

UNIT-I

Mathematical Logic

Syllabus

Mathematical Logic: Introduction, Statements and Notation, Connectives, Truth tables, Well-formed formulas, Tautology, Contradiction, Contingency, Logical equivalence, Normal Forms, Theory of Inference for the Statement Calculus, The Predicate Calculus, Inference Theory of the Predicate Calculus

Introduction to Discrete Mathematics

- Discrete Mathematics is the study of discrete structures which mathematical models dealing with discrete objects and relationships between them.
- Examples of discrete objects are like Sets, Permutations, graphs and etc.

Why it is important for computer science

- In the world of computers, all the information is stored in bits, units of information that can take the value of either 0 or 1. It's not like in nature, where something can take all the values in between 0 and 1 as well. Instead, everything is binary.
- Since the bits are the building blocks of everything that happens in computer software, every thing becomes discrete. For instance, the hard drive on the laptop I'm using right now can store 1 845 074 329 600 bits of information.
- The study of algorithms is also firmly in the discrete world. An algorithm is a step-by-step list of instructions to the computer and it's what makes computer programs possible. When determining how much time an algorithm needs to run, you count the number of operations it needs to perform. Notice the word count. Again, discrete mathematics.
- In continuous mathematics (the opposite of discrete), the calculation would go like this:
- $\int_0^5 x dx = [1/2 * x^2]_0^5 = 5^2/2 - 0 = 12.5$
- In discrete mathematics, the equivalent calculation would go like this:
- $\sum_{i=0}^4 i = 0 + 1 + 2 + 3 + 4 = 10$

Applications of discrete mathematics with computer applications

- 1) Computer networks
- 2) Programming languages
- 3) Finite state automata or compilers
- 4) Databases

Symbolic logic is used in framing algorithms and their verification and in automatic theorem proving. Set theory, Graph Theory, trees etc are used in storage and retrieval of information (data structures), Algorithms and their complexity studies also use tools from discrete mathematics. Formal Languages, Automata theory, Turing machines etc. are themselves part of discrete mathematics and so is Recursive Function Theory. Undecidability of many problems are established using Turing machines which is the Mathematical model for studying theoretical limitations of Computation. Lattices and Boolean Algebra are used in Computer Science as well as in communications and networking.

Mathematical Logic

Logic

It is the study of the principles and methods that distinguish between valid and invalid argument.

1. Proposition Logic

Proposition or Statement

A proposition or a statement can be defined as a declarative sentence to which we can assign one and only one of the truth values either true (or) false but not both is called a proposition.

The true or false of a proposition is called truth value of a proposition

These two values true and false are denoted by the symbols T and F respectively. Sometimes these are also denoted by the symbols 1 and 0 respectively.

Proposition	truth value
Ex:1)IndiacapitalisnewDelhi	True
2) $2*3=5$	false
3) 5isaprimenumber	true

These are propositions (or statements) because they are either true or false. Next

consider the following sentences:

- 4) How beautiful are you?
- 5) Wish you a happy new year
- 6) $x+y=z$
- 7) Take one book.

These are not propositions as they are not declarative in nature, that is, they do not declare a definite truth value T or F .

Types of Propositions

- 1) Atomic proposition
- 2) Compound Proposition

1) Atomic proposition

- A Proposition which cannot be divided further is called an atomic proposition.
- **Examples:**
 - 1) India's capital is New Delhi
 - 2) $2*3=5$

2) Compound Proposition

- Two or more atomic propositions can be combined to form a compound proposition with help of Connectives. Compound Proposition also called as Propositional function.

- **Examples of Compound statements**
- $3+2=-1$ and Delhi is the capital of India.
- grass is green or — it is hot today.
- Discrete mathematics is not difficult to me.

And, Or, Not are called connectives.

Notations

- Statements are symbolically represented as $A, B, C, \dots, P, Q, R, S, \dots$. These are called propositional variables or notations.
- **Examples:**
- $P \rightarrow$ Delhi is the capital of India.
- $Q \rightarrow$ 17 is divisible by 3.

Logical Connectives

- The words or phrases or symbols which are used to make a compound proposition by two or more atomic propositions are called **logical connectives** or **simply connectives**.
- There are five basic connectives called negation, conjunction, disjunction, conditional and biconditional.

Connectivity	Symbol	Word
Negation	$\neg$	Not
Disjunction	$\vee$	OR
Conjunction	$\wedge$	AND
Conditional	$\rightarrow$	IF AND THEN
Biconditional	$\leftrightarrow$	If and only if

Negation($\sim$)or($\neg$)

The **negation** of a statement is generally formed by writing the word ‘not’ at a proper place in the statement (proposition) or by prefixing the statement with the phrase ($\neg$). It is not the case that. If p denotes a statement then the negation of p is written as $\neg p$ and read as not p . If the truth value of p is T then the truth value of $\neg p$ is F . Also if the truth value of p is F then the truth value of $\neg p$ is T .

Truth table for Negation

P	$\neg P$
F	T

Disjunction(OR)($\vee$)

- If P and Q are any two propositions then ‘**P OR Q**’ symbolically written as **$P \vee Q$** .
- $P \vee Q$ is a proposition whose truth value is false only when both P and Q are false otherwise True. $\wedge$

Truth table for Disjunction

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

P: I shall go to the game.

Q: I shall watch the game on television.

$P \vee Q$: I shall go to the game OR I shall watch the game on television.

Conjunction(AND($\wedge$))

- ☐ If P and Q are any two propositions then P and Q symbolically written as $P \wedge Q$.
- ☐ $P \wedge Q$ is a proposition whose truth value is true only when both P and Q are true. Whole truth
- ☐ value is false when either P or Q are false and both are false.

Truth table for Conjunction

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

P: It is raining today.

Q: There are 10 chairs in the room.

$P \wedge Q$: It is raining today AND There are 10 chairs
in the room.

Conditional(or) Implication($\rightarrow$)

If P and Q are any two statements (or propositions) then the statement $P \rightarrow Q$ which is read as, If P, then Q_ is called a **conditional statement** (or **proposition**) or **implication** and the connective is the **conditional connective**.

Truth table for conditional

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

In this conditional statement, P is called the **hypothesis** or **premise** or **antecedent** and Q is called the **consequence** or **conclusion**.

Biconditional (If and only if)

- If P and Q are any two propositions then P if and only if Q is written as $P \leftrightarrow Q$.
- Its truth value is true only when both P & Q have same truth values.

P	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

TAUTOLOGY AND CONTRADICTION

Tautology: A proposition is said to be a tautology if its truth value is T for any assignment of truth values to its components.

Example: The proposition $P \vee \neg P$ is a tautology.

Contradiction

A proposition is said to be a contradiction if its truth value is F for any assignment of truth values to its components. Example: The proposition $P \wedge \neg P$ is a contradiction.

Contingency: A statement formula which is neither a tautology nor a contradiction is known as a contingency.

Example: $P \rightarrow Q$

Tautology: A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a universally valid formula or a logical truth or a tautology.

How to prove given compound proposition is tautology

1) By Constructing truth table

2) By using substitution method

1) Constructing truth table

Show that following function is tautology

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

Solution

P	Q	$\neg P$	$P \vee Q$	$(P \vee Q) \vee \neg P$
F	F	T	F	T
F	T	T	T	T
T	F	F	T	T
T	T	F	T	T

In the above table $(P \vee Q) \vee \neg P$ is giving all truth values are true so it is a tautology.

Show that given proposition is a tautology $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R)$

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

Implication:

- If P and Q are any two propositions then $P \rightarrow Q$ is, If P then Q
- $P \rightarrow Q$ is a proposition whose truth value is false only when P is true and Q is false.
- Here P is antecedent and Q is Consequent..

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

- Whenever P is false $P \rightarrow Q$ is true

- If, false antecedent P implies any proposition Q
- Whenever Q is true $P \rightarrow Q$ is also true
- If, a true consequent Q implied by any propositional P .

from the implication statement we can write another three statements which are converse, inverse and contrapositive

Converse, Inverse and Contrapositive

If $P \rightarrow Q$ is a conditional statement, then (1).

$Q \rightarrow P$ is called its converse (2).

$\neg P \rightarrow \neg Q$ is called its inverse

(3). $\neg Q \rightarrow \neg P$ is called its contrapositive.

Example:

- **P: Today is Sunday**
- **Q: It is a holiday**
- **Converse Statement:** If it is a holiday, then today is Sunday.
- **Inverse Statement:** If today is not Sunday, then it is not a holiday.
- **Contrapositive Statement:** If it is not a holiday, then today is not Sunday.



your roots to success...

Here Implication and Contrapositive are equal.

Converse and inverse are opposite propositions.

Well formed formulas (wff):

Not all strings can represent propositions of the predicate logic. Those which produce a proposition when their symbols are interpreted must follow the rules given below, and they are called wffs (well-formed formulas) of the first order predicate logic.

Rules for constructing Wffs

A predicate name followed by a list of variables such as $P(x, y)$, where P is predicate name, and x and y are variables, is called an atomic formula.

A well formed formula of predicate calculus is obtained by using the following rules.

1. An atomic formula is a wff.
2. If A is a wff, then $\neg A$ is also a wff.
3. If A and B are wffs, then $(A \vee B)$, $(A \wedge B)$, $(A \rightarrow B)$ and $(A \leftrightarrow B)$.
4. If A is a wff and x is any variable, then $(\forall x)A$ and $(\exists x)A$ are wffs.
5. Only those formulas obtained by using (1) to (4) are wffs.

Since we will be concerned with only wffs, we shall use the term formulas for wff. We shall follow the same conventions regarding the use of parentheses as was done in the case of statement formulas.

Wffs are constructed using the following rules:

1. *True* and *False* are wffs.
2. Each propositional constant (i.e. specific proposition), and each propositional variable (i.e. a variable representing propositions) are wffs.
3. Each atomic formula (i.e. a specific predicate with variables) is a wff.
4. If A , B , and C are wffs, then so are $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, and $(A \leftrightarrow B)$.
5. If x is a variable (representing objects of the universe of discourse), and A is a wff, then so are $\forall x A$ and $\exists x A$. For example, "The capital of Virginia is Richmond." is a specific proposition. Hence it is a wff by Rule 2.

Let B be a predicate name representing "being blue" and let x be a variable. Then $B(x)$ is an atomic formula meaning "x is blue". Thus it is a wff by Rule 3. above. By applying Rule 5. to $B(x)$, $\forall x B(x)$ is a wff and so is $\exists x B(x)$. Then by applying Rule 4. to them $\forall x B(x) \wedge \exists x B(x)$ is seen to be a wff. Similarly, if R is a predicate name representing "being round". Then $R(x)$ is an atomic formula. Hence it is a wff. By applying Rule 4 to $B(x)$ and $R(x)$, a wff $B(x) \wedge R(x)$ is obtained. In this manner, larger and more complex wffs can be constructed following the rules given above. Note, however, that strings that cannot be constructed by using those rules are not wffs. For example, $\forall x B(x) R(x)$, and $B(\exists x)$ are NOT wffs, NOR are $B(R(x))$, and $B(\exists x R(x))$.

More examples: To express the fact that Tom is taller than John, we can use the atomic formula **taller(Tom, John)**, which is a wff. This wff can also be part of some compound statement such as **taller(Tom, John) $\wedge$ taller(John, Tom)**, which is also a wff. If x is a variable representing people in the world, then **taller(x, Tom)**, $\forall x$ **taller(x, Tom)**, $\exists x$ **taller(x, Tom)**, $\exists x \forall y$ **taller(x, y)** are all wffs among others. However, **taller($\exists x$, John)** and **taller(Tom $\wedge$ Mary, Jim)**, for example, are NOT wffs.

Logical Equivalence

Two formulas A and B are said to be equivalent to each other if and only if $A \leftrightarrow B$ is a tautology. If $A \leftrightarrow B$ is a tautology, we write $A \Leftrightarrow B$ which is read as A is equivalent to B .

Note: 1. $\Leftrightarrow$ is only a symbol, but not a connective.

$A \leftrightarrow B$ is a tautology if and only if truth tables of A and B are the same. Equivalence relation is symmetric and transitive.

(or)

Let P and Q be two propositional functions. P is equivalent to Q . Symbolically written

as $P \Leftrightarrow Q$ or $P \equiv Q$ if P and Q have the same truth table.

Ex: $P \rightarrow Q \Leftrightarrow \neg P \vee Q$.

Method I. Truth Table Method: One method to determine whether any two statement formulas are equivalent is to construct their truth tables.

Example: Prove $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

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

In the above table both $P \rightarrow Q$ and $\neg P \vee Q$ have the same truth values. So that $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Equivalence Formulas:

1. Idempotent laws:

$$(a) P \vee P \Leftrightarrow P$$

$$(b) P \wedge P \Leftrightarrow P$$

2. Associative laws:

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

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

3. Commutative laws:

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

$$(b) P \wedge Q \Leftrightarrow Q \wedge P$$

4. Distributive laws:

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

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

Identity laws (or)

5. Domination Law

$$(a)(i) P \vee F \Leftrightarrow P$$

$$(ii) P \vee T \Leftrightarrow T$$

$$(b)(i) P \wedge T \Leftrightarrow P$$

$$(ii) P \wedge F \Leftrightarrow F$$

6. Component laws:

$$(a)(i) P \vee \neg P \Leftrightarrow T$$

$$(ii) P \wedge \neg P \Leftrightarrow F$$

$$(b)(i) \neg \neg P \Leftrightarrow P$$

$$(ii) \neg T \Leftrightarrow F, \neg F \Leftrightarrow T$$

7. Absorption laws:

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

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

8. DeMorgan's Laws

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

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

TABLE 7 Logical Equivalences Involving Conditional Statements.

$$p \rightarrow q \equiv \neg p \vee q$$

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

$$p \vee q \equiv \neg p \rightarrow q$$

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

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

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

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

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

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

S...

Tautological Implications.

A statement formula A is said to *tautologically imply* a statement B if and only if $A \rightarrow B$ is a tautology. In this case we write $A \Rightarrow B$, which is read as " A implies B ".

Note: $\Rightarrow$ is not a connective, $A \Rightarrow B$ is not a statement formula.

$A \Rightarrow B$ states that $A \rightarrow B$ is a tautology.

Clearly $A \Rightarrow B$ guarantees that B has a truth value T whenever A has the truth value T . One can determine whether $A \Rightarrow B$ by constructing the truth tables of A and B in the same manner as was done in the determination of $A \Leftrightarrow B$.

Example: Prove that $(P \rightarrow Q) \Rightarrow (\neg Q \rightarrow \neg P)$.

P	Q	$\neg P$	$\neg Q$	$P \rightarrow Q$	$\neg Q \rightarrow \neg P$	$(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Since all the entries in the last column are true, $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$ is a tautology.

Hence $(P \rightarrow Q)$ is Tautological Implication to $(\neg Q \rightarrow \neg P)$. So that

$(P \rightarrow Q) \Rightarrow (\neg Q \rightarrow \neg P)$.

In order to show any of the given implications, it is sufficient to show that an assignment of the truth value T to the antecedent of the corresponding conditional leads to the truth value T for the

consequent. This procedure guarantees that the conditional becomes tautology, thereby proving the implication.

Example: Prove that $\neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P$.

Solution: Assume that the antecedent $\neg Q \wedge (P \rightarrow Q)$ has the truth value T , then both $\neg Q$ and $P \rightarrow Q$ have the truth value T , which means that Q has the truth value F , $P \rightarrow Q$ has the truth value T .

Hence P must have the truth value F . Therefore, the consequent $\neg P$ must have the truth value T .

$\neg Q \wedge (P \rightarrow Q) \rightarrow \neg P$.

Another method to show $A \Rightarrow B$ is to assume that the consequent B has the truth value F and then show that this assumption leads to A having the truth value F . Then $A \rightarrow B$ must have the truth value T .

Example: Show that $\neg(P \rightarrow Q) \Rightarrow P$.

Solution: Assume that P has the truth value F . When P has F , $P \rightarrow Q$ has T , then $\neg(P \rightarrow Q)$ has F . Hence $\neg(P \rightarrow Q) \rightarrow P$ has T .

So that $\neg(P \rightarrow Q) \Rightarrow P$.

Normal Forms

If a given statement formula $A(p_1, p_2, \dots, p_n)$ involves n atomic variables, we have 2^n possible combinations of truth values of statements replacing the variables.

The formula A is a tautology if A has the truth value T for all possible assignments of the truth values to the variables $p_1, p_2, \dots, p_n$ and A is called a contradiction if A has the truth value F for all possible assignments of the truth values of the n variables. A is said to be *satisfiable* if A has the truth value T for at least one combination of truth values assigned to $p_1, p_2, \dots, p_n$.

The problem of determining whether a given statement formula is a Tautology, or a Contradiction is called a decision problem.

The construction of truth table involves a finite number of steps, but the construction may not be practical. We therefore reduce the given statement formula to normal form and find whether a given statement formula is a Tautology or Contradiction or at least satisfiable. It will be convenient to use the word product in place of conjunction and sum in place of disjunction.

A product of the variables and their negations in a formula is called an *elementary Product*. Similarly, a sum of the variables and their negations in a formula is called an *elementary sum*. Let P and Q be any atomic variables. Then $P, \sim P \wedge Q, \sim Q \wedge P \wedge \sim P, Q \wedge \sim P$ are some examples of elementary products.

On the other hand $P, \sim P \vee Q, \sim Q \vee P \vee \sim P, Q \vee \sim P$ are some examples of elementary sums. Types of Normal forms

- 1) Disjunctive Normal forms
- 2) Conjunctive Normal forms.

Disjunctive Normal Form (DNF)

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

Example: Obtain disjunctive normal form of

$$(a) P \sqcap (P \rightarrow Q)$$

$$P \sqcap (P \rightarrow Q) \Leftrightarrow P \sqcap (\neg P \vee Q) \quad (\text{apply distributive law } P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R))$$

$$= (P \sqcap \neg P) \vee (P \sqcap Q)$$

$$b) \neg(P \vee Q) \leftrightarrow (P \wedge Q)$$

$$\neg(P \vee Q) \leftrightarrow (P \wedge Q) \Leftrightarrow (\neg(P \vee Q) \sqcap (P \wedge Q)) \vee ((P \vee Q) \sqcap \neg(P \wedge Q)) \quad [\text{using } R \leftrightarrow S \Leftrightarrow (R \wedge S) \vee (\neg R \wedge \neg S)]$$

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

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

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

Which is the required disjunctive normal form. Note: The DNF of a given formula is not unique.

Conjunctive Normal Form (CNF)

A formula which is equivalent to a given formula and which consists of a product of elementary sums is called a *conjunctive normal form* of the given formula.

The method for obtaining conjunctive normal form of a given formula is similar to the one given for disjunctive normal form. Again, the conjunctive normal form is not unique.

(a) $P \wedge (P \rightarrow Q)$ obtain the conjunctive normal form

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

(b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

$$\begin{aligned} & \neg(\neg(P \vee Q) \rightarrow (P \wedge Q)) \sqcap ((P \wedge Q) \rightarrow \neg(P \vee Q)) \\ & \neg((P \vee Q) \vee (P \wedge Q)) \wedge (\neg(P \wedge Q) \vee \neg(P \vee Q)) \\ & \neg[(P \vee Q \vee P) \wedge (P \vee Q \vee Q)] \wedge [(\neg P \vee \neg Q) \vee (\neg P \wedge \neg Q)] \\ & \neg(P \vee Q \vee P) \wedge (P \vee Q \vee Q) \wedge (\neg P \vee \neg Q \vee \neg P) \wedge (\neg P \vee \neg Q \vee \neg Q) \end{aligned}$$

Principal Disjunctive Normal Form

In this section, we will discuss the concept of principal disjunctive normal form (PDNF).

Minterm: For a given number of variables, the minterm consists of conjunctions in which each statement variable or its negation, but not both, appears only once.

Let P and Q be the two statement variables. Then there are 2^2 minterms given by $P \wedge Q, P \wedge \neg Q,$

$\neg P \wedge Q$, and $\neg P \wedge \neg Q$

Minterms for three variables P, Q and R are $P \wedge Q \wedge R, P \wedge Q \wedge \neg R, P \wedge \neg Q \wedge R, P \wedge \neg Q \wedge \neg R, \neg P \wedge Q \wedge R, \neg P \wedge Q \wedge \neg R, \neg P \wedge \neg Q \wedge R$ and $\neg P \wedge \neg Q \wedge \neg R$.

your roots to success...

From the truth tables of these minterms of P and Q , it is clear that.

P	Q	$P \wedge Q$	$P \wedge \neg Q$	$\neg P \wedge Q$	$\neg P \wedge \neg Q$
T	T	T	F	F	F
T	F	F	T	F	F
F	T	F	F	T	F
F	F	F	F	F	T

- (i). Not two minterms are equivalent
- (ii). Each minterm has the truth value T for exactly one combination of the truth values of the variables P and Q .

PDNF

Definition: For a given formula, an equivalent formula consisting of disjunctions of minterms only is called the Principal disjunctive normal form of the given formula. The principle disjunctive normal formula is also called the sum-of-products canonical form.

Methods to obtain the PDNF of a given formula.

(a). By Truth table:

(b). without constructing the truth table

(a). By Truth table:

- (i). Construct a truth table of the given formula.
- (ii). For every truth value T in the truth table of the given formula, select the minterm which also has the value T for the same combination of the truth values of P and Q .
- (iii). The disjunction of these minterms will then be equivalent to the given formula

Example: Obtain the PDNF of $P \rightarrow Q$.

Solution: From the truth table of $P \rightarrow Q$

P	Q	$P \rightarrow Q$	Minterm
T	T	T	$P \wedge Q$
T	F	F	$P \wedge \neg Q$
F	T	T	$\neg P \wedge Q$
F	F	T	$\neg P \wedge \neg Q$

The PDNF of $P \rightarrow Q$ is $(P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q)$.

Obtain the PDNF for $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$.

Solution:

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

The PDNF of $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$ is $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$.

(b). Without constructing the truth table:

In order to obtain the principal disjunctive normal form of a given formula is constructed as follows:

(1). First replace $\rightarrow$, by their equivalent formula containing only $\wedge$, $\vee$ and $\neg$.

(2). Next, negations are applied to the variables by De Morgan's laws followed by the application of distributive laws.

(3). Any elementarily product which is a contradiction is dropped. Minterms are obtained in the disjunctions by introducing the missing factors. Identical minterms appearing in the disjunctions are deleted.

Example: Obtain the principal disjunctive normal form of

(a) $\neg P \vee Q$

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

(a) $\neg P \vee Q$

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

- $(\neg P \wedge (Q \vee \neg Q)) \vee (Q \wedge (P \vee \neg P))$ [$\because P \vee \neg P \Leftrightarrow T$]
- $(\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (Q \wedge P) \vee (Q \wedge \neg P)$
- $(\neg P \square Q) \vee (\neg P \square \neg Q) \vee (P \square Q)$ [$\because P \vee P \Leftrightarrow P$]

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

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

$$\begin{aligned} &= (P \wedge Q \wedge (R \vee \neg R)) \vee (\neg P \wedge R \wedge (Q \vee \neg Q)) \vee (Q \wedge R \wedge (P \vee \neg P)) \\ &= (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge R \wedge Q) \vee (\neg P \wedge R \wedge \neg Q) \vee \\ &\quad (Q \wedge R \wedge P) \vee (Q \wedge R \wedge \neg P) \\ &= (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R) \end{aligned}$$

Principal Conjunctive Normal Form

The dual of a minterm is called a Maxterm. For a given number of variables, the *maxterm* consists of disjunctions in which each variable or its negation, but not both, appears only once. Each of the maxterm has the truth value F for exactly one combination of the truth values of the variables. Now we define the principal conjunctive normal form.

For a given formula, an equivalent formula consisting of conjunctions of the max-terms only is known as its *principle conjunctive normal form*. This normal form is also called the *product-of-sums canonical form*. The method for obtaining the PCNF for a given formula is similar to the one described previously for PDNF.

Example: Obtain the principal conjunctive normal form of the formula $(\neg P \rightarrow R) \wedge (Q \leftrightarrow P)$

Solution:

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

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

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

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



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



your roots to success...

Rules of inference:

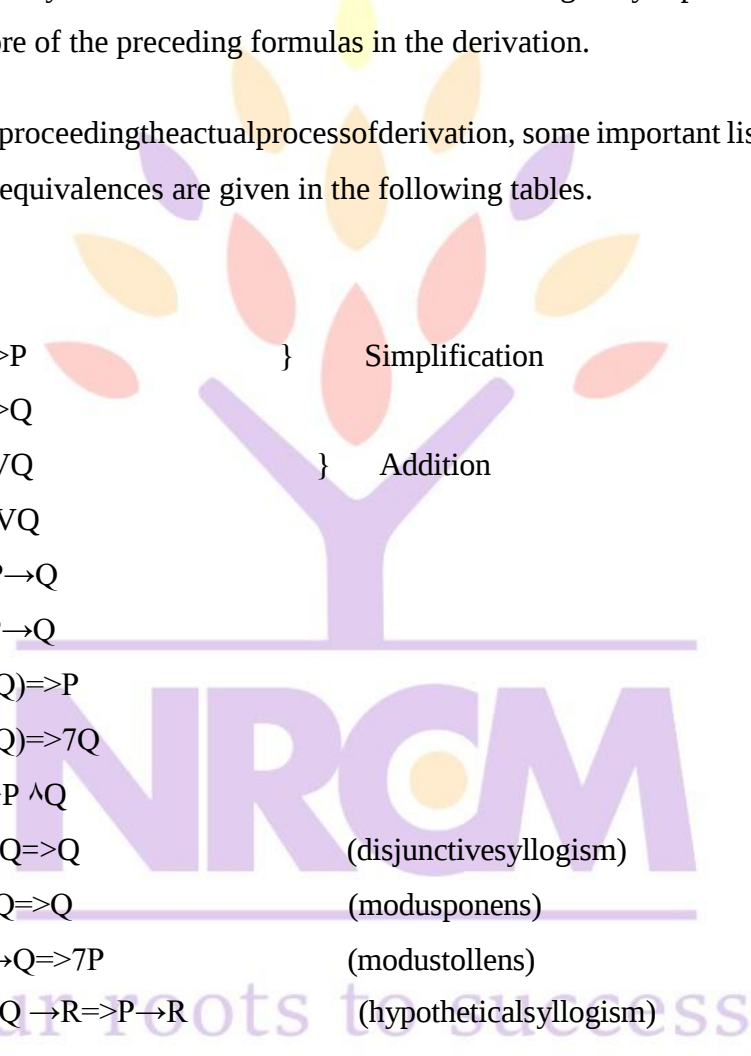
The two rules of inference are called rules P and T.

Rule P: A premise may be introduced at any point in the derivation.

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

Before proceeding to the actual process of derivation, some important list of implications and equivalences are given in the following tables.

Implications



I1	$P \wedge Q \Rightarrow P$	}	Simplification
I2	$PQ \wedge \Rightarrow Q$		
I3	$P \Rightarrow PVQ$	}	Addition
I4	$Q \Rightarrow PVQ$		
I5	$\neg P \Rightarrow P \rightarrow Q$		
I6	$Q \Rightarrow P \rightarrow Q$		
I7	$\neg(P \rightarrow Q) \Rightarrow P$		
I8	$\neg(P \rightarrow Q) \Rightarrow \neg Q$		
I9	$P, Q \Rightarrow P \wedge Q$		
I10	$\neg P, PVQ \Rightarrow Q$		(disjunctive syllogism)
I11	$P, P \rightarrow Q \Rightarrow Q$		(modus ponens)
I12	$\neg Q, P \rightarrow Q \Rightarrow \neg P$		(modus tollens)
I13	$P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$		(hypothetical syllogism)
I14	$PVQ, P \rightarrow Q, Q \rightarrow R \Rightarrow R$		(dilemma)

Equivalences

E1	$\neg\neg P \Leftrightarrow P$	
E2	$P \wedge Q \Leftrightarrow Q \wedge P$	} Commutative laws
E3	$P \vee Q \Leftrightarrow Q \vee P$	
E4	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	} Associative laws
E5	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	
E6	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	} Distributive laws
E7	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	
E8	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	
E9	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	} DeMorgan's laws
E10	$P \vee P \Leftrightarrow P$	
E11	$P \wedge P \Leftrightarrow P$	
E12	$P \vee (\neg P) \Leftrightarrow \text{True}$	
E13	$P \wedge (\neg P) \Leftrightarrow \text{False}$	
E14	$P \rightarrow Q \Leftrightarrow \neg P \vee Q$	
E15	$P \rightarrow Q \Leftrightarrow \neg(P \wedge \neg Q)$	
E16	$P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$	
E17	$P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$	
E18	$\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$	
E19	$P \rightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$	
E20	$(P \rightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$	
E21	$(P \rightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$	
E22	$(P \rightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$	

your roots to success...

Example 1. Show that R is logically derived from $P \rightarrow Q$, $Q \rightarrow R$, and P

Solution.	{1}	(1)	$P \rightarrow Q$	Rule P
	{2}	(2)	P	Rule P
	{1,2}	(3)	Q	Rule (1),(2) and I1
	{4}	(4)	$Q \rightarrow R$	Rule P
	{1,2,4}	(5)	R	Rule (3),(4) and I1.

Example 2. Show that $S \vee R$ is logically implied by $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S)$.

Solution.	{1}	(1)	$P \vee Q$	Rule P
	{1}	(2)	$\neg P \rightarrow Q$	T, (1), E1 and E16
	{3}	(3)	$Q \rightarrow S$	P
	{1,3}	(4)	$\neg P \rightarrow S$	T, (2), (3), and I13
	{1,3}	(5)	$\neg S \rightarrow P$	T, (4), E13 and E1
	{6}	(6)	$P \rightarrow R$	P
	{1,3,6}	(7)	$\neg S \rightarrow R$	T, (5), (6), and I13
	{1,3,6}	(8)	$S \vee R$	T, (7), E16 and E1

Example 3. Show that $\neg Q, P \rightarrow Q \Rightarrow \neg P$

Solution.	{1}	(1)	$P \rightarrow Q$	Rule P
	{1}	(2)	$\neg P \rightarrow \neg Q$	T, and E18
	{3}	(3)	$\neg Q$	P
	{1,3}	(4)	$\neg P$	T, (2), (3), and I11.

Example 4. Prove that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q$, $Q \rightarrow R$, $P \rightarrow M$ and $\neg M$.

Solution.	{1}	(1)	$P \rightarrow M$	P
	{2}	(2)	$\neg M$	P
	{1,2}	(3)	$\neg P$	T, (1), (2), and I12
	{4}	(4)	$P \vee Q$	P

{1,2,4}	(5)	Q	T,(3),(4),and I10.
{6}	(6)	$Q \rightarrow R$	P
{1,2,4,6}	(7)	R	T,(5),(6)and I11
{1,2,4,6}	(8)	$R \wedge (P \vee Q)$	T,(4),(7),and I9.

There is a third inference rule, known as rule CP or rule of conditional proof.

Rule CP: If we can derive S from R and a set of premises, then we can derive $R \rightarrow S$ from the set of premises alone.

- Note.
1. Rule CP follows from the equivalence E10 which states that $(P \wedge R) \rightarrow S \text{ } \phi \text{ } P \rightarrow (R \rightarrow S)$.
 2. Let P denote the conjunction of the set of premises and let R be any formula. The above equivalence states that if R is included as an additional premise and S is derived from $P \wedge R$ then $R \rightarrow S$ can be derived from the premises P alone.
 3. Rule CP is also called the *deduction theorem* and is generally used if the conclusion is of the form $R \rightarrow S$. In such cases, R is taken as an additional premise and S is derived from the given premises and R.

Example 5. Show that $R \rightarrow S$ can be derived from the premises $P \rightarrow (Q \rightarrow S)$, $\neg R \vee P$, and Q.

Solution.	{1}	(1)	$\neg R \vee P$	P
	{2}	(2)	R	P, assumed premise
	{1,2}	(3)	P	T,(1),(2),and I10
	{4}	(4)	$P \rightarrow (Q \rightarrow S)$	P
	{1,2,4}	(5)	$Q \rightarrow S$	T,(3),(4),and I11
	{6}	(6)	Q	P
	{1, 2,4,6}	(7)	S	T,(5),(6),and I11
	{1,4,6}	(8)	$R \rightarrow S$	CP.

Example 6 Show that $P \rightarrow S$ can be derived from the premises, $\neg P \vee Q$, $\neg Q \vee R$, and $R \rightarrow S$.

Solution.

{1}	(1)	$\neg P \vee Q$	P
{2}	(2)	P	P, assumed premise
{1,2}	(3)	Q	T,(1),(2) and I11
{4}	(4)	$\neg Q \vee R$	P
{1,2,4}	(5)	R	T,(3),(4) and I11
{6}	(6)	$R \rightarrow S$	P
{1, 2,4,6}	(7)	S	T,(5),(6) and I11
{2,7}	(8)	$P \rightarrow S$	CP

Example 7. "If there was a ball game, then traveling was difficult. If they arrived on time, then traveling was not difficult. They arrived on time. Therefore, there was no ball game". Show that these statements constitute a valid argument.

Solution. Let P: There was a ball game

Q: Traveling was difficult. R:

They arrived on time.

Given premises are: $P \rightarrow Q$, $R \rightarrow \neg Q$ and R conclusion is: $\neg P$

{1}	(1)	$P \rightarrow Q$	P
{2}	(2)	$R \rightarrow \neg Q$	P
{3}	(3)	R	P
{2,3}	(4)	$\neg Q$	T,(2),(3), and I11
{1,2,3}	(5)	$\neg P$	T,(2),(4) and I12

Consistency of premises: _

Consistency

A set of formulas $H_1, H_2, \dots, H_m$ is said to be consistent if their conjunction has the truth value T for some assignment of the truth values to be atomic appearing in $H_1, H_2, \dots, H_m$.

Inconsistency

If for every assignment of the truth values to the atomic variables, at least one of the formulas $H_1, H_2, \dots, H_m$ is false, so that their conjunction is identically false, then the formulas $H_1, H_2, \dots, H_m$ are called inconsistent.

A set of formulas $H_1, H_2, \dots, H_m$ is inconsistent, if their conjunction implies a contradiction, that is $H_1 \wedge H_2 \wedge \dots \wedge H_m \Rightarrow R \wedge \neg R$

Where R is any formula. Note that $R \wedge \neg R$ is a contradiction and it is necessary and sufficient that $H_1, H_2, \dots, H_m$ are inconsistent the formula.

Indirect method of proof

In order to show that a conclusion C follows logically from the premises $H_1, H_2, \dots, H_m$, we assume that C is false and consider $\neg C$ as an additional premise. If the new set of premises is inconsistent, so that they imply a contradiction, then the assumption that $\neg C$ is true does not hold simultaneously with $H_1 \wedge H_2 \wedge \dots \wedge H_m$ being true. Therefore, C is true whenever $H_1 \wedge H_2 \wedge \dots \wedge H_m$ is true. Thus, C follows logically from the premises $H_1, H_2, \dots, H_m$.

Example 8 Show that $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$. Solution.

We introduce $\neg(P \wedge Q)$ as an additional premise and show that this additional premise leads to a contradiction.

{1}	(1) $\neg(P \wedge Q)$	Assumed premise
{1}	(2) $P \wedge Q$	T, (1) and E1
{1}	(3) P	T, (2) and I1

{1}	{4} $\neg(P \wedge Q)$	P
{4}	(5) $\neg P$	T, (4) and I1
{1,4}	(6) $P \wedge \neg P$	T, (3), (5) and I9

Here (6) $P \wedge \neg P$ is a contradiction. Thus $\{1,4\}$ viz. $\neg(P \wedge Q)$ and $\neg(P \wedge \neg P)$ lead to a contradiction $P \wedge \neg P$.

Example 9 Show that the following premises are inconsistent.

1. If Jack misses many classes through illness, then he fails high school.
2. If Jack fails high school, then he is uneducated.
3. If Jack reads a lot of books, then he is not uneducated.
4. Jack misses many classes through illness and reads a lot of books.

Solution.

P: Jack misses many classes. Q:

Jack fails high school.

R: Jack reads a lot of books. S:

Jack is uneducated.

The premises are $P \rightarrow Q, Q \rightarrow S, R \rightarrow \neg S$ and $P \wedge R$

{1}	(1)	$P \rightarrow Q$	P
{2}	(2)	$Q \rightarrow S$	P
{1,2}	(3)	$P \rightarrow S$	T, (1), (2) and I13
{4}	(4)	$R \rightarrow \neg S$	P
{4}	(5)	$S \rightarrow \neg R$	T, (4), and E18
{1,2,4}	(6)	$P \rightarrow \neg R$	T, (3), (5) and I13
{1,2,4}	(7)	$\neg(P \vee \neg R)$	T, (6) and E16
{1,2,4}	(8)	$\neg(P \wedge R)$	T, (7) and E8
{9}	(9)	$P \wedge R$	P
{1,2,4,9}	(10)	$(P \wedge R) \wedge \neg(P \wedge R)$	T, (8), (9) and I9

The rules above can be summed up in the following table. The "Tautology" column shows how to interpret the notation of a given rule.

Rule of inference

Tautology

Name

Addition

Simplification

Conjunction

Modus ponens

Modus tollens

Hypothetical
syllogism

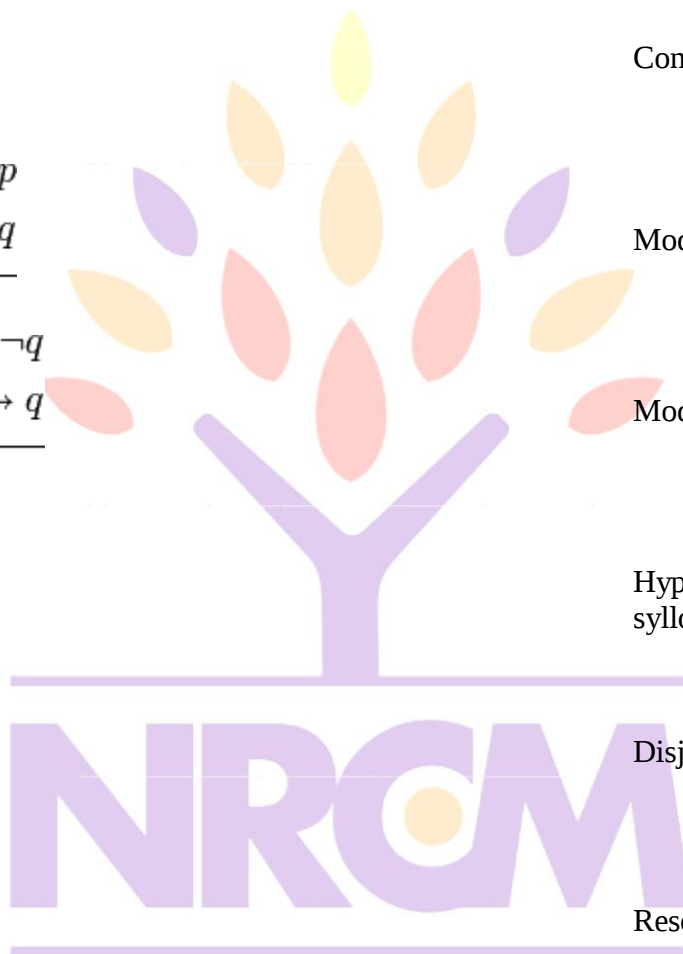
Disjunctive syllogism

Resolution

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$



your roots to success...

Predicative logic:

A predicate or propositional function is a statement containing variables. For instance $\neg x + 2 = 7$, $\neg X \text{ is American}$, $\neg x < y$, $\neg p$ is a prime number are predicates. The truth value of the predicate depends on the value assigned to its variables. For instance if we replace x with 1 in the predicate $\neg x + 2 = 7$ we obtain $\neg 1 + 2 = 7$, which is false, but if we replace it with 5 we get $\neg 5 + 2 = 7$, which is true. We represent a predicate by a letter followed by the variables enclosed between parenthesis: $P(x)$, $Q(x, y)$, etc. An example for $P(x)$ is a value of x for which $P(x)$ is true. A counterexample is a value of x for which $P(x)$ is false. So, 5 is an example for $\neg x + 2 = 7$, while 1 is a counterexample. Each variable in a predicate is assumed to belong to a universe (or domain) of discourse, for instance in the predicate $\neg n$ is an odd integer 'n' represents an integer, so the universe of discourse of n is the set of all integers. In $\neg X \text{ is American}$ we may assume that X is a human being, so in this case the universe of discourse is the set of all human beings.

Free & Bound variables:

Let's now turn to a rather important topic: the distinction between **free variables** and **bound variables**.

Have a look at the following formula:

$$\neg (\text{THERAPIST}(x) \vee \forall x (\text{MORON}(x) \wedge \forall y \text{PERSON}(y)))$$

The first occurrence of x is *free*, whereas the second and third occurrences of x are *bound*, namely by the first occurrence of the quantifier. The first and second occurrences of the variable y are also bound, namely by the second occurrence of the quantifier.

Informally, the concept of a bound variable can be explained as follows: Recall that quantifications are generally of the form:

$$\forall x \phi$$

or

$$\exists x \phi$$

where x may be any variable. Generally, all occurrences of this variable within the quantification are bound. But we have to distinguish two cases. Look at the following formula to see why:

$$\exists x (\text{MAN}(x) \wedge (\forall x \text{WALKS}(x)) \wedge \text{HAPPY}(x))$$

1. x may occur within another, embedded, quantification $\forall x\psi$ or $\exists x\psi$, such as the x in our $\text{WALKS}(x)$ example. Then we say that it is bound by the quantifier of this embedded quantification (and soon, if there's another embedded quantification over x within ψ).
2. Otherwise, we say that it is bound by the top-level quantifier (like all other occurrences of x in our example).

Here's a full formal simultaneous definition of *free* and *bound*:

1. Any occurrence of any variable is free in any atomic formula.
2. No occurrence of any variable is bound in any atomic formula.
3. If an occurrence of any variable is free in ϕ or in ψ , then that same occurrence is free in $\neg\phi$, $(\phi \rightarrow \psi)$, $(\phi \vee \psi)$, and $(\phi \wedge \psi)$.
4. If an occurrence of any variable is bound in ϕ or in ψ , then that same occurrence is bound in $\neg\phi$, $(\phi \rightarrow \psi)$, $(\phi \vee \psi)$, $(\phi \wedge \psi)$. Moreover, that same occurrence is bound in $\forall y\phi$ and $\exists y\phi$ as well, for any choice of variable y .
5. In any formula of the form $\forall y\phi$ or $\exists y\phi$ (where y can be any variable at all in this case) the occurrence of y that immediately follows the initial quantifier symbol is bound.
6. If an occurrence of a variable x is free in ϕ , then that same occurrence is free in $\forall y\phi$ and $\exists y\phi$, for any variable y distinct from x . On the other hand, all occurrences of x that are free in ϕ , are bound in $\forall x\phi$ and in $\exists x\phi$.

If a formula contains no occurrences of free variables we call it a **sentence**.

your roots to success...

Quantifiers

The variable of predicate 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 $\forall$

$\forall x P(x)$ is read as for every value of x , $P(x)$ is true..

Example – "Man is mortal" can be transformed into the propositional form $\forall x P(x)$ 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 $\exists$.

$\exists x P(x)$ is read as for some values of x , $P(x)$ is true.

Example – "Some people are dishonest" can be transformed into the propositional form

$\exists x P(x)$ where $P(x)$ is the predicate which denotes x is dishonest and the universe of discourse is some people.



your roots to success...

UNIT-II

Relations

Syllabus

Introduction, Basic Concepts of Set Theory, Representation of Discrete Structures, Relations, Types of relations, Partial order relation, POSET, External elements in POSET, Lattices, Functions, Types of functions, inverse of functions, invertible functions and Composition of functions

Introduction

The elements of a set may be related to one another. For example, in the set of natural numbers there is the 'less than or equal to' relation between the elements. The elements of one set may also be related to the elements of another set.

Binary Relation

A binary relation between two sets A and B is a rule R which decides, for any elements, whether a is in relation R to b . If so, we write $a R b$.

If a is not in relation R to b , then we shall write $a \not R b$.

We can also consider $a R b$ as the ordered pair (a, b) in which case we can define a binary relation from A to B as a subset of $A \times B$. This subset is denoted by the relation R .

In general, any set of ordered pairs defines a binary relation.

For example, the relation of father to his child is $F = \{(a, b) / a \text{ is the father of } b\}$

In this relation F , the first member is the name of the father and the second is the name of the child.

The definition of relation permits any set of ordered pairs to define a relation.

For example, the set S given by

$$S = \{(1, 2), (3, a), (b, a), (b, \text{Joe})\}$$

Definition

The **domain** of a binary relation S is the set of all first elements of the ordered pairs in the relation. (i.e) $D(S) = \{a / \exists b \text{ for which } (a, b) \in S\}$

The **range** of a binary relation S is the set of all second elements of the ordered pairs in the relation. (i.e) $R(S) = \{b / \exists a \text{ for which } (a, b) \in S\}$.

Forexample

For the relation $S = \{(1,2), (3,a), (b,a), (b, \text{Joe})\}$ $D(S) =$

$\{1, 3, b, b\}$ and

$R(S) = \{2, a, a, \text{Joe}\}$

Let X and Y be any two sets. A subset of the Cartesian product $X * Y$ defines a relation, say C . For any such relation C , we have $D(C) \subseteq X$ and $R(C) \subseteq Y$, and the relation C is said to be from X to Y . If $Y = X$, then C is said to be a relation from X to X . In such case, C is called a relation in X . Thus any relation in X is a subset of $X * X$. The set $X * X$ is called a *universal relation* in X , while the empty set which is also a subset of $X * X$ is called a *void relation* in X .

Forexample

Let L denote the relation—less than or equal to—and D denote the relation

—divides—where $x D y$ means— x divides y . Both L and D are defined on the set $\{1, 2, 3,$

$4\}$

$L = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$D = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$

$L \cap D = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$

$= D$

Properties of Binary Relations:

1. reflexive

Definition: A binary relation R in a set X is **reflexive** if, for every $x \in X$, $x R x$. That is $(x, x) \in R$.

Forexample

- The relation $\leq$ is reflexive in the set of real numbers.
- The set inclusion is reflexive in the family of all subsets of a universal set.
- The relation equality of sets is also reflexive.
- The relation is parallel in the set of lines in a plane.

- The relation of similarity in the set of triangles in a plane is reflexive.

Examples: (i). If $R_1 = \{(1,1), (1,2), (2,2), (2,3), (3,3)\}$ be a relation on $A = \{1,2,3\}$, then R_1 is

- a reflexive relation, since for every $x \in A, (x,x) \in R_1$.

(ii). If $R_2 = \{(1,1), (1,2), (2,3), (3,3)\}$ be a relation on $A = \{1,2,3\}$, then R_2 is not a reflexive relation, since for every $2 \in A, (2,2) \notin R_2$. $\square$

Symmetric

Definition: A relation R in a set X is **symmetric** iff for every x and y in X , whenever $x R y$, then $y R x$.

For example

- The relation of equality of sets is symmetric.
- The relation of similarity in the set of triangles in a plane is symmetric.
- The relation of being a sister is not symmetric in the set of all people.
- However, in the set of females it is symmetric.

Example. If $R_3 = \{(1,1), (1,2), (1,3), (2,2), (2,1), (3,1)\}$ be a relation on $A = \{1,2,3\}$, then R_3 is a symmetric relation.

Transitive

Definition: A relation R in a set X is **transitive** if, for every x, y , and z in X , whenever $x R y$ and $y R z$, then $x R z$.

For example

- The relations $<$ and $>$ are transitive in the set of real numbers
- The relation of similarity in the set of triangles in a plane is transitive.

- **Definition:** A relation R in a set X is **antisymmetric** iff for every x and y in X , whenever $x R y$ and $y R x$, then $x = y$.

Example: If $R = \{(1,2), (2,2), (2,3)\}$ on $A = \{1,2,3\}$ is an antisymmetric relation.

Equivalence Relation:

Definition Type equation here.: A relation R in a set A is called an **equivalence relation** if

- aRa for every i . i.e. R is reflexive
- $aRb \Rightarrow bRa$ for every $a, b \in A$ i.e. R is symmetric
- aRb and $bRc \Rightarrow aRc$ for every $a, b, c \in A$, i.e. R is transitive.

For example

- The relation of equality of numbers on a set of real numbers.
- The relation of being parallel on a set of lines in a plane.

Problem 1: Let us consider the set T of triangles in a plane. Let us define a relation R in T

$$R = \{(a, b) / (a, b \in T \text{ and } a \text{ is similar to } b)\}$$

We have to show that relation R is an equivalence relation

Solution:

- A triangle a is similar to itself. aRa
- If the triangle a is similar to the triangle b , then the triangle b is similar to the triangle a then $aRb \Rightarrow bRa$
- If a is similar to b and b is similar to c , then a is similar to c (i.e.) aRb and $bRc \Rightarrow aRc$.

Hence R is an equivalence relation.

Problem 2: Let $x = \{1, 2, 3, \dots, 7\}$ and $R = \{(x, y) / x - y \text{ is divisible by } 3\}$ Show that

R is an equivalence relation.

Solution: For any $a \in X$, $a - a$ is divisible by 3, Hence a

Ra , R is reflexive

For any $a, b \in X$, if $a - b$ is divisible by 3, then $b - a$ is also divisible by 3,

R is symmetric.

For any $a, b, c \in \mathbb{Z}$, if aRb and bRc , then $a - b$ is divisible by 3 and $b - c$ is divisible by 3. So that $(a - b) + (b - c)$ is also divisible by 3, hence $a - c$ is also divisible by 3. Thus R is transitive.

Hence R is equivalence.

Problem 3. Let Z be the set of all integers. Let m be a fixed integer. Two integers a and b are said to be congruent modulo m if and only if m divides $a - b$, in which case we write $a \equiv b \pmod{m}$. This relation is called the relation of congruence modulo m and we can show that it is an equivalence relation.

Solution:

- $a - a = 0$ and m divides $a - a$ (i.e.) $aRa, (a, a) \in R$, R is reflexive.
- $aRb \Rightarrow m \text{ divides } a - b$

$m \text{ divides } b - a$

$b \equiv a \pmod{m}$

bRa

that is R is symmetric.

- $aRb \text{ and } bRc \Rightarrow a \equiv b \pmod{m} \text{ and } b \equiv c \pmod{m}$
 - $m \text{ divides } a - b \text{ and } m \text{ divides } b - c$
 - $a - b = km \text{ and } b - c = lm \text{ for some } k, l \in \mathbb{Z}$
 - $(a - b) + (b - c) = km + lm$
 - $a - c = (k + l)m$
 - $a \equiv c \pmod{m}$
 - aRc
 - R is transitive

Hence the congruence relation is an equivalence relation.

Equivalence Classes:

Let R be an equivalence relation on a set A . For any $a \in A$, the **equivalence class** generated by a is the set of all elements $b \in A$ such that $a R b$ and is denoted $[a]$. It is also called the R -equivalence class and denoted by $a \in A$.

$$\text{i.e., } [a] = \{b \in A / b R a\}$$

Let Z be the set of integers and R be the relation called —congruence modulo 3 defined by $R = \{(x, y) / x \in Z \text{ and } y \in Z, (x-y) \text{ is divisible by } 3\}$

Then the equivalence classes are

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\}$$

$$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Composition of binary relations:

Definition: Let R be a relation from X to Y and S be a relation from Y to Z . Then the relation $R \circ S$ is a relation from X to Z given by $R \circ S = \{(x, z) / x \in X, z \in Z, \exists y \in Y \text{ such that } (x, y) \in R \text{ and } (y, z) \in S\}$ is called the composite relation of R and S .

The operation of obtaining $R \circ S$ is called the **composition of relations**.

Example: Let $R = \{(1, 2), (3, 4), (2, 2)\}$ and

$$S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$$

$$\text{Then } R \circ S = \{(1, 5), (3, 2), (2, 5)\} \text{ and } S \circ R = \{(4, 2), (3, 2), (1, 4)\}$$

It is to be noted that $R \circ S \neq S \circ R$.

$$\text{Also } R \circ (S \circ T) = (R \circ S) \circ T = R \circ S \circ T$$

Note: We write $R \circ R$ as R^2 ; $R \circ R \circ R$ as R^3 and so on.

Definition

Let R be a relation from X to Y , a relation R from Y to X is called the **converse** of R , where the ordered pairs of $\check{R}$ are obtained by interchanging the numbers in each of the ordered pairs of R . This means for $x \in X$ and $y \in Y$, that $x R y$ if and only if $y \check{R} x$.

Then the relation $\check{R}$ is given by $\check{R} = \{(x, y) / (y, x) \in R\}$ is called the **converse** of R

Example:

Let $R = \{(1, 2), (3, 4), (2, 2)\}$

Then $\check{R} = \{(2, 1), (4, 3), (2, 2)\}$

Note: If R is an equivalence relation, then $\check{R}$ is also an equivalence relation.



your roots to success...

Partial Ordering Relations:

Definition

A binary relation R in a set P is called a *partial order relation* or a *partial ordering* in P if R is reflexive, antisymmetric, and transitive. i.e.,

- aRa for all $a \in P$
- aRb and $bRa \rightarrow a=b$
- aRb and $bRc \rightarrow aRc$

A set P together with a partial ordering R is called a *partial ordered set* or a *poset*. The relation R is often denoted by the symbol $\leq$ which is different from the usual less than or equal to symbol. Thus, if $\leq$ is a partial order in P , then the ordered pair $(P, \leq)$ is called a poset.

Example: Show that the relation "greater than or equal to" is a partial ordering on the set of integers.

Solution: Let Z be the set of all integers and the relation $R = \geq$

(i). Since $a \geq a$ for every integer a , the relation $\geq$ is reflexive.

(ii). Let a and b be any two integers. Let

aRb and $bRa \rightarrow a \geq b$ and $b \geq a$

$\rightarrow a = b$

$\therefore$ The relation $\geq$ is antisymmetric.

(iii). Let a, b and c be any three integers. Let

aRb and $bRc \rightarrow a \geq b$ and $b \geq c$

$\rightarrow a \geq c$

$\therefore$ The relation $\geq$ is transitive.

$\rightarrow a \geq c$

$\therefore$ The relation $\geq$ is transitive.

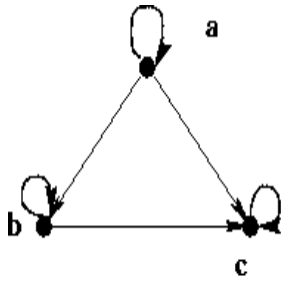
Since the relation $\geq$ is reflexive, antisymmetric and transitive, $\geq$ is a partial ordering on the set of integers. Therefore, $(Z, \geq)$ is a poset.

your roots to success...

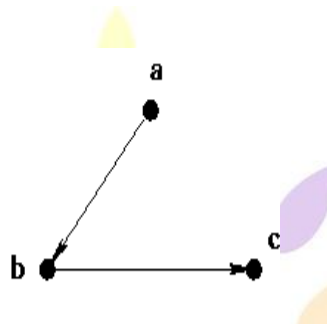
HasseDiagram:

A Hasse diagram is a digraph for a poset which does not have loops and arcs implied by the transitivity.

Example 10: For the relation $\{ \langle a, a \rangle, \langle a, b \rangle, \langle a, c \rangle, \langle b, b \rangle, \langle b, c \rangle, \langle c, c \rangle \}$ on set $\{a, b, c\}$, the Hasse diagram has the arcs $\{ \langle a, b \rangle, \langle b, c \rangle \}$ as shown below.



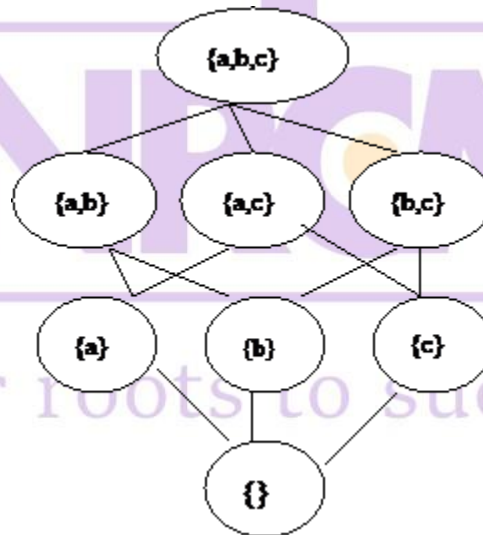
Digraph for Partial Order



Hasse Diagram

Ex: Let A be a given finite set and $r(A)$ its powerset. Let $\hat{r}$ be the subset relation on the elements of $r(A)$.

Draw Hasse diagram of $(r(A), \hat{r})$ for $A = \{a, b, c\}$

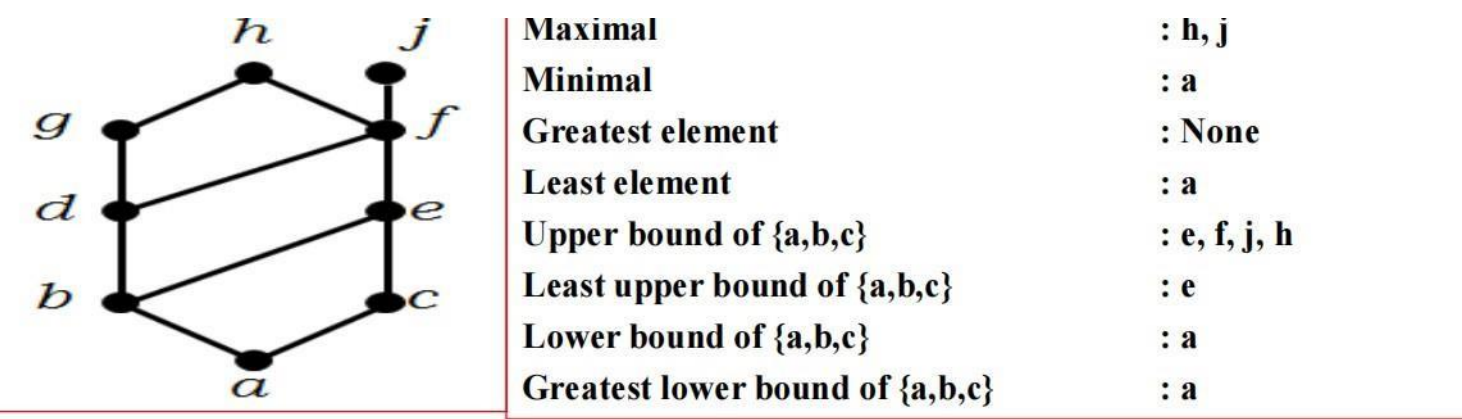


Qn.From the Hasse diagram, find the maximal, Minimal, Greatest element, Least element, Upper bound, Least upper bound, Lower bound and Greatest lower bound of $\{\square,\square,\square\}$

order to qualify as a function.

The first condition is that every $a \in A$ must be related to some $b \in B$, (i.e) the domain of f must be A and not merely subset of A . The second requirement of uniqueness can be expressed as $(a, b) \in f \wedge (b, c) \in f \Rightarrow b = c$

Intuitively, a function from a set A to a set B is a rule which assigns to every element of A , a



Functions:

Introduction

A function is a special type of relation. It may be consred as a relation in which each elementof the domain belongsto only one ordered pairin the relation.Thus a function from A to B is a subset of $A \times B$ having the propertythatfor each $a \in A$, there is one and onlyone $b \in B$ such that $(a, b) \hat{=} G$.

Definition

Let A and B be any two sets. A relation f from A to B is calleda functionif for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$.

Notethatthedefinitionoffunctionrequires thatarelationmustsatisfytwo additional conditions in

unique element of B . If $a \in A$, then the unique element of B assigned to a under f is denoted by $f(a)$. The usual notation for a function f from A to B is $f: A \rightarrow B$ defined by $a \mapsto f(a)$ where $a \in A$, $f(a)$ is called the image of a under f and a is called pre image of $f(a)$.

- Let $X=Y=\mathbb{R}$ and $f(x) = x^2 + 2$. $D(f)=\mathbb{R}$ and $R(f) \subseteq \mathbb{R}$.
- Let X be the set of all statements in logic and let $Y = \{\text{True}, \text{False}\}$.

A mapping $f: X \rightarrow Y$ is a function.

- A program written in high level language is mapped into a machine language by a compiler. Similarly, the output from a compiler is a function of its input.
- Let $X=Y=\mathbb{R}$ and $f(x) = x^2$ is a function from $X \rightarrow Y$, and $g(x^2) = x$ is not a function from $X \rightarrow Y$.

A mapping $f: A \rightarrow B$ is called **one-to-one** (injective or 1-1) if distinct elements of A are mapped into distinct elements of B . (i.e) f is one-to-one if

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2) \text{ or equivalently } f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

Forexample, $f: \mathbb{N} \rightarrow \mathbb{N}$ given by $f(x) = x$ is 1-1 where $\mathbb{N}$ is the set of natural numbers.

A mapping $f: A \rightarrow B$ is called **onto** (surjective) if for every $b \in B$ there is an $a \in A$ such that $f(a) = b$. i.e. if every element of B has a pre-image in A . Otherwise it is called **into**.

Forexample, $f: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $f(x) = x + 1$ is an onto mapping. A mapping is both 1-1 and onto is called bijective.

Forexample $f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x + 1$ is bijective.

Definition: A mapping $f: \mathbb{R} \rightarrow \mathbb{R}$ is called a **constant mapping** if, for all $a \in \mathbb{R}$, $f(a) = b$, a fixed element.

Forexample $f: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $f(x) = 0$, for all $x \in \mathbb{Z}$ is a constant mapping.

Definition

A mapping $f: A \rightarrow A$ is called the **identity mapping** of A if $f(a) = a$, for all $a \in A$. Usually it is denoted by I_A or simply I .

Composition of functions:

If $f: A \rightarrow B$ and $g: B \rightarrow C$ are two functions, then the composition of functions f and g , denoted by $g \circ f$, is the function is given by $g \circ f: A \rightarrow C$ and is given by

$g \circ f = \{(a, c) / a \in A \wedge c \in C \wedge b \in B : f(a) = b \wedge g(b) = c\}$ and $(g \circ f)(a) = (g(f(a)))$

Example 1: Consider the sets $A = \{1, 2, 3\}$, $B = \{a, b\}$ and $C = \{x, y\}$.

Let $f: A \rightarrow B$ be defined by $f(1) = a$; $f(2) = b$ and $f(3) = b$ and Let $g:$

$B \rightarrow C$ be defined by $g(a) = x$ and $g(b) = y$

(i.e) $f = \{(1, a), (2, b), (3, b)\}$ and $g = \{(a, x), (b, y)\}$.

Then $g \circ f: A \rightarrow C$ is defined by

$$(g \circ f)(1) = g(f(1)) = g(a) = x$$

$$(g \circ f)(2) = g(f(2)) = g(b) = y$$

$$(g \circ f)(3) = g(f(3)) = g(b) = y \text{ i.e., } g \circ f$$

$$f = \{(1, x), (2, y), (3, y)\}$$

If $f: A \rightarrow A$ and $g: A \rightarrow A$, where $A = \{1, 2, 3\}$, are given by

$$f = \{(1, 2), (2, 3), (3, 1)\} \quad \text{and} \quad g = \{(1, 3), (2, 2), (3, 1)\}$$

Then $g \circ f = \{(1, 2), (2, 1), (3, 3)\}$, $f \circ g = \{(1, 1), (2, 3), (3, 2)\}$

$$f \circ f = \{(1, 3), (2, 1), (3, 2)\} \text{ and } g \circ g = \{(1, 1), (2, 2), (3, 3)\}$$

Example 2: Let $f(x) = x+2$, $g(x) = x - 2$ and $h(x) = 3x$ for $x \in \mathbb{R}$, where $\mathbb{R}$ is the set of real numbers.

$$f \circ g = \{(x, x+4) / x \in \mathbb{R}\}$$

$$g \circ f = \{(x, x) / x \in \mathbb{R}\}$$

$$g \circ f = \{(x, x) / x \in \mathbb{R}\}$$

$$g \circ g = \{(x, x-4) / x \in \mathbb{R}\}$$

$$h \circ g = \{(x, 3x-6) / x \in \mathbb{R}\}$$

$$f = \{(x, 3x+6) / x \in \mathbb{R}\}$$

Inverse functions:

Let $f: A \rightarrow B$ be a one-to-one and onto mapping. Then, its inverse, denoted by f^{-1} is given by $f^{-1} = \{(b, a) / (a, b) \in f\}$. Clearly $f^{-1}: B \rightarrow A$ is one-to-one and onto.

Also we observe that $f \circ f^{-1} = I_B$ and $f^{-1} \circ f = I_A$. If f^{-1} exists then f is called **invertible**.

For example: Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x+2$. Then f^{-1}

$f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f^{-1}(x) = x - 2$



your roots to success...

Theorem: Let $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ be one-to-one and onto functions. Then $g \circ f$ is also one-to-one and onto function.

Proof

Let $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ be one-to-one and onto functions. Let $x_1, x_2 \in X$

- $g \circ f(x_1) = g \circ f(x_2)$,
- $g(f(x_1)) = g(f(x_2))$,
- $g(x_1) = g(x_2)$ since f is 1-1

$x_1 = x_2$ since $[g \circ f \text{ is 1-1}]$
so that $g \circ f$ is 1-1.

By the definition of composition, $g \circ f: X \rightarrow Z$ is a function.

We have to prove that every element $z \in Z$ is an image element for some $x \in X$ under $g \circ f$.

Since g is onto $\exists y \in Y: g(y) = z$ and f is onto from X to Y ,
 $\exists x \in X: f(x) = y$.

Now, $g \circ f(x) = g(f(x))$
 $= g(y)$ [since $f(x) = y$]
 $= z$ [since $g(y) = z$]
which shows that $g \circ f$ is onto.

Theorem $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

(i.e) the inverse of a composite function can be expressed in terms of the composition of the inverses in the reverse order.

Proof.

$f: A \rightarrow B$ is one-to-one and onto.

$g: B \rightarrow C$ is one-to-one and onto.

$g \circ f: A \rightarrow C$ is also one-to-one and

onto. $(g \circ f)^{-1}: C \rightarrow A$ is one-to-one and onto.

Let $a \in A$, then there exists an element $b \in B$ such that $f(a) = b$ $\exists a = f^{-1}(b)$. Now $b \in B$ there exists an element $c \in C$ such that $g(b) = c$ $\exists b = g^{-1}(c)$. Then $(g \circ f)(a) = g[f(a)] = g(b) = c$ $\exists a = (g \circ f)^{-1}(c)$ (1)
 $(f^{-1} \circ g^{-1})(c) = f^{-1}(g^{-1}(c)) = f^{-1}(b) = a$ $\exists a = (f^{-1} \circ g^{-1})(c)$ (2)

Combining (1) and (2), we have

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Theorem: If $f: A \rightarrow B$ is an invertible mapping, then $f \circ f^{-1}$

$$= I_B \text{ and } f^{-1} \circ f = I_A$$

Proof: f is invertible, then f^{-1} is defined by $f(a) = b \Rightarrow f^{-1}(b) = a$

where $a \in A$ and $b \in B$.

Now we have to prove that $f \circ f^{-1} = I_B$.

Let $b \in B$ and $f^{-1}(b) = a, a \in A$

$$\begin{aligned} \text{then } f \circ f^{-1}(b) &= f(f^{-1}(b)) \\ &= f(a) = b \end{aligned}$$

$$\text{therefore } f \circ f^{-1}(b) = b \quad \forall b \in B \Rightarrow f \circ f^{-1} = I_B$$

$$\text{Now } f^{-1} \circ f(a) = f^{-1}(f(a)) = f^{-1}(b) = a \text{ therefore } f^{-1} \circ f = I_A$$

$$f(a) = a \quad \forall a \in A \Rightarrow f^{-1} \circ f = I_A.$$

Lattice and its Properties:

Introduction:

A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

The glb of a subset, $\{a, b\} \in L$ will be denoted by $a * b$ and the lub by $a \vee b$.

Usually, for any pair $a, b \in L$, $GLB\{a, b\} = a * b$, is called the **meet** or **product** and $LUB\{a, b\} = a \vee b$, is called the **join** or **sum** of a and b .

Example 1 Consider a non-empty set S and let $P(S)$ be its powerset. The relation $\subseteq$ —contained in—is a partial ordering on $P(S)$. For any two subsets $A, B \in P(S)$

$GLB\{A, B\}$ and $LUB\{A, B\}$ are evidently $A \cap B$ and $A \cup B$ respectively.

A lattice can be conveniently represented by a diagram.

For example, let S be the set of all divisors of n , where n is a positive integer. Let D denote the relation—division—such that for any $a, b \in S$, $a \leq b$ if and only if a divides b .

Two lattices can have the same diagram. For example if $S = \{1, 2, 3\}$ then $(p(s), \hat{I})$ and (S_6, D) have the same diagram viz. fig(1), but the nodes are differently labeled.

Any statement about lattices involving the operations $\wedge$ and $\vee$ and the relations $\leq$ and $\equiv$ remains true if $\wedge$, $\vee$, $\leq$ and $\equiv$ are replaced by $\vee$, $\wedge$, $\leq$ and $\equiv$ respectively.

Properties of lattices:

- $a * a = a$ $a \mathbin{\mathbb{A}} a = a$ (Idempotent)
- $a * b = b * a$, $a \mathbin{\mathbb{A}} b = b \mathbin{\mathbb{A}} a$ (Commutative)
- $(a * b) * c = a * (b * c)$, $(a \mathbin{\mathbb{A}} b) \mathbin{\mathbb{A}} c = a \mathbin{\mathbb{A}} (b \mathbin{\mathbb{A}} c)$

o(Associative)

- $a^*(a \wedge b) = a$, $a \wedge (a^*b) = a$ (absorption)

For any $a \in L$, $a \in a$, $a \in \text{LUB}\{a, b\} \Rightarrow a \in a^*(a \wedge b)$. On the other hand, $\text{GLB}\{a, a \wedge b\} \in a$ i.e., $(a \wedge b) \wedge a$, hence $a^*(a \wedge b) = a$

Theorem 1

Let $(L, \leq)$ be a lattice with the binary operations $*$ and $\wedge$ denote the operations of meet and join respectively. For any $a, b \in L$,

$$a \leq b \iff a^*b = a \iff a \wedge b = b$$

Proof

Suppose that $a \leq b$. We know that $a \in a$, $a \in \text{GLB}\{a, b\}$, i.e., $a \in a^*b$. But from the definition of a^*b , we get $a^*b \in a$.

$$\text{Hence } a \in b \Rightarrow a^*b = a \dots \dots \dots (1)$$

Now we assume that $a^*b = a$; but is possible only if $a \leq b$, that is $a^*b = a \Rightarrow a \leq b \dots \dots \dots (2)$

From (1) and (2), we get $a \leq b \iff a^*b = a$.

Suppose $a^*b = a$.

$$\text{then } b \wedge (a^*b) = b \wedge a = a \wedge b \dots \dots \dots (3)$$

$$\text{but } b \wedge (a^*b) = b \text{ (by iv)} \dots \dots \dots (4)$$

Hence $a \wedge b = b$, from (3) $\Rightarrow$ (4)

Suppose $a \wedge b = b$, i.e., $\text{LUB}\{a, b\} = b$, this is possible only if $a \leq b$, thus (3) $\Rightarrow$ (1)

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). Hence these are equivalent.

Let us assume $a^*b = a$.

Now $(a^*b) \wedge b = a \wedge b$

We know that by absorption law, $(a^*b) \wedge b = b$

$$\text{so that } a \wedge b = b, \text{ therefore } a^*b = a \text{ } \exists a \wedge b = b \dots \dots \dots (5)$$

$$\text{similarly, we can prove } a \wedge b = b \text{ } \exists a^*b = a \dots \dots \dots (6)$$

From (5) and (6), we get

$a * b = a \hat{\cup} a \hat{\cap} b = b$ Hence the theorem.

Theorem 2 For any $a, b, c \in L$, where $(L, \leq)$ is a lattice. $b \leq c$

$$\Rightarrow \{a * b \leq a * c \quad \text{and} \quad a \hat{\cap} b \leq a \hat{\cap} c\}$$

Proof Suppose $b \leq c$. we have proved that $b \hat{\cap} a \hat{\cap} b * c = b \dots \dots \dots (1)$

Now consider

$$\begin{aligned} (a * b) * (a * c) &= (a * a) * (b * c) && \text{(by Idempotent)} \\ &= a * (b * c) \\ &= a * b && \text{(by (1))} \end{aligned}$$

Thus $(a * b) * (a * c) = a * b$ which $\Rightarrow (a * b) \leq (a * c)$

$$\begin{aligned} \text{Similarly } (a \hat{\cap} b) \hat{\cap} (a \hat{\cap} c) &= (a \hat{\cap} a) \hat{\cap} (b \hat{\cap} c) \\ &= a \hat{\cap} (b \hat{\cap} c) \\ &= a \hat{\cap} c \end{aligned}$$

which $\Rightarrow (a \hat{\cap} b) \leq (a \hat{\cap} c)$

note: These properties are known as **isotonicity**.



your roots to success...

Unit III:

Algebraic Structures

Syllabus:

Algebraic structures: Algebraic systems with examples and general properties, semigroups and monoids, groups & its types, Introduction to homomorphism and Isomorphism (Proof of theorems are not required)

Algebraic systems

$N = \{1, 2, 3, 4, \dots\}$ = Set of all natural numbers.

$Z = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$ = Set of all integers. **Q = Set of all rational numbers.**

R = Set of all real numbers.

Binary Operation: The binary operator $*$ is said to be a binary operation (closed operation) on a non-empty set A , if $a * b \in A$ for all $a, b \in A$ (Closure property).

Ex: The set N is closed with respect to addition and multiplication but not w.r.t subtraction and division.

Algebraic System: A set A with one or more binary (closed) operations defined on it is called an algebraic system.

Ex: $(N, +)$, $(Z, +, -)$, $(R, +, \cdot, -)$ are algebraic systems.

Properties

Associativity: Let $*$ be a binary operation on a set A . The operation $*$ is said to be associative in A .

if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$

Identity: For an algebraic system $(A, *)$, an element e in A is said to be an identity element of A if $a * e = e * a = a$ for all $a \in A$.

Note: For an algebraic system $(A, *)$, the identity element, if it exists, is unique.

Inverse: Let $(A, *)$ be an algebraic system with identity e . Let a be an element in A . An element b is said to be inverse of a .

$$if a * b = b * a = e$$

Semigroups

SemiGroup: An algebraic system $(A, *)$ is said to be a semigroup if

1. $*$ is a closed operation on A .
2. $*$ is an associative operation, for all a, b, c in

A. Ex. $(\mathbb{N}, +)$ is a semigroup.

Ex. $(\mathbb{N}, \cdot)$ is a semigroup.

Ex. $(\mathbb{N}, -)$ is not a semigroup.

Monoid

An algebraic system $(A, *)$ is said to be a **monoid** if the following conditions are satisfied.

- 1) $*$ is a closed operation in A .
- 2) $*$ is an associative operation in A .
- 3) There is an identity in A .

Ex. Show that the set N is a monoid with respect to

multiplication. Solution: Here, $N = \{1, 2, 3, 4, \dots\}$

Closure property: We know that the product of two natural numbers is again a natural number.

i.e., $a \cdot b = b \cdot a$ for all $a, b \in N$

$\therefore$ Multiplication is a closed operation.

Associativity: Multiplication of natural numbers is associative.

i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in N$ Identity:

We have, $1 \in N$ such that

$a \cdot 1 = 1 \cdot a = a$ for all $a \in N$.

$\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication

Examples

Ex. Let $(\mathbb{Z}, *)$ be an algebraic structure, where $\mathbb{Z}$ is the set of integers

and the operation $*$ is defined by $n * m = \max(n, m)$.

Show that $(\mathbb{Z}, *)$ is a semigroup. Is $(\mathbb{Z}, *)$ a monoid? Justify your answer.

Solution: Let a, b and c be any three integers.

Closure property: Now, $a * b = \max(a, b) \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$

Associativity: $(a * b) * c = \max\{a, b, c\} = a * (b * c)$

$\therefore (\mathbb{Z}, *)$ is a semigroup.

Identity: There is no integer x such that

$$a * x = \max(a, x) = a \quad \text{for all } a \in \mathbb{Z}$$

$\therefore$ Identity element does not exist. Hence, $(\mathbb{Z}, *)$ is not a monoid.

Ex. Show that the set of all strings S is a monoid under the operation concatenation of strings.

Is S a group w.r. to the above operation? Justify your answer.

Solution: Let us denote the operation

concatenation of strings by $+$.

Let s_1, s_2, s_3 be three arbitrary strings in S .

Closure property: Concatenation of two strings is again a string, i.e., $s_1 + s_2 \in S$

Associativity: Concatenation of strings is associative. $(s_1 +$

$$s_2) + s_3 = s_1 + (s_2 + s_3)$$

Identity: We have a null string, $l \in S$ such that $s_1 + l = s_1$.

$\therefore S$ is a monoid.

Note: S is not a group, because the inverse of a nonempty string does not exist under concatenation of strings.

Groups

Group: An algebraic system $(G, *)$ is said to be a **group** if the following conditions are satisfied.

- 1) $*$ is a closed operation.
- 2) $*$ is an associative operation.
- 3) There is an identity in G .
- 4) Every element in G has an inverse in G .

Abelian group (Commutative group): A group $(G, *)$ is said to be **abelian** (or **commutative**) if

$$a * b = b * a \quad \text{for all } a, b \in G.$$

Properties

In a group $(G, *)$ the following properties hold good

1. Identity element is unique.
2. Inverse of an element is unique.
3. Cancellation laws hold good

$a*b = a*c \Rightarrow b=c$ (left cancellation law)

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

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

In a group, the identity element is its own inverse.

Order of a group: The number of elements in a group is called order of the group. Finite group: If the order of a group G is finite, then G is called a finite group.

Ex1. Show that, the set of all integers is an abelian group with respect to addition.

Solution: Let Z = set of all integers.

Let a, b, c be any three elements of Z .

1. Closure property: We know that, Sum of two integers is again an integer. i.e., $a + b \in Z$ for all $a, b \in Z$
2. Associativity: We know that addition of integers is

associative. i.e., $(a+b)+c=a+(b+c)$ for all $a, b, c \in \mathbb{Z}$.

3. Identity: We have $0 \in \mathbb{Z}$ and $a+0=a$ for all $a \in \mathbb{Z}$.

$\therefore$ Identity element exists, and 0 is the identity element.

4. Inverse: To each $a \in \mathbb{Z}$, we have $-a \in \mathbb{Z}$ such that

$$a+(-a)=0$$

Each element in $\mathbb{Z}$ has an inverse.

5. Commutativity: We know that addition of integers is

commutative. i.e., $a + b = b + a$ for all $a, b \in \mathbb{Z}$.

Hence, $(\mathbb{Z}, +)$ is an abelian group.

Ex2. Show that set of all non zero real numbers is a group with respect to multiplication.

Solution: Let $\mathbb{R}^*$ = set of all non zero real numbers.

Let a, b, c are any three elements of $\mathbb{R}^*$.

1. Closure property: We know that, product of two non zero real numbers is again a non zero real number.

i.e., $a.b \in \mathbb{R}^*$ for all $a, b \in \mathbb{R}^*$.

2. Associativity: We know that multiplication of real numbers is

associative.

i.e., $(a.b).c = a.(b.c)$ for all $a, b, c \in \mathbb{R}^*$.

3. Identity: We have $1 \in \mathbb{R}^*$ and $a.1 = a$ for all $a \in \mathbb{R}^*$.

$\therefore$ Identity element exists, and 1 is the identity element.

4. Inverse: To each $a \in \mathbb{R}^*$, we have $1/a \in \mathbb{R}^*$ such that $a.(1/a) = 1$. i.e., Each element in $\mathbb{R}^*$ has an inverse.

5. Commutativity: We know that multiplication of real numbers is commutative.

i.e., $a . b = b . a$ for all $a, b \in \mathbb{R}^*$.

Hence, $(\mathbb{R}^*, \cdot)$ is an abelian group.

Note: Show that set of all real numbers $\mathbb{R}$ is not a group with respect to multiplication.

Solution: We have $0 \in \mathbb{R}$.

The multiplicative inverse of 0 does not exist.

Hence, $\mathbb{R}$ is not a group.

Example: Let S be a finite set, and let $F(S)$ be the collection of all functions $f: S \rightarrow S$ under the operation of composition of functions, then show that $F(S)$ is a monoid.

Is S a group w.r.t. the above operation? Justify your answer.

Solution: Let f_1, f_2, f_3 be three arbitrary functions on S .

Closure property: Composition of two functions on S is again a function on S .

i.e., $f_1 \circ f_2 \in F(S)$

Associativity: Composition of functions is associative.

i.e., $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$ Identity:

We have identity function $I: S \rightarrow S$

such that $f \circ I = f$.

$\therefore F(S)$ is a monoid.

Note: $F(S)$ is not a group, because the inverse of an bijective function on S does not exist.

Ex. If M is the set of all nonsingular matrices of order $n \times n$. then show that M is a group w.r.t. matrix multiplication. Is $(M, *)$ an abelian group? Justify your answer.

Solution: Let $A, B, C \in M$.

1. Closure property: Product of two non-singular matrices is again a non-singular matrix, because $|\square \square| = |\square| |\square| \neq 0$ (Since, A and B are non-singular)

i.e., $AB \in M$ for all $A, B \in M$.

2. Associativity: Matrix multiplication is associative.

i.e., $(AB)C = A(BC)$ for all $A, B, C \in M$.

3. Identity: We have $I_n \in M$ and $AI_n = A$ for all $A \in M$.

$\therefore$ Identity element exists, and I_n is the identity element.

4. Inverse: To each $A \in M$, we have $A^{-1} \in M$ such that AA^{-1}

$= I_n$

i.e., Each element in M has an inverse.

$\therefore M$ is a group w.r.t. matrix multiplication.

We know that, matrix multiplication is not commutative. Hence, M is not an abelian group.

Ex. Show that the set of all positive rational numbers forms an abelian group under the composition $*$ defined by

$$a * b = (ab)/2.$$

Solution: Let A = set of all positive rational numbers.

Let a, b, c be any three elements of A .

1. Closure property: We know that, Product of two positive rational numbers is again a rational number.

$$\text{i.e., } a * b \in A \text{ for all } a, b \in A.$$

2. Associativity: $(a * b) * c = (ab/2) * c = (abc)/4$

$$a * (b * c) = a * (bc/2) = (abc)/4$$

3. Identity: Let e be the identity element.

We have $a * e = (ae)/2 \dots (1)$, By the definition of a again, $a * e = a$

$\dots (2)$, Since e is the identity.

$$\text{From (1) and (2), } (ae)/2 = a \Rightarrow e = 2 \text{ and } 2 \in A$$

$\therefore$ Identity element exists, and 2 is the identity element in A .

4. Inverse: Let $a \in A$ let us suppose b is inverse of a

Now, $a * b = (ab)/2 \dots (1)$ (By definition of inverse.)

Again, $a * b = e = 2 \dots (2)$ (By definition of inverse) From

(1) and (2), it follows that $(ab)/2 = 2$

$$\Rightarrow b = (4/a) \in A$$

$\therefore (A, *)$ is a group.

Commutativity: $a * b = (ab)/2 = (ba)/2 = b * a$

Hence, $(A, *)$ is an abelian group.

Finite groups

Ex. Show that $G = \{1, -1\}$ is an abelian group under multiplication.

Solution: The composition table of G is

*	1	-1
1	1	-1
-1	-1	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.
2. Associativity: The elements of G are real numbers, and we know that multiplication of real numbers is associative.
3. Identity: Here, 1 is the identity element and $1 \in G$.
4. Inverse: From the composition table, we see that the inverse elements of 1 and -1 are 1 and -1 respectively.

Hence, G is a group w.r.t multiplication.

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

Hence, G is an abelian group w.r.t. multiplication..

Ex. Show that $G = \{1, w, w^2\}$ is an abelian group under multiplication.

Where $1, w, w^2$ are cube roots of unity.

Solution: The composition table of G is

*	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

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

2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.

3. Identity: Here, 1 is the identity element and $1 \in G$.

4. Inverse: From the composition table, we see that the inverse elements of $1, w, w^2$ are $1, w^2, w$ respectively.

Hence, G is a group w.r.t. multiplication.

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

Hence, G is an abelian group w.r.t. multiplication.

Modulo systems

Addition modulo $(+_m)$

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

$$a +_m b = a + b \quad \text{if } a + b < m$$

$$a +_m b = r \quad \text{if } a + b > m \text{ where } r \text{ is the remainder obtained by dividing } (a+b) \text{ with } m.$$

Multiplication modulo $(*_m)$

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

$$a *_m b = ab \quad \text{if } ab < p$$

$$a *_m b = r \quad \text{if } ab \geq p \text{ where } r \text{ is the remainder obtained}$$

by dividing (ab) with p .

$$\text{Ex. } 3 *_5 4 = 2, \quad 5 *_5 4 = 0, \quad 2 *_5 2 = 4$$

Example: The set $G = \{0, 1, 2, 3, 4, 5\}$ is a group with respect to addition modulo 6.

Solution: The composition table of G is

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

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

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

$$\text{for ex. } (2+_63)+_64 = 5+_64 = 3 \quad \text{and}$$

$$2+_6(3+_64) = 2+_61 = 3$$

3. Identity: Here, The first row of the table coincides with the top row. The element heading that row, i.e., 0 is the identity element.

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

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

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

Example: The set $G = \{1, 2, 3, 4, 5, 6\}$ is a group with respect to multiplication modulo 7.

Solution: The composition table of G is

$*_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $*_7$.

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

$$\text{for ex. } (2 *_7 3) *_7 4 = 6 *_7 4 = 3 \quad \text{and}$$

$$2 *_7 (3 *_7 4) = 2 *_7 5 = 3$$

3. Identity: Here, The first row of the table coincides with the top row. The element heading that row, i.e., 1 is the identity element.

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

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

Hence, $(G, *_7)$ is an abelian group. More on

finite groups

In a group with 2 elements, each element is its own inverse

In a group of even order there will be at least one element (other than identity element) which is its own inverse. The

set $G = \{0, 1, 2, 3, 4, \dots, m-1\}$ is a group with respect to addition modulo m .

The set $G = \{1, 2, 3, 4, \dots, p-1\}$ is a group with respect to multiplication modulo p , where p is a prime number.

Subgroups

Def. A non-empty subset H of a group $(G, *)$ is a subgroup of G ,

if $(H, *)$ is a group.

Note: For any group $(G, *)$, $\{e, *\}$ and $(G, *)$ are trivial subgroups.

Ex. $G = \{1, -1, i, -i\}$ is a group w.r.t. multiplication.

$H_1 = \{1, -1\}$ is a subgroup of G . $H_2 = \{1\}$ is a trivial subgroup of G .

Ex. $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are subgroups of the group $(\mathbb{R}, +)$. Theorem: A non-empty subset H of a group

$(G, *)$ is a subgroup of G iff

$$i) \quad a * b \in H \quad \forall a, b \in H$$

$$ii) \quad a^{-1} \in H \quad \forall a \in H$$

Homomorphism and Isomorphism

Homomorphism: Consider the groups $(G, *)$ and $(G^1, \oplus)$

A function $f: G \rightarrow G^1$ is called a homomorphism iff $f(a * b) = f(a) \oplus f(b)$

Isomorphism: If a homomorphism $f: G \rightarrow G^1$ is a bijection then f is called an isomorphism between G and G^1 .

Then we write $G \cong G^1$

Example: Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f: R \rightarrow R^+$ defined by $f(x) = 2^x$ for all $x \in R$ is an isomorphism.

Solution: First, let us show that f is a homomorphism. Let $a, b \in R$. Now,

$$f(a+b) = 2^{a+b}$$

$$= 2^a 2^b$$

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

$\therefore f$ is a homomorphism.

Next, let us prove that f is a Bijection. For

any $a, b \in R$, Let, $f(a) = f(b)$

$$\Rightarrow 2^a = 2^b$$

$$\Rightarrow a = b$$

$\therefore f$ is one-to-one.

Next, take any $c \in R^+$.

Then $\log_2 c \in R$ and $f(\log_2 c) = 2^{\log_2 c} = c$

.

$\Rightarrow$ Every element in R^+ has a preimage in R . i.e., f is onto.

$\therefore f$ is a bijection.

Hence, f is an isomorphism.

Ex. Let R be a group of all real numbers under addition and R^+ be a group of all positive real

Numbers under multiplication. Show that the mapping $f: R \rightarrow R^+$ defined by $f(x) = \log_{10} x$ for all $x \in R$ is an isomorphism.

Solution: First, let us show that f is a homomorphism. Let a, b

$\in R^+$.

Now, $f(a \cdot b) = \log_{10}(a \cdot b)$

$$= \log_{10} a + \log_{10} b$$

$$= f(a) + f(b)$$

$\therefore f$ is a homomorphism.

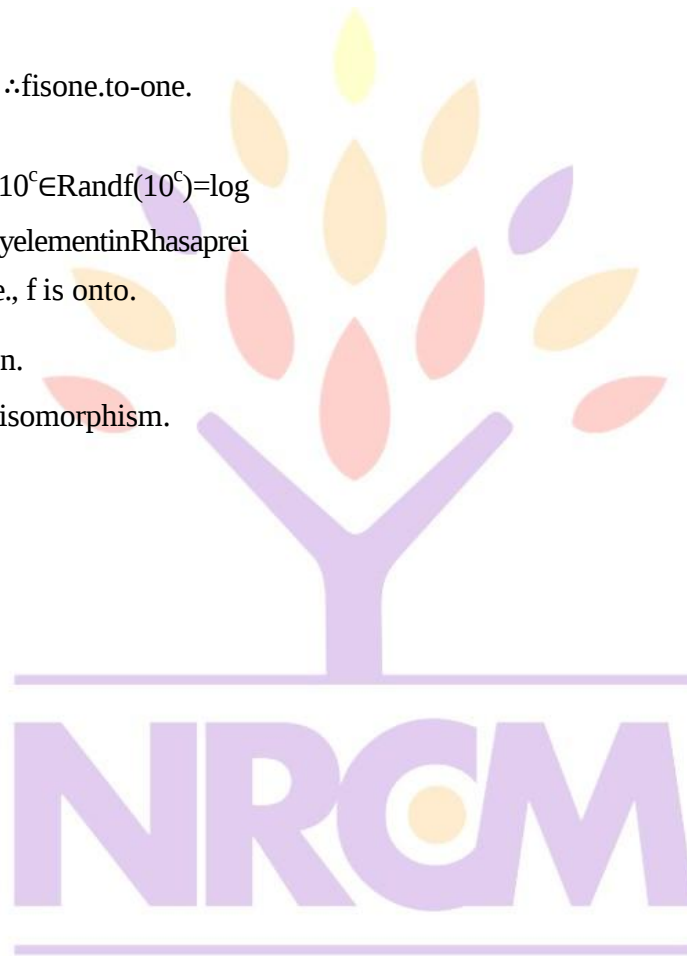
Next, let us prove that f is a
 Bijection. For any $a, b \in \mathbb{R}^+$, Let,
 $f(a) = f(b)$
 $\Rightarrow \log_{10} a = \log_{10} b$
 $\Rightarrow a = b$

$\therefore f$ is one-to-one.

Next, take
 any $c \in \mathbb{R}$. Then $10^c \in \mathbb{R}$ and $f(10^c) = \log_{10} 10^c = c$. Every element in $\mathbb{R}$ has a preimage in $\mathbb{R}^+$. i.e., f is onto.

$\therefore f$ is a bijection.

Hence, f is an isomorphism.



your roots to success...

UNIT-IV COMBINATORICS

Basis of counting:

If X is a set, let us use $|X|$ to denote the number of elements in X .

Two Basic Counting Principles

Two elementary principles act as—building blocks—for all counting problems. The first principle says that the whole is the sum of its parts; it is at once immediate and elementary.

Sum Rule: The principle of disjunctive counting:

If a set X is the union of disjoint nonempty subsets $S_1, \dots, S_n$, then $|X| = |S_1| + |S_2| + \dots + |S_n|$.

We emphasize that the subsets $S_1, S_2, \dots, S_n$ must have no elements in common. Moreover, since $X = S_1 \cup S_2 \cup \dots \cup S_n$, each element of X is in exactly one of the subsets S_i . In other words, $S_1, S_2, \dots, S_n$ is a partition of X .

If the subsets $S_1, S_2, \dots, S_n$ were allowed to overlap, then a more profound principle will be needed—the principle of inclusion and exclusion.

Frequently, instead of asking for the number of elements in a set *per se*, some problems ask for how many ways a certain event can happen.

The difference is largely in semantics, for if A is an event, we can let X be the set of ways that A can happen and count the number of elements in X . Nevertheless, let us state the sum rule for counting events.

If $E_1, \dots, E_n$ are mutually exclusive events, and E_1 can happen e_1 ways, E_2 can happen e_2 ways, ..., E_n can happen e_n ways, E_1 or E_2 or ... or E_n can happen $e_1 + e_2 + \dots + e_n$ ways.

Again we emphasize that mutually exclusive events E_1 and E_2 mean that E_1 or E_2 can happen but both cannot happen simultaneously.

The sum rule can also be formulated in terms of choices: If an object can be selected from a reservoir in e_1 ways and an object can be selected from a separate reservoir in e_2 ways, then the selection of one object from either one reservoir or the other can be made in $e_1 + e_2$ ways.

Product Rule: The principle of sequencing counting

If $S_1, \dots, S_n$ are nonempty sets, then the number of elements in the Cartesian product $S_1 \times S_2 \times \dots \times S_n$ is the product $\prod_{i=1}^n |S_i|$. That is,

$$|S_1 \times S_2 \times \dots \times S_n| = \prod_{i=1}^n |S_i|.$$

Observe that there are 5 branches in the first stage corresponding to the 5 elements of S_1 and to each of these branches there are 3 branches in the second stage corresponding to the 3 elements of S_2 giving a total of 15 branches altogether. Moreover, the Cartesian product $S_1 \times S_2$ can be partitioned as $(a_1 \times S_2) \cup (a_2 \times S_2) \cup (a_3 \times S_2) \cup (a_4 \times S_2) \cup (a_5 \times S_2)$, where $(a_i \times S_2) = \{(a_i, b_1), (a_i, b_2), (a_i, b_3)\}$. Thus, for example, $(a_3 \times S_2)$ corresponds to the third branch in the first stage followed by each of the 3 branches in the second stage.

More generally, if $a_1, \dots, a_n$ are the distinct elements of S_1 and $b_1, \dots, b_m$ are the distinct elements of S_2 , then $S_1 \times S_2 = \bigcup_{i=1}^n (a_i \times S_2)$.

For if x is an arbitrary element of $S_1 \times S_2$, then $x = (a, b)$ where $a \in S_1$ and $b \in S_2$. Thus, $a = a_i$ for some i and $b = b_j$ for some j . Thus, $x = (a_i, b_j) \in (a_i \times S_2)$ and therefore $x \in \bigcup_{i=1}^n (a_i \times S_2)$.

Conversely, if $x \in \bigcup_{i=1}^n (a_i \times S_2)$, then $x \in (a_i \times S_2)$ for some i and thus $x = (a_i, b_j)$ where b_j is some element of S_2 . Therefore, $x \in S_1 \times S_2$.

Next observe that $(a_i \times S_2)$ and $(a_j \times S_2)$ are disjoint if $i \neq j$ since if

$$x \in (a_i \times S_2) \cap (a_j \times S_2) \text{ then } x = (a_i, b_k) \text{ for some } k \text{ and } x = (a_j, b_l) \text{ for some } l.$$

But then $(a_i, b_k) = (a_j, b_l)$ implies that $a_i = a_j$ and $b_k = b_l$. But since $i \neq j$, $a_i \neq a_j$.

Thus, we conclude that $S_1 \times S_2$ is the disjoint union of the sets $(a_i \times S_2)$. Furthermore $|a_i \times S_2| = |S_2|$ since there is obviously a one-to-one correspondence between the sets $a_i \times S_2$ and S_2 , namely, $(a_i, b_j) \rightarrow b_j$.

Then by the sum rule $|S_1 \times S_2| = \sum_{i=1}^n |a_i \times S_2|$

$$= \underbrace{(n \text{ summands})}_{7.} |S_2| + |S_2| + \dots + |S_2|$$

$$= 8. n |S_2|$$

$$= 9. nm.$$

Therefore, we have proved the product rule for two sets. The general rule follows by mathematical induction.

We can reformulate the product rule in terms of events. If events $E_1, E_2, \dots, E_n$ can happen $e_1, e_2, \dots, e_n$ ways, respectively, then the sequence of events E_1 first,

followed by $E_2, \dots$, followed by E_n can happen $e_1 e_2 \dots e_n$ ways.

In terms of choices, the product rule is stated thus: If a first object can be chosen e_1 ways, a second e_2 ways, ..., and an n th object can be made in $e_1 e_2 \dots e_n$ ways.

Combinations & Permutations

Definition.

A combination of n objects taken r at a time (called an r -combination of n objects) is an unordered selection of r of the objects.

A permutation of n objects taken r at a time (also called an r -permutation of n objects) is an ordered selection or arrangement of r of the objects.

Note that we are simply defining the terms r -combinations and r -permutations here and have not mentioned anything about the properties of the n objects.

For example, these definitions say nothing about whether or not a given element may appear more than once in the list of n objects.

In other words, it may be that the objects do not constitute a set in the normal usage of the word.

General formulas for enumerating combinations and permutations will now be presented. At this time, we will only list formulas for combinations and permutations without repetitions or with unlimited repetitions. We will wait until later to use generating functions to give general techniques for enumerating combinations where other rules govern these selections.

Let $P(n, r)$ denote the number of r -permutations of n elements without repetitions.

Theorem 5.3.1. (Enumerating r -permutations without repetitions).

$$P(n, r) = n(n-1) \dots (n-r+1) = n! / (n-r)!$$

Proof. Since there are n distinct objects, the first position of an r -permutation may be filled in n ways. This done, the second position can be filled in $n-1$ ways since no repetitions are allowed and there are $n-1$ objects left to choose from. The third can be filled in $n-2$ ways. By applying the product rule, we conclude that

$$P(n, r) = n(n-1)(n-2) \dots (n-r+1).$$

From the definition of factorials, it follows that

$$P(n, r) = n! / (n-r)!$$

When $r = n$, this formula becomes

$$P(n, n) = n! / 0! = n!$$

When we explicit reference is not made, we assume that all the objects are to be arranged; thus we talk about the permutations of n objects we mean the case $r = n$. Corollary 1. There are $n!$ permutations of n distinct objects.

Number of permutations that can be formed from a collection of n objects of which n_1 are of one type, n_2 are of second type, ..., n_k are of k th type with $n_1 + n_2 + \dots + n_k = n$. Then the number of permutations of the n objects is $\frac{n!}{n_1! n_2! \dots n_k!}$.

$$\frac{n!}{n_1! n_2! \dots n_k!}$$

Example 1.

There are $3! = 6$ permutations of $\{a, b, c\}$.

There are $4! = 24$ permutations of $\{a, b, c, d\}$.

The number of 2-permutations $\{a, b, c, d, e\}$ is $P(5, 2) = \frac{5!}{(5-2)!} = 5 \times 4 = 20$.

The number of 5-letter words using the letters a, b, c, d , and e at most once is $P(5, 5) = 120$.

Example 2 There are $P(10, 4) = 5,040$ 4-digit numbers that contain no repeated digits since each such number is just an arrangement of four of the digits $0, 1, 2, 3, \dots, 9$ (leading zeroes are allowed). There are $P(26, 3) P(10, 4)$ license plates formed by 3 distinct letters followed by 4 distinct digits.

Example 3. In how many ways can 7 women and 3 men be arranged in a row if the 3 men must always stand next to each other?

There are $3!$ ways of arranging the 3 men. Since the 3 men always stand next to each other, we treat them as a single entity, which we denote by X . Then if $W_1, W_2, \dots, W_7$ represents the women, we next are interested in the number of ways of arranging $\{X, W_1, W_2, W_3, \dots, W_7\}$. There are $8!$ permutations these 8 objects. Hence there are $(3!)(8!)$ permutations altogether. (of course, if there has to be a prescribed order of an arrangement on the

3 men then there are only $8!$ total permutations).

Example 4. In how many ways can the letters of the English alphabet be arranged so that there are exactly 5 letters between the letters a and b?

There are $P(24, 5)$ ways to arrange the 5 letters between a and b, 2 ways to place a and b, and then $20!$ ways to arrange any 7-letter word treated as one unit along with the remaining 19 letters. The total is $P(24, 5)(20!)(2)$.

Note: If instead of arranging objects in a line, we arrange them in a circle, then the number of permutations decreases.

Example 5. In how many ways can 5 children arrange themselves in a ring?

Solution: Here, the 5 children are not assigned to particular places but are only arranged relative to one another. Thus, the arrangements (see Figure 2-3) are considered the same if the children are in the same order clockwise. Hence, the position of child C1 is immaterial and it is only the position of the 4 other children relative to C1 that counts. Therefore, keeping C1 fixed in position, there are $4!$ arrangements of the remaining children.

Example 6. A certain question paper contains 3 parts A, B, C with 4 questions in part A, 5 questions in part B and 6 questions in part C. It is required to answer 7 questions selecting at least 2 questions from each part. In how many different ways can a student select his seven questions for answering?

Solution: The different possible ways in which a student can make a selection are

(1) 2 questions from part A, 2 from part B and 3 from part C

(2) 2 questions from part A, 3 from part B and 2 from part C

(3) 3 questions from part A, 2 from part B and 2 from part C

Selection (1) can be made in $C(4, 2) \times C(5, 2) \times C(6, 3) = 1200$ ways

Selection (2) can be made in $C(4, 2) \times C(5, 3) \times C(6, 2) = 900$ ways

Selection (3) can be made in $C(4, 3) \times C(5, 2) \times C(6, 2) = 600$ ways

Therefore number of possible selection is $1200 + 900 + 600 = 2700$

1. **How many different strings (sequences) of length 4 can be formed using the letters of the word FLOWER. Sol:**

The given word FLOWER has 6 letters where all of which are distinct.

$$\text{The required number of strings is } P(6, 4) = \frac{6!}{(6-4)!} = \frac{6!}{2!} = 360$$

2. **Find the number of permutations of the letters of the word SUCCESS.**

Sol: The given word SUCCESS has 7 letters, of which 3 are S's, 2 are C's and 1 each are U and E.

$$\text{The required number of permutations is } \frac{7!}{3!2!1!1!} = 420$$

3. **Find the number of permutations of the letters of the word MASSASAUGA. In how many of these, all four A's are together? How many of them begin with S?**

Sol: The given word MASSASAUGA has 10 letters of which 4 are A's, 3 are S's and 1 each are M, U and G.

$$\text{Required number of permutations is } \frac{10!}{4!3!1!1!1!} = 25,200$$

If all A's are together, we treat all A's as one single letter.

Then required number of permutations is $\frac{7!}{1!3!1!1!1!} = 84$

If the word begins with letter S, there occurs 9 open positions to fill, where 2 are S's, 4 are A's and one each are M, U, G

Then required number of permutations is $\frac{9!}{2!4!1!1!1!} = 7560$

4. How many positive integers can we form using the digits 3, 4, 4, 5, 5, 6, 7 if we want not to exceed 5,000,000 Sol: Here

n must be of the form $n = x_1x_2x_3x_4x_5x_6x_7$

Where $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ are the given digits with $x_1 = 5$ or 6 or 7

Suppose we take $x_1 = 5$ then $x_2, x_3, x_4, x_5, x_6, x_7$ is an arrangement of the remaining 6 digits which contains two 4's and one each of 3, 5, 6, 7

Then number of such arrangements is $\frac{6!}{2!1!1!1!1!} = 36$

Next, suppose we take $x_1 = 6$ then $x_2, x_3, x_4, x_5, x_6, x_7$ is an arrangement of the remaining 6 digits which contains two each of 4 and 5 and one each of 3, 7

Then number of such arrangements is $\frac{6!}{2!2!1!1!} = 18$

Similarly, we take $x_1 = 7$ then $x_2, x_3, x_4, x_5, x_6, x_7$ is an arrangement of the remaining 6 digits which contains two each of 4 and 5 and one each of 3, 6

Then number of such arrangements is $\frac{6!}{2!2!1!1!} = 18$

According to Sum Rule,

Then number of n's of desired type is $= 36 + 18 + 18 = 720$

5. Four different Mathematics books, five different computer science books and two different control theory books are to be arranged in a shelf. How many different arrangements are possible if

a) the books in each particular subject must all be together?

b) Only the Mathematics books must be together?

Sol: a) The Mathematics books can be arranged among themselves in $4!$ ways, the Computer science book in $5!$ ways, the control theory books in $2!$ ways and the three groups in $3!$ ways

then number of possible arrangements is $4! \times 5! \times 2! \times 3! = 34,560$

b) Consider the four mathematics books as one single book. Then we have 8 books which can be arranged in $8!$ ways. In all of these ways the mathematics books are together. But the mathematics books can be arranged among themselves in $4!$ ways.

Hence, the number of arrangements is $8! \times 4! = 967,680$

6. Find the value of n such that $2P(n, 2) + 50 = P(2n, 2)$ Sol:

$$2P(n, 2) + 50 = P(2n, 2)$$

$$2 \times \frac{n!}{(n-2)!} + 50 = \frac{(2n)!}{(2n-2)!}$$

$$2n(n-1) + 50 = 2n(2n-1)$$

$$n^2 = 25$$

$$n = 5 \text{ or } -5$$

Since n cannot be negative, the value of $n = 5$

THE PRINCIPLE OF INCLUSION-EXCLUSION:

Consider a finite set S containing n number of elements. Here, the number n is called **order**, size or the cardinality of the set S and is denoted by $n(S)$, or $|S|$ or $|S|$.

For example, if $S = \{1, 2, 6\}$ and $T = \{a, b, c, d\}$ then $n(S) = |S| = 3$ and $n(T) = |T| = 4$. It is obvious that $|\emptyset| = 0$, and $|S| \geq 1$ for every non-empty finite set S . Further for any two finite sets A and B , if $A \subseteq B$ then $|A| \leq |B|$ and if $A \subset B$ then $|A| < |B|$.

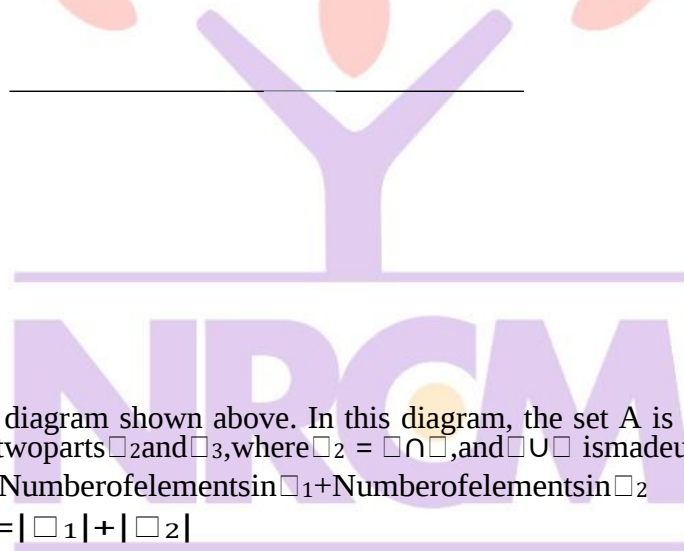
If A is a subset of a finite universal set U , then the number of elements in the complement A^c (of A in U) is given by-

$$|A^c| = |U| - |A| \quad (1)$$

Suppose we consider the union of two finite sets A and B and wish to determine the number of elements in $A \cup B$. Since, the elements of $A \cup B$ consist of all elements which are in A or in B or both A and B , the number of elements in $A \cup B$ is equal to the number of elements in A plus the number of elements in B minus the number of elements (if any) that are common to A and B . That is,

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (2)$$

A more explicit (visual) way of obtaining this result is through the use of a Venn Diagram.



Consider the Venn diagram shown above. In this diagram, the set A is made up of two parts A_1 and A_2 and the set B is made up of two parts B_2 and B_3 , where $A_2 = A \cap B$, and $A \cup B$ is made up of parts A_1 , A_2 and B_3 . Therefore,

$$\begin{aligned} |A| &= \text{Number of elements in } A_1 + \text{Number of elements in } A_2 \\ &= |A_1| + |A_2| \end{aligned}$$

Similarly, $|B| = |B_2| + |B_3|$, $|A \cup B| = |A_1| + |A_2| + |B_3|$

From these, we get

$$\begin{aligned} |A \cup B| &= |A_1| + |A_2| + |B_3| = (|A_1| + |A_2|) + (|A_2| + |B_3|) - |A_2| \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

Thus, for determining the number of elements in $A \cup B$, we first include all elements in A and all elements in B , and then exclude all elements that are common to A and B .

If U is a finite universal set of which A and B are subsets, then, by virtue of a De Morgan Law and the expression (1) above, we have-

$$|A \cap B| = |A| + |B| - |A \cup B|$$

With the use of formula (2) above, this becomes

$$|A \cap B| = |A| - \{|A| + |B| - |A \cup B|\}$$

$$= |A| - |A| - |B| + |A \cup B| \quad (3)$$

Expressions (2) and (3) are equivalent to one another. Either of these is referred to as the Addition Principle (Rule) or the Principle of inclusion-exclusion for two sets.

In the particular case where A and B are disjoint sets so that $A \cap B = \emptyset$, the addition rule (2) becomes-

$$|A \cup B| = |A| + |B| - |\emptyset| = |A| + |B| \quad (4)$$

This is known as the Principle of disjunctive counting for two sets.

Binomial Coefficients: In mathematics, the **binomial coefficient** $\binom{n}{k}$ is the coefficient of the term x^k in the polynomial expansion of the binomial power $(1+x)^n$.

In combinatorics, $\binom{n}{k}$ is interpreted as the number of k -element subsets (the k -combinations) of an n -element set, that is the number of ways that k things can be "chosen" from a set of n things.

Hence, $\binom{n}{k}$ is often read as " n choose k " and is called the choose function of n and k . The notation $\binom{n}{k}$ was introduced by Andreas von Ettingshausen in 182, although the numbers were already known centuries before that (see Pascal's triangle). Alternative notations include $C(n, k)$,

nC_k , C_k^n , nC_k , C_k^n , in all of which the C stands for combinations or choices.

For natural numbers (taken to include 0) n and k , the binomial coefficient $\binom{n}{k}$ can be defined as the coefficient of the monomial X^k in the expansion of $(1+X)^n$. The same coefficient also

your roots to success...

occurs (if $k \leq n$) in the binomial formula

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$$

(valid for any elements x, y of a commutative ring), which explains the name "binomial coefficient".

Another occurrence of this number is in combinatorics, where it gives the number of ways, disregarding order, that k objects can be chosen from among n objects; more formally, the number of k -element subsets (or k -combinations) of an n -element set. This number can be seen to be equal to the one of the first definition, independently of any of the formulas below to compute it.

If in each of the factors of the power $(1+X)^n$ one temporarily labels the term X with an index i (running from 1 to n), then each subset of k indices gives after expansion a contribution

X^k , and the coefficient of that monomial in the result will be the number of such subsets. This shows in particular that $\binom{n}{k}$ is a natural number for any natural numbers n and k . There are many other combinatorial interpretations of binomial coefficients (counting problems for which the answer is given by a binomial coefficient expression), for instance the number of words formed of n bits (digits 0 or 1) whose sum is k , but most of these are easily seen to be equivalent to counting k -combinations.

Several methods exist to compute the value of $\binom{n}{k}$ without actually expanding a binomial power or counting k -combinations.

Method of generating functions for First-Order Recurrence Relations:-

Suppose the recurrence relation to be solved is of the form $a_n =$

$$c a_{n-1} + F(n) \quad \text{for } n \geq 1$$

$$\text{or } a_{n+1} = c a_n + \phi(n) \quad \text{for } n \geq 0$$

$$\text{generating function is } f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + \sum_{n=1}^{\infty} a_n x^n$$

then we get

$$f(x) = a_0 + \sum_{n=1}^{\infty} (c a_{n-1} + \phi(n)) x^n = a_0 + c x \sum_{n=0}^{\infty} a_n x^n + \sum_{n=1}^{\infty} \phi(n) x^n$$

Problems:

1. Find a generating function for the recurrence relation $a_{n+1} - a_n = 3^n, n \geq 0$ and

$a_0 = 1$. Hence solve the relation.

Sol: Given $a_{n+1} - a_n = 3^n$

$$\Rightarrow a_{n+1} = a_n + 3^n$$

this is of the form $a_{n+1} = c a_n + \phi(n)$ for $n \geq 0$

Here $c = 1, a_0 = 1$ and $\phi(n) = 3^n$

Generating function is $f(x) = \sum_{n=0}^{\infty} (1-3x)^n$

$$= \sum_{n=0}^{\infty} (1-3x)^n = (1-3x)^{-1}$$

$$f(x) = \frac{1}{1-3x}$$

is the required G.F

Let $\frac{1-2x}{(1-3x)(1-x)} = \frac{A}{1-3x} + \frac{B}{1-x}$

$$1-2x = A(1-x) + B(1-3x)$$

On solving $A = B = \frac{1}{2}$

$$f(x) = \frac{1-2x}{(1-3x)(1-x)} = \frac{1}{2} \left(\frac{1}{1-3x} + \frac{1}{1-x} \right)$$

$$= \frac{1}{2} \left(\sum_{n=0}^{\infty} (3x)^n + \sum_{n=0}^{\infty} x^n \right)$$

$$= \frac{1}{2} \sum_{n=0}^{\infty} (1+3^n) x^n = \sum_{n=0}^{\infty} \frac{(1+3^n)}{2} x^n$$

Hence required solution is $a_n = \frac{(1+3^n)}{2}$

2. Find the generating function for the recurrence relation $a_{n+1} - a_n = n^2, n \geq 0$ and $a_0 = 1$. Hence solve it.

Sol: Given $a_{n+1} - a_n = n^2 \Rightarrow a_{n+1} = a_n + n^2, n \geq 0$ this is of the form $a_{n+1} = c a_n + f(n)$ for $n \geq 0$. Here $c = 1$

$a_0 = 1$ and $f(n) = n^2$

Generating function is $f(x) = \sum_{n=0}^{\infty} (1+x)^n$

$$= \sum_{n=0}^{\infty} (1+x)^n = \frac{1}{1-x}$$

i.e., $g(x)$ is the G.F for $\langle n^2 \rangle = 0^2, 1^2, 2^2, \dots$

then $g(x) = \frac{x(1+x)}{(1-x)^3}$

$$f(x) = \frac{1}{1-x} + \frac{x^2(1+x)}{(1-x)^3}$$

$$f(x) = \frac{1-3x+4x^2}{(1-x)^4}$$

is the required G.F

$$f(x) = \frac{(1-3x+4x^2)(1-x)^{-4}}{1} = (1-3x+4x^2) \left[\sum_{n=0}^{\infty} \binom{n+3}{3} x^n \right]$$

$$= \sum_{n=0}^{\infty} \binom{n+3}{3} x^n - 3 \sum_{n=0}^{\infty} \binom{n+2}{2} x^{n+1} + 4 \sum_{n=0}^{\infty} \binom{n+1}{1} x^{n+2}$$

Since $f(x) = \sum_{n=0}^{\infty} a_n x^n$

Coeff. of x^n is

$$\begin{aligned}
 a_n &= \binom{n+3}{2} - 3 \binom{n+1}{1} + 4 \binom{n-2}{0} \\
 &= \frac{(n+3)!}{2!3!} - 3 \frac{(n+1)!}{1!3!} + 4 \frac{(n-2)!}{0!3!} \\
 &= \frac{(n+3)!}{6} - 3 \frac{(n+1)!}{6} + 4 \frac{(n-2)!}{6} \\
 &= \frac{(n+3)(n+2)(n+1) - 3(n+1)n(n-1) + 4(n-2)(n-3)(n-4)}{6} \\
 &= \frac{(n+1)(2n^2 - 5n + 6)}{6} \quad \text{is the required solution.}
 \end{aligned}$$

Method of generating functions for second-order Recurrence relations:-

Consider the second order recurrence relation $a_n +$

$A a_{n-1} + B a_{n-2} = F(n)$ for $n \geq 2$

or $a_{n+2} + A a_{n+1} + B a_n = \phi(n)$ for $n \geq 0$

Generating function $f(x) = \sum_{n=0}^{\infty} a_n x^n$

then we get

$$f(x) = \frac{a_0 + (a_1 + a_0 A)x + \frac{a_0 B}{1 + Ax + Bx^2}}{1 + Ax + Bx^2} \quad \phi(x) = \sum_{n=0}^{\infty} \phi(n) x^n$$

Note: If $\phi(n) = 0$ then generating function is $f(x) = \frac{a_0 + (a_1 + a_0 A)x}{1 + Ax + Bx^2}$

1. Find generating function for the recurrence relation $a_n + a_{n-1} - 6a_{n-2} = 0$ for $n \geq 2$

Given $a_0 = -1, a_1 = 8$

Sol: Given $a_n + a_{n-1} - 6a_{n-2} = 0$ for $n \geq 2$

$a_{n+2} + a_{n+1} - 6a_n = 0$ for $n \geq 0$

and $a_0 = -1, a_1 = 8, A = 1, B = -6, \phi(n) = 0$

then generating function $f(x) = \frac{a_0 + (a_1 + a_0 A)x}{1 + Ax + Bx^2}$

$$f(x) = \frac{-1 + (8 - 1)x}{1 + x - 6x^2} \quad \text{is the required generating function.}$$

2. Find generating function for the recurrence relation $a_{n+2} - 2a_{n+1} + a_n = 2^n$ for $n \geq 0$ Given

$a_0 = 1, a_1 = 2$ Hence solve it.

Sol: Given $a_{n+2} - 2a_{n+1} + a_n = 2^n$ for $n \geq 0$

Here $a_0 = 1, a_1 = 2, A = -2, B = 1$ and $\phi(n) = 2^n$

then generating function

$$f(x) = \frac{a_0 + (a_1 + a_0 A)x + \frac{a_0 B}{1 + Ax + Bx^2}}{1 + Ax + Bx^2} \quad \phi(x) = \sum_{n=0}^{\infty} \phi(n) x^n$$

$$\phi(x) = \sum_{n=0}^{\infty} 2^n x^n$$

$$n=0$$

$$\infty$$

$$\infty$$

$$\phi(x) = \sum_{n=0}^{\infty} 2^n x^n = \sum_{n=0}^{\infty} (2x)^n = (1 - 2x)^{-1}$$

Thus,

$$\begin{aligned} \frac{f(x)}{1-x} &= \frac{1-2x+x^2}{(1-x)^2(1-2x)} = \frac{1}{1-2x} \\ f(x) &= (1-2x)^{-1} \\ &= \sum_{n=0}^{\infty} (2x)^n = \sum_{n=0}^{\infty} 2^n x^n \\ a_n &= 2^n \text{ is the required solution.} \end{aligned}$$

3. Find a generating function for the recurrence relation $a_{n+2} - 5a_{n+1} + 6a_n = 2$ for $n \geq 0$ Given

$a_0 = 3, a_1 = 7$ Hence solve it.

Sol: Given $a_{n+2} - 5a_{n+1} + 6a_n = 2$ for $n \geq 0$

Here $a_0 = 3, a_1 = 7, A = -5, B = 6$ and $c(n) = 2$

then generating function

$$f(x) = \sum_{n=0}^{\infty} (a_{n+2} - 5a_{n+1} + 6a_n)x^{n+2} = \sum_{n=0}^{\infty} 2x^{n+2}$$

$$= \frac{2x^2}{1-x}$$

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

$$= \sum_{n=0}^{\infty} a_n x^n$$

$$= \sum_{n=0}^{\infty} 2^n x^n$$

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

$$\text{Thus } f(x) = \frac{3-8x+2x^2}{1-5x+6x^2}$$

$$= \frac{10x^2 - 11x + 3}{(1-2x)(1-3x)(1-x)}$$

$$= \frac{10x^2 - 11x + 3}{(1-2x)(1-3x)(1-x)}$$

is the required generating function.

Now, Let

$$\frac{10x^2 - 11x + 3}{(1-2x)(1-3x)(1-x)} = \frac{A}{1-2x} + \frac{B}{1-3x} + \frac{C}{1-x}$$

$$10x^2 - 11x + 3 = A(1-3x) + B(1-x)(1-3x) + C(1-x)(1-2x)$$

On solving $A=1, B=0, C=2$

$$f(x) = \frac{10x^2 - 11x + 3}{(1-2x)(1-3x)(1-x)} = \frac{1}{1-x} + \frac{2}{1-3x}$$

$$= (1-x)^{-1} + 2(1-3x)^{-1}$$

$$= \sum_{n=0}^{\infty} x^n + 2 \sum_{n=0}^{\infty} (3x)^n$$

$$= \sum_{n=0}^{\infty} (1+2 \cdot 3^n) x^n$$

Hence $a_n = 1 + 2 \cdot 3^n$ is the required solution.

4. Find a generating function for the Fibonacci sequence $\langle F_n \rangle$ and hence obtain an expression for F_n

Sol: Recurrence relation for Fibonacci sequence is

$$F_{n+2} = F_{n+1} + F_n \quad \text{for } n \geq 0 \text{ with } F_0 = 0, F_1 = 1$$



$$F_{n+2} - F_{n+1} - F_n = 0$$

$F_n = 0$ for $n \geq 0$. Here $F_0 = 0, F_1 = 1, A = -1, B = -1$ and $\square(n) = 0$

the generating function $f(x) = \frac{0 + (1 + 0x)}{1 + x + x^2}$



your roots to success...

$$\text{Now, } f(x) = \frac{-x}{x^2 + x - 1} = \frac{A}{x - \alpha} + \frac{B}{x - \beta}$$

$$\alpha, \beta = \frac{-1 \pm \sqrt{5}}{2}$$

$$-x = A(x - \beta) + B(x - \alpha)$$

$$\frac{1}{x - \alpha} = \frac{1}{x - \beta} + \frac{1}{x - \alpha}$$

$$\text{Now } f(x) = \frac{1}{x - \alpha} - \frac{1}{x - \beta}$$

$$= -\frac{1}{\alpha} (1 - \frac{\alpha}{x}) - \frac{1}{\beta} (1 - \frac{\beta}{x})$$

$$= -\sum_{n=0}^{\infty} (\frac{\alpha^n}{\alpha^{n+1}} + \frac{\beta^n}{\beta^{n+1}})$$

$$\text{Thus } F_n = -\frac{1}{\alpha^{n+1}} - \frac{1}{\beta^{n+1}}$$

$$= -\frac{1}{(-1)^n \sqrt{5}} \left[\frac{1}{\alpha^{n+1}} + \frac{1}{\beta^{n+1}} \right]$$

$$= -\frac{1}{(-1)^n \sqrt{5}} \left[\frac{1}{\alpha^{n+1}} + \frac{1}{\beta^{n+1}} \right]$$

$$= -\frac{1}{(-1)^n \sqrt{5}} \left[\frac{1}{\alpha^{n+1}} + \frac{1}{\beta^{n+1}} \right]$$

$$= \frac{1}{(-1)^n \sqrt{5}} \left[\alpha^{n+1} - \beta^{n+1} \right]$$

Second order linear homogeneous Recurrence relations BY CHARACTERISTIC ROOTS

Consider these second order RR

$$C_n a_n + C_{n-1} a_{n-1} + C_{n-2} a_{n-2} = 0 \text{ for } n \geq 2 \rightarrow (1)$$

C_n, C_{n-1}, C_{n-2} are constants with $C_n \neq 0$.

We want to get the solution of (1) in the form $a_n = ck^n$ $C \neq 0$

& $k \neq 0$, put $a_n = ck^n$ in (1)

$$C_n (Ck^n) + C_{n-1} Ck^{n-1} + C_{n-2} (Ck^{n-2}) = 0$$

$$Ck^{n-2} [C_n k^2 + C_{n-1} k + C_{n-2}] = 0$$

$$C_n k^2 + C_{n-1} k + C_{n-2} = 0 \rightarrow (2)$$

$a_n = Ck^n$ is the solution of (1) if (2) is true. This quadratic equation (2) in k is called auxiliary equation or Characteristic equation of RR (1). Then $\exists$ three cases

- 1) The two roots k_1 & k_2 are real and distinct then solution is $a_n = Ak_1^n + Bk_2^n$.
- 2) The two roots k_1 & k_2 are real but equal then solution is $a_n = (A + Bn)k^n$.
- 3) k_1 & k_2 are complex conjugates like $k_1 = p + iq$ & $k_2 = p - iq$

$$A_n = r^n (A \cos n\theta + B \sin n\theta) \text{ where } r = \sqrt{a^2 + b^2} \text{ and } \theta = \tan^{-1}\left(\frac{b}{a}\right)$$

Q1: Solve the recurrence relation $a_n + a_{n-1} - 6a_{n-2} = 0$ for $n \geq 2$, $a_0 = -1$, $a_1 = 8$

Sol: General form of second order RR is $c_n a_n + c_{n-1} a_{n-1} + c_{n-2} a_{n-2} = 0$

$$\therefore c_n = 1, c_{n-1} = 1, c_{n-2} = -6$$

Now the characteristic equation is $k^2 + k - 6 = 0$, on solving it $k_1 = -3, k_2 = 2$ (real and distinct).

$$a_n = A(-3)^n + B(2)^n \text{ where } A \text{ \& } B \text{ are constants.}$$

Now using the initial condition find A & B $a_0 =$

$$A + B = -1$$

$$a_1 = -3A + 2B = 8 \Rightarrow -3A + 2B = 8 \text{ then } A = -2, B = 1$$

$$\therefore \text{Solution is } a_n = -2(-3)^n + (2)^n$$

Q2: Solve $a_n = 2(a_{n-1} - a_{n-2})$ for $n \geq 2$, $a_0 = 1$ & $a_1 = 2$ Sol: $a_n - 2a_{n-1} + 2a_{n-2} = 0$, $c_n = 1, c_{n-1} = -2, c_{n-2} = 2$

characteristic equation is $k^2 - 2k + 2 = 0, k = 1 \pm i$

$$\therefore \text{General solution } a_n = r^n [A \cos n\theta + B \sin n\theta]$$

$$= \sqrt{1^2 + 1^2}, \theta = \tan^{-1}\left(\frac{1}{1}\right) = \frac{\pi}{4}$$

$$= \sqrt{2}, \theta = \tan^{-1}(1) = \frac{\pi}{4} \Rightarrow \sqrt{2} e^{i\theta} = \sqrt{2} e^{i\frac{\pi}{4}} = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) = \sqrt{2} \left(\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \right) = 1 + i$$

$$\therefore a_n = (\sqrt{2})^n [A \cos \frac{n\pi}{4} + B \sin \frac{n\pi}{4}]$$

$$\text{To get } A \text{ \& } B \text{ using initial conditions, } a_0 = 1 \Rightarrow A \cos 0 + B \sin 0 = 1 \Rightarrow A = 1$$

$$a_1 = 2 \Rightarrow (\sqrt{2}) [A \cos \frac{\pi}{4} + B \sin \frac{\pi}{4}] = 2$$

$$= \sqrt{2} [A \frac{1}{\sqrt{2}} + B \frac{1}{\sqrt{2}}] = 2$$

$$A + B = 2 \text{ then } B = 1 \Rightarrow a_n = (\sqrt{2})^n \left[\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right]$$

Q3: Solve $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$, $F_0 = 0$, $F_1 = 1$ Sol: $F_{n+2} - F_{n+1} - F_n = 0$, $c_n = 1, c_{n-1} = -1, c_{n-2} = -1$

$$\text{Characteristic equation } F_n = A \left(\frac{1+\sqrt{5}}{2} \right)^n + B \left(\frac{1-\sqrt{5}}{2} \right)^n$$

Using critical values, $A + B = 0 \Rightarrow (1) \Rightarrow B = -A$

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

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

$$1 = 2A \frac{\sqrt{5}}{2} \Rightarrow A = \frac{1}{\sqrt{5}}, B = -\frac{1}{\sqrt{5}}$$

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right] \text{ is the solution.}$$

Third and Higher Order Linear Homogeneous Recurrence Relation:

Q1. Solve $2a_{n+3} - a_{n+2} + 2a_{n+1} - a_n = 0$ for $n \geq 0$ given $a_0 = 0, a_1 = 1, a_2 = 2$

Sol: Let $2a_{n+3} - a_{n+2} + 2a_{n+1} - a_n = 0$ for $n \geq 0$

We have $C_n = 2, C_{n-1} = -1, C_{n-2} = -2, C_{n-3} = 1$

Characteristic equation is $2k^3 - k^2 - 2k + 1 = 0 \Rightarrow k_1 = \frac{1}{2}, k_2 = 1, k_3 = -1$

The roots are real and distinct.

$$\therefore a_n = A \left(\frac{1}{2}\right)^n + B(1)^n + C(-1)^n$$

To find A, B & C:

$$a_0 = 0 = A + B + C \text{ ----- (1)}$$

$$a_1 = 1 = \frac{A}{2} + B - C \text{ ----- (2)}$$

$$a_2 = 2 = \frac{A}{4} + B + C \text{ ----- (3)}$$

$$\text{Adding (1) + (2) gives } 3A + 4B = 2 \text{ ----- (4)}$$

$$\text{Adding (2) + (3) gives } 3A + 8B = 12 \text{ ----- (5)}$$

$$\text{Now, solving (4) \& (5) we get } A = \frac{-8}{3}, B = \frac{5}{2}, C = \frac{1}{6}$$

$$\therefore a_n = \frac{-8}{3} \left(\frac{1}{2}\right)^n + \frac{5}{2} (1)^n + \frac{1}{6} (-1)^n$$

This is the required solution.

Q2. Solve the recurrence relation $a_n + a_{n-1} - 8a_{n-2} - 12a_{n-3} = 0$, given $a_0 = 1, a_1 = 5, a_2 = 1$.

Sol: Given $a_n + a_{n-1} - 8a_{n-2} - 12a_{n-3} = 0$

We have $C_1 = 1, C_2 = 1, C_3 = -8, C_4 = -12$

Characteristic equation is $k^3 + k^2 - 8k - 12 = 0 \Rightarrow k_1 = -2, k_2 = 3, k_3 = 3$

The roots are real and repeated.

Hence the solution is $a_n = (A + Bn)(-2)^n + C(3)^n$

$$a_0 = 1 = A + C \text{ ----- (1)}$$

$$a_1 = 5 = -2(A + B) + C \text{ ----- (2)}$$

$$a_2 = 1 = 4(A + 2B) + 9C \text{ ----- (3)}$$

Solving (1), (2) and (3), we get $A = 0, B = -1, C = 1$

$\therefore a_n = (-n)(-2)^n + 3^n$ is the required solution.

Non-Homogeneous Recurrence Relation of Second and Higher Order:

Recurrence relation is of the form,

$$c_n a_n + c_{n-1} a_{n-1} + c_{n-2} a_{n-2} + \dots = f(n) \text{ where } n \geq k \geq 2 \text{ \& } c_n \neq 0 \text{ ----- (1)}$$

A general solution for this RR be $a_n = a_n^{(h)} + a_n^{(p)}$ where $a_n^{(h)}$ is the solution of the LHS part.

your roots to success...

To get $a^{(p)}$ consider the following cases:

Case(i): Suppose $f(n)$ is a polynomial of degree $q > 1$ is not a root of the characteristic equation of the homogeneous part (LHS) of relation in equation (1). In this case $a^{(p)}$ can be taken as

$$a_n^{(p)} = A_0 + A_1 n + A_2 n^2 + \dots + A_q n^q. \text{ Then } A_0, A_1, A_2, \dots, A_q \text{ should be evaluated.}$$

Case(ii): Suppose $f(n)$ is a polynomial of degree $q > 1$ is a root of multiplicity m , $a^{(p)}$ can be taken as

$$a_n^{(p)} = n^m (A_0 + A_1 n + A_2 n^2 + \dots + A_q n^q). \text{ Then } A_0, A_1, A_2, \dots, A_q \text{ should be evaluated.}$$

Case(iii): Suppose $f(n) = ab^n$ where a is constant and b is not a root of the characteristic equation then $a^{(p)} = Ab^n$

Case(iv): Suppose $f(n) = ab^n$ where a is constant and b is a root of multiplicity m of the characteristic equation then $a_n^{(p)} = An^m b^n$

Problems:

Q1. Solve the recurrence relation $a_n + 4a_{n-1} + 4a_{n-2} = 8$ for $n \geq 2$ and $a_0 = 1, a_1 = 2$

Sol: Given recurrence relation is $a_n + 4a_{n-1} + 4a_{n-2} = 8$ ----- (1)

Consider the homogeneous part, $a_n + 4a_{n-1} + 4a_{n-2} = 0$ We

have $C_n = 1, C_{n-1} = 4, C_{n-2} = 4$

The characteristic equation is $k^2 + 4k + 4 = 0 \Rightarrow k = k = -2$ ----- (2)

The roots are real and repeated, so the required solution is $a_n^{(h)} = (A + Bn)(-2)^n$ ----- (3)

Consider the RHS, it is a constant 8, consider it as a polynomial with degree 0. (ie., $n=0$) and 1 is not a root for LHS.

By case (i), $a_n^{(p)} = A$ ----- (4)

Put (4) in (1), we get $A + 4A + 4A = 8 \Rightarrow A = \frac{8}{9}$. So we have $a_n^{(p)} = A = \frac{8}{9}$

Therefore, the general solution of (1) is $a_n = a_n^{(h)} + a_n^{(p)}$

$$\Rightarrow a_n = (A + Bn)(-2)^n + \frac{8}{9} \text{ ----- (5)}$$

Now, for finding values of A & B,

$$a_0 = 1 = A + \frac{8}{9} \Rightarrow A = 1 - \frac{8}{9} = \frac{1}{9} \text{ ----- (6)}$$

$$a_1 = 2 = -2(A + B) + \frac{8}{9} \Rightarrow -2A - 2B = 2 - \frac{8}{9} \text{ ----- (7)}$$

Solving (6) & (7), we get $B = -\frac{6}{9}$

Substituting the values of A & B in (5), we have $a_n = \left(1 - \frac{2}{3}n\right)(-2)^n + \frac{8}{9}$

Q2. Solve the recurrence relation $a_{n+2} - 4a_{n+1} + 3a_n = -200$ for $n \geq 0$ and given $a_0 = 3000, a_1 = 3300$

Sol: Given $a_{n+2} - 4a_{n+1} + 3a_n = -200$ for $n \geq 0$ ----- (1)

We have $C_n = 1, C_{n-1} = -4, C_{n-2} = 3$

Characteristic equation is $k^2 - 4k + 3 = 0 \Rightarrow k_1 = 1, k_2 = 3$

The roots are real and distinct, so we have $a_n^{(h)} = A(1)^n + B(3)^n$

Since 1 is the root of the characteristic equation with multiplicity $m=1$, we can write $a_n^{(p)} = n^1(A)$, now substituting this in eqn. (1) we get,

$$(n+2)A_0 - 4(n+1)A_0 + 3nA_0 = -200 \Rightarrow -2A_0 = -200 \Rightarrow A_0 = 100$$

Hence, we have $a_n^{(p)} = 100n$

We know that the general solution is given by $a_n = a_n^{(h)} + a_n^{(p)}$

$$\therefore a_n = A + B(3)^n + 100n \text{ ----- (2)}$$

Also, we have

$$a_0 = 3000 = A + B \Rightarrow B = 3000 - A \text{ ----- (1)}$$

$$a_1 = 3300 = A + B(3)^1 + 100(1) \text{ ----- (2)}$$

Solving (1) & (2) we get $A = 2900, B = 100$

Hence the particular solution is given by $a = 2900 + 100(3)^n + 100n$

Q3. Solve the recurrence relation $a_{n+2} - 10a_{n+1} + 21a_n = 3n^2 - 2, n \geq 0$.

Sol: Given $a_{n+2} - 10a_{n+1} + 21a_n = 3n^2 - 2, n \geq 0$ ----- (1)

We have $C_n = 1, C_{n-1} = -10, C_{n-2} = 21$

Characteristic equation is $k^2 - 10k + 21 = 0 \Rightarrow k_1 = 3, k_2 = 7$

The roots are real and distinct, so we have $a_n^{(h)} = A(3)^n + B(7)^n$ ----- (2)

Since RHS is a polynomial of degree 2 and 1 is not a root of the characteristic equation, we can write

$$a_n^{(p)} = A_0 + A_1n + A_2n^2 \text{ ----- (3)}$$

now substituting (3) in eqn. (1) we have,

$$[A_0 + A_1(n+2) + A_2(n+2)^2] - 10[A_0 + A_1(n+1) + A_2(n+1)^2] + 21[A_0 + A_1n + A_2n^2] = 3n^2 - 2$$

On solving this equation we get $A_0 = \frac{13}{72}, A_1 = \frac{1}{3}, A_2 = \frac{1}{4}$

$$\text{Hence, we have } a_n^{(p)} = \frac{13}{72} + \frac{n}{3} + \frac{n^2}{4}$$

We know that the general solution is given by $a_n = a_n^{(h)} + a_n^{(p)}$

$$\therefore a_n = A(3)^n + B(7)^n + \frac{13}{72} + \frac{n}{3} + \frac{n^2}{4} \text{ is the required solution.}$$

Q4. Solve $a_{n+1} + 4a_{n-1} = 5 \times (-2)^n$

Sol: Given $a_{n+1} + 4a_{n-1} = 5 \times (-2)^n$ ----- (1)

We have $C_n = 1, C_{n-1} = 4, C_{n-2} = 0$

Characteristic equation is $k^2 + 4k + 4 = 0 \Rightarrow k_1 = -2, k_2 = -2$

The roots are real and repeated, so we have $a_n^{(h)} = (A + Bn)(-2)^n$ ----- (2)

Here RHS is of the form $5 \times (-2)^n = ab^n$ where $b = -2$ is a root of the characteristic equation with multiplicity, $m=2$.

So $a^{(p)}$ is of the form $a^{(p)} = A n^m b^n \Rightarrow a^{(p)} = A n^2 (-2)^n$ (3)

Now substitute (3) in (1) to get $[An^2(-2)^n] + 4[A(n-1)^2(-2)^{n-1}] + 4[A(n-2)^2(-2)^{n-2}] = 5 \times (-2)^n$

$$(-2)^{n-2} \{ [An^2(-2)^2] + 4[A(n-1)^2(-2)^1] + 4[A(n-2)^2] \} = 5 \times (-2)^n$$

$$\Rightarrow 4An^2 - 8A(n-1)^2 + 4A(n-2)^2 = 5 \times (-2)^2$$

$$\Rightarrow 4An^2 - 8A(n^2 - 2n + 1) + 4A(n^2 - 4n + 4) = 20$$

$$\Rightarrow 8A = 20 \Rightarrow A = \frac{5}{2}$$

Substituting this value in (3), we get $a^{(p)} = \frac{5}{2} n^2 (-2)^n$

We know that the general solution is given by $a_n = a_n^{(h)} + a_n^{(p)}$

$$\therefore a_n = (A + Bn)(-2)^n + \frac{5}{2} n^2 (-2)^n \text{ is the required solution.}$$



your roots to success...

UNIT-V

Graph Theory

Syllabus

Graph Theory: Representation of Graph, DFS, BFS, Spanning Trees, planar Graphs.

Representation of Graphs:

There are two different sequential representations of a graph. They are

- Adjacency Matrix representation
- Path Matrix representation

Adjacency Matrix Representation

Suppose G is a simple directed graph with m nodes, and suppose the nodes of G have been ordered and are called $v_1, v_2, \dots, v_m$. Then the adjacency matrix $A = (a_{ij})$ of the graph G is the $m \times m$ matrix defined as follows:

$$a_{ij} = \begin{cases} 1, & \text{if } v_i \text{ is adjacent to } v_j, \text{ that is, if there is an edge } (v_i, v_j) \\ 0 & \text{otherwise} \end{cases}$$

Suppose G is an undirected graph. Then the adjacency matrix A of G will be a symmetric matrix, i.e., one in which $a_{ij} = a_{ji}$; for every i and j .

Drawbacks

1. It may be difficult to insert and delete nodes in G .
2. If the number of edges is $O(m)$ or $O(m \log^2 m)$, then the matrix A will be sparse, hence a great deal of space will be wasted.

Path Matrix Representation

Let G be a simple directed graph with m nodes, $v_1, v_2, \dots, v_m$. The path matrix of G is the m -square matrix $P = (p_{ij})$ defined as follows:

$$P_{ij} = \begin{cases} 1 & \text{if there is a path from } V_i \text{ to } V_j \\ 0 & \text{otherwise} \end{cases}$$

Graphs and Multigraphs

A graph G consists of two things:

1. A set V of elements called nodes (or points or vertices)
2. A set E of edges such that each edge $e \in E$ is identified with a unique (unordered) pair $[u, v]$ of nodes in V , denoted by $e = [u, v]$

Sometimes we indicate the parts of a graph by writing $G = (V, E)$.

Suppose $e = [u, v]$. Then the nodes u and v are called the endpoints of e , and u and v are said to be adjacent nodes or neighbors. The degree of a node u , written $\deg(u)$, is the number of edges containing u . If $\deg(u) = 0$ — that is, if u does not belong to any edge — then u is called an isolated node.

Path and Cycle

A path P of length n from a node u to a node v is defined as a sequence of $n+1$ nodes. $P = (v_0, v_1, v_2, \dots, v_n)$ such that $u = v_0$; v_{i-1} is adjacent to v_i for $i = 1, 2, \dots, n$ and $v_n = v$.

Types of Path

1. Simple Path
2. Cycle Path

(i) Simple Path

Simple path is a path in which first and last vertex are different ($V_0 \neq V_n$)

(ii) Cycle Path

Cycle path is a path in which first and last vertex are same ($V_0 = V_n$). It is also called as Closed path.

Connected Graph

A graph G is said to be connected if there is a path between any two of its nodes.

Complete Graph

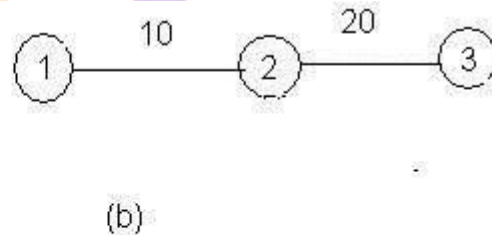
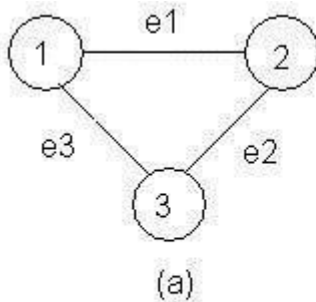
A graph G is said to be complete if every node in G is adjacent to every other node in G .

Tree

A connected graph T without any cycles is called a tree graph or free tree or, simply, a tree.

Labeled or Weighted Graph

If the weight is assigned to each edge of the graph then it is called as Weighted or Labeled graph.



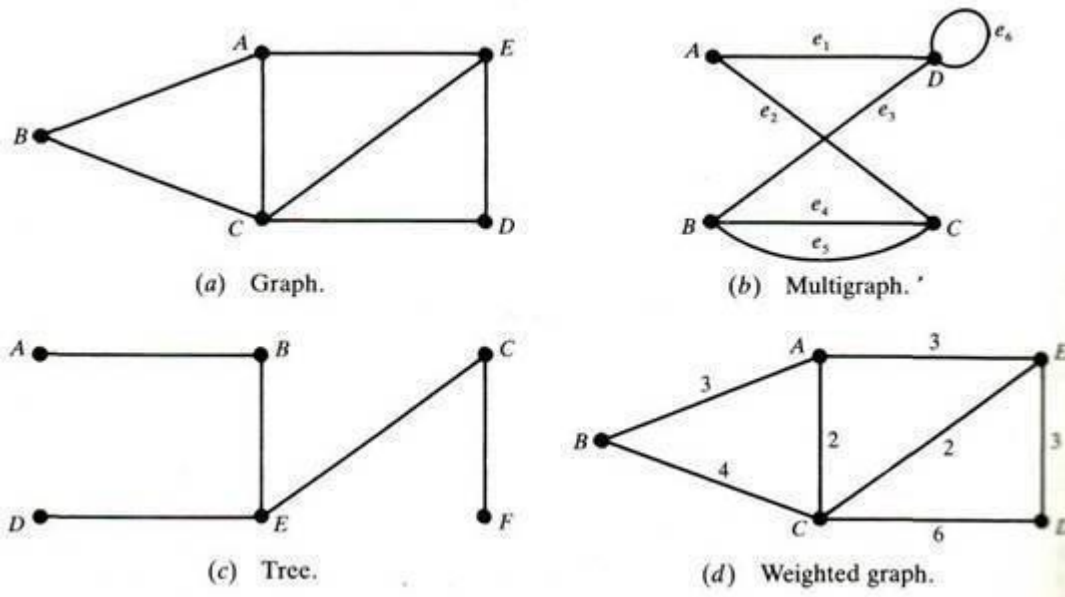
weighted or Labeled Graph

The definition of a graph may be generalized by permitting the following:

1. **Multiple edges:** Distinct edges e and e' are called multiple edges if they connect the same endpoints, that is, if $e = [u, v]$ and $e' = [u, v]$.
2. **Loops:** An edge is called a loop if it has identical endpoints, that is, if $e = [u, u]$.

your roots to success...

3. **Finite Graph:** A multigraph M is said to be finite if it has a finite number of nodes and a finite number of edges.



Directed Graphs

A directed graph G , also called a digraph or graph, is the same as a multigraph except that each edge in G is assigned a direction, or in other words, each edge is identified with an ordered pair (u, v) of nodes in G .

Outdegree and Indegree

Indegree: The indegree of a vertex is the number of edges for which it is head.

Example

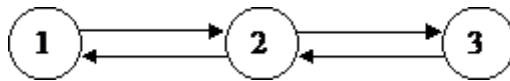


Indegree of 1 = 1

Indegree of 2 = 2

Outdegree: The outdegree of a node or vertex is the number of edges for which it is tail.

Example



Outdegree of 1 = 1

Outdegree of 2 = 2

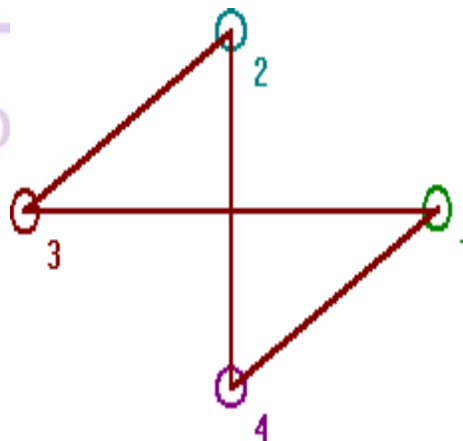
Simple Directed Graph

A directed graph G is said to be simple if G has no parallel edges. A simple graph G may have loops, but it cannot have more than one loop at a given node.

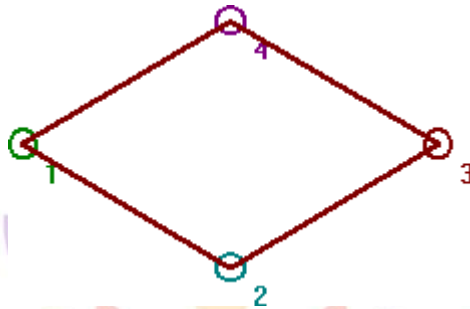
Basic Concepts Isomorphism:

Let G_1 and G_2 be two graphs and let f be a function from the vertex set of G_1 to the vertex set of G_2 . Suppose that f is one-to-one and onto and $f(v)$ is adjacent to $f(w)$ in G_2 if and only if v is adjacent to w in G_1 .

Then we say that the function f is an isomorphism and that the two graphs G_1 and G_2 are isomorphic. So two graphs G_1 and G_2 are isomorphic if there is a one-to-one correspondence between vertices of G_1 and those of G_2 with the property that if two vertices of G_1 are adjacent then so are their images in G_2 . If two graphs are isomorphic then as far as we are concerned they are the same graph though the location of the vertices may be different. To show you how the program can be used to explore isomorphism draw the graph in figure 4 with the program (first get the null graph on four vertices and then use the right mouse to add edges).



SavethisgraphasGraph1(youneedtoclickGraphthenSave). Nowgetthecircuit graphwith4 vertices. It looks like figure 5, and we shall call it $C(4)$.

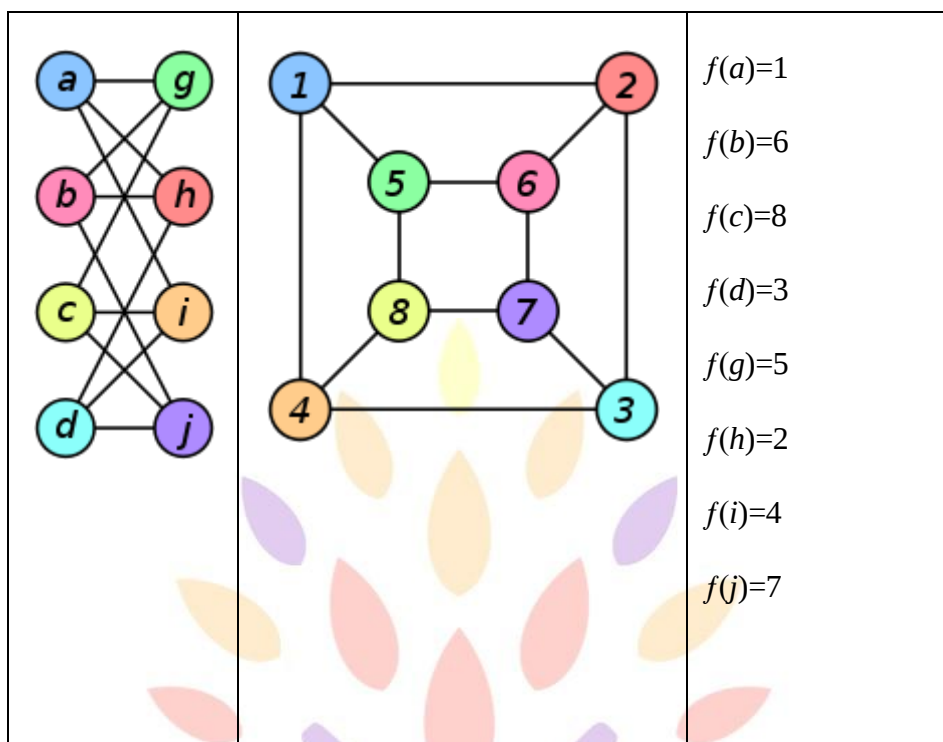


Example:

Thetwographsshownbelowareisomorphic, despitetheirdifferentlooking drawings.

GraphG	GraphH	Anisomorphism betweenGandH
--------	--------	-------------------------------

your roots to success...



Subgraphs:

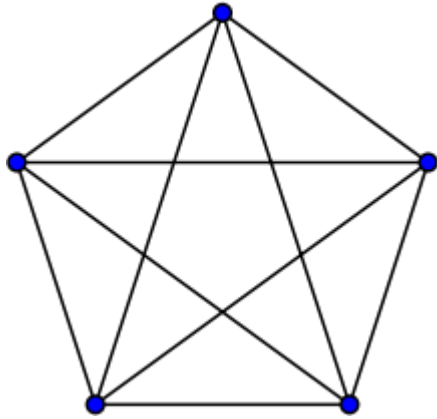
A **subgraph** of a graph G is a graph whose vertex set is a subset of that of G , and whose adjacency relation is a subset of that of G restricted to this subset. In the other direction, a **supergraph** of a graph G is a graph of which G is a subgraph. We say a graph G **contains** another graph H if some subgraph of G is H or is isomorphic to H .

A subgraph H is a **spanning subgraph**, or **factor**, of a graph G if it has the same vertex set as G . We say H spans G .

A subgraph H of a graph G is said to be **induced** if, for any pair of vertices x and y of H , xy is an edge of H if and only if xy is an edge of G . In other words, H is an induced subgraph of G if it has all the edges that appear in G over the same vertex set. If the vertex set of H is the subset S of $V(G)$, then H can be written as $G[S]$ and is said to be **induced by S** .

A graph that does not contain H as an induced subgraph is said to be **H -free**.

A **universal graph** in a class K of graphs is a simple graph in which every element in K can be embedded as a subgraph.



K_5 , a complete graph. If a subgraph looks like this, the vertices in that subgraph form a clique of size 5.

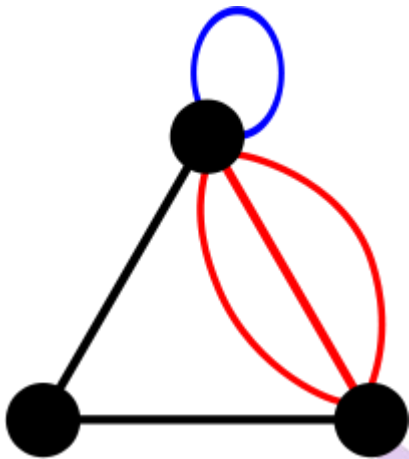
Multi graphs:

In mathematics, a **multigraph** or **pseudograph** is a graph which is permitted to have multiple edges, (also called "parallel edges"), that is, edges that have the same end nodes. Thus two vertices may be connected by more than one edge. Formally, a multigraph G is an ordered pair $G := (V, E)$ with

- V a set of vertices or nodes,
- E a multiset of unordered pairs of vertices, called edges or lines.

Multigraphs might be used to model the possible flight connections offered by an airline. In this case the multigraph would be a directed graph with pairs of directed parallel edges connecting cities to show that it is possible to fly both *to* and *from* these locations.

your roots to success...



A multigraph with multiple edges (red) and a loop (blue). Not all authors allow multigraphs to have loops.

Eulercircuits:

In graph theory, an **Eulerian trail** is a trail in a graph which visits every edge exactly once. Similarly, an **Eulerian circuit** is an Eulerian trail which starts and ends on the same vertex. They were first discussed by Leonhard Euler while solving the famous Seven Bridges of Königsberg problem in 1736. Mathematically the problem can be stated like this:

Given the graph on the right, is it possible to construct a path (or a cycle, i.e. a path starting and ending on the same vertex) which visits each edge exactly once?

Euler proved that a necessary condition for the existence of Eulerian circuits is that all vertices in the graph have an even degree, and stated without proof that connected graphs with all vertices of even degree have an Eulerian circuit. The first complete proof of this latter claim was published in 1873 by Carl Hierholzer.

The term **Eulerian graph** has two common meanings in graph theory. One meaning is a graph with an Eulerian circuit, and the other is a graph with every vertex of even degree. These definitions coincide for connected graphs.

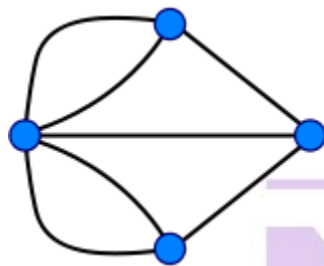
For the existence of Eulerian trails it is necessary that no more than two vertices have an odd degree; this means the Königsberg graph is *not* Eulerian. If there are no vertices of odd degree, all Eulerian trails are circuits. If there are exactly two vertices of odd degree, all Eulerian trails start at one of them and end at the other. Sometimes a graph that has an Eulerian trail but not an Eulerian circuit is called **semi-Eulerian**.

An **Eulerian trail**, **Eulerian trail** or **Euler walk** in an undirected graph is a path that uses each edge exactly once. If such a path exists, the graph is called **traversable** or **semi-Eulerian**.

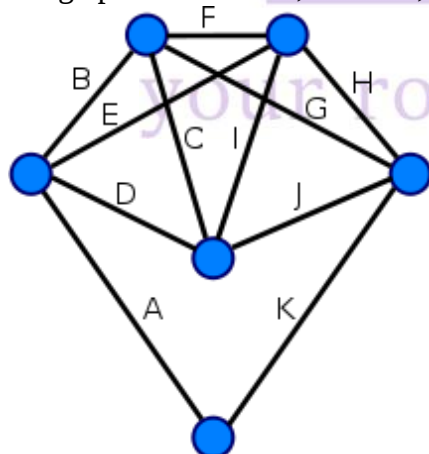
An **Eulerian cycle**, **Eulerian circuit** or **Euler tour** in an undirected graph is a cycle that uses each edge exactly once. If such a cycle exists, the graph is called **unicursal**. While such graphs are Eulerian graphs, not every Eulerian graph possesses a Eulerian cycle.

For directed graphs path has to be replaced with directed path and cycle with directed cycle.

The definition and properties of Eulerian trails, cycles and graphs are valid for multigraphs as well.



This graph is not Eulerian, therefore, a solution does not exist.



Every vertex of this graph has an even degree, therefore this is an Eulerian graph. Following the edges in alphabetical order gives an Eulerian circuit/cycle.

Hamiltonian graphs:

In the mathematical field of graph theory, a **Hamiltonian path** (or **traceable path**) is a path in an undirected graph which visits each vertex exactly once. A **Hamiltonian cycle** (or **Hamiltonian circuit**) is a cycle in an undirected graph which visits each vertex exactly once and also returns to the starting vertex. Determining whether such paths and cycles exist in graphs is the Hamiltonian path problem which is NP-complete.

Hamiltonian paths and cycles are named after William Rowan Hamilton who invented the Icosian game, now also known as *Hamilton's puzzle*, which involves finding a Hamiltonian cycle in the edge graph of the dodecahedron. Hamilton solved this problem using the Icosian Calculus, an algebraic structure based on roots of unity with many similarities to the quaternions (also invented by Hamilton). This solution does not generalize to arbitrary graphs.

A *Hamiltonian path* or *traceable path* is a path that visits each vertex exactly once. A graph that contains a Hamiltonian path is called a **traceable graph**. A graph is **Hamilton-connected** if for every pair of vertices there is a Hamiltonian path between the two vertices.

A *Hamiltonian cycle*, *Hamiltonian circuit*, *vertex tour* or *graph cycle* is a cycle that visits each vertex exactly once (except the vertex which is both the start and end, and so is visited twice). A graph that contains a Hamiltonian cycle is called a **Hamiltonian graph**.

Similar notions may be defined for *directed graphs*, where each edge (arc) of a path or cycle can only be traced in a single direction (i.e., the vertices are connected with arrows and the edge traced "tail-to-head").

A **Hamiltonian decomposition** is an edge decomposition of a graph into Hamiltonian circuits.

Examples

- a complete graph with more than two vertices is Hamiltonian
- every cycle graph is Hamiltonian
- every tournament has an odd number of Hamiltonian paths
- every platonic solid, considered as a graph, is Hamiltonian

Planar Graphs:

In graph theory, a **planar graph** is a graph that can be embedded in the plane, i.e., it can be drawn on the plane in such a way that its edges intersect only at their endpoints.

A planar graph already drawn in the plane without edge intersections is called a **plane graph** or **planar embedding of the graph**. A planar graph can be defined as a planar graph with a mapping from every node to a point in 2D space, and from every edge to a planar curve, such that the extreme points of each curve are the points mapped from its end nodes, and all curves are disjoint except on their extreme points. Plane graphs can be encoded by combinatorial maps.

It is easily seen that a graph that can be drawn on the plane can be drawn on the sphere as well, and vice versa.

The equivalence class of topologically equivalent drawings on the sphere is called a **planar map**.

Although a plane graph has an **external** or **unbounded** face, none of the faces of a planar map have a particular status.

Applications

- Telecommunications—e.g. spanning trees
- Vehicle routing—e.g. planning routes on roads without underpasses
- VLSI—e.g. laying out circuits on computer chip.
- The puzzle game Planarity requires the player to "untangle" a planar graph so that none of its edges intersect.

Example graphs:

**Planar
Graph**

**Nonplanar
Graph**

your roots to success...

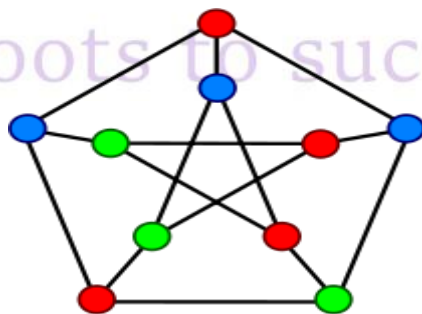
Chromatic Numbers:

In graph theory, **graph coloring** is a special case of graph labeling; it is an assignment of labels traditionally called "colors" to elements of a graph subject to certain constraints. In its simplest form, it is a way of coloring the vertices of a graph such that no two adjacent vertices share the same color; this is called a **vertex coloring**. Similarly, an **edge coloring** assigns a color to each edge so that no two adjacent edges share the same color, and a **face coloring** of a planar graph assigns a color to each face or region so that no two faces that share a boundary have the same color.

Vertex coloring is the starting point of the subject, and other coloring problems can be transformed into a vertex version. For example, an edge coloring of a graph is just a vertex coloring of its line graph, and a face coloring of a planar graph is just a vertex coloring of its planar dual. However, non-vertex coloring problems are often stated and studied *as is*. That is partly for perspective, and partly because some problems are best studied in non-vertex form, as for instance edge coloring.

Graph Colouring:

Graph coloring enjoys many practical applications as well as theoretical challenges. Beside the classical types of problems, different limitations can also be set on the graph, or on the way a color is assigned, or even on the color itself. It has even reached popularity with the general public in the form of the popular number puzzle Sudoku. Graph coloring is still a very active field of research.



A proper vertex coloring of the Petersen graph with 3 colors, the minimum number possible.

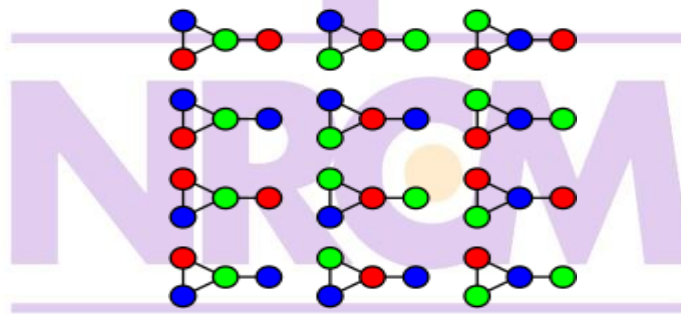
Vertex coloring

When used without any qualification, a **coloring** of a graph is almost always a *proper vertex coloring*, namely a labelling of the graph's vertices with colors such that no two vertices sharing the same edge have the same color. Since a vertex with a loop could never be properly colored, it is understood that graphs in this context are loop less.

The terminology of using *colors* for vertex labels goes back to map coloring. Labels like *red* and *blue* are only used when the number of colors is small, and normally it is understood that the labels are drawn from the integers $\{1, 2, 3, \dots\}$.

A coloring using at most k colors is called a (proper) **k -coloring**. The smallest number of colors needed to color a graph G is called its **chromatic number**, $\chi(G)$. A graph that can be assigned a (proper) k -coloring is **k -colorable**, and it is **k -chromatic** if its chromatic number is exactly k . A subset of vertices assigned to the same color is called a *color class*, every such class forms an

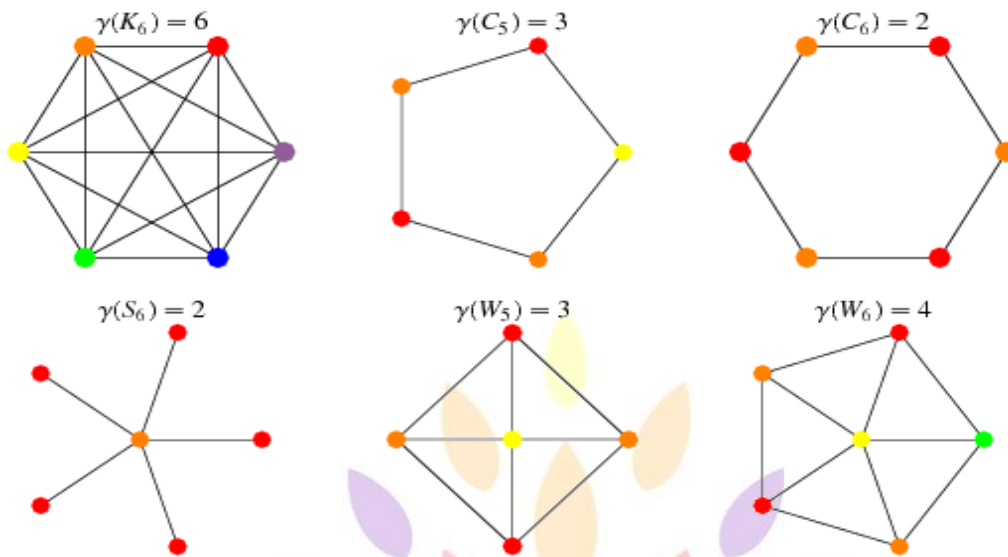
independent set. Thus, a k -coloring is the same as a partition of the vertex set into k independent sets, and the terms *k -partite* and *k -colorable* have the same meaning.



This graph can be 3-colored in 12 different ways.

The following table gives the chromatic number for familiar classes of graphs.

graph G	$\chi(G)$
complete graph	n
cycle graph C_n ,	$\begin{cases} 3 & \text{for } n \text{ odd} \\ 2 & \text{for } n \text{ even} \end{cases}$
star graph S_n ,	2



Trees and its basic properties:

A graph is called a tree if it is connected and has no cycles.

A pendant vertex (a vertex has degree one) of a tree is called a leaf.

Theorem 1: Prove that T is a tree if and only if there is one and only one path between every pair of vertices.

Proof: Let T be a tree. Then T is a simple graph. Since T is connected, there is at least one path between each pair of vertices. If there are two paths between one pair of vertices, the union of these two paths will make a cycle in T , contradicting the fact that T is a tree. Therefore, in a tree, there is one and only one path between every pair of vertices.

Now conversely, assume that in T there is one and only one path between every pair of vertices. Then it is connected. Since there is one and only one path between every pair of vertices in T , T cannot have a cycle. Therefore, T is a tree.

Theorem 2: A tree with n vertices has $n-1$ edges.

Proof: Proof is done by induction on the number of vertices n . The theorem is true for $n=1, n=2$ and $n=3$ (we can see this using graphs). Assume the theorem is true for $n=k$ vertices. Consider a tree T with $k+1$ vertices. Let $e=uv$ be an edge in T . Now $T-e$ is a disconnected graph (since T is a tree). There exist 2 components of $T-e$, say T_1 and T_2 . T_1 contains say k_1 vertices and T_2 contains say k_2 vertices: $k_1+k_2=k+1$. Since T_1 and T_2 have a number of vertices less than or equal to k by our assumption, T_1 and T_2 contain k_1-1 and k_2-1 edges respectively. Then $T-e$ contains $(k_1+k_2)-2$ edges, that is $(k+1)-2$ edges, $k-1$ edges. Therefore T contains $k-1+e$ edges, which implies k edges. The theorem is proved for $n=k+1$ vertices. Therefore, the theorem is true for all positive integer n .

Result: Any connected graph with n vertices and $n-1$ edges is a tree.

Problems:

- a. S. The complete graph K_n is not a tree for $n > 2$.

Solution: Let, v_1, v_2, v_3 be any three vertices of K_n . Since, K_n is a complete graph there exists an adjacency between each pair of vertices.

$\therefore v_1$ is adj v_2, v_2 will be adj to v_3 and v_1 is adj to v_3 also.

$\therefore v_1 v_2 v_3$ creates a cycle inside K_n implies K_n is not a cycle.

- b. S. The complete bipartite graph $K_{n,n}$ is not a tree when $n \geq 2$.

Solution: Let, v_1, v_2 be any two vertices in the first vertex set & v'_1, v'_2 be two vertices of second set of the given complete bipartite graph $K_{n,n}$ with $n \geq 2$. Since, $K_{n,n}$ is complete there exists 'adj' from $v_1 \rightarrow v'_1$ & $v_2 \rightarrow v'_2$.

$v_1 \rightarrow v'_1$ & $v_2 \rightarrow v'_2$

$\therefore v_1 v'_1 v_2 v'_2 v_1$ is a cycle in $K_{n,n}$ which implies $K_{n,n}$ is not a tree.

Minimally Connected Graph:

A connected graph is said to be minimally connected if the removal of any one edge from it disconnects the graph.

* All trees are minimally connected.

Theorem: A connected graph is a tree iff it is minimally connected.

Proof: G is a connected graph which is not a tree implies there exists a cycle. From the cycle remove one edge 'e' implies $G - e$ is still connected implies G is not minimally connected.

If a graph is not a tree, then it is not minimally connected. By contraposition we proved that, if a connected graph is minimally connected then it is a tree.

Conversely, let G be non-minimally connected graph then $\exists$ 'e' such that $G - e$ is disconnected.

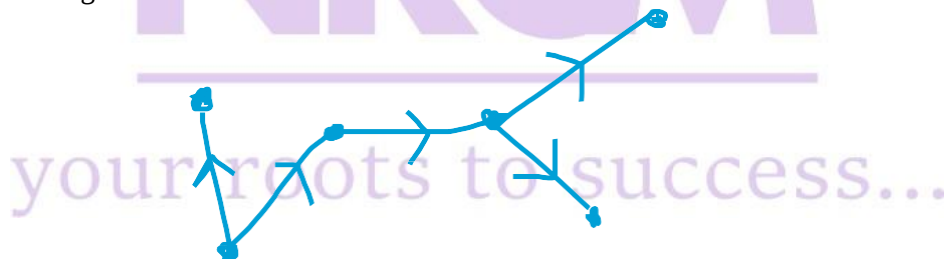
$\therefore$ e must be a part of a cycle i.e. G contains a cycle i.e. G is not a tree. By contraposition if G is a tree then it is minimally connected.

Rooted Tree:

A directed tree is a directed graph whose underlying graph is a tree. A directed tree T is called a rooted tree T contains -

- 1) a unique vertex, called the root (r) whose indegree is zero
- 2) the indegrees of all other vertices of T are 1

Eg.

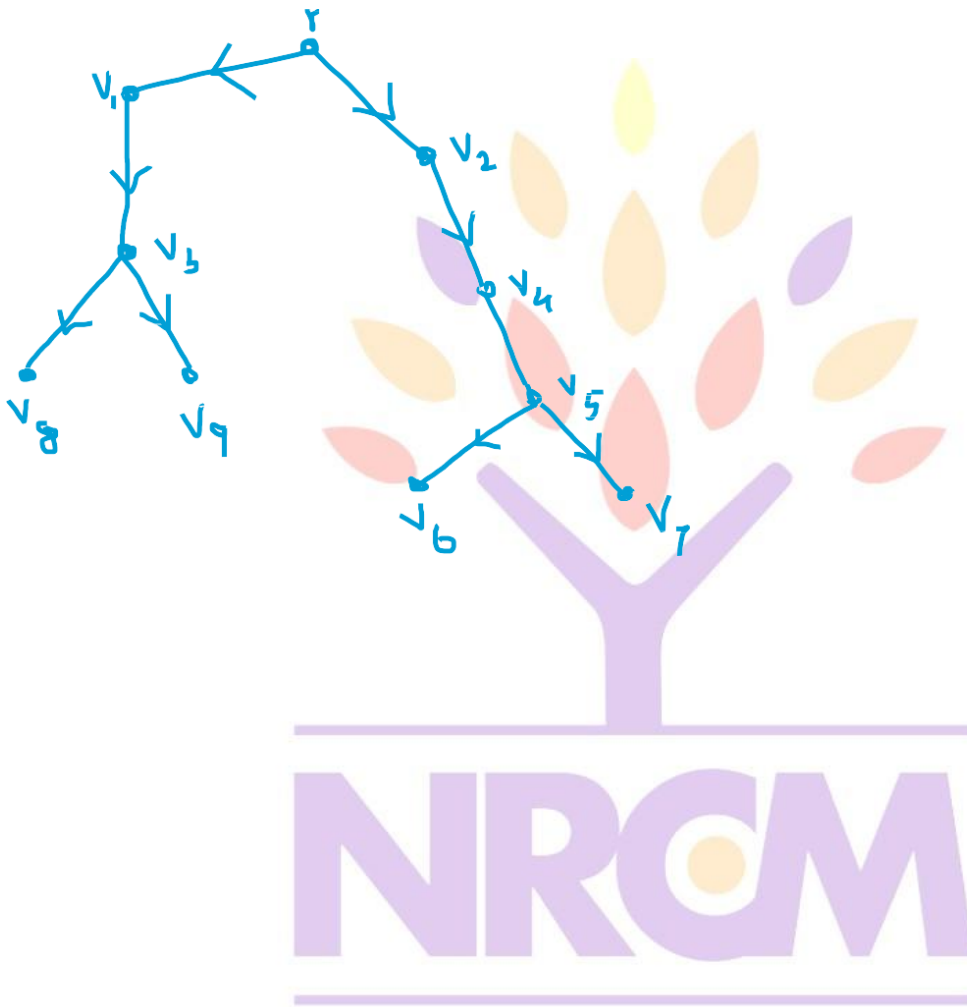


A vertex v of the rooted tree is said to be at the n^{th} level if the path from $r \rightarrow v$ is of length n . In the above figure, v is at the 3rd level.

If v_1 & v_2 are two vertices: v_1 has a lower level than v_2 and there is a path from v_1 to v_2 then we say that v_1 is an

ancestor of v_2 and v_2 is a descendant of v_1 . If v_1 & v_2 are adjacent i.e. there exists an edge from $v_1 \rightarrow v_2$, then v_1 is called parent of v_2 and v_2 is the child of v_1 . Two vertices with a common parent are called siblings. A vertex whose outdegree is zero is called a leaf. A vertex which is not a leaf is called an internal vertex.

Eg



your roots to success...

- 1) v_1 is the root.
- 2) v_1, v_2, v_3, v_4 are in 1st level.
- 3) v_5, v_6, v_7, v_8 are in 2nd level.
- 4) v_1 is the ancestor of v_3, v_8, v_9 and v_1 is the parent of v_3 .
- 5) v_8, v_9 are children of v_3 and are called siblings.
- 6) v_8, v_9, v_6, v_7 are leaves.

Binary Tree

A rooted tree T is called a binary rooted tree, if every internal vertex is of out degree 1 or 2. That is every vertex has at most 2 children. It is called a complete binary tree, if each vertex is of out degree 2.

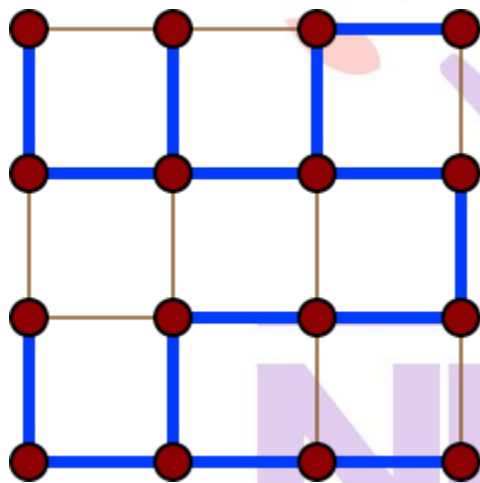
Spanning Trees

Let G be a connected graph. A subgraph T of G is called a spanning tree of G if

- (1) T is a tree
- (2) T contains all vertices of G

The edges of the spanning tree are called branches.

Example:



Chords and Cotree

Let T be a spanning tree of G . Then the edges of G that are not in T are called chords of G with respect to T . The set of all chords of G is called a chord set or a cotree of T in G and is represented by $\bar{T}$. Therefore $G = T \cup \bar{T}$.

DFS (depth first search) Algorithm to find the spanning tree of a graph:

Let $G = (V, E)$ be a connected graph of order 'n', with vertices labelled $v_1, v_2, \dots, v_n$ in some specified order.

Step I: Assign the vertex ' v_1 ' to the variable x and initial T as the tree consisting of just this vertex. (this vertex will become the root of the tree T)

Step II: Select the smallest subscript k , for $2 \leq k \leq n$: $\{v_i, v_k\} \in E$ & v_k has not already been selected in T . If no such subscript is found go to Step III, otherwise:

- (i) Attach the edge $\{v_i, v_k\}$ to the tree T
- (ii) Assign v_k to x
- (iii) Return to Step II.

Step III: If $u = v_1$, the tree T is the spanning tree.

Step IV: For $u \neq v_1$, backtrack from u . If u is the parent of the vertex assigned to v in T , then assign v to u and return to Step II.

BFS (breadth first search) Algorithm to find the spanning tree of a graph:

Let $G=(V,E)$ be a connected graph of order n with vertices labelled $v_1, v_2, \dots, v_n$ in some specified order. We refer to an ordered list Q of vertices of G as a queue in G . Vertices are inserted in this list at one end (called the rear of the queue) and deleted from the list at the other end (called the front of the queue). The BFS algorithm specifies the following steps.

Step I: Assign the first vertex v_1 and insert this vertex in the queue and initialize T as the tree made up of this one vertex v_1 .

Step II: Delete v from the front of Q . When v is deleted, consider v_i for each $2 \leq i \leq n$. If the edge $\{v, v_i\} \in E$ and v_i has not been visited (considered) previously, attach this edge to T . If we examine all of the vertices previously visited and obtain no new edge, the tree T (generated to this point) is the desired spanning tree.

Step III: Insert the vertices adjacent to each v (from Step II) at the rear of the queue Q , according to the order in which they are (first) visited. Then return to Step II.

Show that a Hamiltonian path is a spanning tree.

Proof: By definition of a Hamiltonian path, we know that a Hamiltonian path in a graph G contains all the vertices of G . A path is a tree since it doesn't contain a cycle.

$\therefore$ A Hamiltonian path is a tree that contains all the vertices of the given graph G . A Hamiltonian path is a spanning tree.

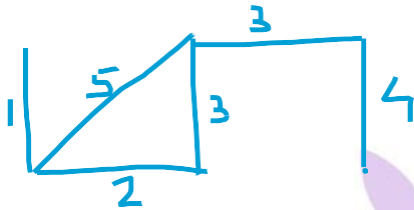
Weighted Graph: Let G be a graph in which there is a positive number associated with each edge is called a weighted graph.

Minimal spanning tree: The spanning tree of a weighted graph whose weight is least is called the minimal spanning tree.



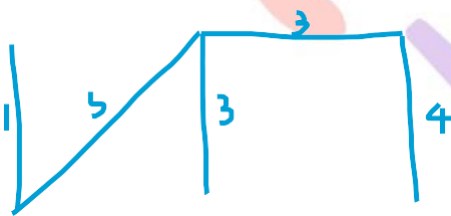
your roots to success...

Example:

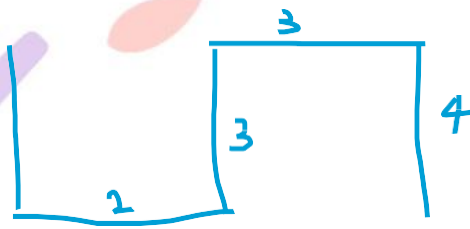


(G)

The following are some spanning trees of G



(T1)



(T2)

T1 and T2 are spanning trees of G but since the weight of T2 is 13 and it is the minimal spanning tree of G.

Algorithm to find minimal spanning tree:

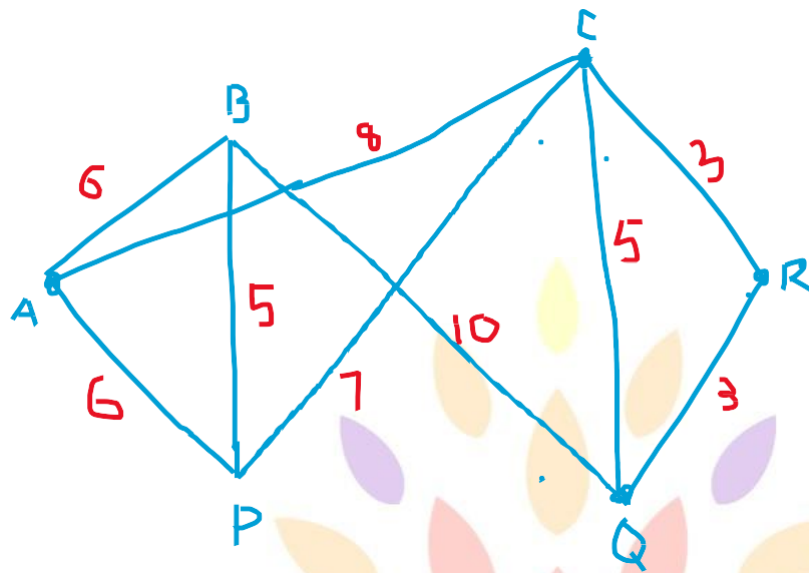
1. Kruskal's Algorithm:

Step I: Let G be a connected weighted graph G with n vertices. List the edges of G in increasing weights.

Step II: Starting with a smallest weighted edge, proceed sequentially by selecting one edge at a time: no cycle is formed.

Step III: Stop the process of Step II when $n-1$ edges are selected as above. These $n-1$ edges constitute a minimal spanning tree G .

Example: •



(G)

Edge:	CR.	QR.	CQ.	BP.	AB.	AP.	CP.AC.	BQ	
Weight:	3.	3.	5.	5.	6.	6.	7.	8.	10
Selection:	Yes.	Yes	No.	Yes.	Yes.	No.	Yes.	-	-

By Kruskal's Algorithm, the following tree T is the minimal spanning tree of the above graph with weight 24

your roots to success...

•
Prims Algorithm to get minimum spanning tree.

Step I: Prepare an $n \times n$ table in which weights of all edges are shown. Indicate the weights of non-existing edges as ∞

Step II: Start from vertex v_1 and connect it to the nearest neighbor which has a smaller weight in the v_1 row say v_k . Now consider edge $v_1 v_k$ and connect this edge to a new vertex which has a minimum value in the v_1 and v_k rows. Let this vertex be v_m .

Step III: Start from v_m and repeat step II. Stop the process when all the n vertices are connected by $n-1$ Edges.



your roots to success...