 1 of lattice ~~satisfies~~ $\langle L, *, \oplus, 0, 1 \rangle$ satisfy the following identities.

For any $a \in L$,

$$a + 0 = a \quad ; \quad a * 1 = a$$

$$a \oplus 1 = 1 \quad ; \quad a * 0 = 0.$$

obviously, 0 is the identity of the operation $\oplus$, and 1 is the identity of the operation $*$.

Complemented Lattice

A lattice $\langle \wp(S), \subseteq \rangle$ of the power set of any set S is isomorphic to the lattice $\langle L^n, \leq_n \rangle$ provided S has n elements. The meet and join operations on $\wp(S)$ are $\cap$ and $\cup$ respectively, while the bounds are ϕ and S. The lattice $\langle \wp(S), \subseteq \rangle$ is Complemented lattice in which the complement of any subset A of S is the set $S - A$.

Distributive lattice

A lattice $\langle L, *, \oplus \rangle$ is called a distributive lattice if for any $a, b, c \in L$,

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

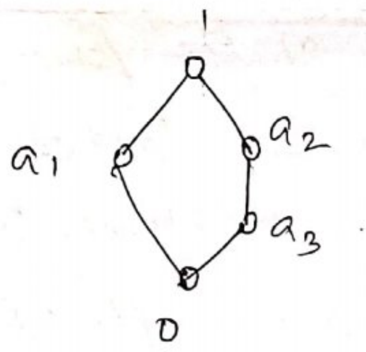
and $$a \oplus (b * c) = (a \oplus b) * (a \oplus c).$$

In otherwords, in a distributive lattice the operations $*$ and $\oplus$ distributtive over each other.

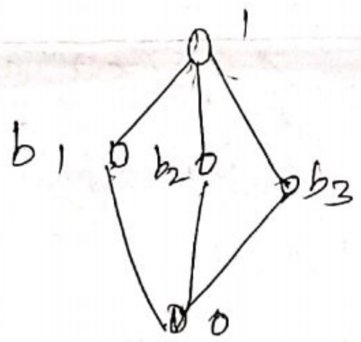
Example: Consider a set $A = \{a, b, c\}$

Then $\langle P(A), \cap, \cup \rangle$ is a distributive lattice with ~~0 and~~ $0 = \phi$ and $1 = A$.

Example: Show that the following lattices are not distributive.



(a)



(b).

Soln (a) $a_3 * (a_1 \oplus a_2) = a_3 * 1 = a_3 = (a_3 * a_1) \oplus (a_3 * a_2)$

$a_1 * (a_2 \oplus a_3) = 0 = (a_1 * a_2) \oplus (a_1 * a_3)$.

but $a_2 * (a_1 \oplus a_3) = a_2 * 1 = a_2$

$(a_2 * a_1) \oplus (a_2 * a_3) = 0 \oplus a_3 = a_3$.

Hence the lattice is not distributive.

(b) $b_1 * (b_2 \oplus b_3) = b$.

$(b_1 * b_2) \oplus (b_1 * b_3) = 0 \oplus = 0$.

$\Rightarrow$ The given lattice is not distributive.

<u>Theorem</u>: Every chain is a distributive lattice.

<u>proof</u>: Let $\langle L, \leq \rangle$ be a chain and let $a, b, c \in L$.

Consider the following possible case

(i) $a \leq b$ (or) and $a \leq c$ and

(ii) $a \geq b$ and $a \geq c$.

<u>case (i)</u> $a \leq b$ and $a \leq c$.

$\Longrightarrow a \leq b \oplus c$

$\therefore a * (b \oplus c) = a$.

Similarly $(a * b) \oplus (a * c) = a \oplus b = a$.

Thus $a * (b \oplus c) = (a * b) \oplus (a * c)$

<u>Case (ii)</u> $a \geq b$ and $a \geq c$.

$\Longrightarrow b \oplus c \leq a$.

$\therefore a * (b \oplus c) = b \oplus c$

Similarly $(a * b) \oplus (a * c) = b \oplus c$

Thus $a * (b \oplus c) = (a * b) \oplus (a * c)$.

By duality principle the other inequality holds.

Theorem: Let $\langle L, *, \oplus \rangle$ be a distributive lattice

(10)

for any $a, b, c \in L$,

if $(a*b) = (a*c)$ and $a \oplus b = a \oplus c$

then $b = c$.

proof:

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

$$= c \quad \text{(by absorption law)}. \quad \text{— (1)}$$

But

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

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

$$= b \oplus (a*c) \quad \text{(by associativity and commutative)}$$

$$= b \oplus (a*b)$$

$$= b \quad \text{(by absorption law)} \quad \text{— (2)}$$

$\therefore$ from (1) & (2) $b = c$.

(1)

Coding Theory

Any element of the alphabet will be called a letter (or) a character.

A finite sequence of characters of the alphabet is called a message or a word.

The length of a word denoted by l(x) for the word x, is the number of symbols in the word.

The encoding (or) enciphering process is a ~~problem~~ procedure for associating words from one language with given words of another ~~language~~ language in a one-to-one fashion.

The decoding (or) deciphering process is either the inverse operation (or) some other one-to-one mapping.

Examples of Codes

Morse code – used in telegraphy

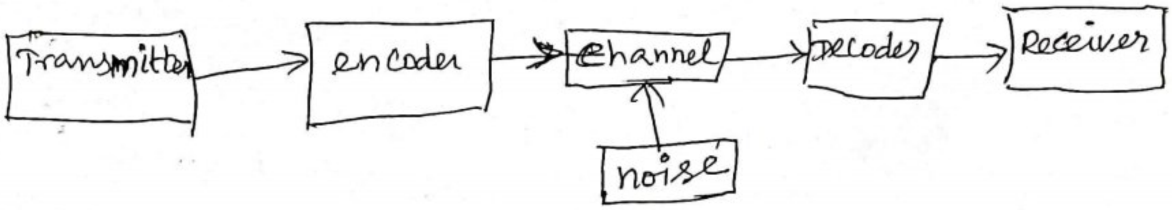
punch-card code – in the digital computer systems

ASCII (~~American~~ American Standard Code for Information Interchange) – used in digital computer systems

EBCDIC – (Extended Binary Coded Decimal Interchange Code) – used in digital computer systems.

General structure of a typical data Communication system with noise.

2



The communication channel is restricted to a binary value alphabet, whose signals may be designated by 0 and 1. Such a channel is called a binary channel.

Hamming codes were constructed by introducing redundant digits called ~~parity checks~~ parity digits.

In a message, n digits long the m digits (m<n) are used to represent the information part of the remaining k = n−m digits are used for the detection and correction of errors. The latter digits are called parity check

The information contents of the message is contained in the first n−1 digits of a code word and the last digit position is set to 0 or 1 so as to make the entire message contain an even number of 1's. Such as encoding procedure is called an even parity check. Alternatively, an odd parity check can be used. (3)

Example : The messages are 00, 01, 10, 11 becomes 000, 011, 101, 110 — single even-parity digit is added and become 001, 010, 100, 111 — in the case of an odd parity check.

Hamming distance:

Let $x = \langle x_1, x_2, \cdots x_n \rangle$ and $y = \langle y_1, y_2, \cdots y_n \rangle$ be n-tuples representing messages $x_1, x_2, \cdots x_n$ and $y_1 y_2 \cdots y_n$ respectively, where $x_i, y_i \in \{0, 1\}$ for all i.

The Hamming distance between x and y denoted by $H(x,y)$, is the number coordinates for which all x_i and y_i are different.

Clearly $H(x,y) = \sum_{i=1}^{n} (x_i \bar{\vee} y_i)$.

$\bar{\vee}$	0	1
0	0	1
1	1	0

(18)

Example: $x = \langle 1,1,1,0,1 \rangle$
$y = \langle 0,1,1,1,0 \rangle$

$H(x,y) = 3$

Properties of Hamming distance

$H(x,y) \geq 0$

$H(x,y) = 0 \iff x = y$

$H(x,y) = H(y,x)$

$H(x,y) + H(y,z) \geq H(x,z)$.

Minimum distance: The minimum distance of a code, whose words are n-tuples, is the minimum of the Hamming distances between all pairs of code words in that code.

Example: $x = \langle 1,0,0,1 \rangle$
$y = \langle 0,1,0,0 \rangle$
$z = \langle 1,0\,0\,0 \rangle$

$H(x,y) = 3$

$H(y,z) = 2$

$H(x,z) = 1$.

The minimum distance between these words is 1.

Theorem: A code can detect all combinations of k or fewer errors if and only if the minimum distance between any two code words is atleast k+1.

5

Proof: We are unable to detect a combination of errors if and only if that particular combination transforms a code word u into some code word v. with the minimum distance of atleast k+1, it would take a combination of atleast k+1 errors to change code word u into code word v. Hence, all combination of k or fewer errors can be detected.

Theorem: A code can correct all combinations of k or fewer errors if and only if the minimum distance between any two code word is atleast 2k+1.

Proof: We shall prove that if the code can correct all combinations of k or fewer errors, then the minimum distance between any two codes must be atleast 2k+1. Let us assume, to the contrary, that there is atleast one pair of words u and v such that $H(u, v) < 2k+1$. We may assume that $H(u, v) \geq k+1$; otherwise one cannot even detect k errors. Let us consider a word u' which differs from u in exactly k digits. The k digits are chosen to be any subset of those digits in which u and v differ from one another. This means $H(u, u') = k$. obviously, by our choice $H(u', v) \leq k$ because u and v only differ in at most 2k digits. Therefore

u' cannot be decoded with certainty, since code word v is atleast as close to u' as u is. Thus we have established a contradiction.

6

We shall now prove the converse of the theorem by assuming that the minimum code distance is $2k+1$ and from this assumption deducing that the code can correct all set of k errors. Let u be a code word and u' be a received erroneous record that has no more than k error digits. If a decoding rule correctly decodes u' as u, then we know that u' is nearer to the code word u than any other code word v. From the property of Hamming distance, we have

$$H(u,u') + H(u',v) \geq H(u,v)$$

Since $H(u,v) \geq 2k+1$ and $H(u,u') \leq k$, it then follows that $H(u',v) \geq k+1$. This implies that every code v is farther away from u' than u, and consequently u' can be correctly decoded.

Theorem: The minimum weight of the non-zero code words in a group code is equal to its minimum distance.

proof: Assume that code word x has the minimum weight of the code. We want to show that there exists two code words whose Hamming distance is this minimum weight. Since for any x, $x \oplus x = 0$, it follows that 0 is a code word using Hamming distance equation (7)

$H(x,y) = H(x \oplus y, 0) = W(x \oplus y)$,

we have $W(\gamma) = H(\gamma, 0)$ and therefore γ and 0 are the two required ~~cord~~ code words.

Conversely let x and y be code words such that $H(x,y)$ is equal to the minimum distance for the code. Since $\langle S_n, \oplus \rangle$ is a group, it follows because of ~~closure~~ closure that $x \oplus y = \gamma \in S_n$. Consequently, $W(x \oplus y) = W(\gamma) = H(x,y)$, and we have found a code word whose weight is equal to the minimum distance of the code.

Boolean Algebra:

A Boolean Algebra is a complemented distributive Lattice.

A Boolean Algebra will generally be denoted by $\langle B, *, \oplus, ', 0, 1 \rangle$ and it satisfies the following properties in which a, b and c denote any elements of the set B.

1. $\langle B, *, \oplus \rangle$ is a lattice in which the operations $*$ and $\oplus$ satisfies the following identities

(L-1) $a * a = a$, $a \oplus a = a$

(L-2) $a * b = b * a$, $a \oplus b = b \oplus a$.

(L-3) $(a * b) * c = a * (b * c)$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

(L-4) $a * (a \oplus b) = a$, $a \oplus (a * b) = a$.

2. $\langle B, *, \oplus \rangle$ is a distributive lattice and satisfies the following identities

(D-1) $a * (b \oplus c) = (a * b) \oplus (a * c)$.

(D-2) $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$

(D-3) $(a * b) \oplus (b * c) \oplus (c * a)$

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

(D-4) $a * b = a * c$ and $a \oplus b = a \oplus c$

$$\Longrightarrow b = c.$$

3. $\langle B, *, \oplus, 0, 1 \rangle$ is bounded lattice in which for any $a \in B$, the following identities hold.

(B-1) $0 \leq a \leq 1$.

(B-2) $a * 0 = 0$ (B-2)' $a \oplus 1 = 1$.

(B-3) $a * 1 = a$ (B-3)' $a \oplus 0 = a$.

4. $\langle B, *, \oplus, ', 0, 1 \rangle$ is uniquely Complemented lattice in which the complement of any element $a \in B$ is denoted by $a' \in B$ and satisfies the following identities

(C-1) $a * a' = 0$ (C-1)' $a \oplus a' = 1$

(C-2) $0' = 1$ (C-2)' $1' = 0$

(C-3) $(a * b)' = a' \oplus b'$ (C-3)' $(a \oplus b)' = a' * b'$

5. There exists partial ordering relation $\leq$ on B $\ni$

(P-1) $a * b = GLB\{a, b\}$ (P-1)' $a \oplus b = LUB\{a, b\}$

(p-2) $a \le b \iff a * b = a \iff a \oplus b = b$.

(p-3) $a \le b \iff a * b' = 0 \implies b' \le a' \iff a' \oplus b = 1$.

Example ① Let $B = \{0, 1\}$ be a set. The operations $*$, $\oplus$, $'$, on B are defined by

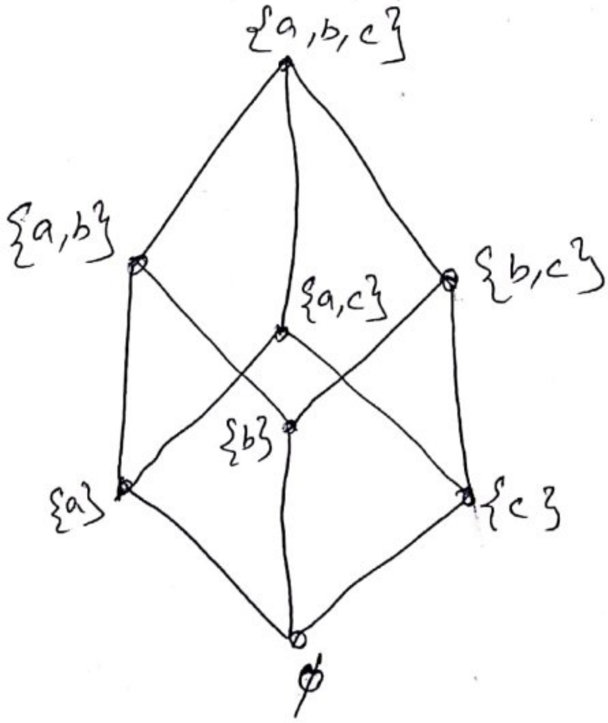
$*$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	1

x	x'
0	1
1	0

clearly $\langle B, *, \oplus, ', 0, 1 \rangle$ is Boolean Algebra.

Example ② Let $A = \{a, b, c\}$ and Consider the lattice $\langle \mathcal{P}(A), \cap, \cup \rangle$



clearly $\langle \mathcal{P}(A), \cap, \cup \rangle$ is a boolean Algebra.

Sub-Boolean Algebra:

Let $\langle B, *, \oplus, ', 0, 1 \rangle$ be a Boolean Algebra and $S \subseteq B$. If S is Contains the element 0 and 1 is Closed under the operation $*$, $\oplus$ and $'$ then $\langle S, *, \oplus, ', 0, 1 \rangle$ is called Sub-Boolean algebrab.

Note: A Sub-Boolean Algebra of a Boolean Algebra is it self a Boolean Algebra.

Direct product of Boolean Algebra:

Let $\langle B_1, *_1, \oplus_1, ', 0_1, 1_1 \rangle$ and $\langle B_2, *_2, \oplus_2, '', 0_2, 1_2 \rangle$ be two Boolean Algebras. The direct product of the two Boolean algebra is defined to be a Boolean algebra that is given by $\langle B_1 \times B_2, *_3, \oplus_3, ''', 0_3, 1_3 \rangle$ in which the operation are defined for any $(a_1, b_1), (a_2, b_2) \in B_1 \times B_2$ as

$$(a_1, b_1) *_3 (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2)$$

$$(a_1, b_1) \oplus_3 (a_2, b_2) = (a_1 \oplus_1 a_2, b_1 \oplus_2 b_2)$$

$$(a_1, b_1)''' = (a_1', b_1'')$$

$0_3 = (0_1, 0_2)$ and $1_3 = (1_1, 1_2)$

~~Examp~~ Boolean Homomorphism

Let $\langle B, *, \oplus, ', 0, 1 \rangle$ and $\langle P, \cap, \cup, -, \alpha, \beta \rangle$ be two Boolean Algebras. A mapping $f: B \longrightarrow P$ is is called Boolean homomorphism, if for any $a, b, \in B$,

$f(a * b) = f(a) \cap f(b)$.

$f(a \oplus b) = f(a) \cup f(b)$.

$f(a') = f(\overline{a})$

$f(0) = \alpha$ and $f(1) = \beta$

Boolean expressions

A Boolean expression in n variables $x_1, x_2 \ldots x_n$ is any finite string of Symbols formed in the following manner.

(i) 0 and 1 are Booleans expressions

(ii) $x_1, x_2, \ldots x_n$ are Boolean expressions.

(iii) If α_1 and α_2 are Boolean expressions then $(\alpha_1) * (\alpha_2)$ and $(\alpha_1) \oplus (\alpha_2)$ are also Boolean expressions.

(iv) If α is a Boolean expression then α' is also a Boolean expression.

(v) No strings of symbols except those formed in accordance with rules 1 to 4 are Boolean expressions.

Examples: (i) x_1 (ii) x_2' (iii) $x_1' \oplus x_2'$

(iv) $x_1' * (x_2' \oplus x_3)$

(v) $x_1' * x_2' * x_3$ are Boolean expressions.

Equivalent Boolean expressions

Two Boolean expressions $\alpha(x_1, x_2, \ldots x_n)$ and $\beta(x_1, x_2, \ldots x_n)$ are called equivalent (or) equal if one can be obtained from the other by the finite number of applications of the identities of a Boolean algebra.

Example: The two Boolean expressions $\{(x_1' * x_2' * x_3') \oplus (x_1' * x_2' * x_3)\}$ and $(x_1' * x_2')$ are equivalent.

Minterms and maxterms

A Boolean expression generated by $x_1, x_2, \ldots x_n$ which has the form

$\ast_{i=1}^{n} y_i$, where y_i may be either x_i or x_i'

is called a minterm (or) complete product (or) a fundamental product of n-Variables.

The form $\bigoplus_{i=1}^{n} y_i$ where y_i may be either x_i or x_i' is called a

maxterm

Ex: 1 Write the following Boolean expressions in an equivalent sum-of-products canonical form in three variables x_1, x_2 and x_3:

(a) $x_1 * x_2$

(b) $x_1 \oplus x_2$ and (c) $(x_1 \oplus x_2)' * x_3$.

Solution:

(a) $x_1 * x_2 = x_1 * x_2 * (x_3 \oplus x_3')$

$= (x_1 * x_2 * x_3) \oplus (x_1 * x_2 * x_3')$

$= min_6 \oplus min_7$

$= \oplus 6, 7.$

(b) $x_1 \oplus x_2 = [x_1 * (x_2 \oplus x_2')] \oplus [x_2 * (x_1 \oplus x_1')]$

$= (x_1 * x_2) \oplus (x_1 * x_2') \oplus (x_2 * x_1) \oplus (x_2 * x_1')$

$= [(x_1 * x_2) * (x_3 \oplus x_3')] \oplus [(x_1 * x_2') * (x_3 \oplus x_3')]$
$\oplus [(x_2 * x_1) * (x_3 \oplus x_3')] \oplus [(x_2 * x_1') * (x_3 \oplus x_3')]$

$= (x_1 * x_2 * x_3) \oplus (x_1 * x_2 * x_3') \oplus (x_1 * x_2' * x_3)$
$\oplus (x_1 * x_2' * x_3') \oplus (x_2 * x_1 * x_3) \oplus (x_2 * x_1 * x_3')$
$\oplus (x_2 * x_1' * x_3) \oplus (x_2 * x_1' * x_3')$

Negelate repeated terms, we get

$= (x_1 * x_2 * x_3) \oplus (x_1 * x_2 * x_3') \oplus (x_1 * x_2' * x_3)$
$\oplus (x_1 * x_2' * x_3') \oplus (x_1' * x_2 * x_3) \oplus (x_1' * x_2 * x_3')$

$= \text{min}\,7 \oplus \text{min}\,6 \oplus \text{min}\,5 \oplus \text{min}\,4 \oplus \text{min}\,3 \oplus \text{min}\,2$

$= \oplus\, 2, 3, 4, 5, 6, 7.$

(c) $(x_1 \oplus x_2)' * x_3 = (x_1' * x_2') * x_3$

$= (x_1' * x_2' * x_3)$

$= \text{min}\,1$

Ex: 2 Show that

$(x_1' * x_2' * x_3' * x_4') \oplus (x_1' * x_2' * x_3' * x_4)$
$\oplus (x_1' * x_2' * x_3 * x_4) \oplus (x_1' * x_2' * x_3 * x_4') = x_1' * x_2'$

Solution:

Consider first two terms

$(x_1' * x_2' * x_3' * x_4') \oplus (x_1' * x_2' * x_3' * x_4)$

$= (x_1' * x_2' * x_3') * (x_4' \oplus x_4)$

$= (x_1' * x_2' * x_3') \quad — (1)$

Now we take last two terms

③

$(x_1' * x_2' * x_3 * x_4) \oplus (x_1' * x_2' * x_3 * x_4')$

$= (x_1' * x_2' * x_3) * (x_4 \oplus x_4')$

$= (x_1' * x_2' * x_3)$ — ②

Using ① & ② in the given problem

$(x_1' * x_2' * x_3' * x_4') \oplus (x_1' * x_2' * x_3' * x_4)$
$\oplus (x_1' * x_2' * x_3 * x_4) \oplus (x_1' * x_2' * x_3 * x_4')$

$= (x_1' * x_2' * x_3') \oplus (x_1' * x_2' * x_3)$.

$= (x_1' * x_2') * (x_3' \oplus x_3)$

$= x_1' * x_2'$.

Hence proved.

EX: 3 obtain the product-of-sums canonical forms to following boolean expressions;

(a) $x_1 * x_2$ (b) $x_1 \oplus x_2$.

Solution: (a) $x_1 * x_2 = [x_1 \oplus (x_2 * x_2')]$
$* [x_2 \oplus (x_1 * x_1')]$

$= (x_1 \oplus x_2) * (x_1 \oplus x_2') * (x_2 \oplus x_1) * (x_2 \oplus x_1'$

$= (x_1 \oplus x_2) * (x_1 \oplus x_2') * (x_1' \oplus x_2)$

$\cancel{= (x_1 \oplus x_2 \oplus x_3) * (x_1 \oplus x_2 + x_3')}$

$= \left[(x_1 \oplus x_2) \oplus (x_3 * x_3')\right] * \left[(x_1 \oplus x_2') \oplus (x_3 * x_3')\right]$

$* \left[(x_1' \oplus x_2) \oplus (x_3 * x_3')\right]$

$= (x_1 \oplus x_2 \oplus x_3) * (x_1 \oplus x_2 \oplus x_3') * (x_1 \oplus x_2' \oplus x_3)$

$* (x_1 \oplus x_2' \oplus x_3') * (x_1' \oplus x_2 \oplus x_3) * (x_1' \oplus x_2 \oplus x_3').$

$= \max_0 * \max_1 * \max_2 * \max_3 * \max_4 * \max_5$

$= * \; 0, 1, 2, 3, 4, 5.$

(b) $x_1 \oplus x_2 = x_1 \oplus x_2 \oplus (x_3 * x_3').$

$= (x_1 \oplus x_2 \oplus x_3) * (x_1 \oplus x_2 \oplus x_3')$

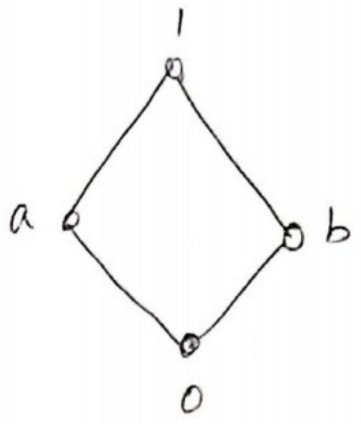
$= \max_0 * \max_1$

Ex : 4 Find the value of

$x_1 * x_2 * \left[(x_1 * x_4) \oplus x_2' \oplus (x_3 * x_1')\right]$

for $x_1 = a$, $x_2 = 1$, $x_3 = b$ and $x_4 = 1$, where

$a, b, 1 \in B$ and the Boolean algebra $\langle B, *, \oplus, ', 0, 1 \rangle$ is show the following diagram.



Solution:

$$x_1 * x_2 * \left[(x_1 * x_4) \oplus x_2' \oplus (x_3 * x_1') \right]$$

$$= (x_1 * x_2 * x_1 * x_4) \oplus (x_1 * x_2 * x_2') \oplus (x_1 * x_2 * x_3 * x_1')$$

$$= (x_1 * x_2 * x_4)$$

$$= a * 1 * 1$$

$$= a.$$

Grammar

A system or language which describes another language is known as metalanguage.

The diagram of a sentce describes its syntax but not its meaning (or) semantics.

We cannected with the syntax of a language and the device which we have defined to give the syntatic definition of the language is called a grammar.

Defn: A (phrase structure) grammer is defined by a 4-tuple $G = (V_N, V_T, S, \phi)$ where V_T and V_N are set of terminal and nonterminal (syntaticlass) symbols respectively. S a distinguished element of V_N and therefore of the vacabulary, is called the starting symbol. ϕ is a finite subset of the relation from

$$(V_T \cup V_N)^* V_N (V_T \cup V_N)^* \text{ to } (V_T \cup V_N)^*.$$

In general an element $\langle \alpha, \beta \rangle$ is written as $\alpha \longrightarrow \beta$ and is called a production rule or a rewriting rule.

Types of Grammar

TYPE-0 grammar, there is no restriction on the production rules.

TYPE-1 grammar, only admissible productions are of the type $w_1 \longrightarrow w_2$ such that $w_1, w_2 \in (V_N \cup T)^*$ and $|w_1| \leq |w_2|$ or $w_1 \rightarrow \Lambda$
(it is called Context ~~free~~ sensitive grammar)

②

TYPE-2 grammar, the admissible productions are of the type $w_1 \rightarrow w_2$
where $|w_1| = 1$ (ie) w_1 is a single non-terminal symbol and $w_2 \in (V_N \cup T)^*$.
(it is also Context-free grammar.)

TYPE-3 grammar, the admissible productions are of the form $w_1 \longrightarrow w_2$ with $w_1 = A$ and either $w_2 = aB \mid Ba \mid a \mid A$
where A and B are single non-terminal Symbol and a is any terminal symbol. The type of grammar is called regular grammar;

Defn: Let $G = (V_N, V_T, S, \phi)$ be a grammar. The string ψ produces σ (σ reduces to ψ, or σ is the derivation of ψ), written as $\psi = \sigma$, if the Strings $\phi_0, \phi_1, \dots \phi_n$ $(n > 0)$ such that $\psi = \phi_0 \Rightarrow \phi_1$, $\phi_1 \Rightarrow \phi_2$, $\dots$ $\phi_{n-1} \Rightarrow \phi_n$ and $\phi_n = \sigma$. The relation $\overset{+}{\Longrightarrow}$ is the transitive ~~closure~~ Closure of the relation $\Longrightarrow$.
If we let $n = 0$ then we can define the reflexive transitive closure of $\Longrightarrow$ as
$$\psi \overset{*}{\Longrightarrow} \sigma \iff \psi \overset{+}{\Longrightarrow} \sigma \text{ or } \psi = \sigma.$$
Returning to grammar G_1, we show that the String abc12 is derived from I.

(5)

$I \Rightarrow ID \Rightarrow IDD \Rightarrow ILDD \Rightarrow ILLDD$

$\Rightarrow LLLDD \Rightarrow aLLDD \Rightarrow abLDD$

$\Rightarrow abcDD \Rightarrow abc1D \Rightarrow abc12.$

<u>Defn:</u> A <u>Sentential form</u> is any derivative of the unique non-terminal symbol S. The language L generated by a grammar G is the set of all sentential forms whose symbols are terminal, (ie)

$$L(G) = \{\sigma \mid S \overset{*}{\Rightarrow} \sigma \text{ and } \sigma \in V_T^*\}$$

∴ The language is a ~~as~~ merely subset of the set of all terminal strings over V_T.

<u>Example:</u> ~~Let~~ Let $G_2 = \langle \{E, T, F\}, \{a, +, *, (,)\}, E, \phi \rangle$

where ϕ consists of the productions

$E \longrightarrow E + T$

$E \longrightarrow T$

$T \longrightarrow T * F$

$T \longrightarrow F$

$F \longrightarrow (E)$

$F \longrightarrow a$

Where the variables E, T, and F represent the names "expression", "term" and "factor" commonly used in conjunction with arithmetic expressions. A derivation for the expression $a * a + a$ is

~~Ex~~: $E \Rightarrow E + T$

$\Rightarrow T + T$

$\Rightarrow T * F + T$

$\Rightarrow F * F + T$

$\Rightarrow a * F + T$

$\Rightarrow a * a + T$

$\Rightarrow a * a + F$

$\Rightarrow a * a + a$.

Example: The language $L(G_3) = \{a^n b^n c^n \mid n \geq 1\}$ is generated by the following grammar.

$G_3 = \langle \{S, B, C\}, \{a, b, c\}, S, \phi \rangle$

Where ϕ consists of the productions

$S \rightarrow aSBC$

$S \rightarrow aBC$

$CB \rightarrow BC$

$aB \rightarrow ab$

$bB \rightarrow bb$

$bC \rightarrow bc$

$cC \rightarrow cc$

Derivation for the string $a^2 b^2 c^2$

$S \Rightarrow aSBC$

$\Rightarrow aaBCBC$

$\Rightarrow aaBBCC$

$\Rightarrow aabBCC$

$\Rightarrow aabbCC$

$\Rightarrow aabbcC$

$\Rightarrow aabbcc$

Example The language

$L(G_4) = \{a^n b a^n \mid n \geq 1\}$ is generated by the grammar

$$G_4 = \langle \{S, C\}, \{a, b\}, S, \phi \rangle$$

where ϕ is the set of productions

$$S \longrightarrow aCa$$
$$C \longrightarrow aCa$$
$$C \longrightarrow b$$

Derivation for a^2ba^2 ~~consists of th~~

$$S \Longrightarrow aCa$$
$$\Longrightarrow aaCaa$$
$$\Longrightarrow aabaa$$

Example: The language $L(G_5) = \{a^n b a^m \mid n, m \geq 1\}$ is generated by the grammar

$$G_5 = \langle \{S, A, B, C\}, \{a, b\}, S, \phi \rangle$$

where the set of productions are

$$S \longrightarrow aS$$
$$S \longrightarrow aB$$
$$B \longrightarrow bC$$
$$C \longrightarrow aC$$
$$C \longrightarrow a$$

Derivation of the string a^2ba^3

$$S \Longrightarrow aS$$
$$\Longrightarrow aaB$$
$$\Longrightarrow aabC$$
$$\Longrightarrow aabaC$$
$$\Longrightarrow aabaaC$$
$$\Longrightarrow aabaaa$$

Defn: A Context-sensitive grammar (b) contains only productions of the form $\alpha \longrightarrow \beta$ where $|\alpha| \leq |\beta|$.

A Conten-free grammer contains productions of only the form $\alpha \longrightarrow \beta$ where $|\alpha| \leq |\beta|$ and $\alpha \in V_N$

A regular grammar. contains only productions of the form $\alpha \longrightarrow \beta$ where $|\alpha| \leq |\beta|$, $\alpha \in V_N$ and β has the form aB or a where $a \in V_T$ and $B \in V_N$.

Note:

The metalanguage is known as Backus Nour Form (BNF) and has been used extensively in the formal definition of many programming languages. A popular language described using BNF is ALGOL.

The definition of an Identifier in BNF is given as

<identifier> ::= <letter> | <identifier letter> | <identifier><digit>

<letter> := a|b|c| --- |y|z

<digit> := 0|1|2|3| --- |8|9

The symbol ::= replaces the symbol $\rightarrow$ in the gramma notation, and | is used to ~~different~~ separate different righ-hand sides of productions corresponding to the same left hand side. The symbol ::= is interpreted as "is defined as" and | as "or".