New Edition

Discrete Structure

B.Sc. CSIT Second Semester

Jagdish Bhatta

Chapter 1

Basic Discrete Structures

1.1 Sets

The theory of set was originated in the 1895 by the German mathematician G. Cantor who defined a set as a collection or aggregate of definite and distinguishable objects selected by means of some rules or description. The theory of sets is the basis for all the branches of modern mathematics. Any branch of knowledge which utilizes the tools of modern mathematics has to use the algebra of sets for the simplification of its concepts. The algebra of sets is aid to preparing the program for feeding into the computers.

Meaning of a Set

A set is any well defined un-ordered collection of distinct objects, called as elements or members of the set. Some examples of a set are:

(a) All vowel alphabets

(b) All Zone of Nepal

(c) All odd numbers

Notations

In general capital letters **A, B, C, X, Y, Z, ...** are used to denote **sets** while the small letter **a, b, c, x, y, z,...** are used to denote the members of the sets unless other wise stated. If 'a' is an element of a set A we write this as $a \in A$ and read as "a belongs to the set A". Again if 'a' is not an element of the set A we write this as $a \notin A$ and read as "a does not belong to the set A."

If A be the set of three numbers 1, 2 and 3 then it is written as:

$$A = \{1, 2, 3\}$$

Here, the elements of the set must be enclosed within the Corley bracket { }.

Representation of a Set

A set may be specified by the following methods:

1. Description Method
2. Tabulation Method
3. Rule Method or Set-builder method

Description Method

In this method a set is specified by a verbal description.

For example, the set S of numbers 1, 2 and 3 is designated as:

S = the set of positive integers less than 4.

Tabulation Method

In this method a set is specified by listing all elements in a set. Thus, we can write the set S of numbers 1, 2 and 3 as:

$$S = \{1, 2, 3\}$$

Note that each of the sets {1, 2, 3}, {2, 3, 1} and {3, 1, 2} are the same.

Rule Method

In this method a set is specified by stating a characteristic property common to all elements in the set. Referring to the above example, we can express the set S as:

$S = \{x \rightarrow x$ is an integer and $1 \leq x \leq 3\}$

This is read as the set of all elements x such that x is a positive integer less than 4. The vertical bar denotes 'such that'.

The representation of a set by the rule method is suitable when the set has a larger number of elements. For example, if we take all men in Kathmandu city using 'close-up tooth paste' it will be inconvenient to write the names of all persons within braces. But we can write this set briefly as:

S = {x: x is a man in Kathmandu who uses close-up tooth paste}

Definitions of Sets Terminologies

Finite Set: A set consisting of finite number of elements is called finite set. Thus, the set of days in a week is a finite set.

Infinite set: A set consisting of infinite number of elements is called infinite set. A set of all odd numbers is an infinite set.

Thus, A = {1, 3, 5, ...} is an infinite set.

Empty Set: A set without any element is called an empty set or null set or void set and is usually denoted by the symbol ϕ or, { }.

(i) P = {x: x is the male students of Padma Kanya Campus} = ϕ

(ii) B = {b: b is a married bachelor} = ϕ

Note that the set {0} is not an empty set since it contains zero as its element. Also *any two empty sets are equal.*

Unit Set: A set consisting of only one element is called a unit set or *singleton* set. Examples of a unit set are:

(i) S = {0} is a unit set with single element zero.

(ii) N = {2} is a unit set with single element 2.

Universal Set: A universal set is the original set that contains all elements under consideration of a particular situation and is denoted by U. If we want to study the problem concerned with the workers of an industry then the set of all workers in the industry will be the universal set.

Subset

A set that consists of some or all elements of another set is called subset of the set. The set A is subset of the set B if and only if each elements of A is also an element of B. In symbols we write $A \subset B$ (and read as 'A is subset of B') if and only if $x \in A$ implies that $x \in B$.

Some examples of a subset are as follows:

(i) If A = {1, 2} and B = {1, 2, 3} then, $A \subset B$.

(ii) Every set is a subset of itself that is $A \subset A$.

(iii) Null set $\varnothing$ is a subset of any set S.

(iv) If A = {a, b, c} and B = {b, a, c}, then $A \subset B$ and $B \subset A$. Then A = B.

Power Set

The possible subsets in a set {a} will be ϕ and {a}. Hence, the number of subsets that can be formed out of a set consisting of one element is $2^1 = 2$.

Similarly, the possible subsets in a set {a, b} will be ϕ, {a}, {b} and {a, b} which are $4 = 2^2$ in number. If we take a set {a, b, c} with the three elements a, b and c then its possible subsets will be ϕ, {a}, {b}, {c}, {a, b}, {b, c}, {c, a} and {a, b, c} which are $8 = 2^3$ in number.

Proceeding in this manner, we conclude by induction that *a set with n elements has 2^n subsets*. This includes the null set and the given set.

So, the set of possible subsets from any set is known as power set of that set.

Let A={a, b, c} be any set then power set of A is

P(A)={ϕ, {a}, {b}, {c}, {a, b}, {b, c}, {c, a} and {a, b, c}}

Ordered Pair

A set of two elements 'a' and 'b' written as {a, b} is called a pair. If we consider the order of the elements, the pair is called ordered pair denoted by (a, b). Here, 'a' is called the first element and 'b; is called the second element of the ordered pair (a, b).

In ordered pair, $(a, b) \neq (b, a)$

Cartesian Product of Two Sets

The Cartesian product of two non-empty sets A and B is defined as the set of all possible ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Mathematically, we can write,

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Note that the Cartesian product A × B, read as A cross B, is the collection of ordered pairs of elements (a, b) where a is chosen from A and b is chosen from B.

Thus, in general, $A \times B \neq B \times A$

In particular $A \times B = B \times A$ if and only if A = B.

Example

Let A = {1, 2} and B = {3, 4, 5}. Construct A × B and B × A and then comment.

Solution

$$A \times B = \{(1, 3)\ (1, 4), (1, 5)\ (2, 3)\ (2, 4)\ (2, 5)\}$$

$$B \times A = [(3, 1)\ (3, 2)\ (4, 1)\ (4, 3)\ (5, 1)\ (5, 2)]$$

Venn Diagram

Sets, Subsets and Operation on sets can be represented by diagrams. Such diagrams are called Venn diagrams. In sketching Venn diagram, we usually represent the universal set by a rectangle and its subset by a circle. The elements of U are represented by the points within the rectangle while the elements of the subset of U is represented by the points within the circle. For illustration let us consider the set of vowels as V which is the subset of the universal set U, the English alphabets.

Then, V = {a, e, i, o, u} is represented in Venn diagram

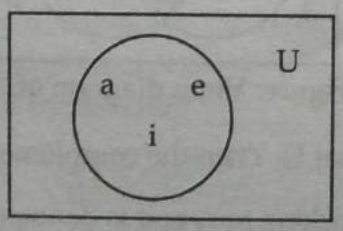


Figure: Venn diagram for set V

Set Operations

Sets may be combined and operated in various ways to form new sets. The basic operations on sets are:

1. Union
2. Intersection
3. Complementation
4. Difference

Union

The union of two sets A and B, denoted by $A \cup B$, is the set of only those elements which belongs to either A or B or both A and B. Symbolically, we write this as:

$$A \cup B = \{x \mid x \in A \text{ or } x \in B \text{ or } x \in \text{ both A and B}\}$$

Here $A \cup B$ is also called the logical sum of A and B and sometimes read as 'A cup B'. The shaded portion on figure 2.2 represents $A \cup B$ which shows the set of objects consisting of the elements of at least one of the sets A and B. Some examples of the union of two sets are as follows:

(a) If $A = \{1, 3\}$ and $B = \{p, q, r\}$,
then $A \cup B = \{1, 3, p, q, r\}$

(b) If $A = \{p, q, r\}$ and $B = \{p, c, s\}$,
then $A \cup B = \{p, q, r, s, c\}$

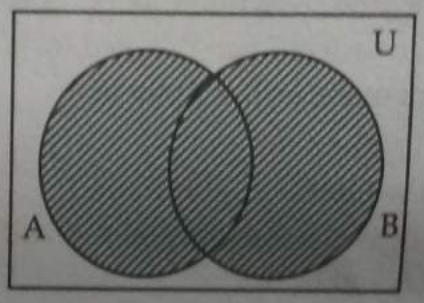


Figure: Venn diagram of $A \cup B$

Intersection

The intersection of two sets A and B, denoted by $A \cap B$, is the set of only those elements which belongs to both A and B. In symbol, we write

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

$A \cap B$ is sometimes read as 'A cap B' and is also known as the logical multiplication of A and B. The shaded area in figure 2.3 shows the common elements of A and B and form a new set $A \cap B$. Some examples of the intersection of two sets are as follows:

(a) If $A = \{2, 3, 4\}$ and $B = \{3, 5\}$ then, $A \cap B = \{3\}$

(b) If M = {Ram, Shyam, Hari, Krishna}
and N = {Shyam, Krishna, Mahesh}
then, $M \cap N$ = {Shyam, Krishna}

(c) If $P = \{a, b, c, d\}$ and $Q = \{a, b, e, f\}$ then $P \cap Q = \{a, b\}$

(d) If $R = \{1, 3, 5\}$ and $S = \{2, 4\}$ then $R \cap S = \phi$

In this case the sets R and S are called disjoint sets.

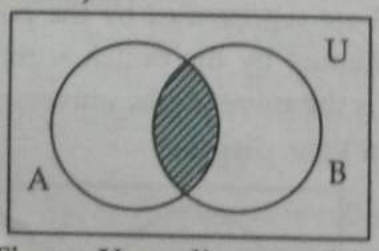


Figure: Venn diagram of $A \cap B$

Complement of a Set

Let A be the subset of a universal set U. Then the complement of A with respect to U is the set of those elements of U which do not belong to A and is denoted by $\bar{A}$ or A' or A^c. In symbols, we write this as:

$A' = \{x \mid x \in U \text{ and } x \notin A\}$

The shaded portion in figure 2.4 stands for the complement of A. Some examples of the complement sets are as follows:

(a) If U = {1, 2, 3, 4, 5} and A = {2, 4} then A' = {1, 3, 5}

(b) If U = set of English alphabets and V = set of vowels then V' = set of consonants.

(c) If U = set of books in the library and A = set of all books on management in the library, then A' = set of all books in the library which are not the books on 'management'.

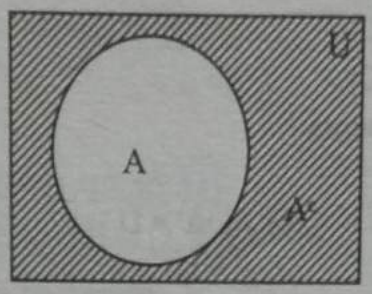


Figure: Venn diagram of A' or A^C

Difference

Let A and B be two sets and each set is the subset of a universal set U. Then, A difference B denoted by A – B, is the set of all those elements which belong to A but not B. In symbols, we write this as:

$A - B = \{x \mid x \in A \text{ and } x \notin B\}$

Also, $B - A = \{x \mid x \in B \text{ and } x \notin A\}$

The difference, A – B, which is sometimes called 'A minus B' is also known a complement of B with respect to A. The shaded portion in figure 2.5 represents the difference of A and B. The following are some examples of the difference between two sets.

(a) If A = {a, b, x, y} and B = {c, d, x, y} then,

A – B = {a, b} and B – A = {c, d}

Thus, $A - B \neq B - A$

(b) Let S be the set of all students in a campus and M, the set of all male students. Then, S – M is the set of all female students in the campus.

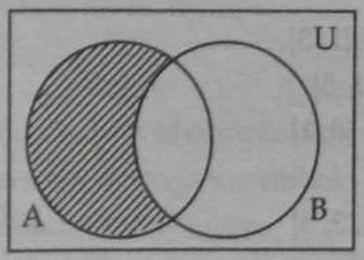


Figure: Venn diagram A – B

Set Identities

The set operations that we discussed above obey some laws. The laws can be verified easily by Venn diagram or abstract mathematical techniques or examples. The laws given below bear a close resemblance to the elementary algebraic laws. The resemblance can be made even more the striking by replacing ∪ by +, ∩ by × and ϕ by 0. Below are the basic laws of set operations which are also known as laws of Boolean Algebras or algebra of sets.

I. The Laws Governing Union and Intersection

1. Identity Laws:

(a) $A \cup \varnothing = A$ (b) $A \cup U = U$

(b) $A \cap \varnothing = \varnothing$ (d) $A \cap U = A$

2. Idempotent Laws:
   (a) $A \cup A = A$ (b) $A \cap A = A$
3. Commutative Laws:
   (a) $A \cup B = B \cup A$ (b) $A \cap B = B \cap A$
4. Associative Laws:
   (a) $A \cup (B \cup C) = (A \cup B) \cup C$
   (b) $A \cap (B \cap C) = (A \cap B) \cup (A \cap C)$
5. Distributive laws:
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

II. The Laws Governing Complements

Complement Laws:

(a) $(A')' = A$ (b) $A \cup A' = U$
(c) $A \cap A' = \phi$ (d) $\phi' = U$
(e) $U' = \phi$

III. The Laws Governing Set Differences

1. $A - B = A \cap B'$ 2. $U - A = A'$
3. $A - U = \phi$ 4. $A - \phi = A$
5. $\phi - A = \phi$ 6. $A - A = \phi$

IV. De-Morgan's Laws

(i) $(A \cup B)' = A' \cap B'$ (ii) $(A \cap B)' = A' \cup B'$

Example

Given $A = \{1, 3, 5\}$; $B = \{0, 1, 2, 3\}$ and $C = \{0, 1, 5\}$, verify the distributive laws.

Solution

The distributive laws for union and intersection are:

(i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(ii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

We have,

$A \cup B = \{0, 1, 2, 3, 5\}$, $A \cap B = \{1, 3\}$
$A \cup C = \{0, 1, 3, 5\}$, $A \cap C = \{1, 5\}$
$B \cup C = \{0, 1, 2, 3, 5\}$, $B \cap C = \{0, 1\}$

(i) L.S. $= A \cup (B \cap C)$
$= \{1, 3, 5\} \cup \{0, 1\} = \{0, 1, 3, 5\}$
R.S. $= (A \cup B) \cap (A \cup C)$
$= \{0, 1, 2, 3, 5\} \cap \{0, 1, 3, 5\} = \{0, 1, 3, 5\}$
$\therefore$ L.S. = R.S.

(ii) L.S. $= A \cap (B \cup C) = \{1, 3, 5\} \cap \{0, 1, 2, 3, 5\} = \{1, 3, 5\}$
R.S. $= (A \cap B) \cup (A \cap C) = \{1, 3\} \cup \{1, 5\} = \{1, 3, 5\}$
$\therefore$ L.S. = R.S.

Example

Given the sets

$U = \{x \mid x$ is a positive integer less than $16\}$
$A = \{5, 10, 15\}$; $B = \{2, 4, 6, 8, 10\}$; $C = \{1, 5, 9, 11, 15\}$

Find: (a) $A \cap B$ (b) $A \cup B \cup C$ (c) $A \cap B \cap C$ (d) $(A \cap B \cap C)'$

(e) $A' \cap B'$ (f) $A' \cup C'$ (g) $A' \cup B$ (h) $A' \cap B$

Solution

(a) $A \cap B = \{5, 10, 15\} \cap \{2, 4, 6, 8, 10\} = \{10\}$

(b) $A \cup B \cup C = \{5, 10, 15\} \cup \{2, 4, 6, 8, 10\} \cup \{1, 5, 9, 11, 15\}$
$= \{1, 2, 4, 5, 6, 8, 9, 10, 11, 15\}$

(c) $A \cap B \cap C = \{5, 10, 15\} \cap \{2, 4, 6, 8, 10\} \cap \{1, 5, 9, 11, 15\} = \phi$

(d) $(A \cap B \cap C)' = (\phi)' = U$

(e) $A' = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14\}$
$B' = \{1, 3, 5, 7, 9, 11, 12, 13, 14\}$

Hence, $A' \cap B' = \{1, 3, 7, 9, 11, 12, 13, 14\}$

(f) $C' = \{2, 3, 4, 6, 7, 8, 10, 12, 13, 14\}$

Hence, $A' \cup C' = \{1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$

(g) $A' \cup B = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14\} \cup \{2, 4, 6, 8, 10\}$
$= \{1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$

(h) $A' \cap B = \{2, 4, 6, 8\}$

Example

Prove that: $\overline{A \cap B} = \bar{A} \cup \bar{B}$. Using set builder notation.

Solution: $\overline{A \cap B} = \{x : x \notin A \cap B)$ $\because$ Complement

$= \{x : \neg (x \in (A \cap B))\}$

$= \{x : \neg (x \in A \wedge x \in B)\}$ Definition of intersection

$= \{x : \neg (x \in A) \vee \neg (x \in B)\}$ De-Morgan's law

$= \{x : x \notin A \vee x \notin B\}$ Does not belongs to symbol

$= \{x : x \in \bar{A} \vee x \in \bar{B}\}$ By definition of complementary

$= \{x : x \in \bar{A} \cup \bar{B}\}$ By definition of union

$= \bar{A} \cup \bar{B}$ By meaning of set builder notation

Example

Prove that: $\overline{A \cup B} = \bar{A} \cap \bar{B}$

Solution: $\overline{A \cup B} = \{x : x \notin \cup B\}$ By definition of complement

$= \{x : \neg (x \in (A \cup B))\}$ Does not belongs to symbol

$= \{x : \neg (x \in A \vee x \in B\}$ By definition of union

$= \{x : \neg (x \in A) \wedge \neg (x \in B)\}$ By De-Morgan's law

$= \{x : x \notin A \wedge x \notin B\}$ Using does not belongs to symbol

$= \{x : x \in \bar{A} \wedge x \notin \bar{B}\}$ By definition of complement

$= \{x : x \in \bar{A} \cap \bar{B}\}$ By definition of union

$= \bar{A} \cap \bar{B}$

Example

Prove that: $\overline{A \cup B} = \bar{A} \cap \bar{B}$

Proof: To prove $\overline{A \cup B} = \bar{A} \cap \bar{B}$.

We have to show that $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$ and $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$.

Now

To show $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Let $x \in \overline{A \cup B}$, By definition of complement.

$x \notin A \cup B$.

By definition of union, $\neg((x \in A) \vee (x \in B))$.

Applying De-Morgan's law,

We see that,

$\neg(x \in A)$ and $\neg(x \in B)$

Hence by definition of negation,

$x \notin A$ and $x \notin B$.

By definition of complement,

$x \in \bar{A}$ and $x \in \bar{B}$

It follows that, $x \in \bar{A} \cap \bar{B}$

$\therefore \quad \overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$.

Now, to show $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$.

Suppose, $x \in \bar{A} \cap \bar{B}$

By definition of intersection,

$x \in \bar{A}$ and $x \in \bar{B}$

By using definition of complement, we get

$x \notin \bar{A}$ and $x \notin B$.

Consequently, $\neg(x \in A)$ and $\neg(x \in B)$

By De-Morgan's law, $\neg((x \in A \vee (x \in B))$

By definition of union, $\neg(x \in A \cup B)$

By using definition of complement,

$x \in \overline{A \cup B}$.

$\therefore \quad \bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\therefore \quad \overline{A \cup B} = \bar{A} \cap \bar{B}$. Proved.

Example

Let A, B, and C be sets. Show that

$\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}$.

Solution: We have

$\overline{A \cup (B \cap C)}$	$= \bar{A} \cap (\overline{B \cap C})$	By the De Morgan's law
	$= \bar{A} \cap (\bar{B} \cup \bar{C})$	By the De Morgan's law
	$= (\bar{B} \cup \bar{C}) \cap \bar{A}$	By the commutative law for intersections
	$= (\bar{C} \cup \bar{B}) \cap \bar{A}$	By the commutative law for unions.

Inclusion and Exclusion and Applications

Let A and B be any two disjoint sets then we extensively use inclusion exclusion principle. Given set A and set B the union of A and B is given by the formula

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

That is to find the number $n(A \cup B)$ of elements in the union $A \cup B$, we add $n(A)$ and $n(B)$ and then subtract $n(A \cap B)$ i.e. include $n(A)$ and $n(B)$ and exclude $n(A \cap B)$.

Similarly, for any finite sets A, B and C we have,

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C).$$

Example:

There are 345 students at a college who have taken a course in calculus, 212 who have taken a course in discrete mathematics, and 188 who have taken course in both calculus and discrete mathematics. How many students have taken the course in either calculus or discrete mathematics?

Solution:

Here we have $|C| = 345$ (students taking the calculus course), $|D| = 212$ (students taking the discrete mathematics course), and $|C \cap D| = 188$ (students taking both discrete mathematics and calculus courses). Number of students taking either discrete mathematics or calculus,

$$|C \cup D| = |C| + |D| - |C \cap D| = 345 + 212 - 188 = 369.$$

Computer Representation of Sets

One method to represent sets in computer is to store the elements of set in an unordered list. If this method is used, the operations of computing the union, intersection of sets would be time consuming because each of these operations would require large time in searching for elements.

So, we use method for storing elements using an arbitrary ordering of the elements of the universal set.

Specify an arbitrary ordering of elements of U, for instance $a_1, a_2, \ldots\ldots, a_n$ represent a subset A of U with bit string of length n, where i^{th} bit in this string is 1 if $a_i \in A$ and 0 if $a_i \notin A$.

Example:

Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}.

(i) What bit strings represent the subset of all odd integers in U?

The bit string that represents the set of odd integers in U, {1, 3, 5, 7, 9}, has a one bit in the first, third, fifth, seventh, and ninth positions. It is 1 0 1 0 1 0 1 0 1 0.

(ii) What bit strings represent the subset of all even integers in U?

The bit string that represent the subset of even integers in U,{2, 4, 6, 8, 10}.

It is 0 1 0 1 0 1 0 1 0 1.

(iii) What bit strings represent the subset of integers not exceeding 5 in U?

The set of all integers in U that do not exceed 5, {1, 2, 3, 4, 5}, is represented by the string 1 1 1 1 1 0 0 0 0 0.

To find the bit string for the complement of a set from the bit string for that set, change each 1 to 0 and each 0 to 1.

Example:

The bit string for the set {1, 3, 5, 7, 9} (with universal set {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}) is 1 0 1 0 1 0 1 0 1 0.

What is the bit string for the complement of this set?

The bit string for the complement of this set is obtained by replacing 0s with 1s.

This yields the string 0 1 0 1 0 1 0 1 0 1, which corresponds to the set {2, 4, 6, 8, 10}.

To obtain the bit string for the union and intersection of two sets we perform bitwise Boolean Operations on the bit strings representing the two sets.

Example:

The bit strings for the sets {1, 2, 3, 4, 5} and {1, 3, 5, 7, 9} are 1 1 1 1 1 0 0 0 0 0 and 1 0 1 0 1 0 1 0 1 0. Find union and intersection of sets using given bit strings.

Solution

Union:

The bit string for the union of these sets is 11 1110 0000 ∨ 10 1010 1010 = 11 1110 1010, which corresponds to the set {1, 2, 3, 4, 5, 7, 9}.

If either of the bits in the ith position in the two strings is 1 (or both are 1), the bit in the ith position of the bit string of the union is 1. When both bits are 0, is 0. Hence, the bit string for union is the bitwise OR of the bit strings for the two sets.

Intersection:

The bit string for the intersection of these sets is

11 1110 0000 ∧ 10 1010 1010 = 10 1010 0000, which corresponds to the set {1, 3, 5}.

When the bits in the corresponding position in the two strings are both 1,the bit in the ith position of the bit string of the intersection is 1. When either of the two bits is 0 (or both are 0) ,is 0. Hence, the bit string for the intersection is the bitwise AND of the bit strings for the two sets.

Exercise

1. Let A = {1, 2, 3, 4, 5}, B = {2, 3, 6}. Find
   (a) $A \cup B$ (b) $A \cap B$ (c) $A - B$ (d) $B - A$
2. Let A and B be sets. Show that
   (a) $A \cup B = B \cup A$ (b) $A \cap B = B \cap A$
3. Find the sets A and B if $A - B = \{1, 5, 7, 8\}$, $B - A = \{2, 10\}$ and $A \cap B = \{3, 6, 9\}$.
4. Show that if A, B and C are three sets, then $\overline{A \cap B \cap C} = \bar{A} \cup \bar{B} \cup \bar{C}$.
5. Let A = {0, 2, 4, 6, 8, 10}, B = {0, 1, 2, 3, 4, 5, 6} and C = {4, 5, 6, 7, 8, 9, 10}. Find
   (a) $A \cap B \cap C$ (b) $A \cup B \cup C$ (c) $(A \cup B) \cap C$ (d) $(A \cap B) \cup C$
6. Suppose that the universal set is U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. Express each of these sets with bit strings representation.
7. Suppose that the universal set is U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. Find the set specified by each of these bit strings.
   (a) 1 1 1 1 0 0 1 1 1 1 (b) 0 1 0 1 1 1 1 0 0 0 (c) 1 0 0 0 0 1 0 0 1 1

1.2 Function

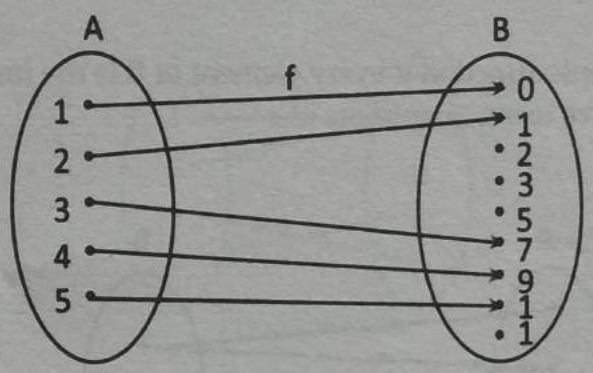
Basic Concepts

Let A and B be two non-empty sets. A function f from A to B is a set of ordered pairs with the property that for each element x in A there is an unique element y in B. The set A is called the domain of the function and the set B is called co-domain. If $(x, y) \in f$, it is customary to write $y = f(x)$, y is called the image of x and x is a pre-image of y. the set consisting all the images of the elements of A under the function f is called the range of f. It is denoted by f(A).

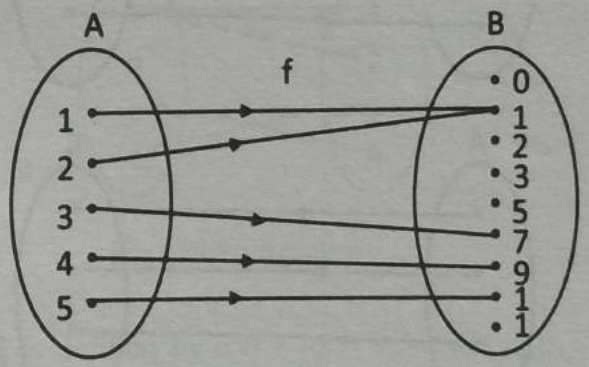
The concept of function is extremely used in mathematics and computer science. For instance functions are used to represent how long it takes to solve a problem of a given size. Many computer program and subroutines are designed to calculate the values of functions.

Example:

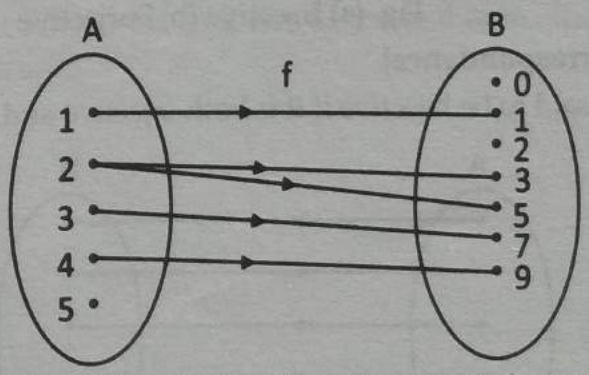
Let A = {1, 2, 3, 4, 5}, B = {0, 1, 2, 3, 5, 7, 9, 12, 13} and f = {(1, 1), (2, 0), (3, 7), (4, 9), (5, 12)}, then f is a function from A to B because each element of A has an unique image in B which can be expressed by a diagram as,



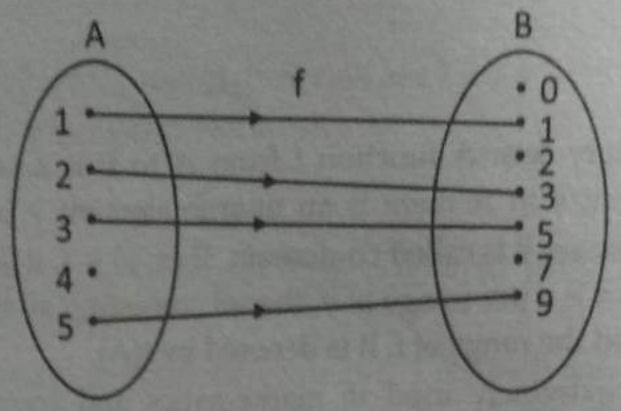
(ii) f = {(1, 1), (2, 1), (3, 7), (4, 9), (5, 12)}, then f is a function from A to B because each element of A has a unique element in B.



(iii) f = {(1, 1), (2, 3), (2, 5), (3, 7), (4, 9)} is not a function because (2, 3) and (2, 5) have the same first component. In a diagram this can be expressed as,



(iv) f = {1, 1), (2, 3), (3, 5), (5, 9)} is not a function since $4 \in A$ has no image in B. In a diagram this can be expressed as,



Sum and Product of Function

Injective function (One to One)

A function from A to B is one-to-one if for all $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$ implies $x_1 = x_2$. We can express that f is one to one using quantifiers as $\forall x_1 \forall x_2 (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$ where universe of discourse is the domain of the function.

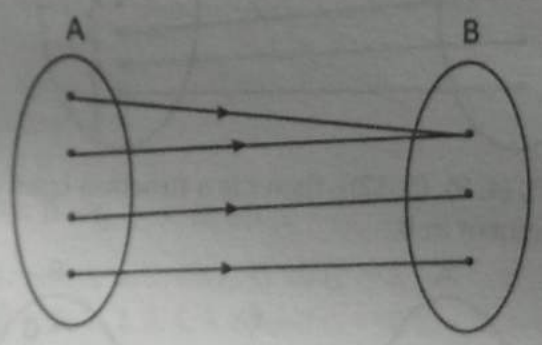
Surjective function (On to)

A function f from A to B is an onto function if every element of B is the image of some element in A. We can express that f is subjective using quantifiers as

$$\forall y \exists x (f(x) = y)$$

Example

(a)



(b)

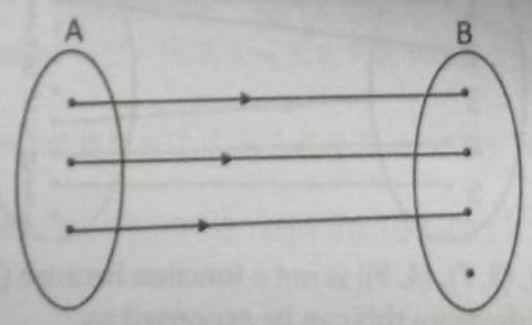


Fig. (a) Injective (b) Surjective

Bijective (One-to-one Correspondence)

A function f from A to B is said to be bijective if it is both injective and surjective.

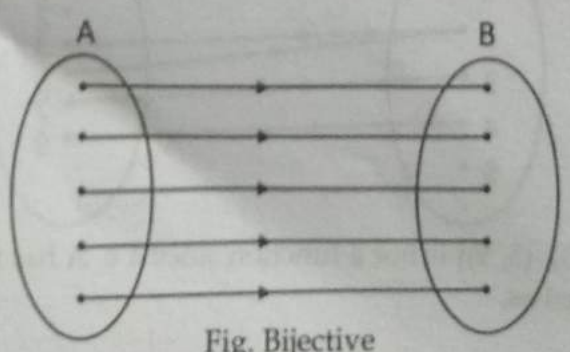


Fig. Bijective

Inverse of a Function

Let $f : A \to B$ be a function which is bijective, then the inverse function of f is the function that assigns to an element b belonging to set B the unique element a in A such that $f(a) = b$. the inverse function of f is denoted by f^{-1}. Hence $f^{-1}(b) = a$ when $f(a) = b$.

A function $f : A \to B$ is invertible if its inverse relation f^{-1} is a function from B to A. In general, the inverse relation f^{-1} may not be a function.

In the case of two functions we define inverse function as,

Let $f : A \to B$ and $g : B \to A$ be two functions then g is said to be inverse of f if $gof = I_A$ and $fog = I_B$

Example

Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ and let $f = \{(1, a), (2, a), (3, d), (4, c)\}$. Show that f is a function and state with a reason, whether f is invertible.

Solution

Here we have $f(1) = a$, $f(2) = a$, $f(3) = d$ and $f(4) = c$. Clearly f is a function. Now $f^{-1} = \{(a, 1), (a, 2), (d, 3), (c, 4)\}$, which is not a function so f is not invertible since $f^{-1}(a) = \{1, 2\}$.

Diagram of f:

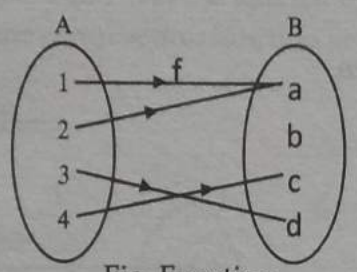


Fig. Function.

Diagram of f^{-1}:

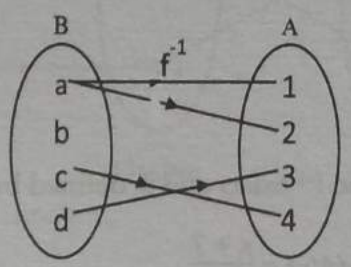


Fig.: Not a function

Example

Show that the mapping $f: R \to R$ is defined by $f(x) = ax + b$, where $a, b, x \in R$, $a \neq 0$, is invertible. Define its inverse.

Solution

Inverse of a function exists if that function is both one-to-one and onto. Therefore, we first show f is one-to-one and then we show it is onto.

For, if $x_1, x_2, \in R$ then $f(x_1) = f(x_2)$

$\Rightarrow \quad ax_1 + b = ax_2 + b$

$\Rightarrow \quad x_1 = x_2$

This proves f is one-to-one.

Again, if $y \in R$, $y = f(x) = ax + b$

$$\Rightarrow \quad x = \frac{(y - b)}{a} \in R$$

and

$$f\left(\frac{(y-b)}{a}\right) = a\frac{(y-b)}{a} + b = y$$

$\therefore$ y is the image of $\frac{(y-b)}{a}$.

Thus, f is onto.

Hence f is one-to-one and onto therefore f^{-1} exists and is defined by $f^{-1}(y) = \frac{(y-b)}{a}$, is a formula defining the inverse function. Here, y is just a dummy variable and can be replaced by x, then $f^{-1}(x) = \frac{(x-b)}{a}$.

Example

Let f: R →R be defined by f(x) = 3x – 7. Find a formula for the inverse function of f and also sketch, in a single diagram, the graphs of y = f(x) and y = $f^{-1}(x)$, making clear relationships between the two graphs.

Solution

Suppose $x_1, x_2 \in R$ and $f(x_1) = f(x_2)$. Then

$f(x_1) = f(x_2) \quad \Rightarrow 3x_1 - 7 = 3x_2 - 7$

$\Rightarrow x_1 = x_2$

Hence f is one-to-one

Also, let $y \in R$ then $y = f(x) = 3x - 7$

$$\Rightarrow \quad x = \frac{y+7}{3}$$

$$\therefore \quad f\left(\frac{y+7}{3}\right) = 3\frac{(y+7)}{3} - 7 = y$$

Thus f is onto.

Since f is both one-to-one and onto. So f^{-1} exists and is defined by $f^{-1}(y) = \frac{y+7}{3}$

In terms of x, the inverse function is, $f^{-1}(x) = \frac{x+7}{3}$

Example

Given function $g(x) = x^2$. Find the inverse of this function and plot both functions in XY-plane.

Solution

Suppose $x_1, x_2 \in R$ such that $g(x_1) = g(x_2)$

$\Rightarrow \quad x_1^2 = x_2^2$

$\Rightarrow \quad x_1 = x_2$

So g is one-to-one.

Also. Let $y \in R$. Then $y = g(x) = x^2$

$x = \sqrt{y}$

and $g(\sqrt{y}) = (\sqrt{y})^2 = y$

$\therefore$ g is onto.

Hence, g is both one-to-one and onto, g^{-1} exists and is

$g^{-1}(y) = \sqrt{y}$.

In terms of x, the inverse is $g^{-1}(x) = \sqrt{x}$

Composition of Functions

Let $f : A \to B$ and $g : B \to C$ be two functions. The composition of f and g, denoted by gof, is a new function from A to C defined by $(gof)(x) = g(f(x))$, for all $x \in A$.

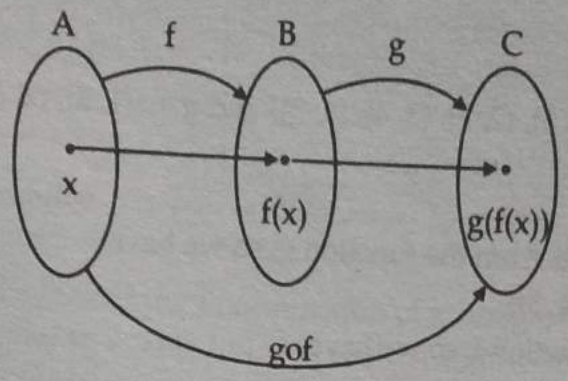


Figure: Illustrates the composition of the two functions f and g.

Example

Let $A = \{1, 2, 3\}$, $B = \{a, b\}$ and $C = \{r, s)$ and $f : A \to B$ defined by $f(1) = a$, $f(2) = a$, $f(3) = b$ and $g : B \to C$ defined by $g(a) = s$, $g(b) = r$. Find the composition function $gof : A \to C$.

Solution

Given that $f : A \to B$ and $g : B \to C$, then,

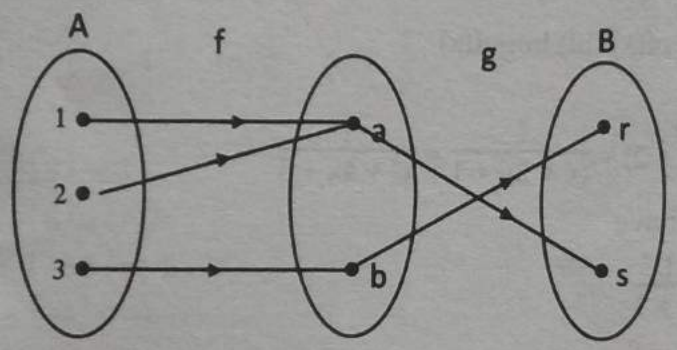


Figure:

Using the definition of composition of function,

$gof(1) = g(f(1)) = g(a) = s$

$gof(2) = g(f(2)) = g(a) = s$

and $gof(3) = g(f(3)) = g(b) = r$

Example

Show that the functions $f(x) = x^3$ and $g(x) = x^{1/3}$, for all $x \in R$ are inverse of one another.

Solution

Since $(fog)(x) = f(g(x)) = f(x^{1/3}) = x = I_x$

$(gof)(x) = g(f(x)) = g(x^3) = x = I_x$

Thus, $g = f^{-1}$ or $f = g^{-1}$.

Example

Let the functions f and g be defined by $f(x) = 2x + 1$ and $g(x) = x^2 - 2$. Find the formula defining the composition function gof.

Solution

We have,

$f(x) = 2x + 1$ and $g(x) = x^2 - 2$

Therefore,

$$\begin{aligned} gof(x) &= g(f(x)) = g(2x+1) \\ &= (2x+1)^2 - 2 \\ &= 4x^2 + 4x + 1 - 2 \\ &= 4x^2 + 4x - 1 \end{aligned}$$

Example

Let V = {1, 2, 3, 4} and let f = {(1, 3), (2, 1), (3, 4), (4, 3)} and g = {(1, 2), (2, 3), (3, 1), (4, 1)}. Find: (a
(b) gof (c) fof.

Solution

The composite function fog starts from the function g, so we have

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

Similarly, gof starts from the function f, so we have,

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

and

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

Example

Let f, g and h : R → R be defined by

$$f(x) = x + 2,\ g(x) = \frac{1}{x^2+1},\ h(x) = 3.$$

Compute (i) gof(x) (ii) $gof^{-1}of(x)$ (iii) hogof(x)

Solution

(i) $gof(x) = g(f(x)) = g(x+2) = \dfrac{1}{(x+2)^2+1} = \dfrac{1}{x^2+4x+5}$

(ii) Since $f^{-1}of(x) = x$ we have

$$gof^{-1}of(x) = g(x) = \frac{1}{x^2+1}$$

(iii) Since $gof(x) = \dfrac{1}{x^2+4x+5}$, then

$$hogof(x) = h\left(\frac{1}{x^2+4x+5}\right) = 3. \text{ (since } h(x) = 3, \forall x)$$

Graph a Functions

We can associate a set of pairs in A×B to each of functions from A to B. This set of pairs is calle
graph of functions.

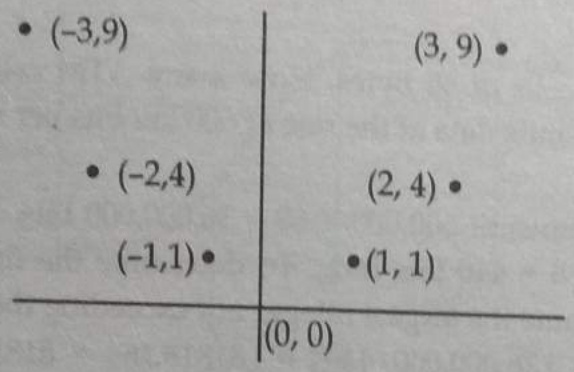
Let f be a function from set A to set B then graph of function f is set of ordered pairs {(a, b): a ∈ A an
f(a) = b}.

Example:

Display the graph of the function $f(x) = x^2$ from the set of integers to set of integers.

Solution

The graph of f is the set of ordered pairs of the form $(x, f(x)) = (x.x^2)$ where x is an integer. This gra
is displayed in figure.



Functions for Computer Science

Floor Function

Let x be a real number then $\lfloor x \rfloor$ called the floor function of x, assigns to the real number x the largest integer that is less than or equal to x. This function rounds x down to the closest integer less than or equal to x. The floor function is often also called the greatest integer function.

Ceiling Function

If x is a real number then $\lceil x \rceil$ called the ceiling function of x, assigns to the real number x the smallest integer that is greater than or equal to x. This function rounds x up to the closest integer greater than or equal to x.

Example

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the value of x.

(i) 8 (ii) 6.02 (iii) −8.5 (iv) −4 (v) $\frac{1}{2}$ (vi) $-\frac{1}{2}$

Solution

(i) $\lfloor 8 \rfloor = 8$ and $\lceil 8 \rceil = 8$

(ii) $\lfloor 6.02 \rfloor = 6$ and $\lceil 6.02 \rceil = 7$

(iii) $\lfloor -8.5 \rfloor = -9$ and $\lceil -8.5 \rceil = -8$

(iv) $\lfloor -4 \rfloor = -4$ and $\lceil -4 \rceil = -4$

(v) $\lfloor \frac{1}{2} \rfloor = 0$ and $\lceil \frac{1}{2} \rceil = 1$

(vi) $\lfloor -\frac{1}{2} \rfloor = -1$ and $\lceil \frac{1}{2} \rceil = 0$

Example

Prove or disprove that $\lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil$ for all real numbers x and y.

Solution

A counter example is supplied by $x=\frac{1}{2}$ and $y=\frac{1}{2}$. With these values we found that $\lceil x+y \rceil = \lceil \frac{1}{2}+\frac{1}{2} \rceil = \lceil 1 \rceil = 1$

but $\lceil x \rceil + \lceil y \rceil = \lceil \frac{1}{2} \rceil + \lceil \frac{1}{2} \rceil = 1+1=2$

Example

Data stored on a computer disk or transmitted over a data network are usually represented as a string of bytes. Each byte is made up of 8 bits. How many bytes are required to encode 300 bits of data?

Solution

To determine the number of bytes needed, we determine the smallest integer that is at least as large as the quotient when 300 is divided by 8. Therefore, the number of bytes required $= \lceil 300/8 \rceil = \lceil 37.5 \rceil$ = 38 bytes.

Example

In ATM, data are organized into cells of 55 bytes. How many ATM cells can be transmitted in 1 minute over a connection that transmits data at the rate of 600 kilobits per second?

Solution

In 1 minute, this connection can transmit 600,000 × 60 = 36,000,000 bits. Each ATM cell is 55 bytes long, which means that it is 55 × 8 = 440 bits long. To determine the number of cells that can be transmitted in 1 minute, we determine the largest integer not exceeding the quotient when 36,000,000 is divided by 440. Consequently, $\lfloor 36{,}000{,}000/440 \rfloor = \lfloor 81818.18 \rfloor = 81818$ ATM can cells can be transmitted in 1 minute over 600,000 kilobit per second connection.

Example

Evaluate $\lceil \log_2 50 \rceil - \lfloor \frac{3}{4} \rfloor$

Solution

Here,

$\lceil \log_2 50 \rceil = 6$, since

$2^5 = 32$ and $2^6 = 64$

So, $\lceil \log_2 50 \rceil - \lfloor \frac{3}{4} \rfloor = 6 - \lfloor 0.75 \rfloor$

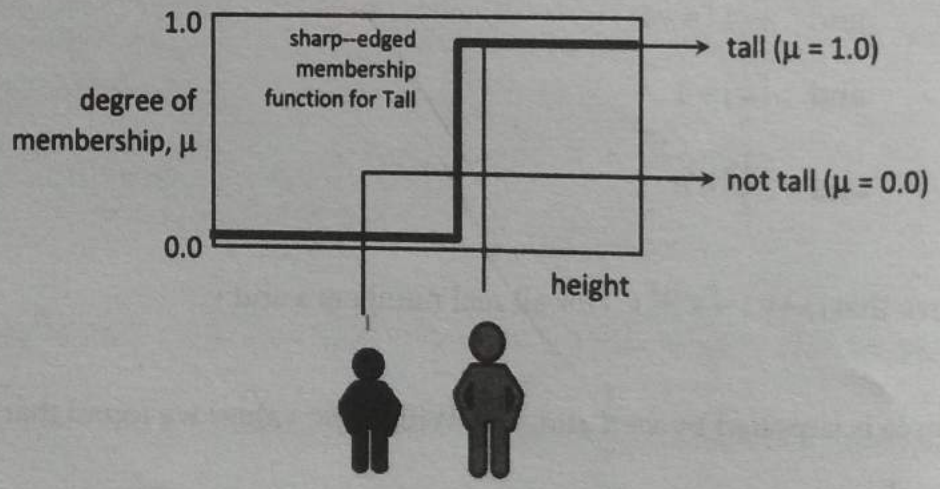
$= 6 - 0$

$= 6$

Fuzzy Set

By definition, set is a collection of things that belong to some domain. Any element either belongs to that set or does not belong to that set.

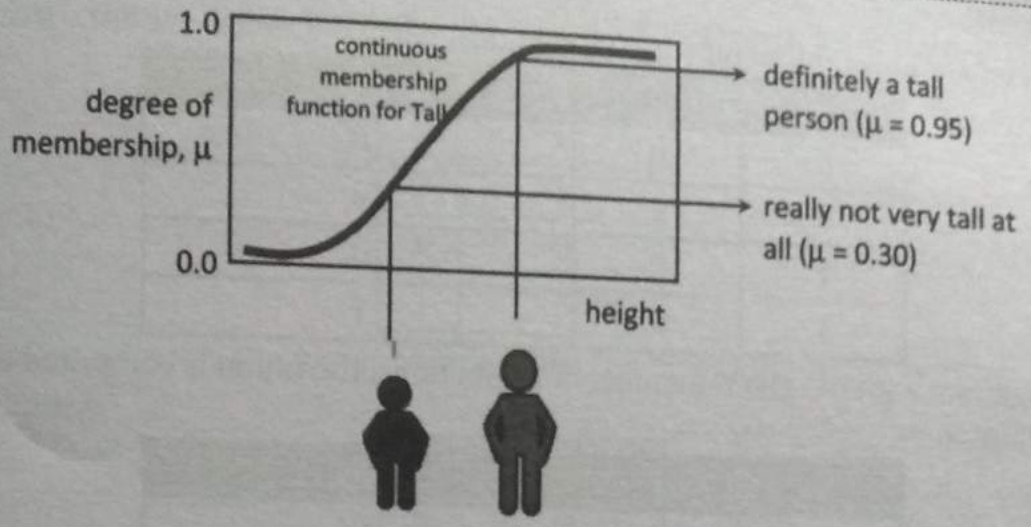
For example, let we have set of tall people where people taller than or equal to 5 feet are considered as tall. This set can be represented graphically as follows:



Figure

This membership functions works nicely for binary operations and mathematics, but it does not work properly in describing the real world. The membership function makes no distinction between somebody who is 6'1" and someone who is 7'1", they are both simply tall. Clearly there is a significant difference between the two heights.

The fuzzy set approach to the set of tall men provides a much better representation of the tallness of a person. The set, shown below, is defined by a continuously inclining function.



Figure

Formal Definition of Fuzzy Set (by Lofti A. Zadeh)

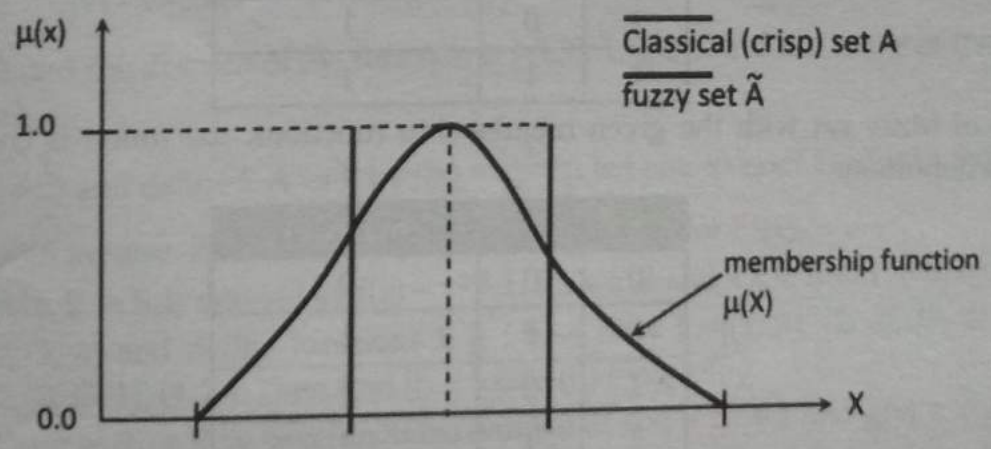
The definition of a fuzzy set by Zadeh's is:

Let **X** be a space of points, with a generic element of **X** denoted by x. Thus $\mathbf{X} = \{x\}$.
A fuzzy set **A** in **X** is characterized by a membership function $f\mathbf{A}(x)$ which associates with each point in **X** a real number in the interval **[0,1]**, with the values of $f\mathbf{A}(x)$ at x representing the "grade of membership" of x in **A**. Thus, the nearer the value of $f\mathbf{A}(x)$ to unity, the higher the grade of membership of x in **A**.

Membership function

For any set X, a membership function on X is any function from X to the real unit interval [0,1] The membership function which represents a fuzzy set A is usually denoted by μA. For an element x of X, the value μA (x) is called the *membership degree* of x in the fuzzy set A The membership degree μA (x) quantifies the grade of membership of the element x to the fuzzy set A .

The value 0 means that x is not a member of the fuzzy set; the value 1 means that x is fully a member of the fuzzy set. The values between 0 and 1 characterize fuzzy members, which belong to the fuzzy set only partially.



Fuzzy Set Operations

Intersection

The membership function of the Intersection of two fuzzy sets A and B with membership functions μ_A and μ_B respectively is defined as the minimum of the two individual membership functions. This is called the *minimum* criterion.

$$\mu_{A \cap B} = \min(\mu_A, \mu_B)$$

For Example: In binary logic, union represent the logical AND operation with the truth table:

x	y	x AND y
0	0	0
0	1	0
1	0	0
1	1	1

But in case of fuzzy set with the given membership functions, the union is computed as follows using above definition:

x	y	min(x,y)
0	0	0
0	1	0
1	0	0
1	1	1
0.2	0.5	0.2
0.7	0.2	0.2
0.6	0.6	0.6

Unions

The membership function of the Union of two fuzzy sets A and B with membership functions μ_A and μ_B respectively is defined as the maximum of the two individual membership functions. This is called the *maximum* criterion.

$$\mu_{A \cup B} = \max(\mu_A, \mu_B)$$

For Example: In binary logic, union represent the logical OR operation with the truth table:

x	y	x OR y
0	0	0
0	1	1
1	0	1
1	1	1

But in case of fuzzy set with the given membership functions, the union is computed as follows using above definition:

x	y	max(x,y)
0	0	0
0	1	1
1	0	1
1	1	1
0.2	0.5	0.5
0.7	0.2	0.7
0.6	0.6	0.6

Complement

The membership function of the Complement of a Fuzzy set A with membership function μ_A is defined as the negation of the specified membership function. This is called the *negation* criterion.

$$\mu_{\bar{A}} = 1 - \mu_A$$

For Example: In binary logic, union represent the logical OR operation with the truth table:

x	NOT x
0	1
0	1
1	0
1	0

But in case of fuzzy set with the given membership functions, the union is computed as follows using above definition

x	1 - x
0	1
0	1
1	0
1	0
0.2	0.8
0.7	0.3
0.6	0.4

Exercise

1. Let X = {1, 2, 3, 4}. Determine whether or not each relation below is a function from X into X.
   (i) f = {(1, 1), (2, 1), (3, 1), (4, 1), (3, 3)}
   (ii) f = {(1, 1), (2, 1), (3, 1), (4, 1)}
   (iii) f = {(2, 1), (3, 4), (4, 4)}
2. Find the value of
   (i) $\lfloor 8.3 \rfloor$ (ii) $\lfloor -8.7 \rfloor$ (iii) $\lceil -5.9 \rceil$
   (iv) $\lceil \frac{1}{3} \rceil$ (v) $\lceil \log_2 51 \rceil$ (vi) $\lfloor \log_3 29 \rfloor$
3. If $f(x) = x^2 - 2$ and the domain of the function is {-1, 0, 1, 2, 3}. Find the range of the function. Is it one-to-one?
4. Let $A = \{x : x \neq \frac{1}{2}\}$ and define $f: A \to R$ by $f(x) = \frac{4x}{2x - 1}$. Is f one-to-one? Find R(f). Explain why $f : A \to R(f)$ has an inverse. Find dom f^{-1}, ran f^{-1} and a formula for $f^{-1}(x)$.
5. If the function $f: R \to R$ is defined by $f(x) = x^2 + 1$, for $x \in R$ and $x \geq 0$, find $f^{-1}(-8)$ and $f^{-1}(17)$.
6. Let S = {1, 2, 3, 4} and define functions $f, g : S \to S$ by f ={(1, 3), (2, 2), (3, 4), (4, 1)} and g = {(1, 4), (2, 3), (3, 1), (4, 2)}. Then find (i) $g^{-1}ofog$ (ii) $f^{-1}og^{-1}ofog$.
7. Let $f: R \to R$ and $g: R \to R$ be two functions defined as $f(x) = 2x + 1$ and $g(x) = x^2 - 2$ then find the composite functions.
   (a) fog (b) fof (c) gof (d) gog (e) fogof
8. Let $f: R \to R$ defined by $f(x) = 3x - 7$. Find the formula for inverse function of f.
9. Find the formula for inverse of $f(x) = \frac{3x + 2}{5x - 7}$

10. Let A = B = R, the set of real numbers. Function f: A → B be given by formula $f(x) = 2x^3$

g: B→A be given by $g(y) = \sqrt[3]{\frac{y}{2}+\frac{1}{2}}$. Show that f is bijection between A and B a bijection between B and A.

11. Let A = B = C = R and consider the function and g: B→C defined by f(a) = 2a + 1, g(verify that $(gof)^{-1} = f^{-1} og^{-1}$.

12. Let F: R→R be a function defined by $f(x) = x^2 + 1$ then find $f^{-1}(-8)$ and $f^{-1}(5)$.

13. Let the function f: R→R defined by

$$f(x) = \begin{cases} 2x - 9 & \text{for } x > 4 \\ 3x^2 + 4 & -1 < x \leq 4 \\ x^2 + 7 & x \leq -1 \end{cases} \text{ find } f^{-1}(6)$$

14. Let f: A→B and g: B→A verify that $g = f^{-1}$ of where

$A = B = R$, $f(a) = \frac{a+1}{2}$, $g(b) = 2b - 1$

15. If the function f: R→R defined by

$$f(x) = \begin{cases} 2x - 4 & x > 1 \\ -3x + 5 & x \leq 1 \end{cases}$$

Determine: $f(1)$, $f\left(\frac{1}{2}\right)$, $f^{-1}(2)$ and $f^{-1}(-5)$.

1.3 Sequence and Summations

Basic Concept of Sequences

Sequences are used to represent ordered lists of elements. Sequences are used in discrete structure to represent solution to certain accounting problems as well as they are also important data structure in computer science.

Definition 1

A sequence is a function from a subset of the set of integers to a set S. We use the notation to denote the image of the integer n and call an as term of sequences. We use notation $\{a_n\}$ to represent a sequence $a_1, a_2, a_3, \ldots\ldots a_n$. here a_i represent the individual terms of sequence $\{a_n\}$

In other words, the succession of quantities each of which is formed according to some definite rule is called a sequence. Examples of a sequence are:

Example consider a sequence $\{a_n\}$, where the nth terms is

$$a_n = \frac{1}{n+1}$$

The list of the terms of the sequence is

$$a_1 = 1/2, a_2 = 1/3, a_3 = 1/4 \ldots\ldots\ldots\ldots$$

Example

(i) 1, 2, 3, 4, 5,..... (ii) 2, 4, 8, 16, 32,..... (iii) $25, 5, 1, \frac{1}{5}, \frac{1}{25}, \ldots\ldots\ldots\ldots$

Geometric Progression

A geometric progression is a sequence of the form a, ar, ar^2, ar^3 ..... ar^n, where the initial term 'a' and common ration 'r' are real numbers.

Example:

The sequence $\{b_n\}$ with $b_n = 2.5^n$. The list of terms are: $b_1 = 2$, $b_2 = 10$ and so on.

Example:

10, 50, 250, 1250, ...

$2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \ldots\ldots$

Arithmetic Progression

An arithmetic progression is a sequence of form a, a + d, a + 2d, ... a + and where initial term is a and common difference is d.

Example

The sequence $\{s_n\}$ with $S_n = -1 + 4n$ with initial term – 1 is

$s_0 = -1$

$s_1 = -1 + 4 \times 1 = 3$

$s_2 = -1 + 4 \times 2 = 7$

$s_3 = -1 + 4 \times 3 = 11$

.....

$\therefore \quad \{s_n\} = -1, 3, 7, 11, \ldots\ldots$

Example

The sequence $\{t_n\}$ with $t_n = 7 - 3n$ with initial term 7 is

$s_0 = 7$

$s_1 = 7 - 3 \times 1 = 4$

$s_2 = 7 - 3 \times 2 = 1$

$s_3 = 7 - 3 \times 3 = -2$

.....

$\therefore \quad \{t_n\} = 7, 4, 1, -2, \ldots\ldots$

Special Integer sequences

A common problem in discrete mathematics is finding a formula or a general rule for constructing the terms of sequence. Sometimes only a few terms of sequence solving a problem are known; the goal is to identify the sequence. Even though the first few term may not totally determine the whole sequence, these first few terms may help us to find the general formula for the sequences.

An integer sequence is a sequence (i.e., an ordered list) of integer numbers

Example

Find formulae for the sequence with the following first five terms: 1,1/2,1/4,1/8,1/16.

Solution:

We recognize that the denominators are power of 2. The sequence with $a_n=a/2^n$, n = 0,1,2..... is a possible match. This proposed sequence is a geometric progression with a=1 and r=1/2.

Example

How can we produce the terms of sequence if the first 10 terms are 5, 11, 17, 23, 29, 35, 41, 47, 53, 59?

Solution

Here each next term in the sequence is greater than previous term by 6. So n the term could be found by starting with 5 and adding 6 for n-1 terms.

i.e $a_n=5+6(n-1)$

Example

An integer is even if it is 'evenly divisible' by two. For example, 2 is even because the result of dividing it by itself is 1.

A formal definition of an even number is that it is an integer of the form n = 2k, where k is an integer. Therefore the sequence of even integer number $\{a_n\}$ can be represented with $a_n=2n$ for all n.

Summations

Summation is the operation of adding a sequence of numbers. If numbers are added sequentially from left to right, any intermediate result is a partial sum, prefix sum, or running total of the summation. The numbers to be summed (called addends, or sometimes summands) may be integers, rational numbers, real numbers.

For the summation of the sequence of consecutive integers from 1 to 100 one could use an addition expression involving an ellipsis to indicate the missing terms: 1 + 2 + 3 + 4 + ... + 99 + 100. In this case the reader easily guesses the pattern; however, for more complicated patterns, one needs to be precise about the rule used to find successive terms, which can be achieved by using the summation operator "Σ".

Using this sigma notation the above summation is written as:

$$\sum_{j=m}^{n} a_j$$

Here the variable j is called the index of summation, and the choice of the letter j as the variable is arbitrary i.e. we may choose name as k, i and so on.

Example

Express the sum of first 100 terms of the sequence $\{a_n\}$ where $a_n=2n$ in terms of summation notations

Solution:

The lower limit for the index of summation is 1 and the upper limit is 100. Hence

Series

The summation of an infinite sequence of values is called a series.

Some useful summation formulae

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

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

$$\sum_{k=1}^{n} k^3 \qquad \frac{n^2(n+1)^2}{4}$$

$$\sum_{k=0}^{n} ar^k \qquad \frac{ar^{n+1} - a}{r-1}, r \neq 1$$

$$\sum_{k=0}^{¥} x^k \qquad \frac{1}{(1-x)}$$

Example

What is the value of $\sum_{k=1}^{6} k^2$?

Solution: We have $\sum_{k=1}^{6} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2$

$= 1 + 4 + 9 + 16 + 25 + 36$

$= 91$

Example

What is value of $\sum_{i=1}^{4} \sum_{j=1}^{3} ij$?

Solution

To evaluate the double sum, first expand the inner summation and then continue by computing the outer summation:

$$\sum_{i=1}^{4} \sum_{j=1}^{3} ij = \sum_{i=1}^{4} (i + 2i + 3i)$$

$$= \sum_{i=1}^{4} 6i$$

$= 6 + 12 + 18 + 24$

$= 60$

Example

What are the values of each of these sums of a geometric progression?

(i) $\sum_{j=0}^{5} 3.2^j$ (ii) $\sum_{j=1}^{6} 2^j$ (iii) $\sum_{j=0}^{3} 2.(-3)^j$

Solution

(i) $\sum_{j=0}^{5} 3.2^j = 3.2^0 + 3.2^1 + 3.2^2 + 3.2^3 + 3.2^4 + 3.2^5$

$= 3 + 6 + 12 + 24 + 48 + 96 = 189$

(ii) $\sum_{j=1}^{6} 2^j = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6$

$= 2 + 4 + 8 + 16 + 32 + 64 = 126$

(iii) $\sum_{j=0}^{3} 2.(-3)^j = 2(-3)^0 + 2(-3)^1 + 2(-3)^2 + 2(-3)^3$

$= 2 - 6 + 18 - 54 = -40$

Exercise

1. Find at least three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule.
2. For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list.
   a. 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, ...
   b. 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, ...
   c. 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, ...
   d. 3, 6, 12, 24, 48, 96, 192, ...
   e. 15, 8, 1, -6, -13, -20, -27, ...
   f. 2, 16, 54, 128, 250, 432, 686, ...
3. Find the value of following summations:

   a) $\sum_{x=1}^{6}(x+1)$ b) $\sum_{j=0}^{4}(-2)^j$ c) $\sum_{k=0}^{4}(2^{k+1}-2^k)$
4. Compute each of these double sums.

   a) $\sum_{i=1}^{2}\sum_{j=1}^{3}(i-j)$ b) $\sum_{i=0}^{3}\sum_{j=0}^{2}(3i+2j)$
5. What is the value of each of these sums of a geometric progression?

   (i) $\sum_{j=0}^{6}(3^j - 2^j)$ (ii) $\sum_{j=0}^{5}(2.3^j + 3.2^j)$ (iii) $\sum_{i=0}^{7} 3.2^{i-1}$
6. What are the terms a_0, a_1, a_2 and a_3 of the sequence $\{a_n\}$, where a_n equals:

   a) $(-2)^n$ b) $7+4^n$ c) $2^n+(-2)^n$
7. List the first ten terms of each of these sequences
   a) The sequence that begins with 2 and in which each successive term is 3 more than the preceding terms.
   b) The sequence that begins with 3, where each succeeding term is three times the preceding term.
   c) The sequence whose first two terms are 1 and each succeeding terms is the sum of the preceding terms.
   d) The sequence whose n^{th} term is $3^n - 2^n$.

□□□

Chapter 2

The Fundamentals: Integers and Matrices

Integer and Division

Introduction

The branch of mathematics which study about the integers and their properties is called number theory. Computer science uses the different concept related to number theory. In this section, we will discuss the basic concept of number theory, properties of integer, prime numbers, divisibility and modular arithmetic.

Divisibility

If a and b are integers where a! = 0, we say a divides b if there is an integer c such that b =ac. When a divides b then we say a is a factor of b and the b is a multiple of a. notational representation a | b is for a divides b.

Example

4 | 12 means 4 divides 12 where a = 4, b = 12and c = 3.

Example

Determine whether 5 | 7 and whether 4 | 16.

Here, $5 \nmid 7$ since 7/5 is not an integer. On the other hand, 4 | 16 because 16/4 is an integer.

Division Algorithm

Let 'a' be integer and 'd' a positive integer. Then there are unique integers q and r, with 0 < r < d, such that a = dq + r. here, 'a' is called dividend, d is called divisor, q is called quotient, and r is called remainder. For e.g. 305(dividend) = 10(divisor)*30(quotient) +5(remainder).

Theorem

Let a,b, and c be integers. Then

1.if a | b and a | c, then a | (b+c);

2.if a | b, then a | bc for all integers c;

3.if a | b and b | c, then a | c.

Proof:

1. Given that a | b and a | c, so by the definition of divisibility we can say that there are integers and q such that b = ap and c = aq. From this we can write, b+c = ap + aq i.e. b+c = a(p+q) form this we can say that a divides b+c.
2. Given that a | b, by the definition of divisibility we can say there is an integer p such that b = so for any integer c we can write, bc = apc this means a divides bc since pc is an integer too.
3. Given that a | b and b | c, by the definition of divisibility we have integers p and q such that b ap and c = bq i.e. c = apq Since, pq is an integer we conclude that a divides c.

Modular Arithmetic

This is an arithmetic calculation system which works only with integer number. When an integer is divided by another positive integer 'm'. Then the remainder 'r' is obtained - such that a = m quotient +r. The operation which gives remainder is known as modular operation and the process called modular arithmetic.

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides a We use the notation ab(mod m) to indicate that a is congruent to b modulo m. for e.g. 23 is congru to 11 modulo 2 since 23 -11 = 12 is divisible by 2.

Example:

Determine whether 19 is congruent to 1 modulo 3.

Solution

Here, a = 19

b = 1

m = 3

Then

a = b mod in divides a - b

i.e. 3 divide 19 - 1 ⇒ 3 divide 18 is true.

Applications of Modular Arithmetic: Congruence

(a) Hashing function

Hashing is the mapping of key or information into a fixed message. Suppose a bank has records each of its customers. Now, to access these records quickly, the account number of customer can used as key information and using hashing function, we can map key into particular memo location where record is kept.

There are different hash functions, but most commonly used one is

h(k) = k mod m

Where,

k is the key value

m is the size of hash table

and h(k) is the memory location for the records that has 'k' as its key

Example

Which memory locations are assigned by the hashing function h(k) = k mod 100, the rewards of b customers with following A/c numbers?

(a) 104578690 (b) 432222187

Solution

Here,

$k = 104578690$

$m = 100$

Then,

$h(k) = k \bmod m$

$h(104578690) = 104578690 \bmod 100$

$= 90 \rightarrow$ hash value or memory location and record of customer with account number 104578690 is assigned to memory location '90'.

(b) Pseudo Random Number

Numbers that are generated by a process or algorithm or machine whose outcome is unpredictable, are called random numbers.

- Numbers that are generated by a process or algorithm or machine whose outcome is unpredictable, are called random numbers.
- Pseudo means false (not true), so pseudo random numbers means numbers are that are generated using computer or machine.
- The most commonly used method/procedure to generate pseudo-random numbers is linear congruential method.
- The linear congruential method produces sequence of integer between zero and m - 1.

Using the following recursive formula:

$x_{i+1} = (ax_i + c) \bmod m$

Where,

x_0 = is the sled or initial value

a & c are constant

m is the modulus

For example: Generate first five random numbers using LCM method with $X_0 = 27$, $a = 17$, $C = 43$ and $m = 100$.

Solution

Here,

$x_0 = 27$

$x_1 = (a*x_0 + c) \bmod 100$

$= (17 * 27 + 43) \bmod 100$

$= 502 \bmod 100$

$= 2$

Similarly,

$x_2 = (a * x_1 + c) \bmod 100$

$= (17 * 2 + 43) \bmod 100$

$= 77 \bmod 100 = 77$

$x_3 = (a * x_2 + c) \bmod 100$

$= (17 * 22 + 43) \bmod 100$

$= 1352 \bmod 100$

$= 52$

$x_4 = (a * x_3 + c) \bmod 100$
$= (17 * 52 + 43) \bmod 100$
$= 927 \bmod 100 = 27$

Therefore, sequence of random number is 27, 2, 77, 52, 27, ...

Primes

A positive integer greater than 1 and divisible by only 1 or itself is called prime. If the positive integer is not a prime then it is a composite number. For e.g.: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 and 37.

Theorem (The Fundamental Theorem of Arithmetic)

Statement: Every positive integer greater than one can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Example

Find the prime factorization of 99, 110, 645 and 875.

Solution: The prime factorization of 99, 110, 645and 875 are given by

$99 = 3 . 3 . 11 = 3^2 . 11$

$110 = 2 . 5 . 11$

$645 = 3 . 5 . 43$

$875 = 5 . 5 . 5 . 7 = 5^3 . 7$

Example

Find the prime factorization of 7007.

Solution

To find prime factorization of 7007, first perform divisions of 7007 by successive primes beginning with 2. Since, none of the primes 2,3, 5 divides 7007. However 7 divides so we do 7007/7=1001.

Next, divide 1001 by successive primes, beginning with 7. So, 1001/7=143. Continue by dividing 143 beginning with 7. Although 7 does not divide 143, so we try through 11 and 11 divides 143. 143/11=13 and 13 is prime itself.

Therefore, prime factorization of 7007 is 7 . 7 . 11 . 13

GCD and LCM

Let a and b be integers, not both zero. The largest integer d such that d|a and d|b is called the **greatest common divisor (gcd)** of a and b. we denote gcd of a and b by gcd(a,b).

Relative prime

Two integers a and b are set to be relative prime if gcd(a, b) = 1. For example, gcd(3, 5) = 1, so 3 and 5 are relatively prime.

The **least common multiple (lcm)** of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by lcm(a,b).

Prime factorization method to calculate GCD and LCM

⇒ Suppose let a and b are two integers which are not equal to zero i.e. a, b ≠ 0.

⇒ The prime factor of $a = P_1^{a_1}, P_2^{a_2}, ..., P_n^{a^n}$

and The prime factor of $b = P_1^{b_1}, P_2^{b_2}, ..., P_n^{b_n}$

Then,

$$\gcd(a, b) = P_1^{\min(a_1, b_1)} * P_2^{\min(a_2, b_2)} * \ldots P_n^{\min(a_n, b_n)}$$

and $\text{LCM}(a, b) = P_1^{\max(a_1, b_1)} * P_2^{\max(a_2, b_2)} * \ldots P_n^{\max(a_n, b_n)}$

Pairwise relative prime

The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ where $1 \le i \le j \le n$.

Example:

Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution

Since gcd (10, 17) = 1

gcd (10, 21) = 1

and gcd (17, 21) = 1

Therefore, the given number sequence 10, 17 and 21 are pairwise relatively prime.

Example

Use prime factorization to find the gcd of 12 and 30.

Solution

Prime factorization of 12 and 30 are

$12 = 2.2.3$ $\qquad$ $30 = 2.3.5$

$12 = 2^2.3^1.5^0$ $\qquad$ $30 = 2^1.3^1.5^1$

$\therefore \quad \gcd(12, 30) = 2^{\min(2, 1)}.3^{\min(1, 1)}.5^{\min(0, 1)}$

$= 2^1.3^1.5^0$

$\gcd(12, 30) = 6$

Example

Use prime factorization to find the LCM of 12 and 18.

Solution

Prime factorization of 12 and 18 are:

$12 = 2.2.3$ $\qquad$ $18 = 2.3.3.3$

$= 2^2.3^1$ $\qquad$ $= 2^1.3^3$

$\therefore \quad \text{LCM}(12, 18) = 2^{\max(2, 1)}.3^{\max(1, 3)}$

$= 2^2.3^3$

$= 4.27$

$\text{LCM}(12, 18) = 108$

The Euclidean Algorithm

It is used to compute greatest common divisor. The greatest common divisor, represented as gcd(a,b) and is defined as:

gcd(a,b)=d , where *d* is the largest number that divide both *a* and *b*.

If gcd(a, b) = 1 then we say that a and b are relatively prime, which means that both a and b do not divide each other.

Pseudo code for Euclidean Algorithms:

INPUT: Two non-negative integers *a* and *b* with $a \ge b$.

OUTPUT: gcd(a, b).

1. While b > 0, do
   - Set r = a mod b,
   - a = b,
   - b = r
2. Return *a*

Question 1(a): Find gcd(421, 111).

Answer:

Example 1: Find gcd(421,111)

Solution: The use of Euclidean algorithm gives following table:

421 = 111 x 3 + 88	(larger number on left)
111 = 88 x 1 + 23	(shift left)
88 = 23 x 3 + 19	(Note how 19 moves down the "diagonal")
23 = 19 x 1 + 4	
19 = 4 x 4 + 3	
4 = 3 x 1 + 1	(last non-zero remainder is 1)
3 = 1 x 3 + 0	

The last non-zero remainder is 1 and therefore gcd(421, 111) = 1.

Extended Euclidean Algorithm

It is just another way of finding greatest common division as we did it using Euclidean algorithm. The pseudo code is illustrated below:

INPUT: Two non-negative integers *a* and *b* with a ≥ b.
OUTPUT: d = gcd(a, b) and integers *x* and *y* satifying ax + by = d.

1. If b = 0 then set d = a, x = 1, y = 0, and return(*d*, *x*, *y*).
2. Set $x_2 = 1$, $x_1 = 0$, $y_2 = 0$, $y_1 = 1$
3. While b > 0, do
   a. q = floor(a/b), r = a - qb, $x = x_2 - qx_1$, $y = y_2 - q\,y_1$.
   b. a = b, b = r, $x_2 = x_1$, $x_1 = x$, $y_2 = y_1$, $y_1 = y$.
4. Set d = a, $x = x_2$, $y = y_2$, and return(*d*, *x*, *y*).

Algorithms for Integer Operations

The algorithms for performing operations with integers using their binary expansions are extremely important in computer arithmetic because to analyze the computational complexity of these algorithms in terms of the actual number of bit operations.

Addition of Integers

```
procedure add(a, b: positive integers)
{the binary expansions of a and b are (a_{n-1} a_{n-2} ..... a_1a_0)_2
    and (b_{n-1} b_{n-2} ..... b_1b_0)_2, respectively}
c = 0
for j = 0 to n - 1
begin
```

$d = \lfloor (a_j + b_j + c)/2 \rfloor$

$s_j = a_j + b_j + c - 2d$

$c = d$

end

$s_n = c$

{the binary expansion of the sum is $(s_n\, s_{n-1} \ldots s_0)_2$}

Example

Add $a = (1110)_2$ and $b = (1011)_2$.

Solution

Following the procedure specified in the algorithm, first note that

$a_0 + b_0 = 0 + 1 = 0 . 2 + 1,$

so that $c_0 = 0$ and $s_0 = 1$. Then, since

$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 . 2 + 0.$

it follows that $c_1 = 1$ and $s_1 = 0$. Continuing,

$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 . 2 + 0,$

so that $c_2 = 1$ and $s_2 = 0$. Finally, since

$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 . 2 + 1,$

it follows that $c_3 = 1$ and $s_3 = 1$. This means that $s_4 = c_3 = 1$. Therefore, $s = a + b = (11001)_2$.

Multiplication of Integers

Let a and b be two binary integers then we can compute a.b using

$ab_j = a$ if $b_j = 1$ and $abj = 0$ if $b_j = 0$

Each time we multiply a term by 2, we shift its binary expansion one place to the left and add a zero at the tail end of expansion. Similarly, we can obtain $(ab_j)\, 2^j$ by shifting the binary expansion of ab_j j places to the left, adding j zero bits at the tail.

Finally we obtain ab by adding the n-integers

$ab_j\, 2^j, j = 0, 1, 2, \ldots, n - 1$

Algorithm

Procedure multiply (a.b: positive integers)

The binary expansion of a and b are

$(a_{n-1}\, a_{n-2} \ldots a_1\, a_0)_2$ and $(b_{n-1}\, b_{n-2} \ldots b_1\, b_0)_2$

For j = 0 to n – 1

begin,

if $b_j = 1$ then c_j =- a shifted j places.

Else $c_j = 0$

and

{$c_0\, c_1 \ldots, c_{n-1}$ are the partial product]

P = 0

For j = 0 to n – 1

$P = P + c_j$

{P is the value of ab]

Integer Division Algorithm

Procedure division (a : integer, d: positive integer)

```
    a = 0
    r = |a|
While r ≥ d
begin
    r = r - d
    q = q + 1
end
    if a < 0 and r > 0 then
begin
    r = d - r
    q = - (q + 1)
    end
{q is quotient and r is remainder}
```

Modular Exponential Algorithm

```
Procedure modular (b: integer, n = (a_{k-1} a_{k-2} .... a_0)_2
                                , m: positive integer
    x = 1
    P = b mod m
for i = 0 to k - 1
begin
    if a_i = 1 then x = (x . p) mod m
    P = (P . P) mod m
end
    {x equals b^n mod m}
```

Euclidean Algorithm

```
Procedure gcd (a, b : positive integers)
    x = a, y = b
while y ≠ 0
begin
    r = x mod y
    x = y
    y = r
end {gcd (a, b) is x}
```

Application of Number Theory

- **Linear combination**

Let a and b are two positive integers. Then gcd (a, b) can be expressed as linear combination integer coefficients of a and b i.e. if a and b are positive integer then there exist integer s and t that

$$\gcd(a, b) = sa + tb$$

Example:

Express gcd (252, 198) = 18 as a linear combination of 252 and 198.

Solution

Using Enclidean algorithm,

$252 = 1.198 + 54$

$198 = 3.54 + 36$

$54 = 1.36 + 18$

$36 = 2 * 18$

Using the next to last division, we can express gcd (252, 198) = 18 as libeal combinations i.e.

$18 = 54 - 1 * 36$ .....(i)

where, s = 1 and t = - 1

Similarly, from second division,

$36 = 198 - 3 * 54$ .....(ii)

From equation (i) and (ii) [Substitute value of 36 into (i)]

$18 = 54 - 1(198 - 3 * 54)$

$= 4 * 54 - 198$ .....(iii)

From first division, we have $54 = 252 - 1 * 198$ .....(iv)

Now, substitute value of 54 from (iv) to (iii), we have

$18 = 4 * [252 - 198] - 198$

$= 4 * 252 - 5 * 198$ which is of the form

$18 = 5 * 252 + t * 198$ with

$s = 4$ & $t = - 5$

Example

Express the gcd of 33 & 44 as linear combination of these integer.

Solution

Using Endidean Algorithm

$44 = 1 * 33 + 11$

$33 = 3 * 21$

From next to last division,

$11 = 44 - 1 * 33$

which is in the form of

$11 = 5 * 44 + t * 33$

with s = 1 & t = - 1

Example

Find 54t when gcd (124, 232) = 1

Using Endedian algo

$232 = 1.124 + 108$ .....(i)

$124 = 1 * 108 + 16$ .....(ii)

$108 = 6 * 16 + 12$ .....(iii)

$16 = 1 * 12 + 4$ .....(iv)

$12 = 3 * 4$ .....(iv)

From next to last division,

$4 = 16 - 1 * 12$ .....(v)

From third step above,

$$12 = 108 - 6 * 16 \quad .....(vi)$$

From (v) and (vi), we have

$$4 = 16 - [108 - 6 * 16]$$

$$4 = 16 - 108 + 6 * 16$$

$$= 7 * 16 - 108 \quad .....(vi)$$

From 2nd steps,

$$16 = 124 - 1 * 108 \quad .....(viii)$$

Again, substituting value from (viii) to (vi)

$$4 = 7[124 - 1 * 108] - 108$$

$$= 7 * 124 - 8 * 108 \quad .....(ix)$$

Finally, from first step,

$$108 = 232 - 1 * 124 \quad .....(x)$$

Now, from (ix) and (x),

$$4 = 7 * 124 - 8[232 - 1 * 124]$$

$$4 = 7 * 124 - 8 * 232 + 8 * 124$$

$$= 15 * 124 - 8 * 232$$

which is in the form of

$$4 = 5 * 124 + t * 232$$

where,

$$s = 15 \ \& \ t = -8$$

- **Cryptology**

Julius Caesar first used the concept of Cryptology. Cryptology means the study of secret massag For example: the massage transferred from one part of world to another part of world by usi internet, and then there is a chance of breaking/hacking this massage. It needs to transfer t massage in coded form so that if someone else gets the message on the way, he/she may not be a to understand that message.

The word ***cryptography*** comes from two Greek words meaning "*secret writing*" and is the art a science of information hiding. This field is very much associated with mathematics and comp science with application in many fields like computer security, electronic comme telecommunication, etc.

In the ancient days, cryptography was mostly referred to as ***encryption*** – the mechanism to con the readable ***plaintext*** into unreadable (incomprehensible) text i.e. ***ciphertext***, and ***decryption*** - opposite process of encryption i.e. conversion of ciphertext back to the plaintext. Though consideration of cryptography was on message confidentiality (encryption) in the past, now cryptography considers the study and practices of authentication, digital signatures, inte checking, and key management, etc.

Encryption mostly provides the secrecy of massage being transmitted over the communic network. This is called confidentiality of massage. The only sender knows the keys and can dec the massage.

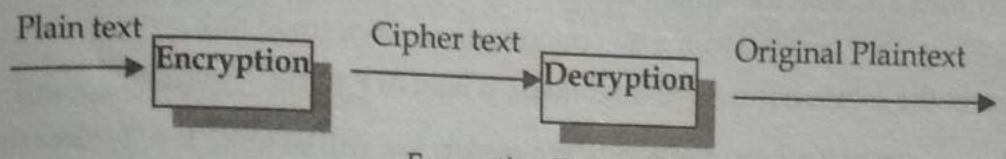
Definitions

Encryption is the process of encoding a message so that its meaning is not obvious i.e. conv information from one form to some other unreadable form using some algorithm called *ciphe*

the help of secret message called ***key***. The converting text is called is ***plaintext*** and the converted text is called ***ciphertext***.

Decryption is the reverse process, transforming an encrypted message back into its normal, original form. In decryption process also the use of key is important.

Alternatively, the terms ***encode*** and ***decode*** or ***encipher*** and ***decipher*** are used instead of ***encrypt*** and ***decrypt***. That is, we say that we encode, encrypt, or encipher the original message to hide its meaning. Then, we decode, decrypt, or decipher it to reveal the original message.



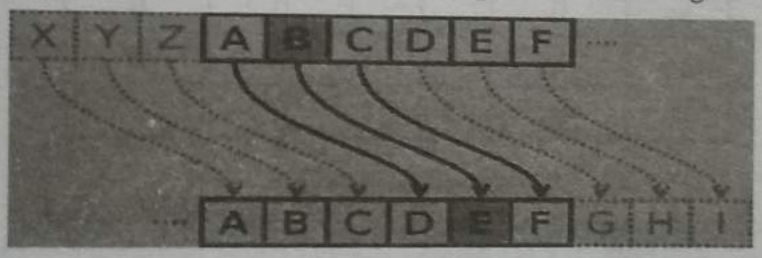
Encryption-Decryption

Crypto analysis is the breaking of codes. Cryptanalysis encompasses all of the techniques to recover the plaintext and/or key from the cipher text.

The combined study of cryptography and cryptanalysis is known as ***cryptology***. Though most of the time we use cryptography and cryptology in the same way.

Example of Encryption:

One of the simplest example of cryptosystem is substitution cipher where each letter is replaced by a letter from some position (k) ahead using the circular alphabetic ordering i.e. letter after Z is A.



Caesar Cipher

So when we encode HELLO WORLD, the cipher text becomes KHOORZRUOG. Here we number each English alphabet starting from 0 (A) to 25 (Z). Each letter of the clear message is replaced by the letter whose number is obtained by adding the key (a number from 0 to 25) to the letter's number modulo 26. See the picture to visualize the Caesar cipher.

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1, ..., Z = 25.

Now, Encryption of a letter c by a shift k can be described mathematically as,

$$c = E_k(m) = (m+k) \bmod 26$$

Decryption is performed similarly,

$$m = D_k(c) = (c+26-k) \bmod 26$$

Example

Encrypt the word DISCRETE MATH using the ceaser cipher E(m) = (m + 2) mod 26.

Solution

Plain text	D	I	S	C	R	E	T	E	M	A	T	H
Value	3	8	18	2	17	4	19	4	12	0	19	7
(Value +2) mod 26	5	11	20	4	19	6	21	6	14	2	21	9
Cipher text	F	K	U	E	T	G	V	G	O	C	V	J

∴ Cipher Text: FKUETGVG OCVJ

Similarly, consider some examples of Caesar cipher;

Plaintext: MEET ME AFTER THE TOGA PARTY

Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB

The Chinese Remainder Theorem

Chinese Remainder Theorem: If $m_1, m_2, .., m_k$ are pairwise relatively prime positive integers, an $a_1, a_2, .., a_k$ are any integers, then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ ...,\ x \equiv a_k \pmod{m_k}$$

have a solution, and the solution is unique modulo m, where $m = m_1 m_2 \cdots m_k$.

Proof that a solution exists: To keep the notation simpler, we will assume k = 4. Note the pro constructive, i.e., it shows us how to actually construct a solution.

Our simultaneous congruences are

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ x \equiv a_3 \pmod{m_3},\ x \equiv a_4 \pmod{m_4}.$$

Our goal is to find integers w_1, w_2, w_3, w_4 such that:

	value mod m_1	value mod m_2	value mod m_3	value mod m_4
w_1	1	0	0	0
w_2	0	1	0	0
w_3	0	0	1	0
w_4	0	0	0	1

Once we have found w_1, w_2, w_3, w_4, it is easy to construct x:

$$x = a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4.$$

Moreover, as long as the moduli (m_1, m_2, m_3, m_4) remain the same, we can use the same w_1, w_2 w_4 with any a_1, a_2, a_3, a_4.

First define:

$$z_1 = m / m_1 = m_2m_3m_4$$
$$z_2 = m / m_2 = m_1m_3m_4$$
$$z_3 = m / m_3 = m_1m_2m_4$$
$$z_4 = m / m_4 = m_1m_2m_3$$

Note that

i) $z_1 \equiv 0 \pmod{m_j}$ for j = 2, 3, 4.

ii) $\gcd(z_1, m_1) = 1$. (If a prime p dividing m_1 also divides $z_1 = m_2m_3m_4$, then p divides m_2, m_3, or m_4.)

and likewise for z_2, z_3, z_4.

Next define:

$$y_1 \equiv z_1^{-1} \pmod{m_1}$$
$$y_2 \equiv z_2^{-1} \pmod{m_2}$$
$$y_3 \equiv z_3^{-1} \pmod{m_3}$$
$$y_4 \equiv z_4^{-1} \pmod{m_4}$$

The inverses exist by (ii) above, and we can find them by Euclid's extended algorithm. Note that

iii) $y_1z_1 \equiv 0 \pmod{m_j}$ for j = 2, 3, 4. (Recall $z_1 \equiv 0 \pmod{m_j}$)

iv) $y_1z_1 \equiv 1 \pmod{m_1}$

and likewise for y_2z_2, y_3z_3, y_4z_4.

Lastly define:

$$w_1 \equiv y_1z_1 \pmod{m}$$
$$w_2 \equiv y_2z_2 \pmod{m}$$
$$w_3 \equiv y_3z_3 \pmod{m}$$
$$w_4 \equiv y_4z_4 \pmod{m}$$

Then w_1, w_2, w_3, and w_4 have the properties in the table on the previous page.

Example

Solve the simultaneous congruences

$$x \equiv 6 \pmod{11},\ x \equiv 13 \pmod{16},\ x \equiv 9 \pmod{21},\ x \equiv 19 \pmod{25}.$$

Solution

Since 11, 16, 21, and 25 are pairwise relatively prime, the Chinese Remainder Theorem tells us that there is a unique solution modulo m, where $m = 11 \cdot 16 \cdot 21 \cdot 25 = 92400$.

We apply the technique of the Chinese Remainder Theorem with

$$k = 4,\ m_1 = 11,\ m_2 = 16,\ m_3 = 21,\ m_4 = 25,$$
$$a_1 = 6,\ a_2 = 13,\ a_3 = 9,\ a_4 = 19,$$

to obtain the solution.

We compute

$$z_1 = m / m_1 = m_2m_3m_4 = 16 \cdot 21 \cdot 25 = 8400$$
$$z_2 = m / m_2 = m_1m_3m_4 = 11 \cdot 21 \cdot 25 = 5775$$
$$z_3 = m / m_3 = m_1m_2m_4 = 11 \cdot 16 \cdot 25 = 4400$$
$$z_4 = m / m_4 = m_1m_3m_3 = 11 \cdot 16 \cdot 21 = 3696$$
$$y_1 \equiv z_1^{-1} \pmod{m_1} \equiv 8400^{-1} \pmod{11} \equiv 7^{-1} \pmod{11} \equiv 8 \pmod{11}$$
$$y_2 \equiv z_2^{-1} \pmod{m_2} \equiv 5775^{-1} \pmod{16} \equiv 15^{-1} \pmod{16} \equiv 15 \pmod{16}$$
$$y_3 \equiv z_3^{-1} \pmod{m_3} \equiv 4400^{-1} \pmod{21} \equiv 11^{-1} \pmod{21} \equiv 2 \pmod{21}$$
$$y_4 \equiv z_4^{-1} \pmod{m_4} \equiv 3696^{-1} \pmod{25} \equiv 21^{-1} \pmod{25} \equiv 6 \pmod{25}$$
$$w_1 \equiv y_1z_1 \pmod{m} \equiv 8 \cdot 8400 \pmod{92400} \equiv 67200 \pmod{92400}$$
$$w_2 \equiv y_2z_2 \pmod{m} \equiv 15 \cdot 5775 \pmod{92400} \equiv 86625 \pmod{92400}$$
$$w_3 \equiv y_3z_3 \pmod{m} \equiv 2 \cdot 4400 \pmod{92400} \equiv 8800 \pmod{92400}$$
$$w_4 \equiv y_4z_4 \pmod{m} \equiv 6 \cdot 3696 \pmod{92400} \equiv 22176 \pmod{92400}$$

The solution, which is unique modulo 92400, is

$$\begin{aligned} x &\equiv a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4 \pmod{92400} \\ &\equiv 6 \cdot 67200 + 13 \cdot 86625 + 9 \cdot 8800 + 19 \cdot 22176 \pmod{92400} \\ &\equiv 2029869 \pmod{92400} \\ &\equiv 51669 \pmod{92400} \end{aligned}$$

Example

What are the solutions of the systems of congruences

$$x \equiv 2 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv \pmod{7}?$$

Solution

To solve the system of congruences, first let $m = 3 . 5 . 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 2$, $M_3 = m/7 = 15$.

We see that 2 is an inverse of $M_1 = 35$ modulo 3, since $35 \equiv 2 \pmod 3$; 1 is an inverse of M_2 modulo 5, since $21 \equiv 1 \pmod 5$; and 1 is an inverse of $M_3 = 15 \pmod 7$, since $15 \equiv 1 \pmod 7$.

The solution to this system are those x such that

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 . 35 . 2 + 3 . 21 . 1 + 2 . 15 . 1$$
$$= 233 \equiv 23 \pmod{105}.$$

It follows that 23 is the smallest positive integer that is a simultaneous solution. That is 23 is smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 divided by 5, and a remainder of 2 when divided by 7.

Example

Find all solutions of $x^2 \equiv 1 \pmod{144}$.

Solution

$$144 = 16 \cdot 9 = 2^4 3^2, \text{ and } \gcd(16,9) = 1.$$

We can replace our congruence by two simultaneous congruences:

$x^2 \equiv 1 \pmod{16}$ and $x^2 \equiv 1 \pmod 9$

$x^2 \equiv 1 \pmod{16}$ has 4 solutions: $x \equiv \pm 1$ or $\pm 7 \pmod{16}$

$x^2 \equiv 1 \pmod 9$ has 2 solutions: $x \equiv \pm 1 \pmod 9$

There are 8 alternatives: i) $x \equiv 1 \pmod{16}$ and $x \equiv 1 \pmod 9$

ii) $x \equiv 1 \pmod{16}$ and $x \equiv -1 \pmod 9$

iii) $x \equiv -1 \pmod{16}$ and $x \equiv 1 \pmod 9$

iv) $x \equiv -1 \pmod{16}$ and $x \equiv -1 \pmod 9$

v) $x \equiv 7 \pmod{16}$ and $x \equiv 1 \pmod 9$

vi) $x \equiv 7 \pmod{16}$ and $x \equiv -1 \pmod 9$

vii) $x \equiv -7 \pmod{16}$ and $x \equiv 1 \pmod 9$

viii) $x \equiv -7 \pmod{16}$ and $x \equiv -1 \pmod 9$

By the Chinese Remainder Theorem with $k = 2$, $m_1 = 16$ and $m_2 = 9$, each case above has a unique solution for x modulo 144.

We compute:

$z_1 = m_2 = 9$, $z_2 = m_1 = 16$,

$y_1 \equiv 9^{-1} \equiv 9 \pmod{16}$, $y_2 \equiv 16^{-1} \equiv 4 \pmod 9$,

$w_1 \equiv 9 \cdot 9 = 81 \pmod{144}$, $w_2 \equiv 16 \cdot 4 \equiv 64 \pmod{144}$.

The 8 solutions are:

(i) $x \equiv 1 \cdot 81 + 1 \cdot 64 \equiv 145 \equiv 1 \pmod{144}$

(ii) $x \equiv 1 \cdot 81 + (-1) \cdot 64 \equiv 17 \equiv 17 \pmod{144}$

(iii) $x \equiv (-1) \cdot 81 + 1 \cdot 64 \equiv -17 \equiv -17 \pmod{144}$

(iv) $x \equiv (-1) \cdot 81 + (-1) \cdot 64 \equiv -145 \equiv -1 \pmod{144}$

(v) $x \equiv 7 \cdot 81 + 1 \cdot 64 \equiv 631 \equiv 55 \pmod{144}$

(vi) $x \equiv 7 \cdot 81 + (-1) \cdot 64 \equiv 503 \equiv 71 \pmod{144}$

(vii) $x \equiv (-7) \cdot 81 + 1 \cdot 64 \equiv -503 \equiv -71 \pmod{144}$

(viii) $x \equiv (-7) \cdot 81 + (-1) \cdot 64 \equiv -603 \equiv -55 \pmod{144}$

Boolean Matrix (Zero One Matrix)

A boolean matrix, or (0,1) matrix is a matrix with entries from the Boolean domain $B = \{0, 1\}$. Such a matrix can be used to represent a binary relation between a

We define Boolean operation $\vee$ and $\wedge$ as

$$b_1 \wedge b_2 = \begin{cases} 1 \text{ if } b_1 = b_2 = 1 \\ 0 \text{ otherwise} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1 \text{ if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 \text{ otherwise} \end{cases}$$

Boolean Product to Two Matrices

Let $A = \{a_{ij}]_{mn}$ and $B = [b_{ij}]_{np}$ be two Boolean matrices. Then the Boolean product of A and B is defined by $C = [c_{ij}]_{mp}$, a Boolean matrix,

where

$$C_{ij} = (a_{i1} \wedge b_1) \vee (a_{i2} \wedge b_2) \vee \ldots\ldots\ldots\ldots \vee (a_{in} \wedge b_{nj}).$$

Example

Find join $A \vee B$ and product $A \wedge B$ of the Boolean Matrices where,

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Solution

$$A \vee B = \begin{bmatrix} 1 \vee 0 & 1 \vee 1 \\ 0 \vee 0 & 1 \vee 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$A \wedge B = \begin{bmatrix} 1 \wedge 0 & 1 \wedge 1 \\ 0 \wedge 0 & 1 \wedge 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Example

Find the Boolean product of A and B where

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Solution

$$A \odot B = \begin{bmatrix} (1\wedge0)\vee(0\wedge1)\vee(1\wedge0) & (1\wedge1)\vee(0\wedge1)\vee(1\wedge0) & (1\wedge0)\vee(1\wedge1)\vee(0\wedge1) \\ (1\wedge0)\vee(1\wedge1)\vee(0\wedge0) & (1\wedge1)\vee(0\wedge1)\vee(1\wedge0) & (0\wedge0)\vee(0\wedge1)\vee(1\wedge1) \\ (0\wedge0)\vee(0\wedge1)\vee(1\wedge0) & (1\wedge0)\vee(0\wedge1)\vee(1\wedge1) & (0\wedge0)\vee(0\wedge1)\vee(1\wedge1) \end{bmatrix}$$

$$= \begin{bmatrix} 0\vee0\vee0 & 1\vee0\vee0 & 0\vee0\vee1 \\ 0\vee1\vee0 & 1\vee1\vee0 & 0\vee1\vee0 \\ 0\vee0\vee0 & 0\vee0\vee0 & 0\vee0\vee1 \end{bmatrix}$$

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

which is Boolean product of A and B, denoted by $A \odot B$.

(Note that the Boolean product of two such matrices is the usual definition of matrix product except that the addition is replaced with the operation $\vee$ and multiplication is replaced with the operation $\wedge$.)

Exercise

1. Express the greatest common divisor of each of these pairs of integers as a linear combination these integers.

   (a) 11, 17 (b) 63, 74 (c) 33, 72

   (d) 21, 55 (e) 101, 203 (f) 128, 325

2. Show that 15 is an inverse of 7 modulo 26.

3. Solve the congruence $4x \equiv 5 \pmod 9$.

4. Determine whether the integers in each of following sequences are pairwise relatively prime

   (a) 21, 34, 45 (b) 17, 18, 23

   (c) 11, 15, 19 (d) 7, 8, 9, 11

5. What are the greatest common divisors and LCM of the following pairs of integers.

   (a) $2\text{-}2 * 3^3 * 5^5, 2^5 * 3^3 * 5^2$

   (b) $2^2 * 7, 5^3 * 13$

   (c) $3^7 * 5^3 * 7^3, 2^1 * 3^5 * 5^9$

6. Find gcd (1000, 625) and LCM (1000, 625) and verify that gcd (1000, 625) & LCM (1000, 625) 1000 * 625

7. Find all solutions to the system of congruences.

   $x \equiv 2 \pmod 3$

   $x \equiv 1 \pmod 4$

   $x \equiv 3 \pmod 5$

8. Find all solutions to the system of congruences.

   $x \equiv \pmod 2$

   $x \equiv 2 \pmod 3$

   $x \equiv 3 \pmod 5$

   $x \equiv 4 \pmod{11}$

9. (a) Find first five random number using linear congruential method with $x_0 = 29$, $a = 9$, $c =$ and $m = 100$.

   (b) Find first three random number using linear congruential method with $x_0 = 37$, $a = 7$, $c =$ and $m = 100$.

10. Let $A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$. Find

    (a) $A \vee B$. (b) $A \wedge B$. (c) $A \odot B$.

11. Find the Boolean product of A and B, where $A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$.

Chapter 3

Logic and Proof Methods

Introduction

The term "logic" came from the Greek word logos, which is sometimes translated as "discourse", "reason", etc. It is the science dealing with the method of reasoning. It uses a symbolic language to express its principles in precise and unambiguous terms. In artificial intelligence field, Logic is defined as the representation language of knowledge. Since logic can helps us to reason the mathematical models it needs some rules associated with logic so that we can apply those rules for mathematical reasoning. There are lots of applications of logic in the field of computer science such as designing circuits, programming, program verifications, artificial intelligence automata theory and computability etc.

The logic, on the basis of its representation capability is of two types: Propositional logic and predicate logic.

Propositional Logic

Propositional Logic also known as sentential logic is the branch of logic that studies way of joining or modifying propositions to form more complicated propositions as well as logical relationships. The propositional logic represents knowledge or informal sentence in terms of propositions. In Propositional Logic, there are two types of sentences- simple sentences and compound sentences. Simple sentences express atomic propositions about the world. Compound sentences express logical relationships between the simpler sentences of which they are composed.

Propositions

Proposition is a declarative sentence that is either true or false, but not both. Example:

- $2 + 2 = 5$. (False), is a proposition.
- $7 - 1 = 6$. (True), is a proposition.
- odd numbers are divisible by 2 (false), is a proposition.
- Kathmandu is the capital of Nepal. (True), is a proposition.
- Open the door. Not a proposition.

The essential property of proposition is that, it is either true or false but not both.

Let us try to analyze the sentences below:

$x > 15$, go there, Who are you?

The above sentences are not propositions since we cannot say whether they are true or false.

Simple Proposition and Compound Proposition

- Any statement whose truth value does not depend on another proposition is called sim proposition. E.g. Kathmandu is capital city of Nepal.
  In Propositional Logic, these are often called propositional constants or, sometimes, lo constants. Propositions are denoted conventionally by using small letters like p, q, r, s ... truth value of proposition is denoted by 'T' for true proposition and 'F' for false propo Reminder: p, q, r, s ... are not actual propositions but they are propositional variables i.e. holders for propositions.
- Compound propositions are formed from simpler propositions and express relation among the constituent sentences. There are six types of compound sentences, viz. nega conjunctions, disjunctions, implications, reductions, and equivalences.

Truth Table

The table which consists of all possible truth value of any propositions (simple as we compound). Truth tables are specially valuable in the determination of the truth value propositions constructed from simple propositions.

Logical Operators or Connectives

Logical operators are used to construct mathematical statements having one or more proposition combining propositions. The combined proposition is called compound Proposition. Here present the logical operators along with their behavior in truth table:

Negation (not)

Let p be any proposition. The negative of given proposition P denoted by ¬ p is called negation Given a proposition p, negation operator (¬) is used to get negation of p denoted by ¬ p called p".

Example

Negation of the proposition "I love animals" is "I do not love animals" if the sentence I love an is denoted by p then its negation is denoted by ¬ p.

Example

Negation of proposition "Today is Sunday "is" It is not the case that today is Sunday" or "Today Sunday "or" It is not Sunday today."

Example

p: The summer in Tarai is very hot.

¬ p:The summer in Tarai is not very hot.

Truth Table

p	¬p
T	F
F	T

Conjunction (AND)

Given two propositions p and q, the proposition "p and q" denoted by p∧ q is proposition that is true whenever both the propositions p and q are true, false otherwise proposition that is obtained by the use of "and" operator is also called conjunction of p and q.

Example

If we have propositions p = "Ram is smart" and q = "Ram is intelligent."

The conjunction of p and q is Ram is smart and intelligent. This proposition is true only when

smart and he is intelligent also, false otherwise.

Example

p:Today is Saturday.

q:Today is holiday.

Then, $p \wedge q$:Today is Saturday and holiday

Truth Table

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction (OR)

Given two propositions p and q, the proposition "p OR q" denoted by $p \vee q$ is the proposition that is false whenever both the propositions p and q are false, true otherwise. The proposition that is obtained by the use of "or" operator is also called disjunction of p and q.

Example

If we have propositions p = "Ram is intelligent" and q = "Ram is diligent."

The disjunction of p and q is Ram is intelligent or he is diligent. This proposition is false only when Ram is not intelligent and not diligent, true otherwise.

Example

Let, p: It is cold.

q:It is raining.

Then, $p \vee q$: It is cold or raining.

Truth Table

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive OR (XOR)

Given two propositions p and q, the proposition exclusive or of p and q denoted by $p \oplus q$ is the proposition that is true whenever only one of the propositions p and q is true, false otherwise. As opposed to the disjunction above which is inclusive the general meaning of the English sentence can be used to know whether the "or" used is inclusive or exclusive.

Example

If we have propositions p = "Ram drinks coffee in the morning" and q = "Ram drinks tea in the morning"

The exclusive or of p and q is Ram drinks coffee or tea in the morning.

Truth Table

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Implication ($\rightarrow$)

Given two propositions p and q, the proposition implication $p \rightarrow q$ is the proposition that is false when p is true and q is false, true otherwise. Here p is called "hypothesis" or "antecedent" or "premise" and q is called "conclusion" or "consequence".

We come across the implication in many places in mathematical reasoning and we use different terminologies to express $p \rightarrow q$ like:

- "if p, then q"
- "q is consequence of p"
- "p is sufficient for q"
- "q if p" "q is necessary for p"
- "q follows from p"
- "if p, q"
- "p implies q"
- "p only if q"
- "q whenever p"
- "q provides p"

Example

p = "today is Sunday" q = "it is hot"

Then the implication can be "if today is Sunday then it is hot today"

Or "today is Sunday only if it is hot today".

Truth Table

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Inverse, Converse and Contra positive

Some of the related implications formed from $p \rightarrow q$ are:

Inverse of Implication:

When we add 'not' to the hypothesis and conclusion of implication $p \rightarrow q$ then it becomes $\neg p \rightarrow \neg q$, which is known as inverse of $p \rightarrow q$.

Example

Implication $p \rightarrow q$	Inverse $\neg p \rightarrow \neg q$
If it is raining, then the road is muddy.	If it is not raining then the road is not muddy.

Converse of Implication

When we interchange/flip the hypothesis and conclusion of implication $p \rightarrow q$ then the result becomes $q \rightarrow p$ which is known as converse of given implication.

Example

Implication $p \rightarrow q$:	Converse $q \rightarrow p$:
If it is raining, then the road is muddy.	If the road is muddy then it is raining.

Contrapositive of Implication

When we interchange/flip the hypothesis and conclusion of inverse statement of implication $p \rightarrow q$ then the resulting statement $\neg q \rightarrow \neg p$ is known as contrapositive.

Example

Implication $p \rightarrow q$:	Contrapositive $\neg q \rightarrow \neg p$:
If it is raining, then the road is muddy.	If the road is not muddy then it is not raining.

Example

Write the inverse, converse and contrapositive of the following statements:

a. If two angles are congruent, then they have same measures.

Statement($p \rightarrow q$)	If two angles are congruent, then they have same measures.
Inverse($\neg p \rightarrow \neg q$)	If two angles are not congruent, then they do not have same measures.
Converse($q \rightarrow p$)	If two angles have the same measures then they are congruent.
Contrapositive($\neg q \rightarrow \neg p$)	If two angles do not have same measures, then they are not congruent.

b. If quadrilateral is rectangle then it has two pairs of parallel sides.

Statement($p \rightarrow q$)	If quadrilateral is rectangle then it has two pairs of parallel sides.
Inverse($\neg p \rightarrow \neg q$)	If quadrilateral is not rectangle then it does not have two pairs of parallel sides.
Converse($q \rightarrow p$)	If quadrilateral has two pairs of parallel sides then it is a rectangle.

Contrapositive($\neg q \rightarrow \neg p$)	then it is not a rectangle.

Biconditional ($\leftrightarrow$)

Given propositions p and q, the biconditional $p \leftrightarrow q$ is a proposition that is true when p and q have same truth values. Alternatively $p \leftrightarrow q$ is true whenever both $q \rightarrow p$ and $q \rightarrow p$ are true.

Some of the terminologies used for biconditional are:

- "p if and only if q"
- "if p then q, and conversely"
- "p is necessary and sufficient for q"

Example

For propositions given in above implication, the biconditional statement is "today is Sunday if and only if it is hot today".

Truth Table

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

Representing English Sentences in Propositional Logic

Translation of English sentence into propositional logic has much importance. For instance, translating English sentence into logical expression removes ambiguity, similarly, after translating English sentence into logical expression, we can use these logical expression to analyze, determine their truth value and manipulate them. We can also use rule of inference on these logical expressions to infer or derive new expressions.

The process of translating English sentences into logical expression consists of following steps:

a) First we break down the given complex English sentences into atomic sentences.

Example

If it is raining, the home team wins the game.

Then we break it into two atomic sentences as:

- "it is raining"
- "home team wins the game"

b) We will represent each atomic sentence by propositional variables.

- P="it is raining"
- q="home team wins the game"

c) Now each atomic sentence is connected with appropriate connectives.

In the above example, the sentences are connected with implication.

Hence the logical expression of above sentence is: $p \rightarrow q$

Example

Translate the following simple declarative sentences:

Let,

p: It is raining

q: Sita is sick.

r: Ram stayed up late last night.

t: Kathmandu is capital of Nepal.

u: Ashok is a loud mouth.

(a) **Translating Negation:**

(i) It is not raining.

$\neg p$, where p : it is raining.

(ii) It is not the case that Sita isn't sick.

Since: q: "Sita is sick"

$\neg q$: Sita isn't sick.

and

$\neg(\neg q)$: it is not the case that Sita isn't sick.

(b) **Translating conjuction**

(i) It is raining and Sita is sick

$(p \wedge q)$

(ii) Kathmandu isn't Capital of Nepal and is isn't raining.

$(\neg t \wedge \neg p)$

(iii) It is not the case that it is raining and Sita is sick.

Translation 1: It is not the case that both it is raining and Sita is sick.

$\neg(p \wedge q)$

Translation 2: Sita is sick and it is not the case that it is raining.

$(\neg p \wedge q)$

(c) **Translating Disjunction**

(i) Kathmandu is capital of Nepal and it is raining or Ashok is a loud mouth.

$[(t \wedge p) \vee u]$ or $[t \wedge (p \vee u)]$

(ii) Sita is sick or Sita isn't sick

$(q \vee \neg q)$

(iii) Ram stayed up at last night or Kathmandu isn't capital of Nepal.

$(r \vee \neg t)$

(d) **Translating Implications**

(i) If it is raining then Sita is sick.

$p \rightarrow q$

(ii) It is raining when Ashok is a loudmouth

$(u \rightarrow p)$

(iii) Sita is sick and it is raining implies that Ram stayed up late last night.

$(q \wedge p) \rightarrow r$

(e) Translating Biconditional

(i) It is raining if and only if sita is sick

$p \leftrightarrow q$

(ii) Kathmandu is capital of Nepal is equivalent to Ram stayed up late last night

$p \leftrightarrow r$

Example

Let p, q and r be the propositions defined as:

p: Ram get A on final exam.

q: Ram does every exercise in this book.

r: Ram got A in this class.

Translate the following into logical expression:

(a) Ram get A in this class but Ram do not do every exercise in this book.

Solution: $p \rightarrow \neg q$

(b) Ram get A on the final exam, Ram does every exercise in this book and Ram get A in this class

Solution: $(p \wedge q \wedge r)$

(c) T get A in this class, it is necessary for Ram to get A on final.

Solution: We may rephrase it as:

If Ram get A on final exam then he will get A in this class.

$p \rightarrow r$

(d) Getting A on final and doing every exercise in this book is sufficient for getting an A in the class

Solution:

$(p \wedge q) \rightarrow r$

Example

Translate the following paragraphs into logical expression:

You can access the internet from the campus only if you are a BIM graduate or Staff of campus.

Solution

Let p = "you can access the internet from campus"

q = "you are a BIM graduate"

s = "you are staff of campus"

Now the logical expression is:

$p \rightarrow (q \vee s)$

Example

Translate the following paragraphs into logical expression:

"Whenever the system software is being upgraded, users cannot access the file system. If users access the file system then, they can save new files. If users cannot save new files then, software is not being upgraded."

Solution

Let u = "The system software is being upgraded"

a = "Users can access the file system"

s = "Users can save new files"

Now the logical expressions are:

a) $u \rightarrow \neg a$

b) $a \rightarrow s$,

c) $\neg s \rightarrow \neg u$

OR

$u \rightarrow \neg a \wedge a \rightarrow s \wedge \neg s \rightarrow \neg u$

Example

Translate given logical expressions into English sentence:

a) $\neg p$ b) $r \wedge \neg p$ c) $\neg r \vee p \vee q$

When, p = "it rained last night"

q = "the sprinkles came on last night"

r = "the lawn was wet this morning"

Solution

a) $\neg p$ = " it didn't rain last night"

b) $r \wedge \neg p$ = "the lawn was wet this morning and it didn't rain last night"

c) $\neg r \vee p \vee q$ = "either the lawn was not wet this morning or it rained last night or the sprinkles came on last night"

Note :

To translate English sentences to the proposition symbolic form follow these steps:

Restate the given sentence into building block sentences. Give the symbol to each sentence and substitute the symbols using connectives.

Example

"if it is snowing then I will go to the beach"

Restate into "it is snowing" give it symbol p and "I will go to the beach" and give it symbol q then we can write it as $p \rightarrow q$.

Tautology, Contradiction and Contingency

A compound proposition that is always true, no matter what the truth values of the atomic propositions that contain in it is called a tautology.

Example

Show that $p \vee \neg p$ is tautology.

Solution:

We can verify this statement with help of truth table as follows:

Truth Table

P	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Here, the last column consists of all truth values so it is always true and is a tautology.

Example

Show that $\neg (p \rightarrow q) \rightarrow \neg q$ is tautology using truth table.

Solution:

We can verify this statement with the help of truth table as follows:

p	q	$p \to q$	$\neg(p \to q)$	$\neg q$	$\neg(p \to q) \to \neg q$
T	T	T	F	F	T
T	F	F	T	T	T
F	T	T	F	F	T
F	F	T	F	T	T

Contradiction

A compound proposition that is always false, no matter what the truth values of the atomic propositions that contain in it is called contradiction.

Example

Show that $p \wedge \neg p$ is contradiction.

Solution:

We can verify this statement with help of truth table as follows:

Truth Table

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

Example

Show that $(p \vee q) \wedge [(\neg p) \wedge (\neg q)]$ is contradiction.

Solution:

We can verify this statement with the help of truth table as follows:

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg p \wedge \neg q$	$(p \vee q) \wedge [(\neg p) \wedge (\neg q)]$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	F

Contingency

A compound proposition that is neither a tautology nor a contradiction is called contingency.

Example

Show that $\neg p \wedge \neg q$ is contingency

Solution:

We can verify this statement with the help of truth table as follows:

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	F	F	F
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Propositional Equivalences

Given two propositions that differ in their syntax we may get the exactly same semantic for both the proposition. If two propositions are semantically identical then we say those two propositions are "equivalent". If two propositions P(p, q, r, ...) and Q(p, q, r, ...) where p, q, r, ... are propositional variables have the same truth values in every possible case, the propositions are called logically equivalent and denoted as

$$P(p, q, r, ...) \equiv Q(p, q, r, ...)$$

To test whether two propositions P and Q are logically equivalent, the following steps are followed:

(i) Construct the truth table for P.

(ii) Construct truth table for Q using same propositional values

(iii) Check each combination of truth values of propositional variables to see whether the value of P is same as value of Q or not. If truth value of P is same as truth value of Q then P and Q are logically equivalent.

Such constructs are very useful in mathematical reasoning where we can substitute such propositions to equivalent propositions to construct mathematical arguments.

Example

Prove that: $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

Solution

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

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

Propositional Equivalences

The compound propositions p and q are logically equivalent, denoted by $p \Leftrightarrow q$ or $p \equiv q$, if proposition $p \leftrightarrow q$ is a tautology.

Identity Law	$p \wedge T \Leftrightarrow p, p \vee F \Leftrightarrow p$
Domination Law	$p \wedge F \Leftrightarrow F, p \vee T \Leftrightarrow T$
Idempotent Law	$p \wedge p \Leftrightarrow p, p \vee p \Leftrightarrow p$
Double Negation Law	$\neg(\neg p) \Leftrightarrow p$
Commutative Law	$p \wedge q \Leftrightarrow q \wedge p, p \vee q \Leftrightarrow q \vee p$
Associative Law	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
Distributive law	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$, $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

De Morgan's Law	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$, $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$
Absorption	$p \vee (p \wedge p) \equiv p$, $p \wedge (p \vee p) \equiv p$

1. Identity Law

a) $p \wedge T \Leftrightarrow p$ b) $p \vee F \Leftrightarrow p$

Verification:

p	p ^ T	p v F
T	T	T
F	F	F

2. Domination Law

a) $p \wedge F \Leftrightarrow F$ b) $p \vee T \Leftrightarrow T$

Verification:

P	p ^ F ≡ F	p V T ≡ T
T	F	T
F	F	T

Similarly, we can prove for $p \vee T \Leftrightarrow T$

3. Idempotent Law

a) $p \wedge p \Leftrightarrow p$

b) $p \vee p \Leftrightarrow p$

Verification:

P	p ^ p ≡ p	p V p ≡ p
T	T	T
F	F	F

Similarly we can prove for $p \vee p \Leftrightarrow p$

4. Double Negation Law

$\neg(\neg p) \Leftrightarrow p$ Double negation law

Verification:

p	¬p	¬(¬p) ≡ p
T	F	T
F	T	F

5. Commutative Law

a) $p \wedge q \Leftrightarrow q \wedge p$

b) $p \vee q \Leftrightarrow q \vee p$

Verification:

p	q	p^q	q^p
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

Similarly we can prove for $p \vee q \Leftrightarrow q \vee p$

6. **Associative Law**

a) $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$

b) $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

Verification:

p	q	r	p^q	(p^q)^r	q^r	p^(q^r)
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

Similarly we can prove for $(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$

7. Distributive law

a) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$

b) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

Verification:

p	q	r	q∨r	p ∧ (q ∨ r)	p ∧ q	p^r	(p ∧ q) ∨ (p ∧ r)
T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T
T	F	T	T	T	F	T	T
T	F	F	F	F	F	F	F
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Similarly, we can prove for $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

8. **De Morgan's Law**

a) $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ b) $\neg (p \vee q) \Leftrightarrow \neg p \wedge \neg q$

Verification:

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

Similarly, we can prove for $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$

Example

Show that $(p \rightarrow r) \wedge (q \rightarrow r)$ and $(p \vee q) \rightarrow r$ are logically equivalent using law of equivalent.

Solution

Here, given first expression

L.H.S. $(p \rightarrow r) \wedge (q \rightarrow r)$

$= (\neg p \vee r) \wedge (\neg q \vee r)$ [Implications]

Let A represent $\neg p$, B represent $\neg$ and C represent r

Then,

$(A \vee C) \wedge (B \vee C) \equiv (C \vee A) \wedge (C \vee B)$

$\equiv C \vee (A \wedge B)$ [Distribution law]

$\equiv (A \wedge B) \vee C$ [Commutative law]

$\equiv (\neg p \wedge \neg q) \vee r$ [Substitution law]

$\equiv \neg(p \vee q) \vee r$ [Demorgan's law]

$\equiv (p \vee q) \rightarrow r$ [Implication law]

Example

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution

To show that this statement is a tautology, we will use logical equivalences to demonstrate that logically equivalent to T.

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

$\equiv \neg(p \vee \neg q) \vee (p \vee q)$ [Demorgan's law]

$\equiv (\neg p \vee p) \vee (\neg q \vee q)$ [Commutative law]

$\equiv T \vee T$ [Commutative law]

$\equiv T$ [Domination law]

Predicate

Any declarative statements involving variables often found in mathematical assertion and computer programs, which are neither true nor false when the values of variables are not specifie called predicate.

Let's take a statement 5>9, this is a propositional statement because it is false. Now let's tak statement "x > 4". Is this statement a proposition? The answer is no. The statement may be ei true or false depending upon the value of x (variable). We can say that any statement involv

variable is not proposition.

The predicate "x > 4" has two parts. The first part, variable x is subject of statement and another is relation part ">4" called "predicate" refers to a property that the subject of statement have. We can denote the statement "x>4" by P(x) where P is predicate ">4" and x is the variable. We also call P as a propositional function where P(x) gives value of P at x. Once value is assigned to the propositional function then we can tell whether it is true or false i.e. a proposition.

For e.g. if we put the value of x as 3 and 7 then we can conclude that P(3) is false since 3 is not greater than 4 and p(7) is true since 7 is greater than 4.

We can also denote a statements with more than one variable using predicate like for the statement "x = y" we can write P(x,y) such that P is the relation "equals to" . Similarly the statements with higher number of variables can be expressed.

Thus a predicate is a sentence that contains a finite number of variables and becomes a proposition when specific values are substituted for the variables.

Note:

The logic involving predicates is called Predicate Logic or Predicate calculus similar to logic involving propositions is Propositional Logic or Propositional Calculus.

Example

Let P(x): x+2<10, find the truth value of P(5)and P(9).

Solution

Given,

$$P(x) : x + 2 < 10$$

When x = 5,

$$P(5) : 5 + 2 < 10$$

$$7 < 10 \text{ (true)}$$

When x = 9,

$$P(9) : 9 + 2 < 10$$

$$11 < 10 \text{ (false)}$$

Example

Let F(x, y) : x = y + 6. Find the truth value of F(1, 5) and F(5, 0).

Solution

Given,

$$F(x, y) : x = y + 6$$

For F(1, 4), Set x = 1 and y = 5 we get,

$$F(1, 5): \ 1 = 5 + 6$$

$$1 = 11 \text{ (False)}$$

Similarly,

For F(6, 0), Set x = 6, y = 0 we get,

$$F(6, 0) : 6 = 0 + 6$$

$$\text{i.e. } 6 = 6 \text{ (true)}$$

∴ F(1, 5) is false and F(6, 0) is true for F(x, y) : x = y + 6.

Quantifiers

Quantifiers are the tools that change the propositional function into a proposition. These are the word that refers to quantities such as "some" or "all" and indicates how frequently a certain statement

is true. Construction of propositions from the predicates using quantifiers is called quantificati
The variables that appear in the statement can take different possible values and all the possi
values that the variable can take forms a domain called "Universe of Discourse" or "Universal set".
There are two types of quantifier Universal quantifier and Existential quantifier.'

Universal Quantifier

The phrase "for all" denoted by $\forall$, is called universal quantifier. The process of converting predica
into proposition using universal quantifier is called universal quantification. So, the univers
quantification of P(x), denoted by $\forall x\ P(x)$, is a proposition where "P(x) is true for all the values o
in the universe of discourse".
We can represent the universal quantification by using the English language like: "for all x P
holds" or "for every x P(x) holds" or "for each x P(x) holds".

Example

Take universe of discourse a set of all students of Kathmandu College.
P(x) represents: x takes Discrete Mathematics class.

Here universal quantification is $\forall x\ P(x)$, which represent the English sentence "all students
Kathmandu college take Discrete Mathematics class", and now it is a proposition.
The universal quantification is conjunction of all the propositions that are obtained by assigning t
value of the variable in the predicate. Going back to above example if universe of discourse is a s
{Ram, Shyam, Hari, Sita} then the truth value of the universal quantification is given by P(ram)
P(Shyam) $\wedge$ P(Hari) $\wedge$ P(Sita) i.e. it is true only if all the atomic propositions are true.

Existential Quantifier

The phrase "there exist", denoted by $\exists$, is called existential quantifier .The process of converti
predicate into proposition using existential quantifier is called existential quantification. T
existential quantification of P(x), denoted by $\exists x\ P(x)$, is a proposition where "P(x) is true for som
values of x in the universe of discourse". The other forms of representation include "there exists
such that P(x) is true" or "P(x) is true for at least one x".

Example

For the same problem given in universal quantification $\exists x\ P(x)$ is a proposition is represe
like " some students of Kathmandu College take Mathematics class".
The existential quantification is the disjunction of all the propositions that are obtained by assigni
the values of the variable from the universe of discourse. So the above example is equivalent
P(Ram) $\vee$ P(Shyam) $\vee$ P(Hari) $\vee$ P(Sita), where all the instances of variable are as in example
universal quantification. Here if at least one of the students takes graphics class then the existen
quantification results true.

Example

Let Z, the set of integer, be the universe of discourse and consider the statements
(i) $\forall x \in Z,\ x^2 = x$ (ii) $\exists x \in Z,\ x^2 = x$
Find the truth values of each of the statements

Solution

Let $P(x) : x^2 = x$ then

$\forall x P(x)$ is false because $2 \in z$, $P(2) : 2^2 = 2$ is false and $\exists\, x P(x)$ is true because at least one proposition is true i.e. $1 \in z$, $P(1) : 1^2 = 1$ is true.

Example

Let $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be set of natural number. Determine the truth value of each of the following statements.

(a) $\exists x \in N, x + 5 = 12$

(b) $\forall x \in N,\ x + 4 < 15$

(c) $\forall x \in N, x + 5 \leq 10$

Solution

Given,

$N = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

(a) $\exists x \in N, x + 5 = 12$ is true

for if $x = 7$ then $x + 5 = 12$

or, $7 + 5 = 12$

i.e. $12 = 12$ (true)

(b) $\forall x \in N, x + 4 < 15$ is true

for every $x \in N$ satisfies $x + 4 < 15$

(c) $\forall x \in N, x + 5 \leq 10$ is false for $6 \in N$, $6 + 5 \leq 10$

$\Rightarrow 11 \leq 10$ (false)

Binding variables

When a quantifier is used on variable, then it is called bounded variable. An occurance of a variable. An occurrence of a variable that is not bounded by a quantifier or set equal to a particular value is said to be free.

The part of a logical expression to which a quantifier is applied is called the scope of quantifier.

Example:

In the statement $\forall\, y\, Q(x, y)$, the variable y is bounded by universal quantifier $\forall\, y$ but variable x is free because it is not bound by a quantifier.

Translating the Sentences into Logical Expression

Example

Translate "not every integer is even" where the universe of discourse is set of integers.

Solution

Let $E(x)$ denotes x is even.

Then $\neg\forall x E(x)$ represents the above statement "not every integer is even"

Example

Translate "every man is mortal"

Let $M(x)$ denote x is mortal, where x is from set of man (here universe of discourse is all man)

Then, $\forall\, x\, M(x)$ represent that "for all x, x is mortal."

Example

Every person is precious.

Solution

We translate this as:

For every x, if x is person then x is precious

$P(x)$: x is a person

$Q(x)$: x is precious

$\therefore \quad \forall x, P(x) \rightarrow Q(x)$

Example

Some student of this college passed CSIT entrance examination.

Solution:

We translate this as

For some x, x is student of this college and x has passed CSIT entrance

Let, $C(x)$: x is student of this college.

$E(x)$: x passed CSIT entrance examination.

$\therefore \quad \exists x, C(x) \wedge E(x)$

where universe of discourse is set of all students.

Example

Every student in this class has studied discrete mathematics where universe of discourse is set of person.

Solution

We translate this as:

for every person x, if x is student of this class then x has studied discrete.

Let, $P(x)$: x is student of this class

$Q(x)$: x has studied discrete

$\therefore \quad \forall x, P(x) \rightarrow Q(x)$

Example

Let $F(x)$: x is man $M(x)$: x is mortal

(a) All man are mortal

$\forall x(F(x) \rightarrow M(x))$

i.e. For all x, if x is man, then x is mortal

(b) Let $I(x)$: x is an integer

$P(x)$: x is either positive or negative

"Any integer is either positive or negative".

This can be expressed as:

for all x, if x is an integer, then x is either positive or negative.

$\forall x(I(x) \rightarrow P(x))$

Example

Let, $S(x)$: x is a student

$C(x)$: x is cleaver

$M(x)$: x is successful

Express the following using quantifier.

(a) There exist a student

$\exists x\, S(x)$

(b) Some students are cleaver

This can be written as:

There exist an x such that x is student and x is cleaver.

$\therefore \quad \exists x(S(x) \wedge C(x))$

(c) "Some students are not successful"

This can be expressed as:

There exist an x such that x is student and x is not successful

$\therefore \quad \exists x(S(x) \wedge \neg M(x))$

Precedence and Binding of Quantifiers

When a variable is assigned a value or associated with a quantifier, it is known as bounded variable. If the variable is not bounded then it is know as free variable.

For example:

(1) P(x, y) - x & y are free variable.

(2) P(3, y) - y is free variable.

(3) $\forall$ x, P(x) - x is bounded variable

(4) $\forall$ x, P(x, y) - Here x is bounded and y is free variable.

set of Note: Any expression with no free variable is proposition and expression with at least one free variable is prodicate.

Nested Quantifier

When we use more than one quantifier in a sequence, then it is known as nested quantifier.

For example: $\forall$ x, $\exists$ y P(x, y). Here quantifier $\exists$ & $\forall$ are rested in a sequences.

Example

Translate following sentence using quantifier.

(a) Everyone loves someone.

(b) Someone loves somebody.

(c) Everyone loves everybody.

Solution

Let L(x, y) : x loves y.

Then,

(a) $\forall x \exists y, L(x, y) \rightarrow$ for all x, there is some y such that x loves y.

(b) $\exists x \exists y\ L(x, y)$

(c) $\forall x \forall y\ L(x, y)$

Negation of Quantified Expression

Let $\forall$ x, P(x) is a quantified statement its negation is $\neg \forall x\ P(x)$, which is logically equivalent to $\exists x \neg P(x)$.

Example

Let x represent any girls in KTM

L(x) : x is lovely.

Then

$\forall x\ L(x)$: every girl in KTM is lovely.

Now, negative of above sentence is

$\forall x\, L(x) = \exists x \neg L(x)$

i.e. there is some (at least, one) girl in KTM who is not lovely.

Example

No one has claimed every mountain in the Himalayas.

Let x represent a people.

$M(x)$ = x claimed every mountain in the Himalayas.

Then,

$\forall x\, M(x)$: everyone has claimed every mountain in the Himalays.

$\forall x \neg m(x)$: Every one has not claimed every mountain

which is logically equivalent to no one has claimed mountain.

Example

No girls in KTM is lovely.

Let,

$L(x)$: X is lovely.

$\forall x\, L(x)$: Every girl is lovely.

$\forall x \neg L(x)$: No girl is lovely

[Note: Equivalence involving negative]

a. $\neg \exists x\, P(x) \equiv \forall x, \neg P(x)$

b. $\neg \forall x\, p(x) \equiv \exists x \neg P(x)$

c. $\forall x \neg p(x) \equiv \neg [\exists x\ P(x)]$

d. $\exists x \neg P(x) \equiv \neg [\forall x\, P(x)]$

Find

The negation of (a) $\forall x \neg P(x)$ (b) $\exists x \neg p(x)$

Solution

(a) $\neg [\forall x, \neg P(x)]$

$\equiv \neg \forall x, \neg P(x)$

$\equiv \forall x, \neg \neg P(x)$

$\equiv \exists x\, P(x)$

(b) $\neg [\exists x, \neg P(x)]$

$\equiv \neg \exists x, \neg P(x)$

$\equiv \forall x\ \neg \neg P(x)$

$\equiv \forall x, P(x)$

The Order of Quantifiers

Many mathematical statements involve multiple quantification of proportional functions involv more than one variable. In such situations it is important to note that order of quantifiers important.

Example:

Let Q(x, y, z) be the statement "x + y = z". What are truth values of $\forall x\, \forall y\, \exists z\, Q(x, y, z)$ $\exists z\, \forall x\, \forall y\, Q(x, y, z)$?

Solution

Suppose x and y are assigned values.

$\forall x \forall y = \exists z\ Q(x, y, z)$ which is the statement for all real number x and for all real number y there is real number z such that $x + y = z$ is true but

$\exists z \forall x \forall y\ Q(x, y, z)$, the statement there is real number of z such that for all real number of x and for all real number y, it is true that $x + y = z$ is false.

Rules of Inference

To draw conclusion from the given premise we must be able to apply some well defined steps that help reaching the conclusion. These steps of reaching the conclusion are provided by the rules of inference. Here some of the rules of inferences are given below:

Rule 1: Modus Ponens (or Law of Detachment)

Whenever two propositions p and $p \rightarrow q$ are both true then we confirm that q is true. We write this rule as $\dfrac{p \rightarrow q,\ p}{\therefore q}$, this rule is valid rule of inference because the implication $[p \wedge (p \rightarrow q)] \rightarrow q$ is a tautology.

Example

Ram is hard working and if Ram is hard working, then he is intelligent. By modus ponens (verify), this logically infers Ram is intelligent.

Rule 2: Hypothetical Syllogism (Transitive Rule)

Whenever two propositions $p \rightarrow q$ and $q \rightarrow r$ are both true then we confirm that implication $p \rightarrow q$ is true. We write this rule as

$$\frac{p \rightarrow q,\ q \rightarrow r}{\therefore p \rightarrow r}$$

This rule is valid rule of inference because the implication $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ is a tautology.

This rule can be extended to larger numbers of implications as

$$\begin{array}{ll} & p \rightarrow q \\ & q \rightarrow r \\ & r \rightarrow s \\ \hline \therefore & p \rightarrow s \end{array}$$

Example

a) If today is Sunday, then today is rainy day and if today is rainy day, then it is wet today. By transitivity rule (verify!!!), this logically infers It is wet today.

Rule 3: Addition

Due to the tautology $p \rightarrow (p \vee q)$, the rule :

$$\frac{p}{\therefore q \vee p}$$ is a valid rule of inference.

Rule 4: Simplification

Due to the tautology $(p \wedge q) \rightarrow p$, rule

$$\frac{p}{\therefore p \wedge q}$$ is a valid rule of inference.

Rule 5: Conjunction

Due to the tautology $[(p) \wedge (q)] \rightarrow (p \wedge q)$, rule

$$\frac{p, q}{\therefore q \wedge p}$$ is a valid rule of inference

Rule 6: Modes Tollens

Due to the tautology $[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$, rule

$$\frac{\neg q, p \rightarrow q}{\therefore \neg p}$$

is a valid rule of inference

Rule 7: Modes Tollens

Due to the tautology $[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$, rule

$$\frac{\neg q, p \rightarrow q}{\therefore \neg p}$$ is a valid rule of inference.

Rule 8 Resolution

Due to the tautology $[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$, rule

$$\frac{p \vee q, \neg p \vee r}{\therefore q \vee r}$$ is a valid rule of inference.

Summary of Rule of Inference

Rule of Inference	Name	Tautology
P $P \rightarrow q$ $\therefore q$	Modus ponens	$[p \wedge (p \rightarrow q)] \rightarrow q$
$\neg q$ $P \rightarrow q$ $\therefore \neg P$	Modus Tollens	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	Hypothetical syllogism	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism	$[(p \vee q) \wedge \neg p] \rightarrow q$
p $\therefore p \vee q$	Addition	$p \rightarrow (p \vee q)$
$p \wedge q$ $\therefore p$	Simplification	$(p \wedge n) \rightarrow p$
$p \vee q$ $\neg p \vee q$ $\therefore q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution

Valid Argument

An argument in propositional logic is valid if the truth of all its premises implies that the conclusion is true.

Valid Argument form

An argument form in a propositional logic is a sequence of compound propositions involving propositional variables. An argument form is valid if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

i.e. the argument form with premises $P_1, P_2, \ldots, P_n$ and conclusion q is valid, when $(P_1 \wedge P_2 \wedge P_3 \wedge \ldots \wedge P_n) \rightarrow q$ is a tautology.

Verification of Inference Rules/Examples

Example

Determine whether the following argument is valid or not. If Ram is human then Ram is mortal. Ram is human. Therefore Ram is mortal.

Solution:

Let p : Ram is human.

q : Ram is mortal.

Now, the given arguments in symbolic form becomes

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

Then, the above argument is valid if $[(p \rightarrow q) \wedge p] \rightarrow q$ is tautology. To prove this, we can construct truth table as follows:

p	q	$(p \rightarrow q)$	$(p \rightarrow q \wedge p)$	$[(p \rightarrow q) \wedge p] \rightarrow q$
F	F	T	F	T
F	T	T	F	T
T	F	F	F	T
T	T	T	T	T

Since last column consists of all truth value, so $[(p \rightarrow q) \wedge p] \rightarrow q$ is tautology. Hence, the above argument is valid.

Example:

If you invest in stock market, then you will become rich.

If you become rich then you will be happy.

Therefore, if you invest in stock market, then you will be happy.

Solution

Let p : you invest to stock markets

q : you will become rich

r : you will be happy

Now, the given arguments/sentences in symbolic form becomes

$p \rightarrow q$

$$\frac{q \to r}{\therefore p \to r} \quad \text{(transitive rule)}$$

The above argument is valid iff the $(p \to q) \wedge (q \to r) \to (p \to r)$ is tautology.

Now, we can prove above tautology using truth table:

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

Hence, the above argument is valid.

Example

If it rains today the college will be closed. The college is not closed today. Therefore, it did not rain today.

Solution

Let p : It rains today.

q : The college will close.

The above argument when changed into symbolic form becomes

$$\begin{array}{l} p \to q \\ \underline{\neg q} \\ \therefore \neg p \end{array}$$

The above argument is valid if $(p \to q) \wedge (\neg q) \to \neg p$ is tautology.

This can be verified using truth table as:

p	q	$\neg p$	$\neg q$	$p \to q$	$(p \to q) \wedge \neg q$	$(p \to q) \wedge \neg q \to \neg p$
F	F	T	T	T	T	T
F	T	T	F	T	F	T
T	F	F	T	F	F	T
T	T	F	F	T	F	T

Hence, the given argument is valid.

Example

State which rule of inference is the basis of the following argument: "it is below freezing now. Therefore, it is either below freezing or raining now.

Solution:

Let p : it below freezing now and q : it is raining now. Then the argument in above sentences will be expressed in symbolic form is:

p

.....

therefore pvq.

This is a valid argument since it confirms form the addition rule of inference.

Example

Which rule of inference is basis for the following arguments: if it is rainy then swimming pool will be closed. It is raining. Therefore the swimming pool is closed.

let p : it is rainy and q : The pool is closed. Then the argument in above sentences when expressed in symbolic form is:

p->q

p

.....

therefore q.

This is a valid argument since it confirms form the modus pones rule of inference.

Example

For each of given set of premises, what relevant conclusion can be drawn? Explain the rule of inference used to obtain each conclusion.

If I eat spicy food, then I have strange dreams. I have strange dreams if there is thunder while I sleep. I didn't have strange dreams.

Solution:

Let

p = "I eat spicy food.

q = " I have strnge dreams",

r = "There is thunder while I sleep"

Then the above premises are

a) $p \rightarrow q$

b) $r \rightarrow q$

c) $\neg q$

Using modus tollens in above premises b and c we have $\neg r$ i.e.

$r \rightarrow q$

$\neg q$

.....

$\neg r$.....d)

Similarly using modus tollens in above premises a and c we have $\neg p$ i.e

$p \rightarrow q$

$\neg q$

.....

$\neg p$.....e)

Therefore from given argument we can conclude either -r or -p i.e I didn't eat spicy food or There is nothunder at time of sleep.

Example

For the set of premises "If I play hockey, then I am sore the next day." "I use the whirlpool if I am sore." " I did not use the whirlpool". What relevant conclusion can be drawn? Explain the rules of

inference used to draw the conclusion.

Solution:

Let

p = "I play hockey",

q = " I am sore",

r = "I use the whirlpool"

Then the above premises are

a) $p \rightarrow q$

b) $q \rightarrow r$

c) $\neg r$

Using hypothetical syllogism in premises a and b we have $p \rightarrow r$ i.e. "if I play hockey, then I use whirlpool"

Using the modus tollens in premise c and inferred proposition $p \rightarrow r$ we conclude $\neg p$ is true. p is false. p is false means " I did not play hockey".

Example

Construct an argument using rules of inference to show that the hypotheses "If it does not rain or is not cloudy today, then the swimming competition will be held and the life saving demonstration will go on,". " If the swimming competition is held, then the trophy will be awarded,' and 'trophy was not awarded" imply the conclusion " It rained".

Solution:

Let

p = "It rains",

q = "It is foggy",

r = "the sailing race is held",

s = "Life saving demonstration is done",

and t = " Trophy is awarded".

Then we have to show that the argument

$[((\neg p \vee \neg q) \rightarrow (r \wedge s)) \wedge (r \rightarrow t) \wedge \neg t] \rightarrow p$ is valid.

Now,

[1] $(r \rightarrow t)$ [Hypothesis]

[2] $\neg t$ [Hypothesis]

[3] $\neg r$ [Modus Tollens using steps 1 and 2]

[4] $((\neg p \vee \neg q) \rightarrow (r \wedge s))$ [Hypothesis]

[5] $\neg(\neg p \vee \neg q) \vee (r \wedge s)$ [Implication of Step 4]

[6] $(p \wedge q) \vee (r \wedge s)$ [De Morgan's Law in Step 5]

[7] $p \vee (r \wedge s)$ [Simplification using step 6]

[8] $p \vee r$ [Simplification using step 7]

Here our original premises changes to $(p \vee r) \wedge \neg r$ [from step 8 and 3]

[9] $r \vee p$ [Commutative law in step 8]

[10] $\neg r \vee p$ [Addition using step 3]

[11] $p \vee p$ [Resolution using steps 9 and 10]

[12] p [Idempotent law]

Hence argument is valid. With conclusion "It rained".

Fallacy

The fallacies are arguments that are convincing but not true and produce faulty inferences. So fallacies are contingencies rather than tautologies. There are following types of falacies that may occur in logical reasoning.

Fallacy of affirming the conclusion (consequence)

This kind of fallacy has the form

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

Hence it is a fallacy.

Example

If economy of Nepal is poor, then the education system in Nepal will be poor. The education system in Nepal is poor. Therefore, Economy of Nepal is poor.

In this argument above the conclusion can be false even if both the propositions "If economy of Nepal is poor, then the education system in Nepal will be poor" and "The education system in Nepal is poor" are true. Denoting with symbols we may write $(p \rightarrow q)$ for first proposition and then the second proposition becomes q. this takes the form $q \wedge (p \rightarrow q) \rightarrow q$, which is not a tautology. Since the education system may not depend on the economy of the country.

i.e. $p \wedge (p \rightarrow q) \rightarrow q$. This is not a tautology

Begging the Question (Circular Reasoning)

If the statement that is used for proof is equivalent to the statement that is being proved then it is called circular reasoning.

Example

- The square root of 2 is irrational since it is not rational.
- Ram is black because he is black.
- Hari is student because he is a student.

Rules of Inference for Quantified Statements

If the sentence given in the argument represent the properties of more than one object then we can't represetn them by a simple propostion. We need predicate to represent suh statement. such statemnet sometimes called open proposition. For logical resoning that involed such statement needs rule of inference designed for quantified sentences.Some of the rules are:

1. Univasal Instantiation

If the proposition of the form $\forall x P(x)$ is supposed to be true then the universal quantifier can be dropped out to get P(c) is true for arbitrary c in the universe of discourse. This can be written as

In universe of discourse of all man every man is mortal implies ram is mortal where ram is a man.

2. Universal Generalization

If all the instances of c makes P(c) true, then $\forall x P(x)$ is true. This can be written as P(c), for all c, Here the chosen c must be arbitrary, not a specific element from the univer discourse. This rule is seldom explicitly used.

3. Existential Instantiation

If the proposition of the form $\exists x P(x)$ is supposed to be true then the there is an element c i universe of discourse such that P(c) is true. This can be written as

$$\exists x P(x)$$

$\therefore$ *P(c), for some c.,*

Here the element c is not arbitrary, it must be specific such that P(x) is true. We generally find difficulty in finding such c.

4. Existential Generalization

If at least a element c from the universe of discourse makes P(c) true, then $\exists x P(x)$ is true.

Example

Reema, a student in this class, knows how to write programs in JAVA. Everyone who knows h write programs in java can get a high paying job. Therefore, someone in this class can get a paying job.

Solution

Let x represent a student in this class.

J(x) : x knows how to program in java.

Then,

J(Reema): Reema knows how to program in java.

Hp(x): x get high paying job.

Now, the above given argument in symbolic form becomes

(i) $\forall x, J(x) \rightarrow Hp(x)$

(ii) J (Reema)

and we have to prove $\exists x, Hp(x)$

Now, the steps are:

(1) $\forall \exists (x) \rightarrow Hp(x)$

(2) J (Reema) $\rightarrow H_p$ (Reema) - using universal instantiation in (i)

(3) J (Reema) - from given argument

(4) H_p (Reema) $\rightarrow$ Using modes process on (2) and (3)

Since we have H_p (Reema), we can now use existential generation rule as

H_p (Reema)

$\therefore$ For some c, $H_p(C)$

i.e. there is source 'C' who get high paying job. Hence proved.

Example

Everyone in descrete structure class has taken a course in computer science and Reema is a st in this class imply the conclusion Reema has taken a course in computer science.

Solution

Let D(x): x is a student in discrete structure class

C(x): x has taken a course in computer science

Then, the premise or given facts are

(a) $\forall D(x) \rightarrow C(x)$

(b) D (Reema)

and we have to prove that conclusion is C(Reema)

Now,

(1) $\forall x, D(x) \rightarrow C(x)$ - given

(2) D(Reema) $\rightarrow$ C(Reema) - using (vi)

(3) D(Reema) $\rightarrow$ given

(4) C(Reema) - using modus person on 2 & 3

Hence, it is concluded that Reema had taken a computer science course.

Example

Prove or disprove the validity of argument: "every living thing is a plant or an animal." "Hari's dog is alive and it is not a plant." "All animals have heart." Hence Hari's dog has heart.

Solution

Let,

P(x) : x is a planet

A(x) : x is an animal

L(x) : x is alive (living things)

H(x) : x has a heart

d : represent Hari's dog.

Then,

(1) $\forall x\ p(x) \vee A(x)$ [given]

(2) $L(d) \wedge \neg P(d)$ [given]

(3) $\forall x, A(x) \rightarrow H(x)$ [given]

(4) $P(d) \vee A(d)$ [universal instantiation on (I)]

(5) $\neg P(d)$ (simplicity on rule on 2)

(6) A(d) (resolution rule)

(7) $A(d) \rightarrow H(d)$ (universal instantiation on 3)

(8) H(d) (modus persons on 6)

The conclusion "Hari's dog has heart" is valid.

Example

There is someone in this class who has visited Pokhara. Everyone who has been in Pokhara visits Fewalake. Therefore some one in this class has visited Fewalake.

Solution

Let P(x) : X has been in Pokhara.

F(x): X has visited Fewalake.

S(X): x is a student of this class.

Then,

(1) $\exists x\ S(x) \wedge P(x)$ (given)

(2) $\forall x\ P(x) \therefore F(x)$ (given)

(3) $S(C) \wedge P(c)$ (using existential instantion, on ID for some constant C)

(4) P(C) (using simple feature)

(5) $P(C) \rightarrow F(C)$ (Using universal instantiation on 2)

(6) F(C) (Using modus ponens on 4 and 5)

(7) $S(C) \wedge F(x)$ (using conjunction rule)

(8) $\exists x\, S(x) \wedge F(x)$ (Using exestented generalization)

Exercise

1. What do you mean by proposition? Give example to justify your answer.
2. Which of the following sentences are propositions? What are the truth values of those that are propositions?
   a. Kathmandu is capital of Nepal. b. CPU is an output device.
   c. 5+8=12 d. x+4=8
   e. What is your name? f. x + y=y + z if x = z
3. Let p and q be propositions
   p : you do every exercise in this book
   q : You get grade A on the final exam
   Express the following into English sentence
   (a) $\neg p$ (b) $p \rightarrow q$ (c) $\neg p \wedge q$
   (d) $p \leftrightarrow q$ (e) $\neg q \rightarrow \neg p$
   (f) $\neg p \wedge (p \vee \neg q)$
4. Let p, q & r be propositions
   p : you have the flu
   q : you miss the final examination
   r : you pass the course
   Translate the following English sentence into propositions using connections:
   a. Whenever you have the flu, you miss the final examination.
   b. You miss the final exam only if you do not pass the course.
   c. If you have the flu, you do not pass the course or you miss the final examination only if you do not pass the course.
5. Determine whether the following propositions are true or false:
   a. 2+3=5 if and only if 2+1=3
   b. 1+1=3 if and only if pigs can fly.
   c. 1+1=3, then God exist.
6. State the converse, contra positive and inverse of the following implications:
   a. If it rains tonight, then I will stay at home.
   b. I go to swimming, whenever it is sunny day.
   c. when I stay up late, it is necessary that I sleep until noon.
7. Write converse, inverse and contrapositive of the following.
   a. All glitter is not gold.
   b. All hexagon are regular polygon.
   c. Fruit juice contain vitamin C.
8. Express the following sentences into logical expressions using proposition and connections
   a. The message is scanned for viruses whenever the message was sent from an unkno

system.

b. The message was sent to from unknown system but it was not scanned for viruses.

c. When a message is not sent from unknown system, it is not scanned for viruses.

9. Construct the truth table for each of following propositions.

a) $(p \vee \neg q) \rightarrow q$ b) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$

c) $(p \leftrightarrow q) \oplus (p \leftrightarrow \neg q)$ d) $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$

10. Explain Tautologies, contradiction and contingences with suitable examples.

11. Show that the statements given below are tautology.

a. $(p \vee q) \wedge (\neg p \vee q) \rightarrow (q \vee r)$ b. $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$

c. $(p \vee q) \vee [(\neg p) \wedge (\neg q)]$ d. $(p \wedge q) \rightarrow (p \rightarrow q)$

12. Show that the following pairs of proposition are logically equivalent.

a. $\neg(p \wedge q)$ and $(\neg p \vee \neg q)$ b. $(p \vee q) \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$

13. Show that $(P \vee q) \wedge [\neg p \wedge \neg q]$ is contradiction.

14. Show that $\neg (p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

15. Show that the propositions $p \vee (q \wedge r)$ and $(r \vee q) \wedge (p \vee q)$ are logically equivalent.

16. Differentiate between existential and universal quantifier with suitable examples.

17. Let P(x) denote the statement "$x \leq 5$". What are the truth values?

(a) P(1) (b) P(3) (c) P(7)

18. Let P(x) be the statement "the word x contains the letter a". What are the truth values?

(a) P(orange) (b) P(apple)

(c) P(monkey) (d) P(crocodile)

19. Let Q(x, y) denote the statement "x is the capital of y". What are these truth values?

(a) Q(Kathmandu, Nepal)

(b) Q(Delhi, India)

(c) Q(Colombo, Japan)

(d) Q(Kulalpur, Australia)

20. Let P(x) be the statement "x spends more than five hours every weekday in class", where the universe of discourse for x consists of all students. Express each of these quantifications in English.

(a) $\exists x\, P(x)$ (b) $\forall x\, P(x)$

(c) $\exists x \neg P(x)$ (d) $\forall x \neg P(x)$

21. Translate these statements into English, where C(x) is "x is a comedian" and F(x) is "x is funny" and the universe of discourse consists of all people.

(a) $\forall x\, (C(x) \rightarrow F(x))$ (b) $\forall x\, (C(x) \wedge F(x))$

(c) $\exists x (C(x) \rightarrow F(x))$ (d) $\exists x\, (C(x) \wedge F(x))$

22. Express the following statements using predicate and quantifier:

a. Every student in this class has studied discrete Math's.

b. Some student in this class are smart.

c. All birds can fly.

d. Some men are genius.

e. Some numbers are not rational.

f. There is student who likes discrete mathematics but not data communication.

g. There is a student at your college who can speak Japanese and who is good in C++.

23. What rule of inference is used in each of these arguments?

a. If it rains today, the college will close. The college is not closed today. Therefore, it will not rain today.

b. Ram is volleyball player and Basketball player. Therefore Ram is volleyball player.

c. Ashma is an excellent swimmer. If Ashma is an excellent swimmer, then she can work as a lifeguard. Therefore, Ashma can work as a lifeguard.

d. If I work all night on this homework, then I can answer all the exercises. If I answer the exercises, I will understand the material. Therefore, if I work all night on this homework, then I will understand the material.

24. What rule of inferences are used in following?

a. All men are mortal. Socrates is a man. Therefore, Socrates is mortal.

25. For each of the following, determine whether the argument is correct or incorrect and explain why?

a. All students in this class understand C-programming. Rina is student in this class. Therefore, Rina understand C-programming.

b. All Parrots like fruits. My pet bird is not a parrot.Therefore, my pet bird does not like fruit.

c. Every computer science major takes discrete structure. John is taking discrete structure. Therefore, John is computer science major.

26. Validate the following argument:

a. If Loknath is a student then he has an internet account. Loknath doesn't have an internet account. Therefore, Loknath is not a student.

b. If I go swimming then I will stay in the sun too long. If I stay in the sun too long, then I will sunburn. Therefore, if I go swimming then I will sunburn.

c. If Bhairav play hockey too much then he will get low marks. Bhairav didn't get low marks. Therefore, Bhairav didn't play hockey.

27. Show that 'q' is a valid conclusion from the premises $p \rightarrow q$, $q \rightarrow r$, $r \rightarrow s$, $\neg s$ and $p \vee q$.

28. State which rule of inference is basis of the following argument. "It is below freezing and raining now, therefore, it is below freezing now.

29. Explain the 4-rules of inference for quantified statements.

30. Give examples of addition rule and simplification rule of inference.

31. What relevant conclusion can be drawn from given premises?

a. Every student has an internet account. Ram does not have an internet account. Hari has an internet account.

b. I am either cleaver or lucky. I am not lucky. If I am lucky then I will win the lottery.

3.2 Proof Methods

A theorem is a mathematical statement that can be shown to be true. A proof of given theorem is said to be well founded if its steps of mathematical statement can be present on argument that makes the theorem true.

This method of understanding correctness of statement by applying sequence of logical argument is known as proof of statement.

Problem solving or proving is not just a science so there is no hard and fast rule that is applied in problem solving. However there are some guiding methods that help us to solve different kinds of problems.

Here we will discuss different methods of proving implication $p \rightarrow q$.

Direct Proofs

The implication $p \rightarrow q$ can be proved by showing that if p is true, then q must also be true. To carry out such a proof, we assume that hypothesis p is true and using information already available if conclusion q becomes true then argument becomes valid.

Example

If a and b are odd integers, then a + b is an even integer.

Proof

We know the fact that if a number is even then we can represent it as 2k, where k is an integer and if the number is odd then it can be written as 2l + 1, where l is an integer. Assume that a = 2k + 1 and b = 2l + 1, for some integers k and m. then a + b = 2k + 1 + 2l + 1 = 2(k + l + 1), here (k + l + 1) is an integer. Hence a + b is even integer.

Example

Prove that: If n is an odd integer, then n^2 is an odd integer.

Solution:

Let $p \rightarrow q$: if n is an odd integer, then n^2 is an odd integer.

We assume that hypothesis of this implication is true i.e. suppose, n is odd then n can be expressed as n = 2k + 1

Now,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

Since $2(2k^2 + 2k)$ is even but one more than even is odd

$\therefore$ n^2 is an odd integer.

Example

Prove that sum of two rational number is rational number.

Proof: Suppose that A and B are two rational number then by definition of rational number, it follows that there are two integers p and q where $q \neq 0$ such that $A = \frac{p}{q}$ and integers x and y with $y \neq 0$ such that $B = \frac{x}{y}$.

Now,

$$A + B = \frac{p}{q} + \frac{x}{y}$$
$$= \frac{py + ax}{ay}$$

Since: $q \neq 0$ and $y \neq 0$, it follows that $ay \neq 0$. Here, we have expressed A + B as the ratio of integers $py + qx$ and qy with $ay \neq 0$

$\therefore$ A + B is rational.

Example

Using direct proof, prove that for every positive integer n, $n^3 + n$ is even.

Proof: Case 1: Suppose, n is even, then $n = 2k$ for some k.

Now,

$$n^3 + n = (2k)^3 + 2k = 8k^3 + 2k = 2(4k^3 + k) \text{ which is even.}$$

Case II: Suppose n is odd, then it can be expressed as

$n = 2k + 1$ for some positive integer k.

Now,

$$\begin{aligned} n^3 + n &= (2k + 1)^3 + (2k + 1) \\ &= (8k^3 + 12k^2 + 6k + 1) + (2k + 1) \\ &= 8k^3 + 12k^2 + 8k + 2 \\ &= 2(4k^2 + 6k^2 + 4k + 1) \end{aligned}$$

which is even. Hence, for any positive integer n, $n^3 + n$ is even.

Indirect Proofs

We have $p \rightarrow q \equiv \neg q \rightarrow \neg p$ i.e. contra positive of implication is equivalent to the implication the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\neg q \rightarrow \neg p$ is true prove the implication $p \rightarrow q$ by assuming that the conclusion (q) is false and using the kn facts we show that the hypothesis (p) is also false.

Example

If the product of two integers a and b is even, then either a is even or b is even.

Proof

Suppose both a and b are odd, then we have $a = 2k + 1$ and $b = 2l + 1$.

So $ab = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$, i.e. ab is an odd number. Hence, b and b being odd implies ab is also odd. This is indirect proof.

Example

Using indirect proof, show that if $3n + 2$ is odd then n is odd.

Proof: Let $p \rightarrow q$: if $3n + 2$ is odd then n is odd.

Assume that conclusion of this implication is false i.e. n is even then we can express n as:

$n = 2k$ for some integer k

It follows that

$$\begin{aligned} 3n + 2 &= 3 \times 2k + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \end{aligned}$$

$\therefore$ $3n + 2$ is even since $2(3k + 1)$ is multiple of 2.

Hence, if $3n + 2$ is odd then n is odd.

Proofs by Contradiction

The steps in proof of implication $p \rightarrow q$ by contradiction are:

- Assume $p \wedge \neg q$ is true.
- Try to so that the above assumption $(p \wedge \neg q)$ is false
- When the assumption is found to be false then implication $p \rightarrow q$ is true
- Since $p \rightarrow q$ is equivalent to $\neg p \vee q$ and negation of $\neg p \vee q$ is $p \wedge \neg q$ (By De Morgan's Law), so if our assumption is false then its negation is true.

Alternately, Contradict the statement and show that this leads to the false conclusion; if this is true then the contradicted statement must be false (since $\neg p \rightarrow F$ is true only if $\neg p$ is false), hence the statement is true.

Example

If a^2 is an even number, then a is an even number.

Proof

Assume that a^2 is an even number and a is an odd number. Since a is an odd number we have $a = 2k + 1$, for some integer k. so $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(k^2 + k) + 1$, here $k^2 + k$ is some integer, say l, then $a^2 = 2l + 1$ i.e. a^2 is an odd number This contradicts our assumption that is a^2 even. Hence proved.

Example

Prove that if $n^3 + 5$ is odd, then n is even.

Solution:

Let: $p \rightarrow q$: if $n^3 + 5$ is odd then n is even

Suppose $n^3 + 5$ is odd and n is also odd.

$\therefore$ n can be expressed as:

$n = 2k + 1$ for some positive integer k.

$$\begin{aligned} \therefore \quad n^3 + 5 &= (2k + 1)^3 + 5 \\ &= 8k^3 + 12k^2 + 6k + 1 + 5 \\ &= 8k^3 + 12k^2 + 6k + 6 \\ &= 2(4k^3 + 6k^2 + 3k + 3) \end{aligned}$$

which is even.

This contradict our assumption that $n^3 + 5$ is odd.

Proofs By Counter Examples

To prove that the statement of the form $\cdot xP(x)$ is false, we just need some value of x. So while proving for falsity we just look for counter example.

Example

Prove or disprove the product of two irrational numbers is irrational.

Proof:

Here we instantly try to get the product of the irrational to try it. Lets take both the number for product be $\sqrt{2}$ then we have $\sqrt{2}*\sqrt{2} = 2$ (not rational). Hence by counter example it is shown that the product of two irrational numbers is not necessarily irrational.

Trivial and Vacuous Proofs

In the implication $p \to q$, if we can show that the consequence q is true then regardless of tru values of p, the implication $p \to q$ is true. Such type of proof technique is called **trivial proof**.

In the implication $p \to q$, if we can show that the hypothesis p is false, then regardless of truth valu of q, the implication $p \to q$ is true. Such kind of proof of an implication $p \to q$ is called **vacuo proof**.

Example

If x is an integer, then 3 is an odd integer. (Trivial) If a black is white, then pink is blue. (Vacuous)

Existence Proofs

A proof of a proposition of the form $\exists x P(x)$ is called an existence proof. There are different ways proving a theorem of this type. Sometime some element a is found to show P(a) to be true, this called constructive existence proof. In other method we do not provide a such that P(a) is true b prove that $\exists x P(x)$ is true in different way, this is called non constructive existence proof.

Example

Prove that there are 100 consecutive positive integers that are not perfect squares.

Proof:

Lets consider 2500 this is a perfect square of 50, and take 2601 this is a perfect square of 51. between 2601 and 2500 there are 100 consecutive positive integers. Hence the proof.

Uniqueness Proofs

To prove the theorem that asserts the existence of unique element with particular property we mu show that the element with this property exists and no other elements has this property. There a two parts in this uniqueness proof

Existence: here we show that the element with desire property exists

Uniqueness: we show that if $y \neq x$, then y does not have the desired property.

The above two steps can be proved if we prove the statement

$$\exists x(P(x) \wedge \forall y(y \neq x \to \neg P(y))).$$

Proof by Cases

The implication of the form $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$ can be prove by using the tautolo $(p_1 \vee p_2 \vee \ldots \vee p_n) \to q \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)]$, i.e. we can show every implicati $(p_i \to q)$ true for i =1, 2, ..., n.

Example

If $|x| > 3$, then $x^2 > 9$, where x is a real number.

Proof:

Here we have to consider two cases $-x > 3$ and $x > 3$ since $|x|$ represent an absolute value of x have the following relations

$x = x$, when $x \geq 0$ and

$-x$ when $x \leq 0$.

If $-x > 3$, then $x^2 > 9$. Similarly, if $x > 3$, then $x^2 > 9$.

Example

If $|x| > 3$ then $x^2 > 9$, where x is a real number.

Proof:

Here we have to consider two cases:

(a) $-x > 3$ (b) $x > 3$

as $|x|$ is a absolnte value of x.

Case 1: If $-x > 3$ then squaring both side gives us

$x^2 > 9$. Proved

Case 2: If $x > 3$ then $x^2 > 9$.

Example

Prove that if a and b are real numbers, where b □ 0, then $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$

Proof: Assume that a and b are real numbers and b □ 0, we consider the following cases:

Case 1: Assume that $a \geq 0$ and $b \geq 0$, so that $\frac{a}{b} \geq 0$, then $|a| = a$, $|b| = b$, and $\left|\frac{a}{b}\right| = \frac{a}{b} = \frac{|a|}{|b|}$

Case 2: Assume that $a \geq 0$ and $b < 0$, so that

$\frac{a}{b} \leq 0$ then $|a| = a$, $|b| = -b$ and

$$\left|\frac{a}{b}\right| = -\frac{a}{b} = \frac{a}{-b} = \frac{|a|}{|b|}$$

Case 3: Assume that $a < 0$ and $b > 0$, so that

$\frac{a}{b} < 0$, then $|a| = -a$, $|b| = b$, and

$$\left|\frac{a}{b}\right| = -\frac{a}{b} = -\frac{a}{b} = \frac{|a|}{|b|}$$

Case 4: Assume that $a < 0$ and $b < 0$, so that

$\frac{a}{b} > 0$. Then $|a| = -a$, $|b| = -b$, and

$$\left|\frac{a}{b}\right| = \frac{a}{b} = \frac{-a}{-b} = \frac{|a|}{|b|}$$

Thus, for all possible cases.

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$$

and $3(k^2 + k + 1)$ is also divisible by 3; is multiple of 3.

Sum of two integer divisible by 3 is also divisible by 3. Hence, $p(k + 1)$ is true.

Example

Prove that if n is a positive integer, then n is even if and only if $7n + 4$ is even.

Proof:

Assume n is even then we have an integer k such that $n = 2k$, so $7n + 4 = 7*2k + 4 = 2(7k + 2)$ here $7k + 4$ is an integer so that $7n + 4 = 2l$, where $l = 7k + 2$ i.e. $7n + 4$ is even. By direct proof it is proved that if n is even, then $7n + 4$ is even.

Assume n is odd then we have an integer m such that $n = 2m + 1$, then $7n + 4 = 14m + 7 + 4 = 2(7m + 5) + 1$here since $7m + 5$ is an integer $7n + 4$ is an odd number by indirect proof it is proved that if $7n + 4$ is even, then n is even.

Hence the proof.

Example

Show that if a, b, and c are real numbers and $a \neq 0$, then there is a unique solution of the equation $+ b = c$.

Proof:

From the equation $ax + b = c$ we get the solution as $x = (c - b)/a$ (since $a \neq 0$, it is possible). The solution is unique because there is no other value for x than $(c - b)/a$ (a real number).

Mistakes in Proof

There are many common error made in constructing mathematical proof. Among them most common is mistakes in arithmetic and basic algebra.

Example

What is wrong with the: If n^2 is positive then n is positive.

Proof: Let (n): n is positive.

Q(n): n^2 is positive

Then given statement is expressed as

$$\forall P(n) \rightarrow Q(n)$$

Now

From the hypothesis Q(n) and statement $\forall n(P(n) \rightarrow Q(n)$ we cannot conclude P(n)

For eg. Let $n = -2$ then $n^2 = (-2)^2 = 4$, which is positive.

but n is negative.

Exercise

1. Prove that square of an even number is also even.
2. Prove that sum of two odd integers is even (direct proof)
3. Prove that the product of two odd integers is odd.
4. Prove that the product of two rational number is rational.
5. Prove that if n is an integer and 3n+2 is even then n is even.
6. Prove that the square of an even number is an even number using:
   a. Direct proof
   b. Indirect proof
   c. Proof by contradiction
7. Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using indirect proof and proof by contradiction.
8. Prove that if n is an integer and $3n + 2$ is even, then n is even using indirect proof and proof by contradiction.
9. Prove that product of two rational number is rational.
10. Explain the method of providing theorem by direct, indirect, contradiction and by cases.
11. Discuss the technique of proof by contradiction and by cases with suitable example.

Chapter 4

Induction and Recursion

Mathematical Induction

hematical induction is an extremely important proof technique that can be used to proof hematical theorems or statements, to analyze the complexity of algorithms and correctness of nputer programs etc. Here, induction means the method of inferring a general statement from the idity of particular cases.

P(n) be a statement on positive integer n then to prove P(n) is valid using induction, we need to ow following steps.

Basic Step:

this step, we need to verify that P(n) is true for n = 0 or 1.

Induction Hypothesis:

this step, we assume that P(n) is true for n = k i.e. P(k) is true.

Inductive step:

this step, by using induction hypothesis, we prove that P(n) is true for n = k + 1

$[P(n_0) \wedge \forall k\,(P_k) \rightarrow P\,(k+1)] \rightarrow \forall n, P(n)$

ample

se mathematical induction to prove that $n^3 - n$ is divisible by 3whenever n is a positive integer.

olution:

et P(n) denote the proposition: $n^3 - n$ is divisible by 3.

) **Basis step:** Let P(n) is true for n = 1

e. P(1): $1^3 - 1 = 0$, is divisible by 3.

ii) **Induction hypothesis**

et P(n) is true for n = k

e. P(k): $k^3 - k$ is divisible by 3

iii) **Inductive step:**

Using induction hypothesis, we try to show that P(n) is true for n = k + 1

Now,

$$P(k+1) = (k+1)^3 - (k+1)$$
$$= k^3 + 3k^2 + 3k + 1 - k - 1$$
$$P(k+1) = (k^3 - k) + 3\,(k^2 + k)$$

Since, both terms in this sum are divisible by 3. It follows that $(k+1)^3 - (k+1)$ is divisible by 3. by principle of mathematical induction, $n^3 - n$ is divisible by 3 whenever n is a positive integer.

Example

Prove by mathematical induction that,

$$1 + 3 + 5 + \ldots\ldots\ldots + (2n-1) = n^2$$

Solution

Let $P(n) = 1 + 3 + 5 + \ldots\ldots\ldots + (2n-1) = n^2$

1. Basis Step: For n = 1, we have

$P(1) = 1 = (1)^2$, hence P(1) is true.

2. Induction Hypothesis: Assume P(k) is true i.e.

$P(k) = 1 + 3 + 5 + \ldots\ldots\ldots + (2k-1) = k^2$

3. Inductive Step: Now, we wish to show P(k + 1) is true. So adding (2k + 1) on both sides of then

$$1 + 3 + 5 + \ldots\ldots + (2k-1) + (2k+1) = k^2 + (2k+1) = (n+1)^2$$

$\therefore \quad P(n+1) = (n+1)^2$, is true

Thus, by mathematical induction P(n) is true for all n.

Example

Prove that 3 divides $n^3 + 2n$ whenever n is a nonnegative integer.

Solution

Let $P(n) = n^3 + 2n$, then

1. Basis Step: For n = 0, we have $n^3 + 2n = 0$, this is divisible by 3 hence the statement is true for n=k+1.

2. Inductive Hypothesis: assume that the $P(k) = k^3 + 2k$ is divisible by 3 for all nonne values for $k \le n$.

3. Inductive Step: here we are going to show that p(k+1) true. We have

$P(k+1) = (k+1)^3 + 2(k+1) = k^3 + 3k^2 + 3k + 1 + 2k + 2$

$= k^3 + 2k + 3k^2 + 3k + 3$

$= (k^3 + 2k) + 3(k^2 + k + 1)$ (since $k^3 + 2k$ is divisible by 3, by hypothesis and $3(k^2 + k + 1)$ is also divisible by 3, multiple of 3)

Hence, P(k+1) is divisible by 3.

So by mathematical induction $n^3 + 2n$ is divisible by three for all nonnegative integers n.

Example

Prove, for $n \ge 1$ and $a \ne 1$, that,

$$1 + a + a^2 + \ldots\ldots\ldots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

Solution

Let $P(n) = 1 + a + a^2 + \ldots\ldots + a^n = \dfrac{a^{n+1} - 1}{a - 1}$

1. Basis Step: For n = 1, we have

$$P(1) = 1 + a = \frac{a^{1+1} - 1}{a - 1} = \frac{a^2 - 1}{a - 1} = a + 1$$

So, P(1) is true.

2. Induction Hypothesis: Suppose, P(k) is true i.e.

$$P(k) = 1 + a + a^2 + \ldots + a^k = \frac{a^{k+1} - 1}{a - 1}$$

Now, we wish to show P(k + 1) is true, for this we add a^{k+1} to both sides of P(n), then

$$1 + a + a^2 + \ldots + a^k + a^{k+1} = \frac{a^{k+1} - 1}{a - 1} + a^{k+1}$$

$$= \frac{a^{k+1} + a^{k+1}(a - 1)}{a - 1}$$

$$= \frac{a^{k+1} - 1 + a^{k+2} - a^{k+1}}{a - 1}$$

$$= \frac{a^{k+2} - 1}{a - 1}$$

$$\therefore \quad P(k + 1) = \frac{a^{(k+1)+1} - 1}{a - 1}, \text{ is true.}$$

Thus P(n) is true for all n.

Example

Use induction to show that $n! \geq 2^{n-1}$ for $n \geq 1$.

Solution

Let P (n) is the given statement.

1. Basis Step: Then for n = 1, $1! \geq 2^{1-1} = 1$, hence P(1) is true.

2. Induction Hypothesis: Assume that P(k) is true i.e. $k! \geq 2^{k-1}$.

3. Inductive Step: Now using induction hypothesis, we wish to show that the statement is true for n=k+1.

Now,

$$P(k+1): (k + 1)! = (k+ 1)k!$$

$$\geq (k + 1).2^{k-1} \quad (\because k! \geq 2^{nk-1})$$

$$\geq 2.2^{k-1} \quad (\because k \geq 1)$$

$$= 2^{k-1+1}$$

$$= 2^k$$

$$\therefore (k + 1)! \geq 2^k$$

Hence P(k + 1) true. Thus, by mathematical induction P(k) is true for all $n \geq 1$.

Example

Use mathematical induction to prove that $n < 2^n$ for all positive integer $n \geq 1$.

Solution:

Let P(n): $n < 2^n$ be a statement

1. Basis step: For n = 1.

$P(1) : 1 < 2^1$ i.e. 1 < 2 (True)

2. Induction hypothesis: Suppose P(n) is true for n = k i.e. P(k): $k < 2^k$ is true.

3. Inductive Step: By using induction hypothesis we show that P(n) is true n = k + 1.

$$\therefore P(k + 1) : k + 1 < 2^k + 1$$

$$\leq 2^k . 2^k$$

$$\leq 2. 2^{k+1}$$

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

Hence, for all positive integers n, $n < 2^n$

Example

Prove that 1.1! + 2.2! + … + n.n! = (n+1)! –1, whenever n is a positive integer.

Solution

Let P(n) = 1.1! + 2.2! + … + n.n! = (n+1)! –1, then

1. **Basis Step:** for n = 1, we have P(1) = 1.1! = 1,
   Similarly P(1) = (1+1)! –1 = 2-1 =1
   Hence P(1) is true.
2. **Inductive Hypothesis:** Assume that P(n) is true, i.e. 1.1! + 2.2! + … + n.n! = (n+1)! –1.
3. **Inductive Step:** if we are able to prove that P(n+1) is true then we are done. So we have

$$
\begin{aligned}
P(n+1) &= 1.1! + 2.2! + \ldots + n.n! + (n+1)(n+1)! \\
&= (n+1)! - 1 + (n+1)(n+1)! \text{ (Using induction hypothesis)} \\
&= (n+1)n! + (n+1)(n+1)! - 1 = (n+1)\,(n! + (n+1)!) - 1 \\
&= (n+1)(n!\,(1 + (n+1)) - 1 = (n+1)n!\,(n+2) - 1 \\
&= (n+2)! - 1
\end{aligned}
$$

P(n+1) is true.

Hence P(n) is true for all positive integers.

Example

Prove that for any positive integer n, 1 + 2 + ... + n = n(n+1)/2.

Solution

Let's let P(n) be the statement "1 + 2 + ... + n = n (n+1)/2." (The idea is that P(n) should be assertion that for any n is verifiably either true or false.)

1. Basis Step: We must verify that P(1) is True. P(1)

Asserts "1 = 1(2)/2", which is clearly true.

So we are done with the initial step.

2. Induction Hypothesis: Let P(n)is true for n=k

i.e. P(k): 1+ 2+3+4+.....+k=k(k+1)/2

3. Inductive Step: Here we must prove the following assertion: "If there is a k such that P(k) is then (for this same k) P(k+1) is true." Thus, we assume there is a k such that 1 + 2 + ... + k (k+1)/2. (We call this the inductive assumption.) We must prove, for this same k, the formula 1 + ... + k + (k+1) = (k+1)(k+2)/2.

This is not too hard: 1 + 2 + ... + k + (k+1) = k(k+1)/2 + (k+1) = (k(k+1) + 2 (k+1))/2 = (k+1)(k+2
The first equality is a consequence of the inductive assumption.

Strong Induction

The strong induction uses the save concept as in the mathematical induction method of proof bu only difference between these two types of induction is on the inductive step. In strong induction as the inductive step as: P(J) is true and show that P(k + 1) must also be true.

This is also known as second principle of mathematical induction.

The formal definition of strong induction can be written as:

To prove P(n) is true for all positive integers n, we use:

(1) Basis step: The proposition P(1) is shown to be true.

(2) Inductive step: It is shown that [P(1) ^ P(2) ..... P(K)] → P(k + 1) is true for every positive integer

Proved by using Strong Induction

Example

Show that if n is an integer greater than 1 then n can be written as products of princes.

Solution:

Let P(n) is the proposition that 'n' can be written as the product of primes.

Basis step: Here n = 2, P(2) is true, since 2 can be written as product of one prime, itself.

Inductive step: Let us suppose that P(j) is true for all positive integer $J \leq k$. Then, we have to show that P(k + 1) is true.

Now, there may be two cases:

(a) When k + 1 is prime (b) when k + 1 is composite.

If k + 1 is prime, then P(k + 1) is immediately true any prime can be written as a product of prime. Otherwise 'k+1' is composite and can be written as product of two positive integer x and y with $2 \leq x \leq y \leq k + 1$.

By induction hypothesis, both x and y < k can be written as product of primes. Hence, if k + 1 is composite, it can be written as product of primes namely, the prime factors of x and prime factors of y.

Example

Use mathematical induction to show that '3' divides $n^3 + 2n$ whenever 'n' is a non-negative integer.

Solution

Let P(n) : $n^3 + 2n$ is divisible by 3.

Basis step: Here n = 0, then P(0) : $0^3 + 2 \times 0 = 0$, which is divisible by 3 i.e. P(0) is true.

Inductive step: Let us suppose that, $n^3 + 2n$ is divisible by 3, for all $n \leq k$.

i.e. P(k): $k^3 + 2k$ is divisible by 3.

Now, we have to prove that P(k+1) is true. For this,

$$p(k + 1) : (k + 1)^3 + 2(k + 1)$$
$$= k^3 + 3k^2 + 3k + 1 + 2k + 2$$
$$= k^3 + 2k + 3k^2 + 3k + 3$$

Since $k^3 + 2k$ is divisible by 3 (from hypothesis).

Well Ordering Property

This property states, "Every nonempty set of nonnegative integers has a least element." Using this property we can verify the validity of proofs using mathematical induction. Using mathematical induction we prove P(1) is true and P(n) → P(n+1) is true for all positive integers n. If the proof by mathematical induction is not valid then P(n) is true for all positive integers n would be false. Let the set of positive integers for which P(n) is false be T. then T is nonempty since there is at least one element in T such that P(n) is false. By the well ordering property, T has a least element, let the least element be k. we know that m cannot be 1 because we have already proved that P(1) is true. So k is a positive integer greater than 1 so k –1 is a positive integer, so we have P(k-1) must be true. Here k –1 is less than k i.e. k-1 is not in the set T. Since the implication P(k-1) → P(k) is also true, P(k) must be true. This contradicts the choice of k. Hence, P(n) must be true for all positive integers n.

Example

Prove $a^n = 1$ for all nonnegative integers n, whenever a is a nonzero real number.

Solution

Basis Step: for n = 0, $a^0 = 1$ by the definition of a^0.

Inductive Hypothesis: assume that $a^k = 1$ for all nonnegative integers $k \leq n$.

Inductive Step: we have $a^{k+1} = a^k . a^k / a^{k-1} = 1.1/1 = 1$.

Hence proved.

4.2 Recursive Definitions and Structural Induction

Sometime it is difficult to define a relation directly but it may be easy to define this relation in terms of it this process is called recursion. The most common application of recursion is in mathematics and computer science, in which it refers to a method of defining functions in which the function being defined is applied within its own definition

Recursively Defined Functions

Let us suppose the domain of function is set of non negative numbers, then We use two steps to define a function:

1. **Basis Step**: specify the value of function at 0.
2. **Recursive Steps**: give a rule for finding its value at an integer from its value at smaller integers. Such a definition is called recursive definition.

Example

(i) Let the given sequence is 2, 5, 8, 11, 14, 17, ...

Then the nth term of this sequence can be defined explicitly as

$t_n = a + (n - 1)d, n \geq 1.$

And the same sequence can be defined recursively as :

(a) basis step: $S(0) = 2$

(b)Recursive Step: $S(n + 1) = S(n) + 3, n \geq 0$

(ii) The sequence 1, 3, 9, 27,.....can be defined recursively as

(a)Basis step: $S(0) = 1$

(b)Recursive Step: $S(n + 1) = 3\,S(n)$, for $n \geq 0$.

Example

Let function f is defined as

$F(0)=2$

$F(n+1)=2f(n)+1$

Then find the value of f(1),f(2) and f(3).

Solution

From the recursive definition, we have

$F(1)=2f(0)+1=2*2+1=5$

$F(2)=2(1)+1=2*5+1=11$

$F(3)=2f(2)+1=2*11+1=23$

Example:

Give a recursive definition of a sequence $\{a_n\}$, n = 1, 2, ..., n if an = 10n.

Solution:

Basis Step: $a1 = 10^1 = 10$.

Recursive Step: $a_n = 10a_{n-1}$. This is the recursive definition required.

Example:

Give a recursive definition of the set of even positive integers.

Solution

Let E be the set of even positive integers.

Basis Step: $2 \in E$

Recursive Step: If $a \in E$, then $a + 2 \in E$.

The above recursive definition gives a set of even positive integers.

Note: To prove that the recursive definition is correct we can use mathematical induction principle.

Example:

Show that $f_1^2 + f_2^2 + \ldots + f_n^2 = fnfn+1$, whenever n is a positive integer. Here fi's are i^{th} fibonacci numbers.

Recursive Algorithms

An algorithm is called recursive if it solves a problem by reducing it into instance of the same problem with smaller input.

Example

An algorithm to find the factorial of given numebr

Input: an integer number n

Algorithm:

factorial(n) //name of algorithm

1. Start
2. If n==0

    then f=1

Else

    f=n*factorial(n-1)

3. Stop

Example

A recursive algorithms for a^n

The power function can be defined recursively as:

a) Base case: $a^0=1$

b) Recursive definition: $a^n=a.a^{n-1}$ for a>1.

power (a,n)

1. start
2. if(n==0)

    return a;

    else

    return a*power(a,n-1)

3. End

Example

Devise a recursive algorithm for computing b^n mod m, where b, n, and m are integers with $m \geq 2$, $n \geq 0$, and $1 \leq b < m$.

Solution

We can base a recursive algorithm on the fact that b^n mod m = (b . (b^{n-1} mod m)) mod m and the initial condition b^0 and m = 1.

However, we can devise a much more efficient ... we describe pseudocode as Algorithm 2.

procedure mpower(b, n, m: integers with $m \geq 2$, $n \geq 0$; $1 \leq b < m$)

if n = 0 then

mpower (b, n, m) = 1

else if n is even then

mpower(b, n, m) = mpower(b, n/2, m)^2 mod m

else

mpower(b, n, m) = (mpower(b, $\lfloor n/2 \rfloor$, m)^2 mod m. b mod m) mod m

{mpower(b, n, m) = b^n mod m}

Example

Give a recursive algorithm for computing the greatest common divisor of two nonnegative integers and b with a < b.

Solution

We can base a recursive algorithm on the reduction gcd(a, b) = gcd(b mod a, a) and the condition gcd(0, b) = b when b > 0. This produces the procedure in Algorithm.

procedure gcd(a, b: nonnegative integers with a < b)

if a = 0 then gcd(a, b) :=b

else gcd(a, b) :=gcd (b mod a, a)

Example

Construct a recursive version of a binary search algorithm.

Solution

Suppose we want to locate x in the sequence $a_1, a_2, \ldots, a_n$. To perform a binary search, we begin by comparing x with the middle term, $a_{\lfloor (n+1)/2 \rfloor}$. Our algorithm will terminate if x equals this term. Otherwise, we reduce the search to a smaller search sequence, namely, the first half of the sequence if x is smaller than the middle term of the original sequence, and the second half otherwise. We have reduced the solution of the search problem to the solution of the same problem with a sequence approximately half as long.

procedure binary search (x, i, j)

m := $\lfloor (I + j)/2 \rfloor$

if x = a_m then

location := m

else if (x < a_m and i < m) then

binary search(x, i, m – 1)

else if (x > a_m and j > m) then

binary search (x, m + 1, j)

else location := 0.

Recursive Algorithm for finding fibonacci number

procedure fibonacci(n: nonnegative integer)

if n = 0 then fibonacci(0) := 0

else if n = 1 then fibonacci(1) : = 1

else fibonacci(n) := fibonacci(n – 1) + fibonacci(n – 2)

The Merge Sort

The merge sort work in three steps

1. Divide Step

If a given array A has zero or one element, simply return; it is already sorted. Otherwise, s A[p .. r] into two sub-arrays A[p .. q] and A[q + 1 .. r], each containing about half of the elements A[p .. r]. That is, q is the halfway point of A[p .. r].

2. Conquer Step

In this step, the each half of array obtained in divide step will be sorted by using merge sort its recursively. i.e the merge sort will be called for first half "A[p .. q]" and second half" A[q + 1 .. separately.

3. Combine Step

Combine the elements back in A[p .. r] by merging the two sorted subarrays A[p .. q] and A[q + 1 .. into a sorted sequence.

Note: that the recursion bottoms out when the sub-array has just one element, so that it is trivial sorted. The following example shows the working of merge sort.

Recursive Merge-sort Algorithm

Procedure merge sort ($L = a_1, a_2, a_3, \ldots\ldots, a_n$)

if $n > 1$ then

$m = \lfloor n/2 \rfloor$

$L_1 := a_1, a_2, a_3, \ldots\ldots, a_m$

$L_2 := a_{m+1}, a_{m+2}, \ldots\ldots, a_n$

L: = merge (merge sort (L_1), merge sort (L_2))

{L is sorted list in non-decreasing order}

Procedure merge (L_1, L_2, L)

L: = empty list

while L_1 and L_2 are non-empty

Begin,

Remove smaller of first element of L_1 and L_2 from the list it is in and put it at L.

If removal of this makes one list empty then remove all elements from other list and append to L.

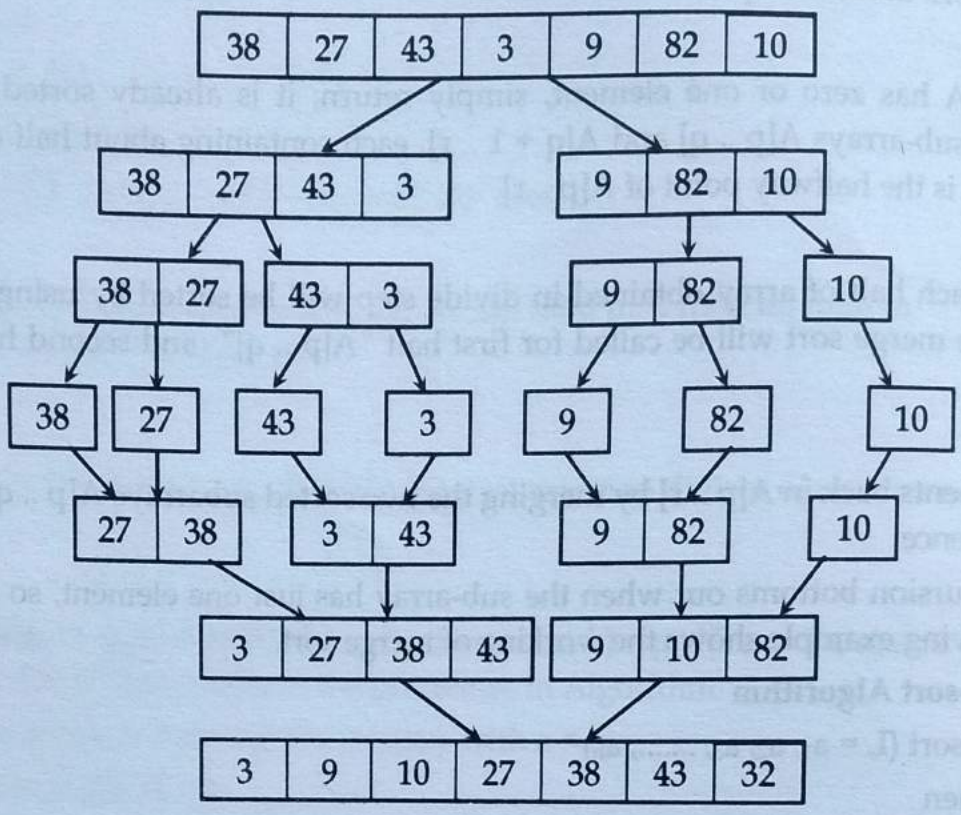
End {L is merged list in increasing order]

Example

Sort the following list of elements using merge sort.

38, 27, 43, 3, 9, 82, 10

Solution



Working of merge sort

Example

Illustration of merging process.

First list (L_1)	Second list (L_2)	Merged list (L)	Comparison
3, 27, 38, 43	9, 10, 82		3 < 9
27, 38, 43	9, 10, 82	3	9 < 27
27, 38, 43	10, 82	3, 9	10 < 27
27, 38, 43	82	3, 9, 10	27 < 82
38, 43	82	3, 9, 10, 27	38 < 82
43	82	3, 9, 10, 27, 38	43 < 82
–	82	3, 9, 10, 27, 38, 43	
	–	3, 9, 10, 27, 38, 43, 82	–

∴ Merged list is 3, 9, 10, 27, 38, 43, 82

Structural Induction

While proving the recursively defined sets we use a form of mathematical induction called structural induction. This method consists two parts.

Basis Step: Show that the result holds for all elements specified in the basis step of the recursive definition to be in the set.

Recursive Step: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

Validity of Structural Induction

The validity of structural induction can be seen as the validity of the mathematical induction. If P(n) denotes the statement that is recursively defined, for all positive integers n. The basis step of the structural induction method correspondence to the basis step of the mathematical induction method. We can see that the recursive step in the structural induction tells if P(k) is true it implies P(k+1), where P(k) is assumed already and the P(k+1) is derived in terms of P(k). Hence it follows the proofs by mathematical induction.

Example:

Recursive definition of the set of leaves and the set of internal vertices of a full binary tree can be defined as:

Basis Step: The root r is a leaf of the full binary tree with exactly one vertex r. This tree has no internal vertices.

Recursive Step: The set of leaves of the tree T = T1.T2 is the union of the set of the leaves of T1 and the set of leaves of T2. The internal vertices of T are the root r of T and the union of the set of internal vertices of T1 and the set of internal vertices of T2.

Exercise

1. Prove that sum of first n even positive integer is n(n+1)
   i.e. 2+4+6+.....2n=n(n+1)
2. Use mathematical induction to prove that
   $1+2+2^2+2^3+.....+2^n=2^{n+1}-1$
3. Use mathematical induction to prove the inequality n < 2n for all positive integers.
4. Use mathematical induction to prove that $2^n < n!$ for every positive integer n with $n \geq 4$.
5. Use mathematical induction to show that
   $$1^2+2^2+3^2+.....n^2=\frac{n(n+1)(2n+1)}{6}$$, where n is positive integer
6. Use mathematical induction to prove that
   $$1^2+3^2+5^2.....(2n+1)^2=\frac{(n+1)(2n+1)(2n+3)}{3}$$, where n is non- negative integer
7. Using mathematical induction prove that
   $$1.2+2.3+3.4+.....+n(n+1)=\frac{1}{3}n(n+1)(n+2) \text{ for all } n \in N$$
8. Prove that $3^n < n!$ whenever n is a positive integer greater than 6.
9. Show that $2^n > n^2$ whenever n is an integer greater than 4.
10. Use mathematical induction to prove tha $n! < n^n$ whenever n is a positive integer greater than 1.
11. Find f(2), f(3), f(4) and f(5) if f is defined recursively by f(0) = - 1, f(1) = 2 and for n = 1, 2, ...
    (a) $f(n+1) = f(n) + 3f(n-1)$
    (b) $f(n+1) = f(n)^2 f(n-1)$
    (c) $f(n+1) = 3f(n)^2 - 4f(n-1)^2$
    (d) $f(n+1) = f(n-1)/f(n)$.

12. Give a recursive definition of the sequence $\{a_n\}$, n = 1, 2, 3, ... if

(a) $a_n = 4n - 2$

(b) $a_n = 1 + (-1)^n$

(c) $a_n = n(n + 1)$

(d) $a_n = n^2$.

❑❑❑

Chapter 5

Counting and Discrete Probability

5.1 Counting

Introduction, Basic counting Principles

Combinatory is that branch of discrete mathematics which concerns with counting problems. Techniques for counting are important in Mathematics and computer science, especially in probability theory and in the analysis of algorithms.

For instance, counting is required to determine whether there are enough telephone numbers or internet protocol addresses to meet demand, it is also used to determine the complexity of algorithms, counting techniques are used extensively when probabilities of events are computed.

Counting problems arise throughout mathematics and computer science. for example, We need to count the number of key operations used in algorithm to study its time complexity.

There are two basic counting principles.

Sum Rule Principle

If an event E can occur in m ways and another event F can occur in n ways, and if these two events cannot occur simultaneously, then one of the two events, i.e. E or F, can occur in m + n ways. More generally, suppose an event E_1 can occur in n_1 ways, a second event E_2 can occur in n_2 ways, a third E_3 can occur in n_3 ways, and so on and suppose no two of the events can occur at the same time. Then one of the events can occur in $n_1 + n_2 + n_3 + \ldots$ ways.

Example

If there are 24 boys and 18 girls in a class, find the number of ways of selecting one student as class representative.

Solution

Using sum rule, there are 24 + 18 = 42 ways of selecting one student as a class representative.

Example

Let E be the event of choosing a prime number less than 10, and F be the event of choosing an even number less than 10, find the number of ways that E or F can occur.

Solution

E can occur in 4 ways [2, 3, 5, 7], and F can occur in 4 ways [2, 4, 6, 8]. However E or F cannot occur in 4 + 4 = 8 ways. Since 2 is both prime number less than 10 and an even number less than 10. In fact, E or F can occur in only 4 + 4 – 1 = 7 ways.

Example

A student can choose a computer project from one of three lists. The three lists contain 23, 15, and possible projects, respectively. How many possible projects are there to choose from?

Solution

The student can choose a project from the first list in 23 ways, from the second list in 15 ways, from the third list in 19 ways. Hence, there are 23+15+19 =57 projects to choose from.

Example

How many ways we can get a sum of 4 or of 8 when two distinguishable dice (say one die is red the other is white) are rolled?

Solution

Since dice are distinguishable outcome (1, 3) is different form (3, 1) so to get 4 as sum we have pairs (1, 3), (3, 1), (2, 2), so total of 3 ways. And similarly getting 8 can be from pairs (2, 6), (6, 2) 5), (5, 3), (4, 4), so total 5 ways. Hence getting sum of 4 or 8 is 3 + 5 = 8 ways

Product Rule Principle

If an event E can occur in m ways and, independent of this event, if another event F can occur ways, then two events can occur simultaneously in mn ways. More generally, suppose an event can occur in n_1 ways, and, following E_1, a second event E_2 can occur in n_2 ways, and, following third can occur in n_3 ways and so on. The all the events can occur simultaneously in $n_1.n_2.n_3$ .... ways

Example

An office building contains 27 floors and has 37 offices on each floor. How many offices are there in the building?

Solution

No. of floors in the office=27

No of offices in each floor=37

Therefore, by the product rule there are 27.37 = 999 offices in the building.

Example

How many different three-letter initials with none of the letters can be repeated can people have?

Solution

Here the first letter can be chosen in 26 ways, since the first letter is assigned we can choose second letter in 25 ways and in the same manner we can choose third letter in 24 ways. So by product number of different three-letter initials are 26.25.24 = 15600

Example

Three persons enter into a car, where there are 5 vacant seats. In how many ways can they take their seats?

Solution

The first person has a choice of 5 seats and can sit in any one of those 5 seats. So there are 5 ways occupying the first seat. The second person has a choice of 4 seats, so there are 4 ways of occupying the second seat. Similarly, there are 3 ways of occupying the third seats.

Hence, the required number of ways in which all the three persons can sit is 5 × 4 × 3 = 60

Example

Suppose a license plate contains two letters followed by three digits with the first digit not zero. How many different license plates can be printed?

Solution

Each letter can be printed in 26 different ways, the first digit in 9 ways and each of the other two digits in 10 ways. Hence,

$26 \times 26 \times 9 \times 10 \times 10 = 608400$ different plates can be printed.

Example

There are 32 microcomputers in a computer center. Each microcomputer has 24 ports. How many different ports to a microcomputer in the center are there?

Solution

The procedure of choosing a port consist of two tasks , first picking a microcomputer and the picking a port on this microcomputer. Since there are 32 ways to choose the microcomputer and 24 ways to choose the port no matter which microcomputer has been selected, using product rule: there are 32 . 24 = 768 ports.

Example

In how many ways can an organization containing 26 members elect a president, treasurer, and secretary (assuming no person is elected to more than one position)?

Solution

The president can be elected in 26 different ways, the treasurer can be elected in 25 different ways and following this, the secretary can be elected in 24 different ways. Thus, there are $26 \times 25 \times 24 =$ 15600 different ways in which the organization can elect a president, a treasurer and a secretary.

Example

How many strings are there of four lowercase letters that have the letter x in them?

Solution

There are total 26.26.26.26 strings of four lowercase letters, by product rule. In the same way we can say that there are 25.25.25.25 strings of four lowercase letters without x, since without x there will be a set of 25 characters only. So there are total of 26.26.26.26- 25.25.25.25 = 66351 four lowercase letter strings with x in them. This is true because we are decrementing total numbers of strings with the number of strings that do not contain x in them so at least one x will be in the strings.

Example

How many functions are there from the set {1, 2, …, n}, where n is a positive integer, to the set {0, 1}.

Solution

Each element from the set {1, 2, …, n}can map the set {0, 1} in 2 ways. Since there are n elements in the first set by the product rule number of possible functions are 2.2.2…..n^{th} term i.e. 2n.

There is a set theoretical interpretation of the above two counting principles. Specifically, suppose n(A) denotes the number of elements in a set A and n(B) denotes the number of elements in set B then,

(i) **Sum Rule Principle:** If A and B are two disjoint sets, then

$n(A \cup B) = n(A) + n(B)$.

(ii) **Product Rule Principle:** If $A \times B$ be the Cartesian product of sets A and B, then

$n(A \times B) = n(A) \times n(B)$.

The Pigeonhole Principle

The pigeonhole principle states that, If k + 1 or more pigeons are placed into k pigeonholes, then there is at least one pigeonhole containing two or more of the pigeons.

Proof

We use proof by contradiction here. Suppose that k+1 or more boxes are placed into k boxes and no boxes contain more than one object in it. If there are k boxes then there must be k objects such that

there are no two objects in a box. This contradicts ... is at least one box containing two or more of the objects.

Generalized Pigeonhole Principle

If N objects are placed into k boxes, then there is at least one box containing at least

_N / k_ objects.

Proof:

Suppose N objects are placed into k boxes and there is no box containing more than _N / k_ -1 objects. So the total number of objects is at most k(_N / k_ -1) < k((N/k + 1) -1) = N. This is the contradiction that N objects are placed into k boxes (since we showed that there are total number of objects less than N). Hence, the proof.

If n pigeonholes are occupied by Kn + 1 or more pigeons, where K is a positive integer, then at least one pigeonhole is occupied by K + 1 or more pigeons.

Example

If 9 books are to be kept in 4 shelves, there must be at least one shelf which contains at least 3 books.

Solution

The nine books can be thought of as pigeons and four shelves as pigeonholes. Then n = 4 (Pigeonholes) and Kn + 1 = 9(Pigeons)

$\therefore \quad K \times 4 + 1 = 9 \Rightarrow K = 2$

So, at least 1 pigeonhole i.e. shelf is occupied by k + 1 =2 + 1 = 3 pigeons i.e. books.

Example

If a class has 24 students, what is the maximum number of possible grading that must be done to ensure that there at least two students with the same grade.

Solution

There are total 24 students and the class and at least two students must have same grade. If the number of possible grades is k then by pigeonhole principle

we have celi(24 / k) = 2.

Here the largest value that k can have is 23 since 24 = 23.1 + 1. So the maximum number of possible grading to ensure that at least two of the students have same grading is 23.

Example

Find the minimum number of students required in a class to be sure that three of them are born in the same month.

Solution

Here, the n = 12 months are pigeonholes and k + 1 = 3(pigeons) are born in same month. Then k + 1 = 3 gives k = 2. Thus kn + 1 = number of students (pigeons) = 2 × 12 + 1 = 25.

Example

Show that if any 15 people are selected, then we may choose a subset of 3 so that all 3 were born on the same day of the week.

Solution

We may assign each person (pigeon) to the day of the week on which she/he was born. So, 15 people (pigeons) are to be assigned to 7 pigeonholes (days of the week).

$\therefore \quad$ n = 7(pigeonholes) and Kn + 1 = 15 (pigeons)

So, Kn + 1= 7 × K + 1 = 15 gives K = 2

Therefore at least 1 day is occupied by k + 1 = 2 + 1 = 3 people.

Example

Suppose a laundry bag contains many red, white and blue socks. Find the minimum number of socks that one needs to choose in order to get two pairs (four socks) of same colour.

Solution

Here n = 3 colours (pigeonholes) and k + 1 = 4(pigeons).So k + 1 = 4 gives k = 3. Thus kn + 1 = number of socks (pigeons) = 3 × 3 + 1 = 10

Example

Find the minimum number of elements that needs to take from the set A = {1, 2, ..., 9} to be sure that two of them add up to 10.

Solution

Here A = {1, 2, ..., 9}. So the pigeonholes are the five sets (1, 9), (2, 8), (3, 7), (4, 6), (5, 5). So, we have n = 5 pigeonholes and k + 1 = 2 (Pigeons). Then k = 1. Now, kn + 1 = 5 × 1 + 1 = 6. Thus any choice of six elements (pigeons) of A will guarantee that two of them add up to ten.

Example

How many numbers must be selected from the set {1, 3, 5, 7, 9, 11, 13, 15} to guarantee that at least one pair of these numbers add up to 16?

Solution

The pairs of numbers that sum 16 are (1, 15), (3, 13), (5, 11), (7, 9) i.e. 4 pairs of numbers are there that add to 16. If we select 5 numbers then by pigeonhole principle there are at least.

Celi(5 / 4) = 2 numbers, that are from the set of selected 5 numbers, that constitute a pair. Hence 5 numbers must be selected.

Example

Find the least number of cables required to connect eight computers to four printers to guarantee that four computers can directly access four different printers. Justify your answer.

Solution

If we connect first 4 computers directly to each of the 4 printers and the other 4 computers are connected to all the printers, then the number of connection required is 4 + 4.4 = 20. To verify that 20 is the least number of cables required we have if there may be less than 20 cables then we would have 19 cables, then some printers would be connected by at most Celi(19 / 4) = 4 cables to the computers. Then the other 3 printers would have to connect the other 4 computers here all the computers cannot simultaneously access different printer. So if we use 20 cables, then at least celi(20 / 4) = 5 cables connects a printer to a computer directly. So the remaining 3 printers are required to connect only 3 computers. Hence the least number of cables required is 20.

Example

Among n + 1 different integral powers of an integer a, there are at least two of them that have same remainder when divided by the positive integer n.

Proof

Let $a_1, a_2, \ldots, a_{n+1}$, be n+1 different integral powers of integer a. when these numbers are divided by n then the set of possible remainders is {0, 1, 2, ..., n – 1). Since there are n remainders and n+1 numbers by pigeonhole principle at least 2 of the reminders must be same.

Permutation

Permutation of a set of objects means an arrangement of objects in some order. An ordered arrangement of r objects from a set of n objects is called r-permutation of n objects. It is denoted by P(n, r) or ^nP_r. consider, for example, the set of letters a, b, c and d. then:

(i) bdca, abcd, cdab, etc are permutations of the four letters taking all of them at a time.

(ii) abc, acd, bcd, etc. are permutation of the four letters taking three letters at a time.

(iii) ab, bc, cd, bd, etc are permutation of the four letters taking two letters at a time.

Note:

The total number of permutations of a set of n objects taking r objects at a time is given by

$$P(n, r) = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!} (r \le n)$$

Example

Show that $(n - r + 1) \cdot {}^{n}p_{r-1} = {}^{n}p_{r}$

Proof:

$$\text{LHS} = (n - r + 1) \cdot {}^{n}p_{r-1}$$

$$= (n - r + 1) \frac{n!}{[n-(r-1)]!} \quad [\because {}^{n}p_{r} = \frac{n!}{(n-r)!}]$$

$$= (n - r + 1) \frac{n!}{(n-r+1)!}$$

$$= (n - r + 1) \frac{n!}{(n-r+1)(n-r)!} \quad [\because n! = n(n-1)!]$$

$$= \frac{n!}{(n-r)!}$$

$$= {}^{n}p_{r}$$

= RHS proved.

Example

If ${}^{56}p_{n+6} : {}^{54}p_{n+3} = 30800 : 1$, find n.

Solution

We have, ${}^{n}p_{r} = \frac{n!}{(n-r)!}$

So, ${}^{56}p_{n+6} = \frac{56!}{(50-n)!}$

Similarly,

${}^{54}p_{n+3} = \frac{54!}{(50-n)!}$

Now,

Given, ${}^{56}p_{n+6} : {}^{54}p_{n+3} = 30800 : 1$

or, $\frac{56!}{(50-n)!} \div \frac{54!}{(50-n)!} = \frac{30800}{1}$

or, $\frac{56 \times 55 \times 54!}{(50-n)!} \times \frac{(51-n)(50-n)!}{54!} = 30800 \; [\because n! = n(n-1)!]$

or, $50 \times 55 (51 - n) = 30800$

or, $51 - n = \frac{30800}{50 \times 55}$

or, $51 - n = 10$

$\therefore$ $n = 41$.

Example

How many license plates consisting of 3 different digits can be made out of given integers 3, 4, 5, 6, 7?

Solution

This is just like arranging 3 objects out of 5 objects. So we have,

$$P(5,3) = \frac{5!}{(5-3)!} \quad [\because {}^{n}P_r = \frac{n!}{(n-r)!}]$$

$$= \frac{5 \times 4 \times 3 \times 2!}{2!}$$

$$= 60$$

This problem can also be solved by product Rule.

Example

How many number of 3 digits can be formed from the digits 3, 4, 5, 6, 7, 8? How many of these are divisible by 5.

Solution

Here, $n = 6,\ r = 3$

$$\therefore\ P(6,3) = \frac{6!}{(6-3)!} = \frac{6 \times 5 \times 4 \times 3!}{3!} = 120$$

To find the number divisible by 5, we fix the digit 5 on unit place.

$\therefore\ n = 6 - 1 = 5,\ \ r = 3 - 1 = 2$

$$\therefore\ P(5,2) = \frac{5!}{(5-2)!} = \frac{5 \times 4 \times 3!}{3!} = 20$$

Example

Find the number of ways in which a party of seven persons can arrange themselves: (a) in a row of seven chairs (b) around a circular table.

Solution

(a) The seven persons can arrange themselves in a row in 7.6.5.4.3.2.1 = 7! ways.
(which is same as P(7, 7))

(b) One person can sit at any place in the circular table. The other six persons can then arrange themselves in 6! ways around the table.
(which is same as, 7 persons can be arranged in a circular table is (7 – 1)! i.e. 6! Ways)

Example

In how many ways can 4 girls and 4 boys be arranged alternately on a round table?

Solution

First, let all the girls i.e. 4 girls can be arranged in (4 – 1)! = 3! Ways. But 4 boys between the girls can be arranged in 4! Ways, since a girl is already been fixed. Hence, 4 girls and 4 boys can be arranged alternately on a round table is 3! × 4! ways.

Example

In how many ways can 8 people be seated (a) in a row of 8 chairs (b) around a circular table, if two people insist on sitting next to each other?

Solution

(a) If two people insist on sitting next to each other, we consider two people as one. Then 7 people can be arranged in a row in 7! Ways. But two people can interchange their position in 2 ways.

∴ Total number of arrangements = 2 × 7! = 10080 ways.

(b) Similarly we consider two people as one. Then 7 people can be arranged in a round table – 1)! ways i.e. 6! ways. But two people can interchange their position in 2 ways.

∴ Total number of arrangements = 2 × 6! = 1440.

Permutations with Repetitions

The permutation of n objects taken all at a time, when there are P objects of one kind, q objects second kind, r objects are of a third kind, is $\frac{n!}{p!q!r!}$.

Example

How many seven – letter words can be formed using the letters of the word "BENZENE"?

Solution

There are seven objects (letters) of which there are three Es and two Ns. Therefore, the numbe permutation is $\frac{7!}{3!\,2!}$

$$= \frac{7 \times 6 \times 5 \times 4 \times 3!}{3! \times 2 \times 1} = 420$$

Example

How many six-letter words can be made using the letters of the word "SUNDAY"?

Solution

There are six-letters of which none is repeated. Therefore, the number of permutation is $\frac{6!}{0!} = 6 \times$ $\times 3 \times 2 \times 1 = 720$.

(which is arrangement of 6 letters out of 6 i.e. P(6, 6))

Example

(a) In how many ways can the letters of the word "arrange" be arranged?

(b) In how many ways can the letters of the word "arrange" be arranged so that the two r_s alw come together?

(c) In how many ways the letters can be arranged so that two r_s never come together?

Solution

(a) There are 7 letters in which there are two a_s and two r_s, so

Total number of alphabet to be arrange (n) = 7

Number of repetition of a (p) = 2

Number f repetition of r (q) = 2.

∴ Total number of arrangements $= \frac{n!}{p!\,q!}$

$$= \frac{7!}{2!\,2!}$$

$$= 1260 \text{ ways.}$$

(b) For the case when two r_s always come together, we consider two r_s as a single one. The word "arrange" becomes "arrange". So there are 6 letters including two a_s.

∴ Total number of arrangements $= \frac{6!}{2!} = 360$ ways.

(c) The total number of arrangements of letters of the word 'arrange' is 1260 and the total number of arrangements of the word 'arrange' where two r_s always come together is 360. So the total number of arrangements of the word 'arrange' where two r_s never come together is (1260 – 360) = 900 ways

Example

(a) Find the number of Permutations that can be formed from the letters of the word ELEVEN.

(b) How many of them begin and end with E?

(c) How many of them have the three Es together?

(d) How many of them never have the three Es together?

(e) How many of them begin with E and end with N?

Solution

(a) There are 6 letters of which three are Es.

So, total number of alphabet to be arrange (n) = 6

Number of repetition of E (p) = 3

$\therefore$ Total number of Permutations $= \frac{6!}{3!} = 120$

(b) Let's consider six boxes for six letters as

E					E

If first and last box is filled by E then remaining 4 letters in 4 boxes (in a row) can be filled in 4! ways i.e. 24 ways. Thus 24 of them begin and end with E

(c) For the case when three Es always come together, we consider three Es a single E. Then there are only four letters E, L, V and N. So four letters can be arranged in a row in 4! ways i.e. in 24 ways.

(d) Since the total number of permutations of the letters of the word ELEVEN is 120 and the number of permutations of the letters of word ELEVEN if 3 Es always come together is 24 then the number of permutations of the letters of the word ELEVEN when 3 Es never come together is (120 – 24) = 96.

(e) Lets consider six boxes for six letters where first box contains E and last box contains N.

E					N

Then out of six letters, only four letters are left which are L, E, V and E. Now the permutations of the 4 letters in which two are Es, is $\frac{4!}{2!} = 12$.

Example

Find the number of permutations of the letters in the word 'COMPUTER' taken four at a time in which

(i) two letters M and R do not occur.

(ii) two letters M and R always occur.

Solution

(i) From the word 'COMPUTER', if two letters M and R do not occur then the number of permutations = P(6, 4) = 360

(ii) If two letters M and R always occur, the number of permutations = P(6, 2) × 2 = 60.

As repetition is allowed, first digit can be chosen in 10 ways. Second digit can also be chosen in 10 ways and similarly third digit can also be chosen in 10 ways. So 3 digits license plate can be made in 10^3 ways i.e. 1000 ways.

Combination

Combination of objects means just their collection without any regard to order or arrangement. An unordered selection of r objects from a set of n objects is called a combination or r–combination. It is denoted by C(n, r) or ${}^nC_r$ and is given by the expression

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

Combination	Permutations
abc	abc, acb, bac, bca, cab, cba
abd	abd, adb, bad, bda, dab,dba
acd	acd, adc, cad, cda, dac, dca
bcd	bcd, bdc, cbd, cdb, dbc, dcb

Example

Calculate the value of C(12, 10).

Solution

$$C(12, 10) = \frac{12!}{10!(12-10)!} \quad [\because C(n, r) = \frac{n!}{r!(n-r)!}]$$

$$= \frac{12!}{10!\,2!}$$

$$= \frac{12! \times 11 \times 10!}{10! \times 2 \times 1}$$

$$= 66 \text{ ways.}$$

Example

In how many ways can a hand of 4 cards be dealt from an ordinary pack of 52 playing cards?

Solution

We need to consider combinations, since the order in which the cards are dealt is not important.

$$\text{Now, } C(52, 4) = \frac{52!}{4!\,(52-4)!} \quad [\because C(n, r) = \frac{n!}{r!(n-r)!}]$$

$$= \frac{52!}{4!\,48!}$$

$$= \frac{(52) \times (51) \times (50) \times (49)}{(4)\,(3)\,(2)\,(1)} \quad [\because n! = n(n-1)!]$$

$$= 270725 \text{ ways.}$$

Example

In a meeting, everyone had shaken hands with everyone else. It was found that 66 handshakes were exchanged. How many members were present at the meeting?

Solution

Let the number of members present at the meeting be 'n'. Any two members can make one handshake.

$\therefore$ The number of handshakes that can be made by n members = ${}^nC_2$

By the given condition, ${}^nC_2 = 66$

or, $\dfrac{n!}{(n-2)!\,2!} = 66$ $\quad [\because {}^nC_r = \dfrac{n!}{(n-r)!r!}]$

or, $\dfrac{n!}{(n-2)!\,2\times1} = 66$

or, $\dfrac{n(n-1)(n-2)!}{(n-2)!\,2} = 66$

or, $\dfrac{n(n-1)}{n!} = 66$

or, $n(n-1) = 132$

or, $n(n-1) = 12 \times (12-1)$

By using hit and trial method, we get,

$n = 12$

Example

Consider the set {a, b, c, d}. In how many ways can we select two of these letters (repetition is not allowed) when (i) order matters (ii) order does not matter?

Solution

(i) If order matters, the number of ways of selecting two letters from four letters is

$P(4, 2) = \dfrac{4!}{(4-2)!}$ $\quad [\because {}^np_r = \dfrac{n!}{(n-r)!}]$

$= 12$ ways.

(ii) If order does not matter, the number of ways of selecting two letters from four letters is

$C(4, 2) = \dfrac{4!}{2!\,(4-2)!}$ $\quad [\because C(n, r) = \dfrac{n!}{r!(n-r)!}]$

$= \dfrac{4!}{2!\,2!} = 6$ ways.

Example

A committee is to be chosen from 12 men and 8 women and is to consist of 3 men and 2 women. How many different committees can be formed?

Solution

3 men can be chosen from 12 men is

$C(12, 3) = \dfrac{12!}{3!(12-3)!} = 220$

2 women can be chosen from 8 women is $C(8, 2) = \dfrac{8!}{2!(8-2)!} = 28$

Hence the total number of different committees possible is

$220 \times 28 = 6160.$

Example

A bag contains six white marbles and five red marbles. Find the number of ways four marbles can be drawn from the bag if

(a) They can be any colour

(b) Two must be white and two red.

(c) They all must be of the same colour.

Solution

(a) Here, total number of marbles is 11. The four marbles of any colour can be chosen from marbles in C(11, 4) ways.

$$\therefore C(11, 4) = \frac{11!}{4!\,(11-4)!}$$

$$= \frac{11 \times 10 \times 9 \times 8 \times 7!}{4! \times 7!}$$

$$= 330.$$

(b) Two white marbles can be chosen in C(6, 2) ways and two red marbles can be chosen in C(5, 2) ways. Thus there are C(6, 2) · C(5, 2) ways of drawing two white marbles and two red marbles.

$$\therefore C(6, 2) \cdot C(5, 2) = \frac{6!}{2!\,(6-2)!} \times \frac{5!}{2!\,(5-2)!}$$

$$= \frac{6!}{2!\,4!} \times \frac{5!}{2!\,3!}$$

$$= 150$$

(c) There are C(6, 4) = 15 ways of drawing four white marbles and C(5, 4) = 5 ways of drawing four red marbles. Thus there are 15 + 5 = 20 ways of drawing four marbles of the same colour.

Permutations with Indistinguishable Objects

The number of different permutations of n objects, where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, ..., and n_k indistinguishable objects of type k, is

$$\frac{n!}{n_1!\,n_2!\,....\,n_k!}.$$

Example

How many different strings can be made by reordering the letters of the word SUCCESS?

Solution

Because some of the letters of SUCCESS are the same, the answer is not given by the number of permutations of seven letters. This word contains three Ss, two Cs, one U, and one E. To determine the number of different strings that can be made by reordering the letters, first note that the three Ss can be placed among the seven positions in C(7, 3) different ways, leaving four positions free. Then the two Cs can be placed in C(4, 2) ways, leaving two free positions. The U can be placed in C(2, 1) ways, leaving just one position free. Hence E can be placed in C(1, 1) way. Consequently, from the product rule, the number of different strings that can be made is

$$C(7, 3)\,C(4, 2)\,C(2, 1)\,C(1, 1) = \frac{7!}{3!\,4!} \cdot \frac{4!}{2!\,2!} \cdot \frac{2!}{1!\,1!} \cdot \frac{1!}{1!\,0!} = \frac{7!}{3!2!1!1!} = 420$$

Binomial Theorem

Let x and y be two variables and n be non-negative integers then the binomial theorem for positive index n states that,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n}y^n$$

The coefficients $\binom{n}{0}, \binom{n}{1}, \ldots \binom{n}{n}$ in the binomial expansion are called binomial coefficients, which are also denoted by $C_0, C_1, C_2, \ldots C_n$ respectively.

General Term

The $(r + 1)^{th}$ term in the expansion of $(x + y)^n$ is usually called its general term, which is denoted by t_{r+1}.

In the expansion of $(x + y)^n$,

$t_1 = 1^{st}$ term $= C(n, 0)x^n$

$t_2 = 2^{nd}$ term $= C(n, 1)x^{n-1}y^1$.

$t_3 = 3^{rd}$ term $= C(n, 2)\, x^{n-2}y^2$

$t_4 = 4$th term $= C(n, 3)\, x^{n-3}y^3$

. . .

. . .

. . .

$t_{r+1} = (r + 1)^{th}$ term $= C(n, r)x^{n-r}y^r$.

Thus the general term in the expansion of $(x + y)^n$ is t_{r+1} which is

$C(n, r)x^{n-r}y^r$.

Example

Show that:

(a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$

(b) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots + (-1)^n\binom{n}{n} = 0$, for all natural numbers n.

Solution

(a) We have

$$(x + y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n}y^n$$

When x = 1 and y = 1 then,

$$(1 + 1)^n = \binom{n}{0}1^n + \binom{n}{1}1^{n-1}1 + \binom{n}{2}1^{n-2}1^2 + \ldots + \binom{n}{n}1^n$$

$$\therefore \quad 2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}.$$

= sum of binomial coefficient.

(b) We have

$$(x + y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \binom{n}{3}x^{n-3}y^3 + \ldots + \binom{n}{n}y^n$$

When x = 1 and y = –1, then

$$(1 - 1)^n = \binom{n}{0}1^n + \binom{n}{1}1^{n-1}(-1) + \binom{n}{2}1^{n-2}(-1)^2 + \binom{n}{3}1^{n-3}(-1)^3 + \ldots + \binom{n}{n}(-1)^n$$

$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots + (-1)^n\binom{n}{n}.$$

Example

Expand $(2a + 5)^5$ by the binomial theorem.

Solution

Here n = 5.

By using binomial theorem,

$$(2a+5)^5 = \binom{5}{0}(2a)^5 + \binom{5}{1}(2a)^{5-1}(5)^1 + \binom{5}{2}(2a)^{5-2}(5)^2 + \binom{5}{3}(2a)^{5-3}(5)^3 + \binom{5}{4}(2a)^{5-4}(5)^4 + \binom{5}{5}(2a)^{5-5}(5)^5$$

$$= \frac{5!}{0!\,(5-0)!}.32a^5 + \frac{5!}{1!\,(5-1)!}.(2a)^4.5 + \frac{5!}{2!\,(5-2)!}(2a)^3.25 + \frac{5!}{3!\,(5-3)!}(2a)^2.125 + (2a)^1.625 + \frac{5!}{5!\,(5-5)!}(2a)^0.3125$$

$$= 32a^5 + 400a^4 + 2000a^3 + 5000a^2 + 6250a + 6250$$

Example

Find the coefficient of the term, containing y^8 in the binomial expansion of $(x + 3y^2)^{17}$.

Solution

The term containing y^8 in the expansion of $(x + 3y^2)^{17}$ is $\binom{17}{4} x^{17-4} (3y^2)^4 = 2380x^{13}81y^8$.

The coefficient of the term containing y^8 is $2380 \times 81 = 192780$.

Example

Find the coefficients of x^{16} in the expansion of $\left(2x^2 - \frac{x}{2}\right)^{12}$.

Solution

Comparing $\left(2x^2 - \frac{x}{2}\right)^{12}$ with $(x + y)^n$ we get, $x = 2x^2$, $y = -\frac{x}{2}$ and $n = 12$

The general term in the expansion of this expression by the binomial theorem is,

$$t_{r+1} = C(12, r)\,(2x^2)^{12-r}\left(\frac{-x}{2}\right)^r$$

$$= C(12, r)\,2^{12-r}\left(\frac{-1}{2}\right)^r x^{2(12-r)+r}$$

$$= C(12, r)\,2^{12-2r}\,(-1)^r x^{24-r}$$

To get the coefficient of x^{16}, we put $24 - r = 16$, thus $r = 8$.

Then the coefficient is $C(12, 8)\,2^{12-16}.\,(-1)^8$

$$= C(12, 8).\frac{1}{2^4}$$

$$= \frac{495}{16}$$

Example

Find the general term in the expansion of $\left(x^2 + \frac{a^2}{x}\right)^5$. Then find the coefficient of x.

Solution

Comparing $\left(x^2 + \frac{a^2}{x}\right)^5$ with $(x + y)^n$ we get $x = x^2$, $y = \frac{a^2}{x}$ and $n = 5$.

Since the general term in the expansion of $(x + y)^n$ is $t_{r+1} = C(n, r)x^{n-r}y^r$, the general term in the expansion of $\left(x^2 + \frac{a^2}{x}\right)^5$ is $t_{r+1} = C(5, r)\,(x^2)^{5-r}\left(\frac{a^2}{x}\right)^r$

$= C(5, r)x^{10-2r}\frac{a^{2r}}{x^r}$

$= C(5, r)\, x^{10-3r}a^{2r}$

To get the coefficient of x,

Let $10 - 3r = 1$

or $3r = 9$

$\therefore$ $r = 3$

$\therefore$ $t_{r+1} = t_{3+1} = t_4 = C(5, 3)xa^{2\times 3}$

$= C(5, 3)\, xa^6$

Thus the coefficient of x is $C(5, 3)a^6 = 10a^6$.

Example

Find the term independent of x in the expansion of $\left(2x + \frac{1}{x^2}\right)^9$.

Solution

Here, comparing $\left(2x + \frac{1}{x^2}\right)^9$ with $(x + y)^n$, we get $x = 2x$ and $y = \frac{1}{x^2}$ and $n = 9$

Since the general term in the expansion of $(x + y)^n$ is $t_{r+1} = C(n, r)\, x^{n-r}y^r$, then the general term in the expansion of $\left(2x + \frac{1}{x^2}\right)^9$ is,

$t_{r+1} = C(9, r)\,(2x)^{9-r}\left(\frac{1}{x^2}\right)^r$

$= C(9, r)\,(2)^{9-r}\,(x)^{9-r}.\frac{1}{x^{2r}}$

$= C(9, r)\,(2)^{9-r}\,x^{9-3r}$

To get the term which is independent of x,

Let $9 - 3r = 0$

$\therefore$ $r = 3$

$\therefore$ $t_{r+1} = t_{3+1} = t_4 = C(9, 3)\,(2)^{9-3}x^0 = C(9, 3)\,(2)^6 = 5376$, is the term independent of x.

Example

Find the 7th term of $\left(x + \frac{1}{x}\right)^{10}$.

Solution

Comparing $\left(x + \frac{1}{x}\right)^{10}$ with $(x + y)^n$ we get, $x = x$ and $y\,\frac{1}{x}$ and $n = 10$

The general term t_{r+1} of the expression $\left(x + \frac{1}{x}\right)^{10}$ is,

$t_{r+1} = C(10, r)\, x^{10-r}.\left(\frac{1}{a}\right)^r$

$= C(10, r)\, x^{10-r}.\, x^{-r}$

$= C(10, r)\, x^{10-2r}$

To get t_7, we put $r = 6$ in t_{r+1}, then

$$t_{6+1} = t_7 = C(10, 6)\, x^{10-2\times 6}$$
$$= \frac{10!}{6!\,(10-6)!} \times x^{-2}$$
$$= \frac{210}{x^2}$$

Middle Term

Now let us find the middle term or terms in the expansion of $(x + y)^n$. We have to consider the c when n is an even number and when it is an odd number.

(i) **When n is even:**

When n is even, the number of terms in the expansion of $(x + y)^n$ is $n + 1$ which is odd, there is exactly one middle term which is $t_{n/2+1}$

(ii) **When n is odd:**

When n is odd, the number of terms in the expansion of $(x + y)^n$ is $n + 1$ which is even there are two middle terms, which are $t_{(n+1)/2}$ and $t_{(n+1)/2+1}$

Example

(i) Find the middle term in the expansion of $(2a+3x)^{30}$

(ii) Find the middle term in the expansion of $\left(x - \frac{1}{x}\right)^{18}$

(iii) Find the middle term in the expansion of $(1+x/2)^{15}$

(iv) Find the middle terms in the expansion of $\left(2x + \frac{1}{2x}\right)^{15}$.

Solution

(i) Comparing $(2a + 3x)^{30}$ with $(x + y)^n$, we get: $x = 2a$, $y = 3x$, $n = 30$

Here, $n = 30$ which is even so there is only one middle term.

$$\text{Middle term} = (t_{30/2}) + 1 = t_{15+1}$$
$$= C(30,15)\,(2a)^{30-15}\,.\,(3x)^{15}$$
$$= C(30,15)\,(2a)^{15}\,.\,(3x)^{15}$$

(ii) Here $n = 18$, is even. So there are $(18 + 1) = 19$ terms in the expansion of $\left(x - \frac{1}{x}\right)^{18}$, which odd.

Therefore there exists exactly one middle term which is $t_{18/2+1}$ i.e. t_{10}.

$$\therefore \quad t_{10} = t_{9+1} = C(18, 9)\,(x)^{18-9}\left(-\frac{1}{x}\right)^9$$
$$= \frac{18!}{9!\,9!}\cdot(x)^{9-9}(-1)^9$$
$$= -\frac{18!}{9!\,9!}$$

(iii) Here the number of terms in the expansion is 15+1=16 which is even. So, there are two middl terms. The middle terms are $t_{(15+1)/2}$ and $t_{(15+1)/2+1}$ i.e. t_8 and t_9

$$t_8 = t_{7+1} = C(15, 7)\,(1)^{15-7}\left(\frac{x}{2}\right)^7 = \frac{15!}{7!8!}\frac{x^7}{2^7}$$

$$t_9 = t_{8+1} = C(15, 8)\,(1)^{15-8}\left(\frac{x}{2}\right)^8 = \frac{15!}{7!8!}\frac{x^8}{2^8}$$

(iv) Here the number of terms in the expansion is 15 + 1 = 16 which is even. So there are two middle terms, which are $t_{(15+1)/2}$ and $t_{(15+1)/2+1}$ i.e. t_8 and t_9

$$t_8 = t_{7+1} = C(15, 7)\,(2x)^{15-7}\left(\frac{1}{2x}\right)^7$$

$$= \frac{15!}{7!\,8!}(2x)^{8-7}$$

$$= \frac{15!}{7!\,8!}(2x)$$

$$t_9 = t_{8+1} = C(15, 8)\,(2x)^{15-8}\left(\frac{1}{2x}\right)^8$$

$$= \frac{15!}{8!\,7!}(2x)^{7-8}$$

$$= \frac{15!}{8!\,7!\,(2x)}$$

Pascal's Triangle

The geometrical arrangement of binomial coefficient in the expansion of $(x + y)^n$ in a triangular form is called Pascal's triangle. i.e. the coefficients of successive powers of x+y can be arranged in a triangular array. This triangular array of numbers is called Pascal's triangle. Which is shown in the following equations.

$(a+b)^0 = 1$

$(a+b)^1 = a + b$

$(a+b)^2 = a^2 + 2ab + b^2$

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + + 4ab^3 + b^4$

$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$

.....

The coefficients of the successive powers of a + b can be arranged in a triangular array of numbers, called Pascal's triangle. This can be shown as,

Coefficient in $(a + b)^0$

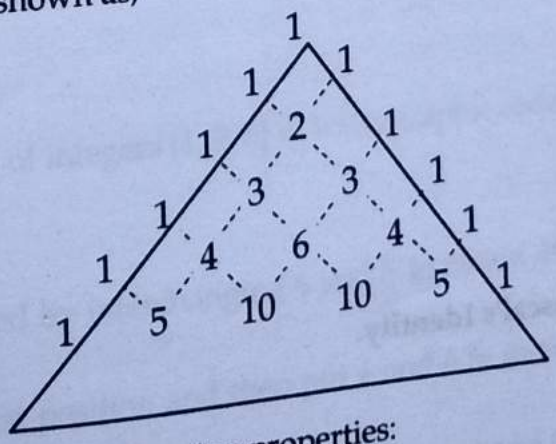
Coefficients in $(a + b)^1$

Coefficients in $(a + b)^2$

Coefficients in $(a + b)^3$

Coefficients in $(a + b)^4$

Coefficients in $(a + b)^5$



The numbers in Pascal's triangle have the following properties:

(i) The first and the last number in each row is 1.

(ii) Every other number in the array can be obtained by adding the two numbers appearing directly above it.

Example

Write down the expansion of $(1 + y)^6$, using Pascal's theorem.

Solution

Here n = 6, so we use Pascal's triangle up to n = 6.

When n = 0 — 1

When n = 1 — 1 1

When n = 2 — 1 2 1

When n = 3 — 1 3 3 1

When n = 4 — 1 4 6 4 1

When n = 5 — 1 5 10 10 5 1

When n = 6 — 1 6 15 20 15 6 1

$$\therefore \quad (1 + y)^6 = 1(1)^6 + 6(1)^5y + 15(1)^4(y)^2 + 20(1)^3(y)^3 + 15(1)^2(y)^4 + 6(1)^1(y)^5 + 1(1)^0(y)^6$$
$$= 1 + 6y + 15y^2 + 20y^3 + 15y^4 + 6y^5 + y^6$$

Example

Prove that: $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

Solution

$$\text{R.H.S.} = \binom{n}{r-1} + \binom{n}{r}$$

$$= \frac{n!}{(r-1)!\,(n-r+1)!} + \frac{n!}{r!\,(n-r)!}$$

$$= \frac{n!\,.r}{r(r-1)!\,(n-r+1)!} + \frac{n!\,.\,(n-r+1)}{(n-r+1)\,r!\,(n-r)!}$$

$$= \frac{n!.r}{r!\,(n-r+1)!} + \frac{n!.\,(n-r+1)}{r!\,(n-r+1)!}$$

$$= \frac{n!\,.\,r + n!.\,(n-r+1)}{r!\,(n-r+1)!}$$

$$= \frac{n!\,(n+1)}{r!\,(n-r+1)!}$$

$$= \frac{(n+1)!}{r!\,(n-r+1)!}$$

$$= \binom{n+1}{r} = \text{L.H.S.}$$

which is also known as **Pascal's Identity**.

Generating Permutation and Combination

Any set of n-elements can be mapped one-to-one with set {1, 2, 3, ... n}. We can find the permutation of any set of n elements by generating the permutation of the n-smallest positive integers and then replacing these integers with the corresponding elements.

To generate permutation of a set of a -element there are many algorithms. One of these algorithm is lexicographic (on dictionary) ordering of the set of permutations of {1, 2, 3, ... n}.

Algorithm

Given a natural number 'n', enlist n! permutations of given n distinct objects say 1, 2, 3,... in ascending order.

Steps:

1. Let C = 1, print first permutation of 1, 2, 3, ... n. If n = 1, go to step 3.
   Let total count = n! = n × n–1 × n – 2 .... 2 ×1.
2. For C = 2, to "Total count", Generate next permutation from permutation a_1, a_2, ... a_n by following the steps:
   a. Scan the digits of given permutation from right to left and note first consecutive pairs (a_{n-1} and a_n) such that $a_{n-1} < a_n$.
   b. Search for the smallest digit among digits a_{m+1}, a_{m+2} ..... a_n that is longer than a_m, call it x.
   c. Interchange a_m and X.
   d. Arrange all digits a_{m+1} to a_n in increasing order as $a_{m+1} < a_{m+2} < a_n$.
   e. Print a_1, a_2, ... a_n
3. Step.

Example:

Using this algorithm, let us generate all permutations of 1, 2, 3, and 4 as:

1234	1243	1324	1342	1423	1432	2134
2143	2314	2341	2413	2431	3124	3142
3214	3241	3412	3421	4123	4132	4213
4231	4312	4321				

Example: To generate permutation of set S {physics, chemistry, math, biology} we first can generate the permutation of set {1, 2, 3, 4} and then maps

1. Physics
2. Chemistry
3. Math
4. Biology

Example: Generate the permutation of integers {4, 5, 6} in lexicographic order:

Solution.

Began with 456.

The next permutation is obtained by interchanging 6 and 5 to obtain 465. Since, 6 > 5 and 4 < 6, permutes the three-integers.

→ Put the smaller of 6 and 5 in first position and then put 4 and 6 in increasing order in position 2 and 3 to obtain 546.

→ The next permutation is 564, which is obtained by interchanging 4 and 6 because 4 < 6 and so on.

Generating Combination

Algorithm

[Select k objects out of n distinct, say 1, 2, 3, 4, ... n]

1. List all a-digits in ascending order.
2. Select first k-digit, print them.
3. J = 1, 2, ... k be index on k-elements.
4. Assign maximum value to each Jth position as n – k + J.
5. Start scanning the list from right to left, stop at location where there are consecutive digits as $a_{n-1} < a_n$. Let m = n – 1. If no such pair, formed, go to step 8.
6. Leave the digits before a_m as they were, follow a_m by a_{m+1}, a_{m+2}, ... and until k-digits in all been listed down such that no digit crosses the limit assigned as in step 4.
7. Go to step 5
8. Stop.

Example:

Find the next layer 4-combination of the set {1, 2, 3, 4, 5, 6} after {1, 2, 5, 6}.

Solution.

The last term among the terms a_i with $a_1 = 1$, $a_2 = 2$, $a_3 = 5$, and $a_4 = 6$ such that $a_1 = 6 - 4 + i$ is
To obtain the next layer 4-combination increment a_2, by 1 to obtain $a_2 = 3$. Then set $a_3 = 3 + 1 =$
$a_4 = 3 + 2 = 5$. Hence, the next layer-4-combination is {1, 3, 4, 5}

Exercise

1. (i) How many automobiles license plates can be made if each plate contains two different letters followed by three different digits?
   (ii) Solve the problem if the first digit cannot be zero.
2. Find the number of permutations of five different objects taken three at a time.
3. If three persons enter a bus in which there are ten vacant seats, find in how many ways they can seat.
4. If a student is offered admission to 4 different Engineering colleges and 5 different medical colleges, find the number of ways of choosing one of the above colleges.
5. Find the minimum number of students needed to guarantee that five of them belong to the same class (Freshman, Sophomore, Junior, Senior).
6. State the Pigeonhole principle. How many students must be in a class to guarantee that at least two students receive the same score on the final exam is graded on a scale from 0 to 100.
7. Find the minimum number of students in a class to guarantee that three of them belong to the same zone (There are 14 zones in Nepal).
8. If ${}^nC_{12} = {}^nC_{10}$. What is the value of ${}^nC_2$?
9. If ${}^{18}C_r = {}^{18}C_{r+2}$, find ${}^{11}C$
10. If ${}^nP_r = 336$ and ${}^nC_r = 56$, find n and r. Also, find ${}^{n+2}C_{r+1}$.
11. Find r in each cases :
    (i) ${}^{28}C_{2r} : {}^{24}C_{2r-4} = 225 : 11$
    (ii) $4 \times {}^rC_2 = {}^{r+2}C_3$
    (iii) ${}^{167}C_{90} + {}^{167}C_r = {}^{168}C_r$

27. Find the general term in the expansion of $\left(\frac{a}{b}+\frac{b}{a}\right)^{2n+1}$

28. Find the coefficient of x^5 in the expansion of $\left(x+\frac{1}{2x}\right)^7$

29. What is the coefficient of x^{27} in the binomial expansion of $\left(\frac{3}{x}+x^2\right)^{18}$?

30. Find the term independent of x in the expansion of

i. $\left(2x+\frac{1}{3x^2}\right)^9$ ii. $\left(\frac{3x^2}{2}-\frac{1}{3x}\right)^9$

31. Find the term free from x in the expansion of $\left(x+\frac{1}{x}\right)^{2n}$

32. Consider the binomial expansion of $(4x - 5y)^{10}$.

(i) How many terms are there altogether?

(ii) Find the coefficient of x^3y^7 in the binomial expansion of $(4x - 5y)^{10}$.

33. Find the middle term or terms in the expansion of

i. $\left(ax+\frac{1}{ax}\right)^{17}$ ii. $\left(\frac{x}{a}-\frac{a}{x}\right)^{2n+1}$ iii. $\left(x+\frac{1}{x}\right)^{18}$

iv. $\left(ax-\frac{1}{ax}\right)^{2n}$ v. $\left(2x+\frac{1}{3x}\right)^{18}$ vi. $\left(y-\frac{1}{y}\right)^{15}$

5.2 Discrete Probability

Introduction

The word probability denotes chance and the theory of probability deals with laws governing the chances of occurrence of phenomena, which are unpredictable in nature. The theory of probability was first developed in the seventh century when certain gambling games were analyzed by the French Mathematician Blaise Pascal. Probability theory today has applications for beyond games of change, its utility is in almost all branches of Science, Engineering, Economics, Business, Industry. The theory of probability plays a vital role in making decisions in situation where there is a lack of certainty.

Discrete probability is concerned with one number or a few numbers that are associated with the outcome of experiments.

Random Experiment

An operation which can produce some well defined outcome is known as experiment. An experiment whose outcome can not be determined in advance is a random experiment. For example, tossing a coin is an experiment because if a coin is tossed either head or tail will turn up.

Example of random experiments are: Tossing a coin, throwing a die etc.

Sample Space

The set of all possible outcomes in a random experiment is called a sample space. Each element of a sample space is called a sample point. The number of sample points in S may be denoted by n(S).

For example, in the rolling of die, the sample space S = {1, 2, 3, 4, 5, 6} and sample points may be 1 or 3.

Event

The results or outcomes of experiments are called events i.e., an event of subset of sample space. For example for the sample space in tossing two coins, a subset E = {HH, HT} is the event. The number of sample points in an event E is denoted by n(E).

Equally likely events

A number of events are said to be equally likely if any one of them cannot be expected to occur in preference to the other.

Exhaustive events

Events are said to be exhaustive when they include all possible outcomes of a random experiment. In tossing a coin, exhaustive events are two.

Mutually Exclusive Events

Two or more events are said to be mutually exclusive or disjoint if the events cannot occur simultaneously i.e. occurrence of one of the events prevents the occurrence of others.

Let A and B are any two events defined on a sample space S and $A \cap B = \Phi$ then event A and B are said to be mutually exclusive. For example, in tossing a coin the events occurrence of head and tails are mutually exclusive because they cannot occur simultaneously

Probability of Events

Every event associated with a random experiment is assigned a weight or measure of the change of it occuring called its probability. The probability of an occurrence of an event E is denoted by P(E) and defined as

$$P(E) = \frac{\text{Number of outcomes favourable to the occurrence of E}}{\text{Total number of all possible outcomes}} = \frac{n(E)}{n(S)}$$

The probability of non-occurrence of the event A is

$$P(E') = \frac{\text{Number of unfavourable}}{\text{Total number of all possible outcomes}} = \frac{\quad}{n(S)} = 1 - \frac{\quad}{n(S)} = 1 - P(E).$$

Example

Three unbiased coins are tossed

(a) Write the sample space S.

(b) Find the probability of: all heads, at most 2 heads.

Solution

(a) Let S denotes the sample space of tossing three coins

$S = \{HHH, HHT, HTH, THH, HTT, TTH, THT, TTT\}$

$\therefore \quad n(S) = 8.$

(b) Let E_1 be the set of favourable events that all are heads

$E_1 = \{HHH\}$ and $n(E_1) = 1$

$$\therefore \quad P(E_1) = \frac{n(E_1)}{n(S)} = \frac{1}{8}$$

Let E_2 be the set of favourable events that atmost two heads.

$E_2 = \{HHT, HTH, THH, HTT, TTH, THT, TTT\}$ and $n(E_2) = 7$

$$\therefore \quad P(E_2) = \frac{n(E_2)}{n(S)} = \frac{7}{8}$$

Example

Three electric bulbs are chosen at random from 15 bulbs of which 5 are defective. Fi probability that: exactly one is defective, at least one is defective.

Solution

The number of ways of selecting one defective from 5 defective bulbs and two non-defective fro non-defective $n(E) = C(5, 1) \times C(10, 2) = 5 \times 45 = 225$.

Three bulbs can be chosen from 15 bulbs in

$$n(S) = C(15, 3) = \frac{15 \times 14 \times 13}{3 \times 2} = 455 \text{ ways}$$

$$\therefore \quad \text{Required probability} = \frac{n(E)}{n(S)} = \frac{225}{455} = \frac{45}{91}.$$

Additional Principle

For any events A and B,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Example

Suppose a student is selected at random 200 students, where 70 are taking C-programming, taking Java and 20 taking both. Find the probability P that the student is taking C or Java.

Solution

Let C: Students taking C-programming

J: Students taking Java

$$\therefore \quad P(C) = \frac{70}{200}, P(J) = \frac{50}{200} P(C \cap J) = \frac{20}{200}$$

then

$$P = P(C \cup J) = P(C) + P(J) - P(C \cap J)$$

$$= \frac{70}{200} + \frac{50}{200} - \frac{20}{200}$$

$$= \frac{70 + 50 - 20}{200} = \frac{100}{200} = \frac{1}{2}$$

Conditional Probability

Let E be an event in a sample space S with P(E) > 0 then probability than an event A occurs once E has occurred or specifically, the conditional probability of A given E, written as P(A/E), is defined as,

$$P(A/E) = \frac{P(A \cap E)}{P(E)}$$

Example

What is the conditional probability that a randomly generated bit string of length four contains at least two consecutive 0s, given that the first bit is a 1? (Assume the probability of a0 and a 1 are the same).

Solution

Let E be the event that a bit string of length four contains at least two consecutive 0s and F be the event that the first bit is a1. The probability that a bit string of length four has at least two consecutive 0s, given that its first bit is a 1 equals P(E/F).

Without restriction the number of ways of bit string of length four can be formed with digits 0 and 1 is $2^4 = 16$. Keeping 1 fixed at the beginning, there are $8(2^3)$ bit strings of length four that start with a1. Thus P(F) = 8/16 = ½. Again $E \cap F = \{1000, 1100, 1001\}$, so $P(E \cap F) = 3/16$. consequently

$$P(E/F) = \frac{P(E \cap F)}{P(F)} = \frac{3/16}{8/16} = \frac{3}{8}.$$

Example

A problem in Discrete Mathematics is given to three students whose chances of solving it are 1/2, 1/3, 1/4 respectively. What is the probability that only one of them solves it correctly?

Solution

Let A be the event that student A will solve the problem. Similarly B and C be the events for the students B and C respectively, to solve the problem.

Then $P(A) = \frac{1}{2}, P(B) = \frac{1}{3}, P(C) = \frac{1}{4}$

$P(A^C)$ = Probability that A will not solve the problem.

$$= 1 - P(A) = 1 - \frac{1}{2} = \frac{1}{2}$$

Similarly,

$$P(B^C) = 1 - \frac{1}{3} = \frac{2}{3}, \text{ and } P(C^C) = 1 - \frac{1}{4} = \frac{3}{4}.$$

The probability that none of the students A, B, C, will solve the problem = $P(A^C), P(B^C). P(C^C)$

$$= \frac{1}{2} \times \frac{2}{3} \times \frac{3}{4} = \frac{1}{4}.$$

[A, B, C are independent events, A^C, B^C, C^C are also independent events.

Hence, the required probability that the problem will be solved (i.e., at least one of A, B, C will solve the problem) $= 1 - \frac{1}{4} = \frac{3}{4}$.

Independence

Events A and B in a probability space S are said to be independent if the occurrence of one of them does not influence the occurrence of the other. In other words, B is independent of A if P(B) is the same as P(B/A).

i.e. events A and B are independent if $P(A \cap B) = P(A).P(B)$.

For example:

In tossing of two coins, the appearance of head on one coin does not affect the appearance of head on second coin.

Example:

Suppose A is the event that a randomly generated bit string of length four begins with a 1 and B is the event that this bit string contains an even number of ones. Are A and B independent, if the 16 bit strings of length four are equally likely?

Solution

There are eight bit strings of length four that begin with a one: 1000, 1001, 1010, 1011, 1100, 1101, 1110, and 1111.

There are also eight bit strings of length four that contain an even number of ones: 0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111.

Since there are 16 bit strings of length four, it follows that:

$$p(E) = p(F) = 8/16 = 1/2$$

Because $A \cap B = \{1111, 1100, 1010, 1001\}$, we that

$$p(A \cap F) = 4/16 = 1/4$$

Since

$$p(A \cap B) = 1/4 = (1/2)\,(1/2) = p(A)\,p(B).$$

Hence, A and F are independent.

Random Variable

Many problems are concerned with a numerical value associated with the outcome of an experiment. For instance, we may want to know the probability that there are nine one bits generated when ten bits are randomly generated. To study problems of this type we introduce the concept of a random variables.

A variable whose numerical value is determined by the outcome of a random experiment is called a random variable. A random variable X is a real valued function, X(x), of the elements of the sample space S where x is an element of the sample space. Random variable assigns a real number to each possible outcome. It should be noted that the range of the random variable will be a set of real numbers.

Example

If we toss a coin and denote the head by 1 and tail by 0, then the random variable X takes only two values 1 and 0. Symbolically, the random variable,

$$X(x) = \{x: x = (1, 0) \in S\}$$

Expected Value and Variance

The expected value of random variable is the sum of overall elements in a sample space of the product of the probability of the element and the value of the random variable at this element.

The expected value of a random variable provides a central point for the distribution of values of the random variable.

Another useful measure of a random variable is its variance, which tells how spread out the values of this random variable are.

∴ The expected value of the random variable X(S) on the sample space S is equal to

$$E(X) = \sum_{s \in S} P(S)\, X(S)$$

Example:

Let X be the number that comes up when a die is rolled. What is the expected value of X?

Solution

The random variable X takes the values 1, 2, 3, 4, 5, or 6, each of them has probability 1/6.

This results: $E(X) = \frac{1}{6}.1 + \frac{1}{6}.2 + \frac{1}{6}3 + \frac{1}{6}.4 + \frac{1}{6}.5 + \frac{1}{6}.6 = \frac{21}{6} = \frac{7}{2}$

Example:

An unbiased coin is tossed three times. Let S be the sample space of the eight possible outcomes and X be the random variable that assigns to an outcome the number of tails in this outcome. What is expected value of X?

Solution

When an unbiased coin is tossed three times, the eight possible outcomes in sample space are

S = {HHH, HHT, HTH, THH, TTH, THT, HTT, TTT}.

Since coin is unbiased and toss are independent then the probability of each outcome is 1/8.

$$\therefore \quad E(X) = \frac{1}{8}[X(HHH) + X(HHT) + X(HTH) + X(THH) + X(TTH) + X(THT) + X(HTT) + X(TTT)]$$

$$= \frac{1}{8}(0 + 1 + 1 + 1 + 2 + 2 + 2 + 3)$$

$$= \frac{12}{8}$$

$$= \frac{3}{2}$$

Example:

Suppose an element X and list of n distinct real numbers are given as input then find the average case complexity of linear search algorithm if the probability that X is in the list is P and it is equally likely that X is any of n element in the list.

Solution

The linear search algorithm locates and element X by successively comparing it to each element in the list and terminates when X is located and when all the elements have been searched and it has been determined that X is not present in the list. 2i + 1 comparisons are used if X equals the ith elements of the list and 2n + 2 comparisons are used if X is not in the list. Then the probability that X equals a_i is p/n and probability that X is not in the list is q = 1 - p.

It follows that the average case complexity of the linear search algorithm is

$$E = \frac{3p}{n} + \frac{5p}{n} + \ldots\ldots + (2n+1)\frac{p}{n} + (2n+2)q$$

$$= \frac{p}{n}(3 + 5 + \ldots\ldots + (2n+1)) + (2n+2)q$$

$$= \frac{p}{n}((n+1)^2 - 1) + (2n+2)q$$

$$= p(n+2) + (2n+2)q$$

Variance

The expected value of a random variable tells us its average value but nothing about how widely its values are distributed. So, the variance of a random variable helps us characterize how widely a random variable is distributed.

Let X be a random variable on a sample space S. The variance of X, denoted by V(X) is

$$V(X) = \sum_{s \in S} (X(S) - E(X))^2 P(S)$$

Example:

What is the variance of the random variable X, where X is the number that comes up when a die is rolled?

Solution

We have $V(X) = E(X^2) - E(X)^2$.

The random variable X takes the values 1, 2, 3, 4, 5, or 6, each of them has probability 1/6.

This results: $E(X) = \frac{1}{6}.1 + \frac{1}{6}.2 + \frac{1}{6}3 + \frac{1}{6}.4 + \frac{1}{6}.5 + \frac{1}{6}.6 = \frac{21}{6} = \frac{7}{2}$

Since X^2 takes the values i^2, i = 1, 2, ..., 6, each with probability $\frac{1}{6}$. It follows that

$$E(X^2) = \frac{1}{6}(1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2) = \frac{91}{6}.$$

Hence, $V(X) = \frac{91}{6} - \left(\frac{7}{2}\right)^2 = \frac{35}{12}$.

Randomized Algorithm

An algorithm that uses random numbers to decide what to do next anywhere in its logic is called Randomized Algorithm. For example, in Randomized Quick Sort, we use random number to pick the next pivot.

Example: Algorithms to find an element 'a' in an array of n elements.

Input: An array of n≥2 elements, in which half are 'a's and the other half are 'b's.

Output: to find 'a' in the array.

There are two randomized algorithms to solve it:

a) one Las Vegas algorithm
b) Monte Carlo algorithm.

Las Vegas algorithm: Pseudocode

```
findingA_LV(array A, n)
begin
        repeat
        Randomly select one element out of n elements.
        until 'a' is found
end
```

Monte Carlo algorithm:

```
findingA_MC(array A, n, k)
begin
        i=0
        repeat
        Randomly select one element out of n elements.
        i = i + 1
        until i=k or 'a' is found
end
```

How to analyse Randomized Algorithms?

Some randomized algorithms have deterministic time complexity. For example, this implementation of Karger's algorithm has time complexity as O(E). Such algorithms are called Monte Carlo Algorithms and are easier to analyse for worst case.

On the other hand, time complexity of other randomized algorithms (other than Las Vegas) is dependent on value of random variable. Such Randomized algorithms are called Las Vegas Algorithms. These algorithms are typically analysed for expected worst case. To compute expected time taken in worst case, all possible values of the used random variable needs to be considered in worst case and time taken by every possible value needs to be evaluated. Average of all evaluated times is the expected worst case time complexity. Below facts are generally helpful in analysis os such algorithms.

Exercise

1. Represent the sample space and the following three events in tossing three coins:
   a. the event of getting two tails and one head
   b. the event of getting three tails
   c. the event of getting at most two tails
2. A bag contains 4 blue and 2 green balls. If a ball is taken out of this bag at random, represent the sample space and the even of this ball being blue.
3. A dice is thrown two times. Find the probability of getting a number greater than 2.
4. A coin is thrown two times. Find the probability of having (i) 2 heads (ii) exactly 1 head.
5. A bag contain 5 red, 4 black and 2 white balls. If one ball is drawn at random, find the probability that it is black.
6. If a dice is tossed. What is the chance of getting (i) a number greater than 2 and (ii) an even number greater than 2.
7. One card is drawn from a pack of cards. Express each of the following probabilities:
   (i) the card is the king of diamonds
   (ii) the card is ace
   (iii) the card is 9 or 10
   (iv) the card is a spade.
8. A ball is drawn at random from a box containing 6 white, 8 red and 10 green balls. Determine the probability, that ball drawn is (i) white (ii) green (iii) not red (iv) red or green.

9. A and B are two mutually exclusive events of an experiment. If P (not A) = 0.64, $P(A \cup B) = 0.8$ and P(B) = x, find the value of x.
10. If P(A) = ¼, P(B) = 2/5 and $P(A \cup B)$ = ½, find (i) $P(A \cap B)$ (ii) $P(A \cap B')$ (iii) $P(A' \cup B')$.
11. There are 3 red and 2 black balls in a bag, 3 balls are taken out at random from the bag. Find the probability of getting 2 red and 1 black or 1 red and 2 black balls.
12. Suppose P(A) = 0.80, P(B) = 0.70 and $P(A \cup B)$ = 0.90, then find (a) conditional probability of A when B has already occurred (b) conditional probability of B when A has already occurred.
13. Let P(A)=0.40, P(B)=0.75, and P(A or B)=0.90. Find the following conditional probability: (i) P(A/B) and (ii) P(B/A).

5.3 Advanced Counting

Recurrence Relations

Suppose a_0, a_1, a_2,...a_n is a sequence. A recurrence relation for the nth term a_n is a formula (i.e., function) giving a_n in terms of some or all previous terms (i.e., a_0; a_1; : : : ; a_n). To find the complete sequence, the rest few initial values are needed. These initial value are called the initial conditions. If a recurrence relation with initial conditions is given, then we can write down as many terms of the sequence as we want. We will just keep applying the recurrence.

For example, $f_0 = 1$ and $f_1 = 1$; are initial condition with recurrence relation $f_n = f_{n+1} + f_{n+2}$; for n>2. The terms of sequence are 1, 1, 2, 3, 5, 8, 13, ..., where each subsequent term is the sum of the preceding two terms. On the other hand, if you are given a sequence, you may or may not be able to determine a recurrence relation with initial conditions which describes it.

Example

If the given recurrence relation is $a_n = a_{n-1} - a_{n-2}$ with $a_0 = 3$ and $a_1 = 5$ find the terms a_2 and a_3.

Solution

Here,

$$a_n = a_{n-1} - a_{n-2}$$

Then,

$$a_2 = a_{2-1} - a_{2-2}$$

$$a_2 = a_1 - a_0 = 5 - 3 = 2$$

and

$$a_3 = a_{3-1} - a_{3-2} = a_2 - a_1 = 2 - 5 = -3$$

Example

Find the recurrence relation and initial conditions of the sequence 3, 8, 13, 18,....

Solution

Here,

$$a_1 = 5$$

$$a_2 = a_1 + 5 = 8$$

$$a_3 = a_2 + 5 = 13$$

$$a_4 = a_3 + 5 = 18$$

.

.

.

$$a_n = a_{n-1} + 5$$

Hence, the recurrence relation is

$$a_n = a_{n-1} + 5, \quad n \geq 2, a_1 = 3$$

Example

Find the recurrence relation of the sequence 2, 5, 11, 23, 47

Solution

$$a_1 = 2$$

$$a_2 = 5 = 2 \times a_1 + 1$$

$$a_3 = 11 = 2 \times a_2 + 1$$

$$a_4 = 23 = 2 \times a_3 + 1$$

.

.

.

$$a_n = 2a_{n-1} + 1$$

Hence, the recurrence relation is $a_n = 2a_{n-1} + 1$ with initial conditions $a_1 = 2, n \geq 2$.

Example

Find the recurrence relation of the sequence 1, 1, 2, 3, 5, 8, 13,.....

Solution

Here,

$$a_1 = 1$$
$$a_2 = 1$$
$$a_3 = 2 = a_1 + a_2$$
$$a_4 = 3 = a_3 + a_2$$
$$a_5 = 5 = a_4 + a_3$$
$$\vdots$$
$$a_n = a_{n-1} + a_{n-2}$$

Hence, the recurrence relation is

$$a_n = a_{n-1} + a_{n-2} \text{ with initial conditions } a_1 = 1, a_2 = 1 \text{ for } n \geq 3.$$

This relation is also known as Fibonacci relation.

Solving Recurrence Relation

If the given recurrence relation involving sequence $a_0, a_1, a_2, \ldots, a_n$ then the solution of such recurrence relation is to find a_n explicit formula for general term a_n.

To solve the recurrence relation, we may replace each of $a_{n-1}, a_{n-2}, \ldots$ by their predecessors. This process continues until an explicit formula for n^{th} term a_n.

Example

Solve the recurrence relation

$$a_n = 2a_{n-1}, n \geq 1 \text{ and } a_0 = 3$$

Solution

Here,

$$a_0 = 3$$
$$a_1 = 2a_0 = 2\,(3)$$
$$a_2 = 2a_1 = 2\,(2 \times 3) = 2^2\,(3)$$
$$a_3 = 2a_2 = 2\,(2^2.3) = 2^3\,(3)$$
$$a_4 = 2a_3 = 2\,(2^3.3) = 2^4\,(3)$$
$$\vdots$$
$$a_n = 2^n\,(3)$$

Hence, general solution for given recurrence relation is $a_n = 2^n\,(3)$

Example

Solve the recurrence relation $a_n = a_{n-1} + 2$ Subject to initial condition $a_1 = 3$

Solution

$$a_n = a_{n-1} + 2 \qquad \text{Step 0}$$
$$= (a_{n-2} + 2) + 2 \qquad \text{Step 1}$$
$$= (a_{n-3} + 2) + 4 \qquad \text{Step 2}$$

$= (a_{n-4} + 2) + 6$ Step 3

$= (a_{n-5} + 2) + 8$ Step 4

.

.

.

$a_n = a_1 + 2(n-1)$ Step $(n-1)$

Example

Show that the solution of Recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ is $a_n = 3n$

Solution

Here,

$$a_n = 2a_{n-1} - a_{n-2}$$
$$3n = 2[3(n-1) - 3(n-2)]$$
$$3n = 2(3n-3) - 3n + 6$$
$$3n = 6n - 6 - 3n + 6$$
$$3n = 3n$$
$$LHS = RHS$$

Example

Find the first five terms of sequence defined by $a_n = 6a_{n-1}$, $a_0 = 2$

Solution

Given, $a_n = 6a_{n-1}$

Then,

$$a_1 = 6a_0 = 6 \times 2 = 12$$
$$a_2 = 6a_1 = 6 \times 12 = 72$$
$$a_3 = 6a_2 = 6 \times 72 = 432$$
$$a_4 = 6a_3 = 6 \times 432 = 2592$$

$\therefore$ First five terms are: 2, 12, 72, 432 & 2592

Example

Find the first three terms of sequence defined by:

$$a_n = a_{n-1} + 3a_{n-2},\ a_0 = 2,\ a_1 = 2$$

Solution

Here,

$$a_n = a_{n-1} + 3a_{n-2}$$
$$a_2 = a_1 + 3a_0$$
$$= 2 + 3 \times 2 = 2 + 6 = 8$$
$$a_3 = a_2 + 3a_1$$
$$= 8 + 3 \times 2 = 14$$

$\therefore$ First three terms are: 2, 8, 14

Example

Solve the recurrence relation $a_n = a_{n-1} + 4$ subject to the initial condition $a_1 = 3$.

Solution

Here,

$$a_n = a_n - 1 + 4,\ a_1 = 2$$

$$\therefore \quad a_1 = 2$$

$$a_2 = a_1 + 4 = 3 + 4 = 7$$

$$a_3 = a_2 + 4 = 7 + 4 = 11$$

$$a_4 = a_3 + 4 = 11 + 4 = 15$$

$$a_5 = a_4 + 4 = 15 + 4 = 19$$

General form of Linear Homogeneous Recurrence Relation

- The homogeneous recurrence relation of degree k_1 with constant coefficient has the general form

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k} \quad \ldots\ldots(i)$$

If $a_n = r^n$ is a solution of eq^n. (i), then, it must satisfy eq^n. (i) i.e.

$$r^n = c_1r^{n-1} + c_2r^{n-2} + \ldots + c_kr^{n-k}$$

Dividing by r^{n-k} on both side, we get

$$r^k = c_1r^{k-1} + c_2r^{k-2} + \ldots + c_k$$

or, $$r^k - c_1r^{k-1} - c_2r^{k-2} - \ldots - c_k = 0 \quad \ldots\ldots(iii)$$

This equation is known as characteristic equation of given recurrence relation and it provides characteristics roots of recurrence relation which are used to give on explicit formula for all the solution of recurrence relation.

Solving Linear Homogeneous Recurrence Relations with Constant Coefficients

A linear homogeneous recurrence relation of degree k with constant coefficients is a recurrence relation of the form $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k}$, where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$. The above relation is linear since right hand side is a sum of the multiples of previous terms of the sequence. It is homogeneous since no term occurs without being multiple of some a_j's. All the coefficients of the terms are constants and degree k is due to the representation of a_n in terms of previous 'k' terms of the sequence.

In solving the recurrence relation of the type above, the approach is to look for the solution of the form $a_n = r^n$, where r is a constant. $a_n = r^n$ is a solution of a recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k}$ if and only if $r^n = c_1r^{n-1} + c_2r^{n-2} + \ldots + c_kr^{n-k}$.

when we divide both sides by r^{n-k} and transpose the right hand side we have

$$r^k - c_1r^{k-1} - c_2r^{k-2} - \ldots - c_k = 0.$$

Here we can say $a_n = r^n$ is a solution if and only if r is the solution if the equation $r^k - c1r^{k-1} - c_2r^{k-2} \ldots - c_k = 0$ (**characteristic equation** of the recurrence relation) and solutions to this equations are called **characteristic roots** of the recurrence relation.

Theorem 1: (without proof)

Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if $a_n = \alpha_1r_1^n + \alpha_2r_2^n$ for n = 0, 1, 2, …, where α1 and α2 are constants.

Example

Solve the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$, $a_0 = 1$ and $a_1 = 0$.

Solution

The given recurrence relation is

$$a_n = 5a_{n-1} - 6a_{n-2} \quad .....(i)$$

The characteristic equation is

$$r^2 - 5r + 6 = 0$$

i.e. $r^2 - 3r - 2r + 6 = 0$

i.e. $r(r - 3) - 2(r - 3) = 0$

i.e. $(r - 2)(r - 3) = 0$

$r = 2, 3$ i.e. $r_1 = 2$, $r_2 = 3$

Since, two characteristics roots are (different) distinct, we use the "theorem 1" to write the general solution.

The general form of solution is

$$a_n = \alpha_1 r_1 + \alpha_2 r_2^n$$

$$a_n = \alpha_1 2^n + \alpha_2 3^n \quad .....(ii)$$

From initial conditions

$$a_0 = \alpha_1 2^\circ + \alpha_2 . 3^\circ$$

$1 = \alpha_1 + \alpha_2$ i.e. $\alpha_1 = 1 - a_2$ .....(iii)

and $a_1 = \alpha_1 2^1 + \alpha_2 3^1$

$0 = 2a_1 + 3\alpha_2$ .....(iv)

i.e. $0 = 2(1 - \alpha_2) + 3\alpha_2$

or, $0 = 2 - 2\alpha_2 + 3\alpha_2$

or, $0 = 2 + \alpha_2$

or, $\alpha_2 = -2$

and $\alpha_1 = 1 - \alpha_2$

$= 1 - (-2)$

$= 1 + 2 = 3$

Therefore, the solution of given recurrence relation is

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

or, $a_n = 3.2^n + (-2) . 3^n$

$$a_n = 3.2^n - 2.3^n$$

Example

Solve the recurrence relation $a_n = 6a_{n-1} - 8a_{n-2}$ for $n \geq 2$, $a_0 = 4$, $a_1 = 10$.

Solution

The given recurrence relation is

$$a_n = 6a_{n-1} - 8a_{n-2} \quad .....(i)$$

The characteristic equation is

$$r^2 - 61r + 8 = 0$$

$$r^2 - 4r - 2r + 8 = 0$$

i.e. $r(r - 4) - 2(r - 4) = 0$

$$(r - 4)(r - 2) = 0$$

i.e. $r = 4, 2$ i.e. $r_1 = 4, r_2 = 2$

Since roots are distinct, the general form of solution is

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

$$a_n = \alpha_1 4 + \alpha_2 . 2^{n2} \quad .....(ii)$$

From initial conditions, we have

$$a_0 = \alpha_1 4^\circ + \alpha_2 . 2^\circ$$

$$4 = \alpha_1 + \alpha_2 \quad .....(iii)$$

and $a_1 = \alpha_1 .4 + \alpha_2 .2^1$

$$10 = 4.\alpha_1 + 2\alpha_2 \quad .....(iv)$$

From equation (iii) and (iv), we have

$$10 = 4(4 - \alpha_2) + 2\alpha_2$$

$$10 = 16 - 4\alpha_2 + 2\alpha_2$$

$$-6 = -2\alpha_2 \text{ i.e. } \alpha_2 = 3$$

and, substituting the value of α_2 in (iii), we have

$$4 = \alpha_1 + \alpha_2 \Rightarrow 4 = \alpha_1 + 3 \Rightarrow \alpha_1 = 1$$

Therefore, the solution of given recurrence relation is

$$a_n = 1.4^n + 3.2^n$$

Example

What is the solution of recurrence relation $a_n=a_{n-1}+2a_{n-2}$ with $a_0=2$ and $a_1=7$?

Solution

Here the given recurrence relation is

$$a_n=a_{n-1}+2a_{n-2}$$

And the initial conditions are $a_0=2$ and $a_1=7$.

Now, we have a characteristic equation for the above given recurrence relation as

$$r^2-r-2=0$$

Now solving this equations by factoring

$$r^2-2r+r-2=0$$

$$r(r-2)+1(r-2)=0$$

$$\text{i.e}(r-2)(r+1)=0 \text{ i.e either } r=2 \text{ or } r=-1.$$

Hence the roots of characteristic equation are $r_1=2$ and $r_2=-1$, both are distinct.

Hence the solution sequence is:

$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ with $r_1 = 2$ and $r_2 = -1$

i.e. $a_n = \alpha_1 2^n + \alpha_2(-1)^n$ .....(1) for some constants α_1 and α_2.

From the initial conditions, we put the value of a_0 and a_1 in (1) and get the equations as

$$a_0=2=\alpha_1+\alpha_2 .....(2)$$

$$a_1=7=\alpha_1 2+\alpha_2(-1) .....(3)$$

Solving these two equations, we have

$$\alpha_1=3 \text{ and } \alpha_2=-1.$$

Hence the solution to the given recurrence relation and initial condition is the sequence $\{a_n\}$ with a_n $3.2^n -1.(-1)^n$

Example

Solve the recurrence relation $a_n = a_{n-1} + 6a_{n-2}$ for $n > 2$, $a_0 = 3$, $a_1 = 6$.

Solution

Characteristic equation of the given relation is $r^2 - r - 6 = 0$. Its roots are $r = 3$ and $r = -2$. Since $(r - 3)(r + 2) = 0$. Hence, the sequence {an} is a solution to the recurrence relation if and only if $a_n = \alpha_1 3^n + \alpha_2(-2)^n$, for some constants α_1 and α_2. From the initial conditions we have $\alpha_0 = 3 = \alpha_1 + \alpha_2$, $\alpha_1 = 6 = 3\alpha_1 + (-2)\alpha_2$. Solving these two equations we have $\alpha_1 = 12/5$ and $\alpha_1 = 3/5$. Hence, the solution is the sequence $\{a_n\}$ with $a_n = (12.3^n + 3(-2)^n)/5$.

Example

Find the solution of recurrence relation $f_n = f_{n-1} + f_{n-2}$, $n > 2$, and $f_0 = 0$, $f_1 = 1$.

OR

Find the explicit formula for fibonancci sequences.

Solution

The characteristics equation of recurrence relation

$$f_n = f_{n-1} + f_{n-2} \text{ is } r^2 - r - 1 = 0 \qquad .....(i)$$

Comparing $r^2 - r - 1 = 0$ with $ax^2 + bx + c = 0$, we get

$$a = 1, b = -1, c = -1$$

Now,

$$\text{Roots} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-(-1) \pm \sqrt{(-1)^2 - 4\times1\times(-1)}}{2} = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

$\therefore$ Taking +ve sign, we get

$$r_1 = \frac{1+\sqrt{5}}{2}$$

Taking -ve sign, we get

$$r_2 = \frac{1-\sqrt{5}}{2}$$

Since characteristics roots are different, the general form of solution is

$$f_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

$$f_n = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right)^n \qquad .....(ii)$$

From initial condition we have,

$$f_0 = \alpha_1 + \alpha_2$$

$$0 = \alpha_1 + \alpha_2 \qquad .....(iii)$$

and $$f_1 = \alpha_1\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right) = 1 \qquad .....(iv)$$

From equation (iii) and (iv) we have,

$$-\alpha_2\left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

$$\frac{-\alpha_2 - \alpha_2 . \sqrt{5} + \alpha_2 - \alpha_2 . \sqrt{5}}{2} = 1$$

$$-2\alpha_2\sqrt{5} = 2$$

$$\alpha_2 = -\frac{2}{2\sqrt{5}} = -\frac{1}{\sqrt{5}}$$

and $\alpha_1 + \alpha_2 = 0$

$$\alpha_1 - \frac{1}{\sqrt{5}} = 0$$

$$\alpha_1 = \frac{1}{\sqrt{5}}$$

$\therefore$ Solution of given recurrence is

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

Example

What is the solution of recurrent relation $a_n = a_{n-1} - 2a_{n-2}$ with initial conditions $a_0 = 2, a_1 = 7$.

Solution

The given recurrence relation is:

$$a_n = a_{n-1} - 2a_{n-2} \quad .....(i)$$

The characteristics equation is

$$r^2 - r - 2 = 0$$

or, $r^2 - 2r + r - 2 = 0$

or, $r(r-2) + 1(r-2) = 0$

$(r-2)(r+1) = 0$

$\therefore$ $r = 2, 1$

i.e. $r_1 = 2, r_2 = 1$

Since roots are distinct, the general form of solution is

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

$$a_n = \alpha_1 . 2^n + \alpha_2 . 1^n \quad .....(ii)$$

From initial conditions we have,

$$a_0 = \alpha_1 . 2^0 + \alpha_2 . 1^0$$

$\therefore$ $2 = \alpha_1 + \alpha_2$

or, $\alpha_1 = \alpha_2 - 2 \quad .....(iii)$

and $a_1 = \alpha_1 . 2^1 + \alpha_2 . 1^1$

$$7 = 2\alpha_1 + \alpha_2 \quad .....(iv)$$

From equation (ii) and (iv), we have,

$$7 = 2(\alpha_2 - 2) + \alpha_2$$

or, $7 = 2\alpha_2 - 4 + \alpha_2$

or, $3\alpha_2 = 11 \quad \therefore \alpha_2 = \frac{11}{3}$

Now, substituting value of α_2 in equation (iii), we have

$$\alpha_1 = \alpha_2 - 2$$

$$\alpha_1 = \frac{11}{3} - 2 = \frac{11-6}{3} = \frac{5}{3}$$

Therefore, the solution of given recurrence relation is

$$\boxed{a_n = \frac{5}{3}2^n + \frac{11}{3}1^n}$$

Theorem 2: (without proof)

Let c1 and c2 be real numbers with $c2 \neq 0$. Suppose that $r^2 - c_1r - c2 = 0$ has only one root r_0. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if $a_n = \alpha_1 r_0{}^n + \alpha_2 n r_0{}^n$ for $n = 0, 1, 2, \ldots$, where $\alpha 1$ and $\alpha 2$ are constants.

Example

Solve the recurrence relation $a_n = 6\, a_{n-1} - 9\, a_{n-2}$ for $n \geq 2$, $a_0 = 1$, $a_1 = 6$.

Solution

Characteristic equation of the given relation is

$$r^2 - 6r + 9 = 0$$

$$\text{or } (r - 3)^2 = 0$$

$$\text{or } r = 3,3$$

Therefore Its only one root is $r = 3$.

Hence, the sequence $\{a_n\}$ is a solution to the recurrence relation if and only if

$a_n = \alpha_1 3^n + \alpha_2 n\, 3^n$, for some constants $\alpha 1$ and $\alpha 2$.

From the initial conditions we have

$a_0 = 1 = \alpha_1$,

$a_1 = 6 = \alpha_1.3 + \alpha_2.3$

Solving these two equations we have $\square_1 = 1$ and $\square_2 = 1$.

Hence, the solution is the sequence $\{a_n\}$ with

$a_n = 1.3^n + 1.n.3^n$.

$a_n = 3^n(1 + n)$

Example

Solve the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$, for $n \geq 2$, $a_0 = 4$, $a_1 = 1$.

Solution

The given recurrence relation is

$a_n = 2a_{n-1} - a_{n-2}$ .....(i)

The characteristic equation is

$r^2 - 2r + 1 = 0$

or, $(r - 1)^2 = 0$

or, $r = 1, 1$

Since, characteristic roots are same, the general form of solution is

$a_n = \alpha_1 . r_0{}^n + \alpha_2 n . r_0{}^n$

i.e. $a_n = \alpha_1. 1^n + \alpha_2. n. 1^n$ .....(ii)

From given initial conditions,

$a_0 = \alpha_1. 1^0 + \alpha_2. 0.1^n$

i.e. $4 = \alpha_1.1 \Rightarrow \alpha_1 = 4$

And $a_1 = \alpha_1. r_0{}^n + \alpha_2.n.r_0{}^n$

$$1 = \alpha_1 . 1^1 + \alpha_2 . 1.1^1$$

$$1 = \alpha_1 + \alpha_2 \quad .....(iii)$$

Putting value of $\alpha_1 = 4$ in equation (iii), we have

$$1 = 4 + \alpha_2 \Rightarrow \alpha_2 = -3$$

Therefore, the solution of given recurrence relation,

$$a_n = 4.1^n + (-3).n.1^n$$

Example

Solve the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n \geq 2$, a0 = 3, a1 = 6.

Solution

Characteristic equation of the given relation is

$$r^2 - 2r + 1 = 0.$$

i.e. $(r - 1)^2 = 0$

i.e. $r = 1, 1$

Therefore, its only one root is $r = 1$.

Hence, the sequence $\{a_n\}$ is a solution to the recurrence relation if and only if

$$a_n = \alpha_1 1^n + \alpha_2 n 1^n, \text{ for some constants } \alpha_1 \text{ and } \alpha_2.$$

From the initial conditions we have

$$a_0 = 3 = \alpha_1,$$

$$a_1 = 6 = \alpha_1 + \alpha_2.$$

Solving these two equations we have $\square_1 = 3$ and $\square_2 = 3$.

Hence, the solution is the sequence $\{a_n\}$ with

$$a_n = 3(1^n + n1^n).$$

Example

Solve: $a_n = -6a_{n-1} - 9a_{n-2}$ for $n \geq 2$, $a_0 = 5$, $a_1 = -1$

Solution

The given recurrence relation is

$$a_n = -6a_{n-1} - 9a_{n-2}$$

The characteristic equation is

$$r^2 + 6r + 9 = 0$$

$$\Rightarrow \quad r^2 + 3r + 3r + 9 = 0$$

$$r(r + 3) + 3(r + 3) = 0$$

or, $(r + 3)(r + 3) = 0$

$$r = -3, -3$$

Since the roots of characteristics equation are same, we have the general form of solution is

$$a_n = \alpha_1 . r_0^n + \alpha_2 . n . r_0^n$$

i.e. $a_n = \alpha_1 (-3)^n + \alpha_2 . n . (-3)^n$

From given initial condition,

$$a_0 = \alpha_1 (-3)^0 + \alpha_2 . 0. (-3)^0$$

$$5 = \alpha_1 . 1 + 0 \Rightarrow a_1 = 5$$

and, $a_1 = \alpha_1 (-3)^1 + \alpha_2 . 1. (-3)^1$

$$-1 = \alpha_1(-3) + \alpha_2(-3)$$

i.e. $-1 = -3\alpha_1 - 3\alpha_2$

i.e. $-1 = -3 \times 5 - 3\alpha_2$

i.e. $-1 + 15 = -3\alpha_2$

$\Rightarrow$ $\alpha_2 = 14/-3 = -\dfrac{14}{3}$

$\Rightarrow$

Therefore, the solution of given recurrence relation is

$$a_n = \alpha_1(-3)^n + \alpha_2 n(-3)^n$$

i.e. $a_n = 5(-3)^n + (-14/3).\, n(-3)^n$

i.e. $a_n = 5(-3)^n - \dfrac{14}{3} n(-3)^n$

Theorem 3: (without proof)

Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that $r^k - c_1r^{k-1} - \ldots - c_k = 0$ has k distinct roots $r_1, r_2, \ldots, r_k$. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k}$ if and only if $a_n = \alpha_1r_1^n + \alpha_2r_2^n + \ldots + \alpha_kr_k^n$ for $n = 0, 1, 2, \ldots$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are constants.

Example

Find the solution to $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$, for $n \geq 3$ with $a_0 = 3$, $a_1 = 6$ and $a_2 = 0$

Solution

The given recurrence is

$$a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3} \quad \text{.....(i)}$$

The characteristic equation is

$$r^3 - 2r^2 - r + 2 = 0$$

or, $r^3 - r^2 - r^2 - r + 2 = 0$

or, $r^3 - r^2 - r^2 - 2r + r + 2 = 0$

or, $r^3 - r^2 - r^2 + r - 2r + 2 = 0$

or, $r^2(r-1) - r(r-1) - 2(r-1) = 0$

or, $(r-1)(r^2 - r - 2) = 0$

or, $(r-1)(r^2 - 2r + r - 2) = 0$

or, $(r-1)[r(r-2) + 1(r-2)] = 0$

or, $(r-1)(r-2)(r+1) = 0$

$\therefore$ $r_1 = 1, r_2 = 2, r_3 = -1$

Since, all three roots are different, we can write the general form of solution as

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \alpha_3 r_3^n$$

$$a_n = \alpha_1.1^n + \alpha_2.2^n + \alpha_3(-1)^n \quad \text{.....(ii)}$$

From given initial conditions, we have

$$a_0 = \alpha_1.1^0 + \alpha_2.2^0 + \alpha_3(-1)^0$$

$$3 = \alpha_1 + \alpha_2 + \alpha_3 \quad \text{.....(iii)}$$

Again,

$$a_1 = \alpha_1.1 + \alpha_2.2^1 + \alpha_3(-1)^1$$

$$6 = \alpha_1 + 2\alpha_2 - \alpha_3 \quad \text{.....(iv)}$$

and

$$a_2 = \alpha_1.1^2 + \alpha_2.2^2 + \alpha_3(-1)^2$$

$$0 = \alpha_1 + 4\alpha_2 + \alpha_3 \quad .....(v)$$

From (iii) and (v)

$$3 = \alpha_1 + \alpha_2 + \alpha_3$$
$$0 = \alpha_1 + 4\alpha_2 + \alpha_3$$
$$3 = -3\alpha_2 \Rightarrow \alpha_2 = -1$$

From (iii) and (iv),

$$3 = \alpha_1 + \alpha_2 + \alpha_3$$
$$6 = \alpha_1 + 2\alpha_2 - \alpha_3$$
$$-3 = -\alpha_2 + 2\alpha_3$$
$$\Rightarrow \quad 2\alpha_3 = -3 + \alpha_2 = -3 - 1 = -4$$
$$\therefore \quad \alpha_3 = -\frac{4}{2} = -2$$

From (iii),

$$\alpha_1 + \alpha_2 + \alpha_3 = 3$$
$$\alpha_1 = 3 - \alpha_2 - \alpha_3$$
$$\alpha_1 = 3 - (-1) - (-2)$$
$$= 3 + 1 + 2 = 6$$

Therefore, the solution of given recurrence relation is

$$a_n = \alpha_1 . 1^n + \alpha_2 . 2^n + \alpha_3 (-1)^n$$
$$a_n = (-1)\, 1^n + 6 . 2^n + (-2)\,(-1)^n$$
$$= -1 . 1^n + 6 . 2^n - 2\,(-1)^n$$

Example

Solve the recurrence relation $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ for $n \geq 3$, $a_0 = 3$, $a_1 = 6$ and $a_2 = 9$.

Solution

Characteristic equation of the given relation is $r^3 - 2r^2 - r + 2 = 0$. Its roots are $r = 1$, $r = -1$, and $r = 2$.

Hence, the sequence $\{a_n\}$ is a solution to the recurrence relation if and only $a_n = \alpha_1 1^n + \alpha_2(-1)^n + \alpha_3 2^n$, for some constants α_1, α_2, and α_3.

From the initial conditions we have

$$a_0 = 3 = \alpha_1 + \alpha_2 + \alpha_3,$$
$$a_1 = 6 = \alpha_1 - \alpha_2 + 2\alpha_3,$$

and $\quad a_2 = 9 = \alpha_1 + \alpha_2 + 4\alpha_3.$

Solving these three equations we have $\alpha_1 = 3/2$, $\alpha_2 = -1/2$, and $\alpha_3 = 2$. Hence, the solution is the sequence {an} with

$$a_n = (3/2)1^n - (1/2)(-1)^n + 2.2^n.$$

Example

Find the solution of recurrence relation $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$, for $n > 3$, $a_0 = 2$, $a_1 = 5$ and $a_2 = 5$.

Solution

The given recurrence relation is

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

The characteristic equation is

$$r^3 - 6r^2 + 11r - 6 = 0$$

Since $r = 1$ satisfy this equation, $r = 1$ is a root of this equation, so we try to find the factor $(r - 1)$ from this equation

$$r^3 - r^2 - 5r^2 + 5r + 6r - 6 = 0$$

$$r^2(r - 1) - 5r(r - 1) + 6(r - 1) = 0$$

$$(r - 1)(r^2 - 5r + 6) = 0$$

$$(r - 1)(r^2 - 3r - 2r + 6) = 0$$

$$(r - 1)\{r(r - 3) - 2(r - 3)\} = 0$$

$$(r - 1)(r - 3)(r - 2) = 0$$

$$r_1 = 1, r_2 = 3, r_3 = 2$$

Since all three roots are different, we have the general form of solution is

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \alpha_3 r_3^n \text{ i.e. } a_n = \alpha_1 1^n + \alpha_2 . 3^n + \alpha_3 . 2^n$$

From initial condition

$$a_0 = \alpha_1 . 1^0 + \alpha_2 . 3^0 + \alpha_3 . 2^0$$

$$2 = \alpha_1 + \alpha_2 + \alpha_3 \quad .....(i)$$

Again,

$$a_1 = \alpha_1 . r_1^n + \alpha_2 . r_2^n + \alpha_3 . r_3^n$$

$$5 = \alpha_1 . 1^1 + \alpha_2 . 3^1 + \alpha_3 . 2^1$$

$$\Rightarrow \quad 5 = \alpha_1 + 3\alpha_2 + 2\alpha_3 \quad .....(ii)$$

$$a_2 = \alpha_1 . 1^2 + \alpha_2 . 3^2 + \alpha_3 . 2^2$$

$$5 = \alpha_1 + 9\alpha_2 + 4\alpha_3 \quad .....(iii)$$

Solving (i) and (ii)

$$2 = \alpha_1 + \alpha_2 + \alpha_3$$

$$5 = \alpha_1 + 3\alpha_2 + 2\alpha_3$$

$$-3 = -2\alpha_2 - \alpha_3$$

$$\therefore \quad 3 = 2\alpha_2 + \alpha_3 \quad .....(iv)$$

Solving (i) and (iii) we get

$$2 = \alpha_1 + \alpha_2 + \alpha_3$$

$$5 = \alpha_1 + 9\alpha_2 + 4\alpha_3$$

$$-3 = -8\alpha_2 - 3\alpha_3$$

$$\therefore \quad 3 = 8\alpha_2 + 3\alpha_3 \quad .....(v)$$

Multiplying eq^n. (iv) by 3 and subtracting (v), we get

$$9 = 6\alpha_2 + 3\alpha_3$$

$$3 = 8\alpha_2 + 3\alpha_3$$

$$6 = -2\alpha_2$$

$$\therefore \quad \alpha_2 = -3$$

Now, substituting value of α_2 in eq^n. (iv)

$$3 = 2\alpha_2 + \alpha_3$$

$$3 = 2 \times (-3) + \alpha_3$$

$$\alpha_3 = 3 + 6$$

$$\alpha_3 = 9$$

Again,

Substituting value of α_2 and α_3 in eq^n. (i)

$$2 = \alpha_1 + \alpha_2 + \alpha_3$$

or, $2 = \alpha_1 - 3 + 9$

or, $2 = \alpha_1 + 6$

or, $\alpha_1 = -4$

Therefore, solution of given recurrence relation is

$$a_n = -4 \cdot 1^n - 3 \cdot 3^n + 9 \cdot 2^n$$

Theorem 4: (without proof)

Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that $r^k - c_1 r^{k-1} - \ldots - c^k = 0$ has t distinct roots $r_1, r_2, \ldots, r_t$ with multiplicity $m_1, m_2, \ldots, m_t$, respectively, so that $m_i \geq 1$ for $i = 1, 2, \ldots, t$ and $m_1 + m_2 + \ldots + m_t = k$.

Then the sequence $\{a_n\}$ is a solution of the recurrence relation

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$ if and only if

$$a_n = (\alpha_{1,0} + \alpha_{1,1} n + \ldots + \alpha_{1,m_1-1} n^{m1-1}) r_1^n$$
$$+ (\alpha_{2,0} + \alpha_{2,1} n + \ldots + \alpha_{2,m_2-1} n^{m2-1}) r_2^n$$
$$+ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$+ (\alpha_{t,0} + \alpha_{t,1} n + \ldots + \alpha_{t,m_t-1} n^{mt-1}) r_t^n$$

for $n = 0, 1, 2, \ldots$, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

Example

Solve the recurrence relation $a_n = 5a_{n-1} - 7a_{n-2} + 3a_{n-3}$ for n □□3, $a_0 = 1$, $a_1 = 9$ and $a_2 = 15$.

Solution

Characteristic equation of the given relation is $r^3 - 5r^2 + 7r - 3 = 0$. Its roots are $r = 1$, $r = 3$, and $r = 1$.

i.e. $r_1 = 1$ with $m_1 = 2$ and $r_2 = 3$ with $m_2 = 1$

Hence, the sequence $\{a_n\}$ is a solution to the recurrence relation if and only if $a_n = (\alpha_{1,0} + \alpha_{1,1} n) 1^n + (\alpha_{2,0}) 3^n$, for some constants $\alpha_{1,0}$, $\alpha_{1,1}$, and $\alpha_{2,0}$.

From the initial conditions we have

$$a_0 = 5 = \alpha_{1,0} + \alpha_{2,0},$$
$$a_1 = 9 = \alpha_{1,0} + \alpha_{1,1} + 3\alpha_{2,0},$$

and $a_2 = 15 = \alpha_{1,0} + 2\alpha_{1,1} + 9\alpha_{2,0}$.

Solving these two equations we have $\alpha_{1,0} = 3/2$, $\alpha_{1,1} = 9$, and $\alpha_{2,0} = -1/2$. Hence, the solution is the sequence $\{a_n\}$ with

$a_n = (3/2)1^n + 9n1^n - (1/2)3^n$.

Solve the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with $a_0 = -5$, $a_1 = 4$ and $a_2 = 15$

Solution

The given recurrence relation is

$$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$$

The characteristic equation is

$$r^3 + 3r^2 + 3r + 1 = 0$$
$$(r)^3 + 3.r^2.1 + 3.r.1^2 + 1^3 = 0$$

$(r+1)^3 = 0$

$r = -1, -1, -1$

Since all three roots are same, i.e. $r = -1$ with multiplicity $m = 3$,

The general solution is

$$a_n = (a_1 + \alpha_2 n + \alpha_3 n^2) r^n = (\alpha_1 + \alpha_2 . n + \alpha_3 n^2)(-1)^n$$

(Note: here we have substituted $\alpha_{1,1}$ by α_1, $\alpha_{1,2}$ by α_2 and $\alpha_{1,3}$ by α_3)

From given initial condition

$$a_0 = (\alpha_1 + \alpha_2 . 0 + \alpha_3 . 0^2)(-1)^0$$

$$-5 = (\alpha_1 + 0 + 0) . 1 \Rightarrow a_1 = -5$$

Again,

$$a_1 = (\alpha_1 + \alpha_2 . 1 + \alpha_3 . 1^2)(-1)^1$$

$$4 = (\alpha_1 + \alpha_2 + \alpha_3) \times -1$$

$$\Rightarrow \quad \alpha_1 + \alpha_2 + \alpha_3 = -4 \quad .....(ii)$$

and

$$a_2 = (\alpha_1 + \alpha_2 . 2 + \alpha_3 . 2^2)(-1)^2$$

$$15 = (\alpha_1 + 2\alpha_2 + 4\alpha_3) \times 1$$

$$\Rightarrow \quad \alpha_1 + 2\alpha_2 + 4\alpha_3 = 15 \quad .....(iii)$$

Solving (i), (ii) and (iii)

$$\alpha_1 + \alpha_2 + \alpha_3 = -4$$

$$\underline{\alpha_1 + 2\alpha_2 + 4\alpha_3 = 15}$$

$$-\alpha_2 - 3\alpha_3 = -19$$

$$\Rightarrow \quad \alpha_2 + 3\alpha_3 = 19$$

Putting value of α in (ii)

$$\alpha_1 + \alpha_2 + \alpha_3 = -4$$

$$\alpha_2 + \alpha_3 = -4 - \alpha_1$$

$$= -4 - (-3)$$

$$\alpha_2 + \alpha_3 = 1 \quad .....(v)$$

Solving (iv) and (v),

$$\alpha_2 + 3\alpha_3 = 19$$

$$\underline{\alpha_2 + \alpha_3 = 1}$$

$$2\alpha_3 = 18$$

$$\Rightarrow \quad \alpha_3 = 9$$

and, $\alpha_2 + 3\alpha_3 = 19$

$$\Rightarrow \quad \alpha_2 = 19 - 3\alpha_3$$

$$= 19 - 3 \times 9$$

$$\alpha_2 = 19 - 27 = -8$$

Therefore, the solution of given recurrence relation is

$$a_n = (-5 + (-8) . n + 9 . n^2) * (-1)^n$$

Example

Solve the recurrence relation $a_n = 2a_{n-1}$, $n \geq 1$, with initial condition $q_0 = 3$.

Solve:

The characteristics equation of recurrence relation $a_n = 2a_{n-1}$ is:

$$r^1 - 2 = 0$$

$$r = 2$$

Since r=2 with multiplicity m=1, the general form of solution is

$$a_n = \alpha r^n \quad .....(i)$$

i.e. $a_n = \alpha 2^n$

From initial condition,

$a_0 = 3$, we have

$a_1 = \alpha 2^n$

i.e. $a_0 = \alpha 2^0$

or, $3 = \alpha 2^\circ \Rightarrow \alpha = 3$

Hence, the solution of given R.R. is

$$a_n = 3.2^n \quad .....(i)$$

Solving Linear Non-homogeneous Recurrence Relations with Constant Coefficients

The recurrence relation of the form

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k} + F(n),$$

where c1, c2, ..., ck are real numbers and F(n) is a function depending upon n. The recurrence relation preceding F(n) is called **associated homogeneous recurrence relation**.

For example an =7an-1 + 3an-2 +6n is a linear non-homogeneous recurrence relation with constant coefficients.

Theorem 5: (without proof)

If $\{a_n(p)\}$ is a particular solution of the non-homogeneous linear recurrence relation with constant coefficients $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k} + F(n)$, then every solution of the form

$$\{a_n(p) + a_n(h)\},$$

where $a_n(h)$ is a solution of the associated homogeneous recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k}$.

Example

Find all the solutions of the recurrence relation $a_n = 4a_{n-1} + n^2$. Also find the solution of the relation with initial condition $a_1 = 1$.

Solution

We have associated linear homogeneous recurrence relation as $a_n = 4a_{n-1}$. The root is 4, so the solutions are $a_n(h) = \alpha 4^n$, where α is a constant. Since $F(n) = n^2$ is a polynomial of degree 2, a trial solution is a quadratic function in n, say, $p_n = an^2 + bn + c$, where a, b, and c are constants.

To determine whether there are any solution of this form, suppose that

$p_n = an^2 + bn + c$ is such solution.

Then the equation $a_n = 4a_{n-1} + n^2$ becomes

$$an^2 + bn + c = 4(a(n-1)^2 + b(n-1) + c) + n^2.$$

$$= 4a\,n^2 - 8an + 4a + 4bn - 4b + 4c + n^2$$

$$= (4a + 1)n^2 + (-8a + 4b)n + (4a - 4b + 4c)$$

Here $an^2 + bn + c$ is the solution if and only if

$4a + 1 = a$ i.e. $a = -1/3$;

$-8a + 4b = b$ i.e. $b = -8/9$;

$4a - 4b + 4c = c$ i.e. $c = -28/27$.

So $a_n(p) = -1/3(n^2 + 8/3.n + 28/9)$ is a particular solution and all solutions are

$a^n = \{a_n(p) + a_n(h)\} = 1/3(n^2 + 8/3.n + 28/9) + \square 4^n$, where $\square\square$ is a constant.

For solution with $a_1 = 1$, we have

$a_1 = 1 = -1/3(1 + 8/3 + 28/9) + \alpha 4$ i.e. $\alpha = 22/27$.

Then the solution is $an = -1/3(1 + 8/3 + 28/9) + 22/27\ 4^n$.

Example

Find all the solution of recurrence relation $a_n = 2a_{n-1} + 3^n$ and a solution with initial condition $a_1 = 5$.

Solution

The given recurrence relation is $a_n = 2a_{n-1} + 3^n$ .....(i)

The linear homogeneous part of above eq^n. is

$a_n = 2a_{n-1}$ .....(ii)

Then, characteristic equation is

$r - 2 = 0 \quad \Rightarrow r = 2$

Now, the solution of equation (ii) is

$a_n = \alpha_1 r_1^r$

$= \alpha_1 2^n$ ....(iii)

To find the particular solution, we write

$F(n) = 3^n$ .....(iv)

The trial solution of (iv) is

$a(p) = c.3^n$ .....(v) where c is constant

Substituting terms of this sequence into recurrence relation, we have

$a_n = 2a_{n-1} + 3^n$ [Put $a_n^{(p)} = c_3^n$ in both side]

i.e. $c.3^n = 2.c.\ 3^{n-1} + 3^n$

$$c.3^n = 2.c.\frac{3^n}{3} + 3^n$$

$$c.3^n = 3^n\left(\frac{2c}{3} + 1\right)$$

Comparing the coefficient of 3^n,

$$c = \frac{2c}{3} + 1 \Rightarrow 3c = 2c + 3,\ c = 3$$

Therefore, the particular solution is

$a_n^{(p)} = 3.3^n$

and the all solution of given R.R. is

$a_n = a_n^{(h)} + a_n^{(p)}$

$a_n = \alpha_1.2^n + 3.3^n = \alpha_1.2^n + 3^{n+1}$

From what conditions,

$a_1 = \alpha_1.2^1 + 3^{1+1}$

$$5 = 2\alpha_1 + 9$$

$$5 - 9 = 2\alpha_1 \Rightarrow \alpha_1 = -\frac{4}{2} = -2$$

Hence, the solution of given R.R. is

$$a_n = -2.2^n + 3^{n+1}$$

Theorem 6: (without proof)

Suppose that {an} satisfies the linear non-homogeneous recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k} + F(n)$, where c1, c2, ..., ck are real numbers and $F(n) = (b_tn^t + b_{t-1}n^{t-1} + \ldots + b_1n + b_0)\, s^n$, where $b_0, b_1, \ldots, b_t$ and s are real numbers.

When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form $(p_tn^t + p_{t-1}n^{t-1} + \ldots + p_1n + p_0)s^n$.

When s is a root of the characteristic equation and its multiplicity is m, there is a particular solution of the form

$$n^m(p_tn^t + p_{t-1}n^{t-1} + \ldots + p_1n + p_0)s^n.$$

Example

Find the solution of the recurrence relation $a_n = 2a_{n-1} + n.2^n$.

Solution

We have the associated linear homogeneous recurrence relation is

$$a_n(h) = 2a_{n-1}.$$

The characteristic equation for this would be r-2 = 0, so the root is 2 and hence the solutions is $a_n(h) = \alpha_1 2^n$, where α is a constant.

We have $F(n) = n.2^n$. (Of the form $n.s^n$) where s is the root of the characteristic equation and the multiplicity of 2 is 1 so, the particular solution has the form

$$c = n.(p_1n)2^n$$

$$\text{or } a_n(p) = p_1n^22^n.$$

The all solution is $a_n = \alpha_1 2^n + p_1n^22^n$.

Recurrences Applications

One of the application areas of recurrence relations is analysis of divide and conquers algorithms.

Divide and Conquer Algorithms

Divide and conquer algorithms divide a problem of larger size to the problem of smaller size so continually such that the problem of the smallest size that has trivial solution is obtained. If f(n) represents the number of operations required to solve the problem of size n, then follows the recurrence relation f(n) = af(n/b) + g(n), called divide and conquer recurrence relation. In the relation above the problem of size n is partitioned into a parts

of the problem of the size n/b and g(n) is the operations required to conquer the solutions. In this section no algorithms are presented but their recurrence relations are tried to achieve.

Example 19: Fibonacci Numbers

We know that the Fibonacci numbers are generated by the formula fn = fn-1 + fn-2. Here nth Fibonacci number is the sum of (n-1)th and (n-2)nd Fibonacci numbers. Here for the initial conditions are f0 = 0, and f1 = 1. Use of the above relation does not exactly produce the recurrence relation

mentioned above, however this is an example of divide and conquer algorithm since each time the problem is changed into two problems of smaller size.

Example: Merge Sort

In merge sorting the input sequence of n items is broken down into 2 halves (here there may be difference in 1 item between two parts). Since the list of size n need more comparisons than list of size n/2, the problem here is simplified. This process continues until all the comparisons are trivial. This problem satisfies the divide and conquer recurrence relation

$$M(n) = 2M(n/2) + O(1).$$

Binary Search

The binary search algorithm reduces the search for an element in a search sequence of size n to the binary search for this element in a search sequence of size n/2, when n is even. The problem size n has been reduced to one problem of size n/2. So to comparisons are needed to implement this reduction. Hence if f(n) is the number of comparisons required to search for an element in a search sequence of size n, then

$$f(n) = f(n/2) + 2$$

when n is even.

Exercise

1. Define linear homogeneous recurrence relation with example.
2. Solve the following recurrence relation with the initial conditions given.
   a. $a_n = 2a_{n-1}$ for $n \geq 1$, $a_0 = 3$
   b. $a_n = 4a_{n-1} - 4a_{n-2}$ for $n \geq 2$, $a_0 = 6$, $a_1 = 8$.
   c. $a_n = 4a_{n-2}$ for $n \geq 2$, $a_0 = 0$, $a_1 = 4$
3. Find an explicit formula for the Fibonacci numbers with recurrence relation $f_n = f_{n-1} + f_{n-2}$ with $f_1 = 1$ and $f_2 = 2$.
4. Define linear homogeneous recurrence relation with degree k with constant coefficient. What is the solution of recurrence relation $a_n = 4a_{n-1} + 4a_{n-2}$ with $a_0 = 3$ and $a_1 = 5$?
5. Find the solution to $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ for n = 3, 4, 5, ..., with $a_0 = 3$, $a_1 = 6$, $a_2 = 0$.
6. Find the solution to $a_n = 7a_{n-2} + 6a_{n-3}$ with $a_0 = 9$, $a_1 = 10$, $a_2 = 32$.
7. Let $\{a_n\}$ be a sequences that satisfies the recursion relation $a_n = a_{n-1} - a_{n-2}$ for $n \geq 2$ and suppose that $a_0 = 3$ and $a_1 = 5$. Find the value of a_2 and a_3.
8. Describe linear homogeneous and non-linear homogeneous recurrence relation with examples.
9. Find the solution of the recurrence relation $a_n = 2a_{n-1} + 3.2^n$.
10. Suppose that f(n) = 2f(n/2) + 3 when n is even, and f(1) = 5. Find
    (a) f(2) (b) f(8) (c) f(64)

□□□

Chapter 6

Relations and Graphs

6.1 Relations

The word relation is used to indicate a relationship between two objects. Relationship between elements of sets are represented using a structure called a relation. Relations can be used to solve problems such as determining which pair of cities are linked by airline flights in a network, producing a useful way to store information in computer databases, to show the relationship between employee and his or her salary in database etc.

In mathematics, an example of relation is 'less than' which is denoted by <, so that x is related to y if $x < y$, two computer programs are related if they share same common data. In this chapter, we discuss the mathematics of relations defined on sets, various ways of representing relations and explore various properties they may have.

Definition

Let A and B be the two non-empty sets. A relation from A to B is any subset of the Cartesian product $A \times B$ satisfying given specific condition.

i.e. $R \subseteq A \times B$

Suppose R is a relation from A to B. Then R is a set of ordered pairs (a, b) where $a \in A$ and $b \in B$. Every ordered pair (a, b) is written as a R b, read as 'a is related to b by R'. If $(a,b) \notin R$, then a is not related to b by R and is written $a \not R\, b$. if R is a relation from a set A to itself, that is, if R is subset of $A^2 = A \times A$, then we say R is relation on A.

Domain and Range

Suppose R is a relation from A to B then, the domain of relation R is the set of all first elements of ordered pairs which belongs to R. It is denoted by Dom (R).

Mathematically, $Dom(R) = \{a \in A : (a, b) \in R, \text{ for some } b \in B\}$ Similarly, the range of relation R is the set of all second elements of ordered pairs belongs to relation R.

Mathematically, $range(R) = \{b \in B : (a, b) \in R, \text{ for some } a \in A\}$

If $R = \{(1, 2), (1, 4), (2, 4)\}$, then

$Dom(R) = \{1, 2\}$

$Ran(R) = \{2, 4\}$

Example

Let $A = \{4,5,6\}$, find the relations in $A \times A$ under the condition $x+y < 10$. Also find domain and range of relation.

Solution

$A \times A = \{(4,4), (4,5), (4,6), (5,4), (5,5), (5,6), (6,4), (6,5), (6,6)\}$

The given condition is: $x + y<10$

So, $R = \{(4, 4), (4, 5), (5, 4)\}$

$Dom(R) = \{4,5\}$ $Range(R) = \{4,5\}$

Properties of Relation

A relation R on a set A satisfies certain properties which are defined as follows:

Reflexive Relation: A relation R on a set A is reflexive if $(a, a) \in R$ for all $a \in A$, that is, if a R a for $a \in A$. A relation R on a set A is irreflexive if a $\not R$ a for every $a \in A$.

Example

(a) If $R = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}$ is a relation on $A = \{1, 2, 3\}$, then R is reflexive relation since for every $a \in A$, $(a, a) \in R$.

(b) If $R = \{(1, 1), (1, 2)\}$ is a relation on $B = \{(1, 2, 3\}$. Then R is irreflexive since for $2 \in B$ there is no $(2, 2)$ in R and for $3 \in B$ there is no $(3, 3) \in R$.

(c) $R = \{(x, y) \in R^2 : x \leq y\}$ is a reflexive relation since $x \leq x$ for any $x \in R$ (a set of real numbers).

(d) $S = \{(x, y) \in R^2 : x < y\}$ is an irreflexive relation since $x < x$ for no $x \in R$ (the set or real numbers)

Symmetric Relation

A relation R on a set A is symmetric if $(b , a) \in R$ whenever $(a , b) \in R$ for all $a ,b \in A$

Asymmetric Relation

A relation R on a set A is asymmetric if $(a , b) \in R$ then $(b , a) \notin R$ for all $a ,b \in A$.

Antisymmetric Relation

A relation R on a set A is antisymmetric if $a = b$ whenever aRb and bRa. The contrapositive of this definition is that R is antisymmetric if a $\not R$ b or b $\not R$ a whenever $a \neq b$.

Example

(a) $R_1 = \{(1, 1), (1, 2), (1, 3), (2, 3), (2, 1), (3, 2), (3, 1)\}$ is a symmetric relation since for $(1, 2), (1, 3), (2, 3)$ there are $(2, 1), (3, 1)$ and $(3, 2)$ respectively.

(b) $R_2 = \{(x, y) \in R^2 : x^2 + y^2 = 1\}$ is a symmetric relation since $y^2 + x^2 = 1$. so clearly R_2 contains (y, x) which satisfies $y^2 + x^2 = 1$.

(c) $S = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$ on $A = \{1, 2, 3\}$ is asymmetric since for $(1, 2) \in S$, there is no $(2, 1)$ in S. Similarly $(3, 2) \notin S$ and $(1, 3) \notin S$.

(d) $R = \{(1, 2), (2, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$ is an antisymmetric since if we choose 1 and 2 then for $1 \neq 2$, $(1, 2) \in R$ but $(2, 1) \notin R$. Again if we choose 2 and 3 then for $2 \neq 3$, $(2, 3) \in R$ but $(3, 2) \notin R$.

Transitive Relation

A relation R on a set A is transitive if whenever aRb and bRc,then aRc i.e. $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$ for all $a, b, c \in A$.

Example

(a) Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (3, 2), (2, 3), (1, 3), (2, 2), (3, 3)\}$ then R is transitive.

(b) Let $A = \{1, 2, 3, 4\}$ and let $R = \{(1, 2), (1, 3), (4, 2)\}$ then R is transitive since there are no elements a, b and c in A such that aRb and bRc, but a $\not R$ c.

Combining Relations

The relation from set A to B subsets of $A \times B$ so two relations from A to B can be combined in a same way that two sets can be combined.

Example

Let $A = \{4, 5, 6\}$ and $B = \{4, 5, 6, 7\}$. The relations $R_1 = \{(4, 4), (5, 5), (6, 6)\}$ and $R_2 = \{(4, 4), (4, 5), (4, 6), (4, 7)\}$ then find $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$.

Solution

$R_1 \cup R_2 = \{(4, 4), (5, 5), (6, 6)\} \cup \{(4, 4), (4, 5), (4, 6), (4, 7)\}$
$= \{(4, 4), (4, 5), (4, 6), (4, 7), (5, 5), (6, 6)\}$

$R_1 \cap R_2 = \{(4, 4), (5, 5), (6, 6)\} \cap \{(4, 4), (4, 5), (4, 6), (4, 7)\}$
$= \{(4, 4)\}$

$R_1 - R_2 = \{(4, 4), (5, 5), (6, 6)\} - \{(4, 4), (4, 5), (4, 6), (4, 7)\}$
$= \{(5, 5), (6, 6)\}$

$R_2 - R_1 = \{(4, 4), (4, 5), (4, 6), (4, 7)\} - \{(4, 4), (5, 5), (6, 6)\}$
$= \{(4, 5), (4, 6), (4, 7)\}$

Types of Relations

Complementary Relation: Let R be a relation from a set A to B. The complementary relation of R is denoted by $\bar{R}$ which consists of those ordered pairs which are not in R, that is

$$\bar{R} = \{(a, b) \in A \times B : (a, b) \notin R\}.$$

Example

Let R be a relation on set A = {1, 2, 6} defined as: R = {(x,y): x<y}. Find the complement relation of R.

Solution

$A \times A = \{(1,1), (1,2), (1,6), (2,1), (2,2), (2,6), (6,1), (6,2), (6,6)\}$

$R = \{(1,2), (1,6), (2,6)\}$

$\bar{R} = A \times A - R = \{(1,1), (2,1), (2,2), (6,1), (6,2), (6,6)\}$

Inverse Relation

Let R be a relation from A to B. the inverse of R, denoted by R^{-1}, is the relation from B to A which consists of those ordered pairs which, when reversed, belong to R; that is,

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

Example

Let A = {1, 2, 3, 4} and B = {a, b, c}.

Let R = {(1, a), (1, b), (2, b), (2, c), (3, b), (4, a)}

and S = {(1, b), (2, c), (3, b), (4, b)}.

Compute: (a) $\bar{R}$ (b) R^{-1} (c) $R \cup S$.

Solution

For A × B

A \ B	A	b	c
1	(1, a)	(1, b)	(1, c)
2	(2, a)	(2, b)	(2, c)
3	(3, a)	(3, b)	(3, c)
4	(4, a)	(4, b)	(4, c)

$\therefore$ $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c), (4, a), (4, b), (4, c)\}$.

(a) $\bar{R} = \{(1, c), (2, a), (3, a), (3, c), (4, b), (4, c)\}$

(b) $R^{-1} = \{(a, 1), (b, 1), (b, 2), (c, 2), (b, 3), (a, 4)\}$

(c) $R \cap S = \{(1, b), (3, b), (2, c)\}$

(d) $R \cup S = \{(1, a), (1, b), (2, b), (2, c), (3, b), (4, a), (4, b)\}$

Identity Relation

A relation R in a set A i.e. a relation R from A to A is said to be a identity relation, generally de by I_A, if

$$I_A = \{(x, x): x \in A\}.$$

Example

Let A = {(1, 2, 3} then I_A = {(1, 1), (2, 2), (3, 3)}

N–ary Relation

Relationship among elements of more than two sets often arise. The relationship among more two sets are called n-ary relations.

For instance, there is a relationship involving the airline, flight number, staring point, destina departure time, arrival time of a flight. n-ary relation are used to represent computer data which help us answer queries about the information stored in databases, such as: which flights at Kathmandu airport between 1 P.M to 3P.M?

Let $A_1, A_2, \ldots, A_n$ be a finite sets. A subset R of $A_1 \times A_2 \times \ldots \times A_n$ is called an n–ary relation on A_1, $\ldots, A_n$.

Example

Let A = {1, 2} and let R be the relation defined by the property 'x + y+ z is even'.

Now, A × A × A = {(1, 1, 1), (1, 1, 2), (1, 2, 1), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2), (1, 2, 2)}

Under 'x + y + z is even ' the relation is

R = {(1, 1, 2), (1, 2, 1), (2, 1, 1), (2, 2, 2)} which is ternary.

Example

Let R be the relation consisting of 5-tuples (A, N, S, D, T) representing airplane flights, where A is airline, N is the flight number, S is the starting point, D is the destination, and T is the depart time. The ordered pairs belongs to such n-ary relations may be: (Fly Dubai, 1024, Kathman Sarjaha, 2:00).

Operations on N-ary Relation

There are a variety of operations on N-ary relations that can be used to form new n-ary relations. T most common operation is determining all N-tuples in the N-ary relation that satisfy cert conditions.

1. Let R be an n-ary relation and C a condition that elements in R may satisfy. Then the select operator s_C maps the N-ary relation R to the N-ary relation of all n-tuples from R that satisfy condition C.
2. The projection $P_{i_1, i_2, \ldots, i_m}$ maps the N-tuple $(a_1, a_2, \ldots, a_n)$ to the m-tuple $(a_{i_1}, a_{i_2}, \ldots, a_{i_m})$, whe $m \leq n$.
3. Let R be a relation of degree m and S a relation of degree n. The join $J_p(R, S)$, where $p \leq m$ a $p \leq n$, is a relation of degree m + n - p that consists of all (m + n - p)-tuples $(a_1, a_2, \ldots, a_{m-p}, c_1, \ldots, c_p, b_1, b_2, \ldots, b_{n-p})$, where the -tuple $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2, \ldots, c_p)$ belongs to R and the n-tu $(c_1, c_2, \ldots, c_p, b_1, b_2, \ldots, b_{n-p})$ belongs to S.

Example

Suppose we have following class schedule for the B.Sc. course in a particular college.

Class_Schedule			
Department	Course_number	Room	Time
Computer Science	415	C101	11:00 am
Mathematics	416	C102	12:00 pm
Mathematics	417	C104	13:00 pm

Physics	418	C104	14:00 pm
Statistics	419	C105	10:00 am
Computer Science	420	C103	13:00 pm

Now we can use selection operation in this N-ary relation (where N = 4) as follows:

```
SELECT room,time
FROM class_schedule
WHERE department="computer science".
```

The output of above selection operation results the following table.

Room	Time
C101	11:00 am
C103	13:00 pm

Composition of Relation

Let A, B, C be three sets. Let R be a relation from A to B and S be a relation from B to C. Then the composite of R and S is denoted by SoR and defined as

$$SoR = \{(a, c) \in A \times C: \text{for some } b \in B, (a, b) \in R \text{ and } (b, c) \in S\}$$

That is, a(SoR)c, if for some $b \in B$, we have aRb and bSc.

Example

If R and S be relations on A = {1, 2, 3, 4} defined by R = {(1, 1), (1, 2), (3, 4), (4, 2)} and S = {(1,1), (2, 1), (3, 1), (4, 4), (2, 2)}. Find RoS and SoR.

Solution

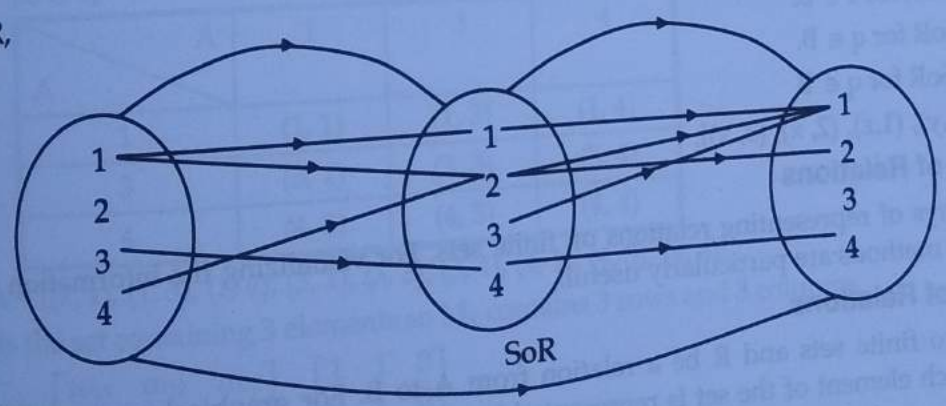
Given, A = {1, 2, 3, 4}

$R : A \to A = \{(1, 1), (1, 2), (3, 4), (4, 2)\}$

$S : A \to A = \{(1, 1), (2, 1), (3, 1), (4, 4), (2, 2)\}$

Now,

For SoR,



From above diagram,

$\because 1 \to 1 \to 1 \therefore (1, 1) \in SoR$

$1 \to 2 \to 1 \Rightarrow (1, 1) \in SoR$

$1 \to 2 \to 2 \Rightarrow (1, 2) \in SoR$

$4 \to 2 \to 1 \Rightarrow (4, 1) \in SoR$

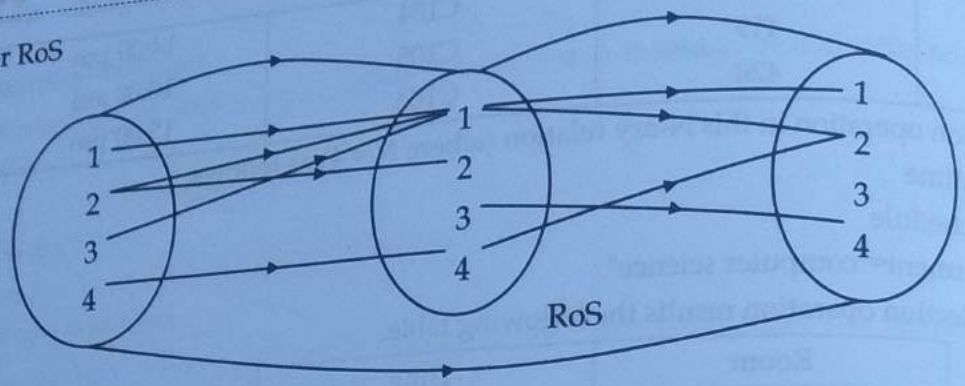
$4 \to 2 \to 2 \Rightarrow (4, 2) \in SoR$

$3 \to 4 \to 4 \Rightarrow (3, 4) \in SoR$

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

Again,

For RoS



From above arrow diagram

$1 \to 1 \to 1 \Rightarrow (1, 1) \in$ RoS

$1 \to 1 \to 2 \Rightarrow (1, 2) \in$ RoS

$2 \to 1 \to 1 \Rightarrow (2, 1) \in$ RoS

$3 \to 1 \to 1 \Rightarrow (3, 1) \in$ RoS

$2 \to 1 \to 2 \Rightarrow (2, 2) \in$ RoS

$3 \to 1 \to 2 \Rightarrow (3, 2) \in$ RoS

$4 \to 4 \to 2 \Rightarrow (4, 2) \in$ RoS

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

Example

Let A = {1, 2, 3}, B = {p, q, r}, C = {x, y, z} and let R = {(1, p), (1, r), (2, q), (3, q)} and S = {(p, y), (q, x), (r, z)}. Compute SoR.

Solution

Clearly R is a relation from A to B and S is a relation from B to C.

The order pairs (1, p) $\in$ R and (p, y) $\in$ S produce the order pair (1, y) $\in$ SoR for some P $\in$ B.

Similarly,

(1, z) $\in$ SoR for r $\in$ B.

(2, x) $\in$ SoR for q $\in$ B.

(3, x) $\in$ SoR for q $\in$ B

$\therefore$ SoR= {(1,y), (1,z), (2, x), (3, x)}.

Representations of Relations

There are many ways of representing relations on finite sets. For visualizing the information about relations, graphical methods are particularly useful.

Directed Graphs of Relations

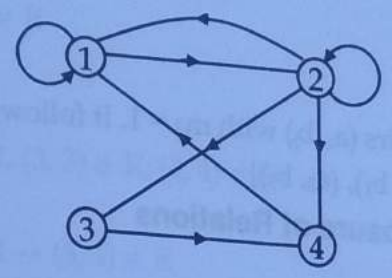
Let A and B be two finite sets and R be a relation from A to B. For graphical representation of relation on a set, each element of the set is represented by a point. These points are called nodes or vertices. An arc is drawn from each point to its related point. If the pair x $\in$ A, y $\in$ B is in the relation, the corresponding nodes are connected by arcs called edges or arcs. The arcs start at the first element of the pair and they go to the second element of the pair. The direction is indicated by an arrow. All arcs with an arrow are called directed arcs. The resulting pictorial representation of R is called a directed graph or digraph of R. An edge of the form (a, a) is represented using an arc from the vertex 'a' back to itself. Such an edge is called a loop.

Example

Let A = {1, 2, 3, 4} and

R = {(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4, 1)}.

Then the diagraph of R is as shown in figure.



Matrix of a Relation

Let $A = \{a_1, a_2, \ldots a_m\}$ and $B = \{b_1, b_2, \ldots b_n\}$ be finite sets containing m and n elements respectively and let R be a relation from A to B, then R can be represented by mn matrix $M_R = [m_{ij}]_{mn}$ where

$$m_{ij} = \begin{cases} 1 \text{ if } (a_i, b_j) \in R. \\ 0 \text{ if } (a_i, b_j) \notin R. \end{cases}$$

Then the matrix M_R is called the matrix of relation R.

Note that the matrix M_R^T is the complement of M_R and it is obtained from M_R by changing 0's into 1's and 1's into 0's, but M_R^T is the transpose of M_R, obtained from M_R by interchanging its rows and columns.

If R and S re the relations on a set a, then using operations on Boolean matrices one can show $M_{R \cup S} = M_R \vee M_S$, $M_{R \cap S} = M_R \wedge M_S$ and $M_{R^{-1}} = M_R^T$.

Example

Let R be a relation from the set $A = \{1, 3, 4\}$ on itself and be defined by $R = \{1, 1), (1, 3), (3, 3), (4, 4)\}$. Then find M_R.

Solution

Here $A = \{1, 3, 4\}$

A \ A	1	3	4
1	(1, 1)	(1, 3)	(1, 4)
3	(3, 1)	(3, 3)	(3, 4)
4	(4, 1)	(4, 3)	(4, 4)

$\therefore A \times A = \{(1, 1), (1, 3), (1, 4), (3, 1), (3, 3), (3, 4), (4, 1), (4, 3), (4, 4)\}$

Since A is the set containing 3 elements so M_R contains 3 rows and 3 columns.

$$\text{Hence } M_R = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Here, $m_{11} = 1$ since $m_{11} = (1, 1) \in R$

$m_{12} = 1$ since $m_{12} = (1, 3) \in R$

$m_{13} = 0$ since $m_{13} = (1, 4) \notin R$ and so on.

Example

Let $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4\}$. Find which ordered pairs are in the relation R represented by the given matrix.

$b_1 \quad b_2 \quad b_3 \quad b_4$

$$M_R = \begin{array}{c} a_1 \\ a_2 \\ a_3 \end{array} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Solution

Since relation R consists of those ordered pairs (a_i, b_j) with $m_{ij} = 1$. It follows that

$R = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3)\}$

Reflexive, Symmetric and Transitive Closure of Relations

Reflexive Closure of R

Let R is a relation, then any new relation R' that contains R and is also contained within every reflexive relation that contains R_1 is called the reflexive closure of R.

Given a relation R on a set A, the reflexive closure of R can be formed by adding to R all pairs of the form (a, a) with $a \in A$, which is not already in R.

Example:

Given $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$ on the set $A = \{(1, 2)\}$ is not reflexive.

Now, this relation can be anode reflexive by adding (2, 2) and (3, 3) to R. Since these on the only pairs of the form (a, a) not in R.

Then,

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

Note: The reflexive closure of R is equals to $R \cup \Delta$ where $\Delta = \{(a, a)/a \in A\}$.

Symmetric Closure of R

The symmetric closure of relation R on set A is the smallest symmetric relation. On set A that contains given relation R.

Transitive Closure

The transitive closure of relation R on set A is the smallest relation on set A that contains R.

Example

For finite sets, we can construct transitive closure of R step by step, starting from R and adding transitives edges. i.e.,

$$R^+ = \bigcup_{i \in \{1,2,3.....\}} R_i$$

Where R_i is the ith power of R, defined inductively as

$$R' = R$$

and $\quad R^{i+1} = RoR^i$, for $i > 0$

Where 'o' denotes the composition of relations.

Equivalence Relation

A relation R on a set A is called an equivalence relation if it is reflexive, symmetrical and transitive.

Example

Let $A = \{1, 2, 3, 4, 5\}$. Show that the relation $R = \{(1, 1), (1, 5), (2, 2), (2, 4), (3, 3), (4, 2), (4, 4), (5, 1), (5, 5)\}$ is an equivalence relation.

Solution

Given,

$$A = \{1, 2, 3, 4, 5\}$$

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

To prove R is equivalence, we need to show that R satisfies reflexive, symmetric and transitive property.

Now,

(i) Reflexive: $\forall$ a$\in$ A, (a, a) $\in$ R

Here, In relation R,

$\forall$ 1, 2, 3, 4, 5 $\in$ A,

(1, 1) $\in$ R, (2, 2)$\in$R, (3, 3) $\in$ R, (4, 4) $\in$ R

In given relation R,

1, 5 $\in$ A, (1, 5) $\in$ R $\rightarrow$ (5, 1) $\in$ R

2, 4 $\in$ A, (2, 4) $\in$ R $\rightarrow$ (4, 2) $\in$

$\therefore$ R is symmetric.

(ii) Transitive: $\forall$ a, b, c$\in$A, (a, b) $\in$ R n (b, c) $\in$ R $\rightarrow$ (a, c) $\in$

In given relation R, $\forall$ 1, 2, 3, 4, 5 $\in$ A,

(1, 5) $\in$ R $\wedge$ (5, 1) $\in$ R $\rightarrow$ (1, 1) $\in$ R

(2, 4) $\in$ R $\wedge$ (4, 2) $\in$ R $\rightarrow$ (2, 2) $\in$ R

(2, 4) $\in$ R $\wedge$ (4, 4) $\in$ R $\rightarrow$ (2, 4) $\in$ R

(5, 1) $\in$ R $\wedge$ (1, 5) $\in$ R $\rightarrow$ (5, 5) $\in$ R

$\therefore$ R is transitive.

Since, R satisfies reflexive, symmetric & transitive behavior. So R is equivalence.

Example

Consider the following relation on {1, 2, 3, 4, 5, 6} R = {(i, j) : |i – j| = 2}

Is R reflexive? Is R symmetric? Is R transitive?

Solution

Let A = {1, 2, 3, 4, 5, 6}. Then

R = {(i, j): |i – j| = 2} on A

= {(1, 3), (2, 4), (3, 1), (4, 2), (3, 5), (5, 3), (4, 6), (6, 4)}

R is not reflexive since (i, i) $\notin$ R for all i $\in$ A.

R is symmetric since for all (i, j)$\in$ R, also (j, i) $\in$ R.

R is not transitive since for all (i, j)$\in$ R, and (j, k) $\in$ R,

(i, k) $\notin$ R. For example (2, 4) $\in$ R and (4, 2) $\in$ R but (2, 2) $\notin$ R.

Congruence Modulo Relation

Let a and b be two integers then a is congruence to b modulo m if m divides a – b.

Notation: a $\equiv$ b(mod m)

E.g. a = 20, b =10 m = 5

Then 20 $\equiv$ 10 (mod 5)

5 | (20-10) or, 20 – 10=5*2

Example

Let m be a positive integer with m>1 show that the relation R={(a, b): a$\equiv$b(mod m) is an equivalence on set of positive integers.

Solution

To prove R is equivalence, we have to show that R satisfies reflexive, symmetric and transitive properties

i) Reflexive: $\forall$ (For all) a $\in$ z+

a$\equiv$ a(mod m) $\Rightarrow$ m | (a-a) $\Rightarrow$ m | 0 (true)

$\therefore$ (a, a) $\in$ R

So R is reflexive.

ii) Symmetric: $\forall$ a, b $\in$ Z+

Let (a , b) $\in$ R

So, a $\equiv$ b(mod m) $\Rightarrow$ m | (a-b)

$\Rightarrow$ a-b = m*k

$\Rightarrow$ b-a =m*(-k)

$\Rightarrow$ b $\equiv$ a(mod m)

$\Rightarrow$ m | (b-a)

$\therefore$ (b , a) $\in$ R.

Hence: R is Symmetric

iii) Transitive: $\forall$ a, b, c $\in$ Z+,

Let (a, b) $\in$ R

$\Rightarrow$ a $\equiv$ b(mod m) $\Rightarrow$ m | (a – b)

$\Rightarrow$ a – b $\equiv$ m*k_1 .....(i)

Again (b, c) $\in$ R

$\Rightarrow$ b $\equiv$ c(mod m)

$\Rightarrow$ m | (b – c)

$\Rightarrow$ b – c = m*k_2.....(ii)

Adding (i) & (ii) we get

a – b + b – c = m*k_1 + m*k_2

or, a – c = m(k_1+k_2)

or, a – c = m*k

$\Rightarrow$ m | (a – c)

$\Rightarrow$ a $\equiv$ c(mod m)

$\therefore$ (a, c) $\in$ R

$\therefore$ R is transitive.

Hence, given relation R is an equivalence relation.

Example

Show that the relation R = {(x, y): x $\equiv$ y(mod 4)}defined on the set A={1, 2, 3, 4, ... 13, 14, 15} is an equivalence. Also find the partition of the set A determined by relation R.

Solution

To prove R is equivalence, we have to show that R satisfies reflexive, symmetric and transitive properties

i) Reflexive: $\forall$ (For all) x $\in$ A

x $\equiv$ x(mod 4) $\Rightarrow$ 4 | (x-x) $\Rightarrow$ 4 | 0 (true)

$\therefore$ (x , x) $\in$ R

So R is reflexive.

ii) Symmetric: $\forall$ x, y $\in$ A

Let (x , y) $\in$ R

So, x $\equiv$ y(mod 4) $\Rightarrow$ 4 | (x-y)

$\Rightarrow$ x-y = 4*k

$\Rightarrow$ y-x =4*(-k)

$\Rightarrow$ $y \equiv x \pmod 4$

$\Rightarrow$ $4 \mid (y-x)$

$\therefore$ $(y, x) \in R$.

Hence: R is Symmetric

iii) Transitive: $\forall\, x, y, z \in A$,

Let $(x, y) \in R$

$\Rightarrow$ $x \equiv y \pmod 4 \Rightarrow 4 \mid (x-y)$

$\Rightarrow$ $x - y \equiv 4*k_1$.....(i)

Again $(y, z) \in R$

$\Rightarrow$ $y \equiv z \pmod 4$

$\Rightarrow$ $4 \mid (y-z)$

$\Rightarrow$ $y - z = 4*k_2$.....(ii)

Adding (i) &(ii) we get

$x - y + y - z = 4*k_1 + 4*k_2$

or, $x-z = 4(k_1+k_2)$

or, $x-z = 4*k$

$\Rightarrow$ $4 \mid (x-z)$

$\Rightarrow$ $x \equiv z \pmod 4$

$\therefore$ $(x, z) \in R$

$\therefore$ R is transitive.

Hence given relation R is equivalence.

Now, to find the partition of set A determined by relation R, we need to find the modulo classes. The possible reminders after performing modulo 4 are 0, 1, 2, 3 So,

$[0]_4 = \{4, 8, 12\}$, $[1]_4=\{1, 5, 9, 13\}$, $[2]_4=\{2, 6, 10, 14\}$ and $[3]_4=\{3, 7, 11, 15\}$

$\therefore$ $P = \{\{4, 8, 12\}, \{1, 5, 9, 13\}, \{2, 6, 10, 14\}, \{3, 7, 11, 15\}\}$

Example

What are equivalence classes of 0&1 for congruence modulo 4 ?

Solution

Note: The congruence class of an integer a modulo m is denoted by [a]m so that :

$[a]_m = \{$.....$a - 2m, a-m, a, a + m, a+2m$.....$\}$

Now, The equivalence class of 0 contains all integers a such that $a \equiv 0 \pmod 4$ the integers in this case are those divisible by 4.

$[0]_4 = \{$ .....$-8, -4, 0, 4, 8,$.....$\}$

The equivalences of 1 contains all integers a such that $a \equiv 1 \pmod 4$ i.e. those that have remainder 1 divisible by 4.

$\therefore [1]_4 = \{$.....$,-7, -4, 0, 4, 8,$.....$\}$

Example

What are the sets in the partition of integers arising from congruence modulo 4?

Solution

Since congruence classes are disjoint so, congruence classes form a partition. The congruence class modulo 4 are denoted by $[0]_4$, $[1]_4$, $[2]_4$ and $[3]_4$.

Therefore, $[0]_4=\{$.....$-8, -4, 0, 4, 8,$.....$\}$

$[1]_4 =\{$.....$-7, -3, 1, 5, 9,$.....$\}$

$[2]_4$={.....-6, -2, 2, 6, 10.....}

$[3]_4$={.....-5, 1, 3, 7, 11,.....}

Equivalence Classes

If R is an equivalence relation on a set A and xRy then x and y are called equivalent with respect to R. Then the class of any element $x \in A$ is denoted by [x] which is defined as

$$[x]_R = \{y \in A : (x, y) \in R\}.$$

The collection of all equivalence classes of elements under an equivalence relation R is denoted by A/R, that is,

$$A/R = \{[x]: x \in A\}.$$

It is called the quotient set of A by R.

Example

Let R = {(1, 2), (2, 1), (1, 1), (2, 2), (3, 3), (4, 4)} be a relation on A = {1, 2, 3, 4}. Find the equivalence classes of each element of A and quotient set of A by R.

Solution

Equivalence class of 1 is,

$$[1]_R = \{1, 2\}$$
$$[2]_R = \{1, 2\}$$
$$[3]_R = \{3\}$$
$$[4]_R = \{4\}$$

And A/R = {{1, 2}, {3}, {4}}.

From example 11, we can conclude that equivalence classes form a partition of a set.

Since $[2] \cup [3] \cup [4] = A$ and

$$[2] \cap [3] = \phi = [2] \cap [4] = \phi = [3] \cap [4].$$

Partitions of a Set

A partition or quotient set of a set A is the collection of subsets of A i.e.

$P = \{A_1, A_2, \ldots\ldots A_n\}$ such that

(i) Union of A_i is A.

(ii) For distinct A_i and A_j, $A_i \cap A_j = \phi$

The sets in P are called blocks or cells of partition.

Example

Let A = {a, b, c, d, e, f, g, h} and P = {A_1, A_2, A_3, A_4, A_5} where

A_1 = {a, b, c, d}, A_2 = {a, c, e, f, g, h}

A_3 = {a, c, e, g}, A_4 = {b, d}

A_5 = {f, h}

Then {A_1, A_2} is not a partition since $A_1 \cap A_2 \neq \phi$.

Also {A_1, A_5} is not a partition. But

P = {A_3, A_4, A_5} is a partition of A since $A_3 \cup A_4 \cup A_5 = A$ and

$A_3 \cap A_4 = \phi$, $A_4 \cap A_5 = \phi$, $A_3 \cap A_5 = \phi$.

Example

Let R = {(1, 1), (2, 1), (3, 2)}, compute R^2.

Solution

$R^2 = RoR$ = {(1, 1), (2, 1), (3, 1)}.

Partial Order Relation

A relation R on a set A is called a partial order if it is reflexive, anti-symmetric and transitive. That is,

(i) Reflexive: aRa for all $a \in A$.

(ii) Anti-symmetric: for all $a, b \in A$, aRb and bRa $\Rightarrow a = b$.

(iii) Transitive: for all $a, b, c \in A$, aRb and bRc $\Rightarrow$ aRc.

A set 'A' together with a partial order relation R is called a partially ordered set or poset and it is denoted by (A, R). It is also denoted by $(A, \prec)$, where $\prec)$ is partial order on a set A.

Comparability

If $(A, \prec)$ is partially ordered set, elements a and b of A are said to be comparable if and only if either $a \prec b$ or $b \prec a$.

If X and Y are subsets of a set S, it need not to be the case that $X \subseteq Y$ or $Y \subseteq X$; for example, {a} and {b, c} are not comparable. But in the poset $(Z^+, /)$, the integers 2 and 4 are comparable, since $\frac{4}{2}$ but 3 and 5 are incomparable, because neither 3 divides 5 nor 5 divides 3.

Totally Ordered Set

If $\prec$ is a partial order on a set A and every two elements of A are comparable, $\prec$ is called a total order and the pair $(A, \prec)$ is a totally ordered set. A totally ordered set is also called a chain.

The real numbers are totally ordered by $\leq$ because for every pair (a, b) of real numbers either $a \leq b$ or $b \leq a$. On the other hand, the set of sets, {{a}, {b}, {c},{a, c}} is not totally ordered by $\subseteq$ since neither {a} $\subseteq$ {b} nor {b} $\subseteq$ {a}.

Example

Prove that the greater or equal ($\geq$) relation is a partial ordering on Z, the set of integers.

Solution:

To prove '$\geq$' is partial ordering, we have to show R satisfies reflexive, anti-symmetric and transitive property.

(i) **Reflexive:** Since $a \geq a$ for every integer $a \in Z$. So $\geq$ is reflexive.

(ii) **Antisymmetric:** Let $a \geq b$ and $b \geq a$. Then clearly $a = b$. So $\geq$ is antisymmetric.

(iii) **Transitive:** Let $a \geq b$ and $b \geq c$. Then clearly $a \geq c$. So $\geq$ is transitive.

Example

Let "/" be the divides relation R on a set N of positive integer. Then prove that "/" is a partial order relation on N.

Solution:

To prove '/' relation is partial ordering, we have to prove that '/' satisfies reflexive anti-symmetric and transitive property.

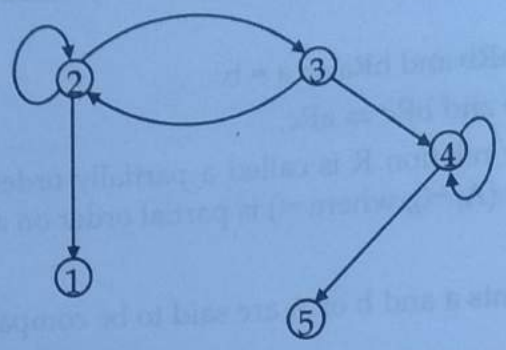
(i) **Reflexive:** Let $a \in N$. Then clearly a is a divider of a i.e. aRa. Therefore, R is reflexive.

(ii) **Antisymmetric:** Let a be a divisor of b i.e. $\frac{b}{a}$ and b be a divisor of a i.e. $\frac{a}{b}$ then clearly we have a = b. Therefore R is antisymmetric.

(iii) **Transitive:** Let a be a divisor of b and b be a divisor of C. then $\frac{b}{a} \cdot \frac{c}{b} = \frac{c}{a}$. Thus, a is a divisor of C. So R is transitive.

Example

Write the relation as a set of ordered pairs from the digraph as shown in below:

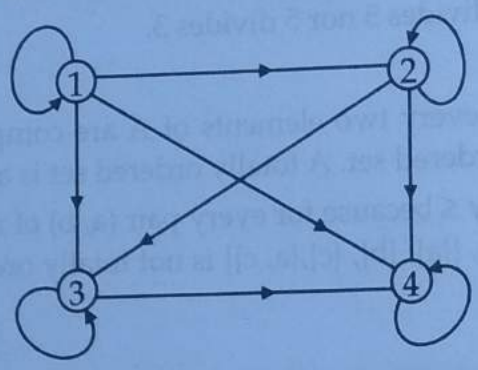


Solution

The ordered pairs in the relation are R = {(2, 1), (2, 2), (2, 3), (3, 2), (3, 4), (4, 4), (4, 5)}

Example

Determine whether the relation for the directed graph or digraph shown in Fig. 5.3 are reflexive, symmetric and transitive.



Solution

(i) **Reflexive:** The relation is reflexive since the diagraph of the relation has a loop at every vertex.

(ii) **Symmetric:** The relation is not symmetric since for a particular directed edge from 2 to 3, there is no directed edge from 3 to 2. This means that 2R3 but 3$\not$R2.

(iii) **Transitive:** The relation is transitive since the digraph has the property that whenever there are directed edges from x to y and from y to z, there is also a directed edge from x to z. For example, 1R2 and 2R4 ⇒ 1R4; 1R3 and 3R4 ⇒ 1R4.

Example

Let R be the following equivalence relation on a set A = {1, 2, 3, 4, 5, 6}:

R = {(1, 1), (1, 5), (2, 2), (2, 3), (2, 6), (3, 2), (3, 3), (3, 6), (4, 4), (5, 1), (5, 5), (6, 2), (6, 3), (6,, 6)}

Find the partition of A induced by R i.e. find the equivalence classes of R.

Solution

Here,

[1] = {1, 5}
[2] = {2, 3, 6}
[3] = {2, 3, 6}
[4] = {4}
[5] = {1. 5}
[6] = {2, 3, 6}

Therefore {{1, 5}, {2, 3, 6}, {4}} is the partition of A induced by R, since {1, 5} ∪ {2, 3, 6} ∪ {4} = A and they are disjoint as well.

Example

If p(s) is the set of all subsets of a given set s, show that the inclusion relation '⊆' is a partial ordering on the power set p(s).

Solution

Let s be a set and p(s) be its power set.

To prove 'C' is partial order, we have to show that 'C' relation satisfies: reflexive, anti-symmetric and transitive.

(i) **Reflexive:** For any $X \in p(s)$, clearly we have $X \subseteq X$.

(ii) **Anti-symmetric:** Let $X, Y \in P(S)$ and $X \subseteq Y, Y \subseteq X$. Which clearly implies that $X = Y$.

(iii) **Transitive:** Let $X, Y, Z \in P(S)$ and $X \subseteq Y, Y \subseteq Z$. Then clearly we get $X \subseteq Z$.

Lexicographic Order

Suppose $(S, \leq_1)$ and $(T, \leq_2)$ are posets. The Cartesian product SxT defined by $(s, t) < (s', t')$ either $s < s'$ or if both $s = s'$ and $t <_2 t'$.

i.e., one ordered pair is less than second pair if the first entry of the first pair is less than (in S) the first entry of the second pair or if the first entries are equal, but the second entry of this pair is less than (in T) the second entry of the second pair.

Example

Determine whether $(3.7) < (4.8)$ and $(3.9) < (3.11)$ in the poset $(ZXZ, \leq)$.

Solution

Since $3 < 4$, it follows that $(3.7) < (4.8)$.

Again $3 = 3$ and $9 < 11$, it follows that $(3.9) < (3.11)$.

Maximal and Minimal elements

Let $(S, \leq)$ be a poset. An element a is the greatest element of S if $x \leq a$ for all $x \in S$. The maximal element of exist is unique. For if a and a' are two greatest elements of S, the we should have $a' \leq a$ and $a \leq a'$. Hence $a = a'$.

Similarly, an element $b \in S$ is called least element if $b \leq x$ for all $x \in P$. The least element is unique if exist.

An element a in the poset is called a maximal element of S if $a < x$ for no x in S. Similarly an element a in the poset is called minimal if it not greater than any element of the poset.

That is, a is minimal if there is no element $x \in S$ such that $x < a$.

Lattices

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a lattice. Lattices have many special properties. Furthermore, lattices are used in many different applications such as models of information flow and play an important role in Boolean algebra.

Example

Determine whether $(P(S), \subseteq)$ is a lattice where S is a set.

Solution

Let A and B be two subsets of S. The least upper bound and the greatest lower bound of A and B are $A \cup B$ and $A \cap B$, respectively, hence $(P(S), \subseteq)$ is a lattice.

Example

Is the poset $(Z^+, |)$ a lattice?

Solution

Let a and b be two positive integers. The least upper bound and greatest lower bound of these two integers are the least common multiple and the greatest common divisor of these integers, respectively, as the reader should verify. It follows that this poset is a lattice.

Exercise

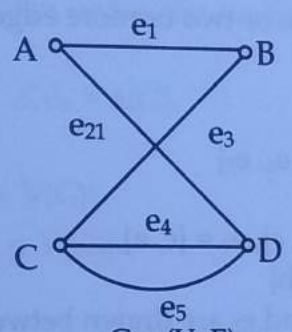
1. Let A = {4, 5, 6}. Find the relations in A × A under the conditions
   (i) $x + y < 10$
   (ii) $\frac{x}{y}$ is an integer.
   Also find the domain of the relations.
2. Let A = {1, 2, 3, 6}. If for x, y ∈ A.
   R = {(x, y) : x ≤ y}
   S = {(x, y) : x divides y}.
   Write R and S as sets and find R∩ S.
3. List the ordered pairs in the relation R from A ={ 0, 1, 2, 3, 4} to B = { 0, 1, 2, 3} where (a, b) ∈ R if and only if
   a) a = b.
   b) a + b = 4.
   c) a > b.
   d) a/b.
4. If R and S be relation on {1, 2, 3, 4} defined by R = {(1, 1), (1, 2), (3, 4), (4, 2)} and S = {(1, 1), (2, 1), (3, 1), (4, 4), (2, 2)} find RoS and SoR.
5. Draw the digraph for the relation congruence modulo 3 on the set {2, 3, 4, 6, 7, 9} and hence show that relation is symmetric and transitive.
6. a) List all the ordered pairs in the relation R = {(a, b): a divides b} on the set {1, 2, 3, 4, 5, 6}.
   b) Display this relation graphically.
   c) Display this relation in matrix form.
7. For each of this relations on the set {1, 2, 3, 4}, decide whether it is reflexive, whether it is symmetric, whether it is anti-symmetric, and whether it is transitive.
   a) {(2,2), (2,3), (2,4), (3,2), (3,3), (3,4)}
   b) {(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)}
   c) {(2,4), (4,2)}
   d) {(1,2), (2,3), (3,4)}
   e) {(1,1), (2,2), (3,3), (4,4)}
   f) {(1,3), (1,4), (2,3), (2,4), (3,1), (3,4)
8. Is the relation R = {(1, 2), (2, 3), (3, 3), (2, 1)} is anti-symmetric on A = {1, 2, 3}.
9. The relation R on set A = {1, 2, 3, 4} is defined by R = {(1, 1), (1, 2), (1, 4), (2, 2), (2, 1), (2, 4), (3, 3), (3,4), (3, 2), (4, 3), (4, 2), (4, 1)}. Draw digraph of R and hence find R^{-1}.
10. Consider the relation R from X to Y, where
    X = {1, 2, 3}; Y = {7, 8} and R = {(1, 7), (2, 7), (1, 8), (3, 8)}
    Find: (i) R^{-1} (the inverse of R) (ii) $\bar{R}$ (the complement of R)
11. If A is a relation in the set of integers Z defined by R = {(x, y) : x ∈ Z, y ∈ Z, (x − y) is multiple of 3}. Show that it is an equivalence relation.
12. Let A = {a, b, c, d) and consider the relation R = {(a, a), (a, b), (a, c), (a, d), (b, b), (b, d), (c, c), (c, d), (d, d)}. Show that R is partial ordering.
13. Verify that the relation R = ({1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2), (4, 5), (5, 4)} on A = {1, 2, 3, 4, 5} is an equivalence relation with the help of the digraph of the relation R.

6.2 Graph Theory

Introduction

Many situations that occur in computer science, physical science, communication science, Economics and many others areas can be analyzed by using techniques found in a relatively new area of mathematics called graph theory. Graphs can be used to represent almost any problem involving discrete arrangements of objects, where concern lies not with the internal properties of these objects but with relationships among them.

Graph is a discrete structure consisting of vertices and edges connecting the vertices. A graph G= (V, E) is a mathematical model consist of two non empty sets: V = $\{v_1, v_2, v_3, v_4, \ldots\ldots v_n\}$ called set of vertices and E=$\{e_1, e_2, e_3, e_4, \ldots\ldots e_n\}$ of ordered or un-ordered pairs of distinct vertices called edges. We usually write G=(V,E) and say V is the vertex set and E is the edge-set of G.



G = (V, E)

In above figure, graph G = (V, E) consist of set of vertices V = {A, B, C, D} and set of edges E = $\{e_1, e_2, e_3, e_4, e_5\}$ where e_1 = {A, B}, e_2 = {A, D}, e_3 {B, C}, e_4 = {C, D}, e_5 = {D, C}.

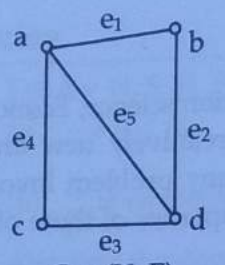
Applications of Graph

Graphs are used to solve problems in many fields. Some of them are as follows:

- Graphs are used to model the geographic maps of cities in which each place in city can be represented by the node and the road connecting such places are represented by an arc (edge).
- Graphs are used to model the computer network in which each node is a machine (computer, hub, router, switch etc) and the link between them represents the edge.
- They are used to analyze the electrical circuits, project planning, genetics etc.
- Any structured problem can be modeled by graphs. Then can help to solve typical problems those concerned with finding shortest path or most economical route between two vertices, or the smallest set of edges which connect all the vertices in a graph.
- Graphs are used to study the structure of WWW.
- It is used to find the number of different combination of flight between two cities in an airline network.
- It can be used to distinguish between two chemical compounds with the same molecular formula but different structure.
- It is also used to assign channels to television stations.

Simple Graph

We define a simple graph as 2 – tuple consists of a non empty set of vertices V and a set of unordered pairs of distinct elements of vertices called edges, having neither loop nor parallel edges. A graph G = (V,E) is said to be simple if G has no lops and no parallel edges.

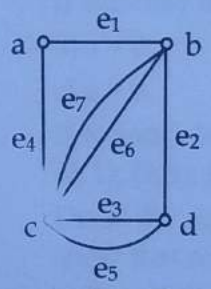


G = (V, E)

Here, V(G) = {a, b, c, d}
E(G) = {e_1, e_2, e_3, e_4, e_5}
Where,
e_1 = {a, b}, e_2 = {b, d},
e_3 = {d, c}, e_4 = {c, a}, e_5 = {a, d}
In this graph, none of the edges are parallel and does not contain loop so, it is simple graph.

Multi-graph

A computer network may contain multiple links between data centers, to model such networks we need graphs that have more than one edge connecting the same pair of vertices. Two or more edges between same pair of vertices are called parallel edges or two or more edges having same end points are called parallel edges.



G = (V, E)

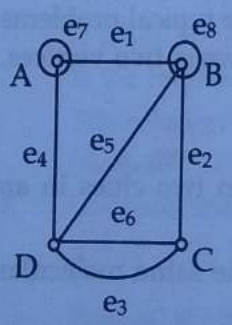
Here, V(G) = {a, b, c, d}
E(G) = {e_1, e_2, e_3, e_4, e_5, e_6, e_7}
Where,
e_1 = {a, b}, e_2 = {b, d}, e_3 = {d, c}, e_4 = {c, a},
e_5 = {d, c}, e_6 = {c, b}, e_7 = {c, b}
In this graph, the edges e_3 and e_5 are drawn between same pair of vertices. Similarly, e_6 and e_7 also so such edges are called parallel and graph is multi-graph.

A graph G = (V, E) consists of a set of vertices V, a set of edges E such that some of edges are parallel edges is called multi-graph.

Pseudograph

Sometimes a communication link connects a data center with itself, perhaps a feedback loop for diagnostic purposes. to model such a network we need to include edges that connects a vertex to itself such a edge is called loop.

A graph G =(V, E) consists of a set of vertices V, a set of edges E is said to be pseudo graph if G has both loops and multiple edges or loops only.



G = (V, E)

Here, V(G) = {A, B, C, D}
E(G) = {e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8}
Where,
e_1 = {A, B}, e_2 = {B, C}, e_3 = {C, D}, e_4 = {D, A},
e_5 = {B, D}, e_6 = {D, C}, e_7 = {A, A}, e_8 = {B, B}
In this graph, the edge e_7 is drawn from vertex A to A and e_8 is drawn from vertex B to B. So, such edges are loop and graph is called pseudo-graph.

Graph Models

Graph Terminologies

- **Order and size of Graph**

  If G=(V,E) be a finite graph then the number of vertices in graph G is called order of graph G and the number of edges in G is called size of G.

- **Degree of vertex**

Let G = (V, E) be a graph and v be a vertex of G. The degree (or valency) of v is denoted by d(v) is the number of edges incident on v.

A vertex v in graph G is said to be even vertex if its degree is even and a vertex v in G is said to be odd vertex if its degree is odd.

- **Isolated vertex and pendant vertex**

In a graph G=(V,E), a vertex having degree zero(0) is called isolated vertex and vertex having degree one(1) called pendant vertex.

Degree Sequence of a Graph

If $v_1, v_2, \ldots\ldots v_n$ are n vertices of G_1 then the sequence $(d_1, d_2, \ldots\ldots, d_n)$ where $d_i = \deg(v_i)$ is the degree sequence of G. In general, we order the vertices so that the degree sequence is monotonically increasing i.e.

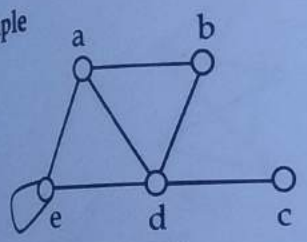
$$\delta(G) = d_1 \le d_2 \le \ldots\ldots \le d_n = \Delta(G),$$

Where,

$$\delta(G) = \min\{\deg v : \in V(G)\}$$

$$\Delta(G) = \max\{\deg v : \in V(G)\}$$

Example



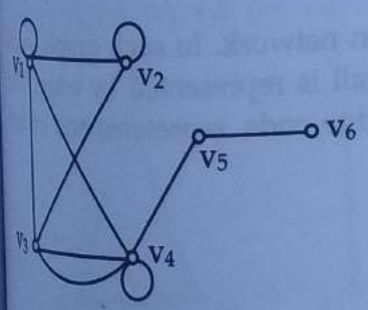
G = (V, E)

In this graph, deg(a) = 3, deg(b) = 2, deg(c) = 1, deg(d) = 4, deg(e) = 4.
Therefore, degree sequence of G is:
(1, 2, 3, 4, 4)

- **Adjacent vertices and adjacent edges**

Two vertices u and v in an undirected graph are called adjacent if there is an edge between u and v.

Two edges e_1 and e_2 in an undirected graph are said to be adjacent if they share a common vertex.



G = (V, E)

In above graph G, Order of graph = no. of vertices = 6, Size of graph= no of edges=9
$\deg(v_1)=5$, $\deg(v_2)=4$, $\deg(v_3)=4$, $\deg(v_4)=6$, $\deg(v_5)=1$ $\deg(v_6) = 0$
Vertex v_5 has degree 1 so it is pendent vertex and v_6 has degree 0 so it is isolated vertex.
Degree sequence of G = (0, 1, 4, 4, 5, 6)
Adjacent vertices of v_1 are v_2, v_3 and v_4 but vertices v_5 and v_6 are non-adjacent to v_1.
Adjacent edges of edge $\{v_1,v_2\}$ are $\{v_1,v_1\}$,$\{v_1,v_3\}$, $\{v_1,v_4\}$, $\{v_2,v_3\}$ and $\{v_2,v_2\}$

Simple and Special Graphs

Special types of Graphs

Some important types of graphs are introduced here. These graphs are often used as examples and arise in many applications.

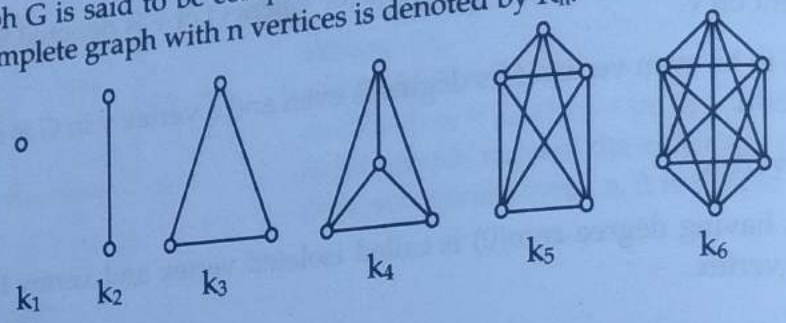
Trivial Graph

A graph with one vertex and no edges is called a trivial graph

K_1

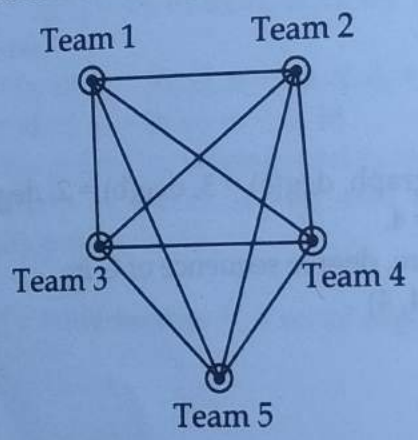
Complete Graph

A graph G is said to be complete if there exists exactly one edge between any pair of vertices in G. The complete graph with n vertices is denoted by K_n.



Round Robin Tournament

A game tournament where each team plays with each other team exactly once, is called round-Robin tournament. Such tournaments can be modelled using complete graph where there exist exactly one edge between each possible parts of vertices except itself. The following figure shows the tournament between 5 teams in Round-Robin fashion. Here, in the graph edge between vertices represent the matches between the teams and vertices represent teams.

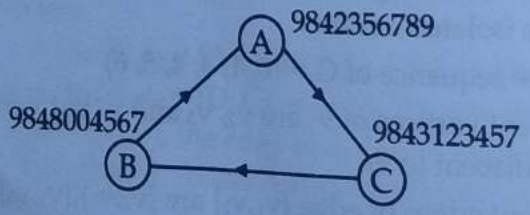


Collaboration Graph

A simple graph that can be used to model joint authorship of academic papers, where vertices represent people and edges between two vertices- represent joint authorship if they have joint written a paper.

Call Graph

Graph can be used to model telephone calls in a telecommunication network. In such graph, each telephone number is represented by a vertex and each telephone call is represented by edge. The source vertex represent a start call (sender) and the vertex where edge ends, represents end of call (receiver).



Regular Graph

A graph in which all vertices are of same (equal) degree is called a regular graph. If the degree of each vertex is r then the graph is a r-regular graph. In fig. k_1, k_2, k_3, k_4, k_5, and k_6 are 0-regular, 1-regular, 2-regular, 3-regular, 4-regular and 5-regular respectively.

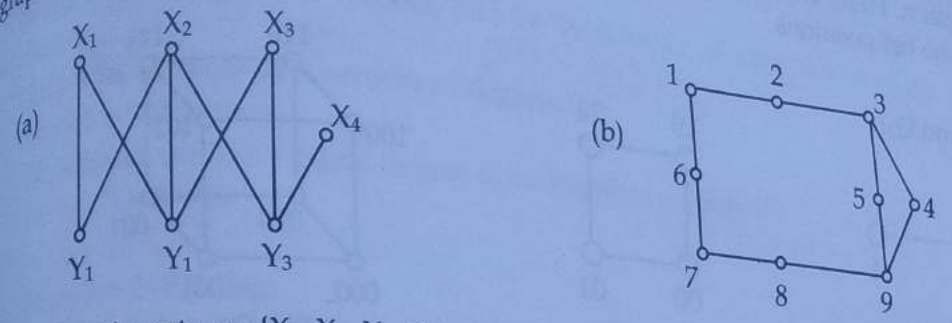
Bipartite Graph

A graph G = (V,E) is said to be bipartite if V is the union of two non-empty disjoint subsets V_1 and V_2 of V such that each edge in E is incident on one vertex in V_1 and one vertex in V_2. or

$V = \{a, b, c, d, e\}$
$V_1 = \{a, b\}$
$V_2 = \{c, d, e\}$.

A graph G=(V,E) is said to be bipartite if its vertex set V can be partitioned into two sunsets V_1 and V_2 such that each edge of G connect the vertex of V_1 to vertex of V_2 so that no edge in G connect two vertices in V_1 or two vertices in V_2.

The graphs shown in figure below are bipartite.

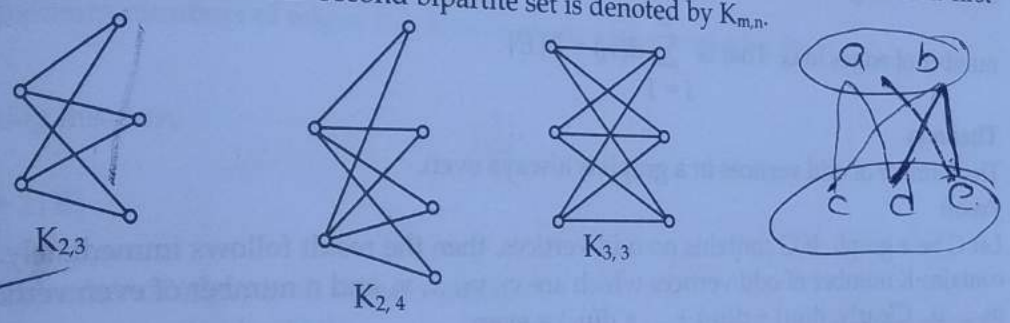


In fig (a), bipartite sets are $\{X_1, X_2, X_3, X_4\}$ and $\{Y_1, Y_2, Y_3\}$.

In fig (b), bipartite sets are {1, 3, 7, 9} and {2, 4, 5, 6, 8}.

Complete Bipartite Graph

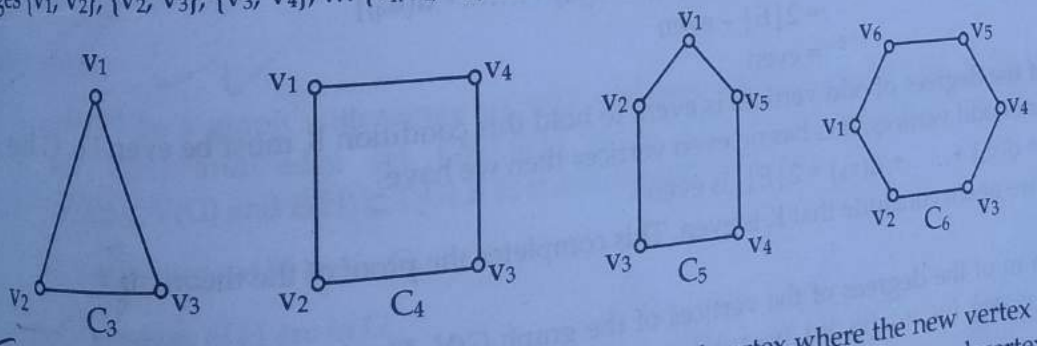
A bipartite graph G is said to be complete if each vertex of first bipartite set is connected to every vertices of another bipartite set. A complete bipartite graph with m number of vertices in first bipartite set and n number of vertices in second bipartite set is denoted by $K_{m,n}$.



Cycle Graph

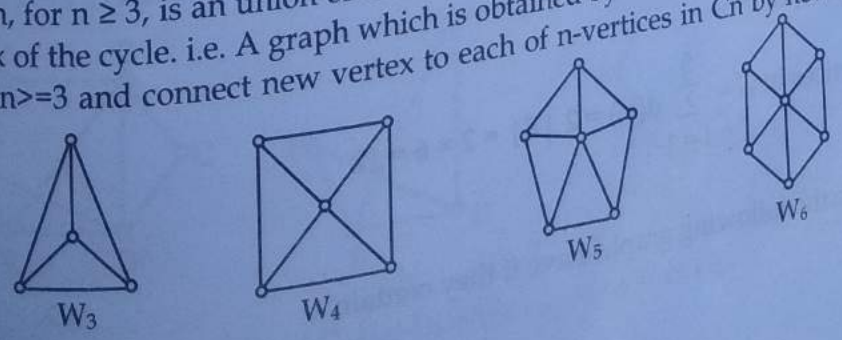
A Graph G = (V,E) with vertex n ≥ 3in which every vertex is connected with two other vertices one on either side of it and last vertex is connected with first one to form a closed path, is called cycle graph.

The cycle graph C_n of lengths n consists of n vertices $v_1, v_2, \ldots, v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \ldots \{v_{n-1}, v_n\}$ and $\{v_n, v_1\}$.



Wheel Graph

The wheel Wn, for n ≥ 3, is an union of Cn and additional vertex where the new vertex is connected by each vertex of the cycle. i.e. A graph which is obtained by adding an additional vertex to the cycle graph Cn for n>=3 and connect new vertex to each of n-vertices in Cn by new edge is called wheel graph.



n-cube graph

The n-dimensional cube, or n-cube denoted by Q_n, is the graph that has vertices representing the 2^n bit strings of length n. Here, two vertices are adjacent if and only if the bit string that they represent differ in exactly one bet-positions.

Example

What are Q_1, Q_2 and Q_3?

Fig. Q_1

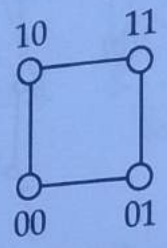


Fig. Q_2

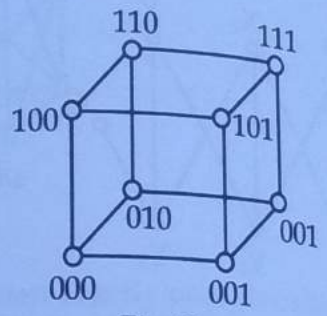


Fig. Q_3

Theorem: (The Handshaking theorem)

The sum of the degrees of the vertices of a graph is equal to twice the number of edges.

Proof: Consider a graph G = (V,E) with n vertices $v_1, v_2, \ldots\ldots v_n$ and $|E|$, the number of edges in G. Since each edge contributes a degree of 2, the sum of the degrees of all the vertices in G is twice the number of edges in G. That is $\sum_{i=1}^{n} d(v_i) = 2|E|$.

Theorem

The number of odd vertices in a graph is always even.

Proof:

Let G be a graph. If G contains no odd vertices, then the result follows immediately. Suppose that G contains K number of odd vertices which are $v_1, v_2, \ldots v_k$ and n number of even vertices which are $u_1, u_2, \ldots u_n$. Clearly, $d(u_1) + d(u_2) + \ldots + d(u_n)$ = even

By Handshaking theorem,

$$[d(v_1) + d(v_2) + \ldots + d(v_k)] + [d(u_1) + d(u_2) + \ldots + d(u_n) + \ldots + d(u_n)] = 2|E|.$$

Where $|E|$ is the total number of edges in G.

Then,

$$\begin{aligned} d(v_1) + d(v_2) + \ldots. + d(v_k) &= 2|E| - [d(u_1) + d(u_2) + \ldots\ldots + d(u_n)] \\ &= 2|E| - \text{even} \\ &= \text{even} \end{aligned}$$

Here, sum of the degrees of odd vertices is even, to hold this condition K must be even i.e. G has an even number of odd vertices. If G has no even vertices then we have

$$d(v_1) + d(v_2) + \ldots\ldots + d(v_k) = 2|E|, \text{ is even}$$

From which we again conclude that K is even. This completes the proof of the theorem.

Example

Find the sum m of the degrees of the vertices of the graph G(V, E) where $V(G) = \{v_1, v_2, v_3, v_4, v_5\}$ and $E(G) = \{(v_1, v_2), (v_1, v_4), (v_1, v_5), (v_2, v_5), (v_2, v_3), (v_3, v_4)\}$

Solution

Number of edges in G = $|E| = 6$

Sum of degrees of vertices in G = $\sum_{i=1}^{5} d(v_i) = 2\,|E| = 2 \times 6 = 12$

Example

How many vertices do the following graphs have if they contain

(a) 16 edges and all vertices of degree 2.

(b) 21 edges, 3 vertices of degree 4 and all other vertices of degree 3.

Solution

Let S be the sum of degrees of vertices, $|E|$ be the number of edges and n be the number of vertices in G. Then,

(a) $|E| = 16$, let there be n vertices of degrees 2.

Since $S = 2|E|$, then

Number of vertices × equal degree of each vertex $= 2|E|$

or $n \times 2 = 2 \times 16$

$\therefore\ n = 16$

(b) Since $S = 2|E|$, then

$3 \times 4 + (n-3) \times 3 = 2 \times 21$

or $12 + 3n - 9 = 42$

or $3n = 39$

$\therefore\ n = 13$

Example

Show that the maximum numbers of edges in a simple graph with n vertices is $\frac{1}{2}n(n-1)$.

Solution

By the handshaking theorem,

$$\sum_{i=1}^{n} d(v_i) = 2|E|$$

Where $|E|$ is the number of edges in G with n vertices.

Or $d(v_1) + d(v_2) + \ldots\ldots + d(v_n) = 2|E|$

Since maximum degree of each vertex in the graph G can be $(n-1)$, then

$(n-1) + (n-1) + \ldots\ldots$ to n terms $= 2|E|$

or $n(n-1) = 2|E|$

$\therefore\ |E| = \frac{1}{2}n(n-1)$.

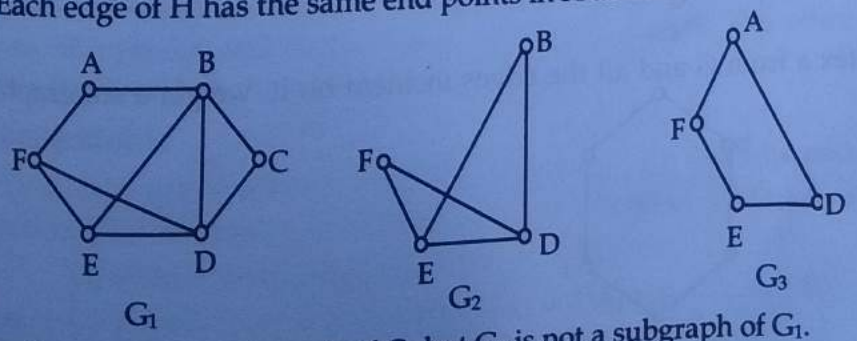
Subgraphs

Let $G = (V, E)$ be a graph with vertex set V(G) and edge set E(G) and $H = (V, E)$ be a graph with vertex set V(H) and edge set E(H).then H is said to be sub-graph of G written as $H \subseteq G$ if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$ If H is a sub-graph of G, then

(i) All the vertices of H are in G.

(ii) All the edges of H are in G.

(iii) Each edge of H has the same end points in H as in G.



In above figures G_2 is a subgraph of G_1 but G_3 is not a subgraph of G_1.

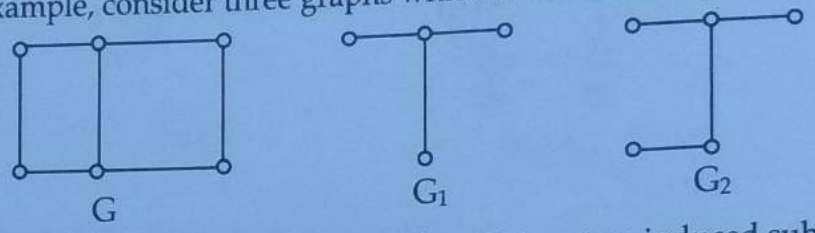
Spanning subgraph

The subgraph H of graph G is said to be spanning subgraph if V(H) = V(G). i.e. H and G has exactly same vertex set.

Induced sub-graph

If G is a graph with vertex set V and U is a subset of V, then the subgraph G(U) with the vertex set U and with edge set consisting of those edges of G that have both ends in U, is called the induced subgraph of G induced by the vertices in U.

For example, consider three graphs which are shown in figure below as



Here G_1 is an induced subgraph of G but G_2 is not an induced subgraph of G.

Vertex deleted sub-graph

Let G = (V,E) be a graph and S be a non empty subset of V. The induced subgraph denoted by G-S is a subgraph obtained by deleting vertices in S. In this method, two form a subgraph:

1) Remove all vertices from V (G) which are in S.

2) Remove all the edges which are incident on vertices in S.

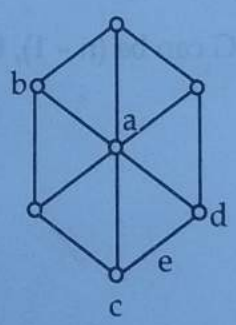
Edge deleted sub graph

If a subset F of E is deleted from G then G – F denotes the subgraph of G with vertex V and edge E-F, then G – F is called an edge deleted subgraph.

Example

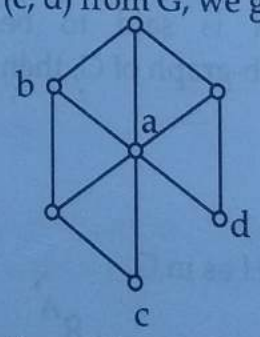
For the graph G shown below, draw the subgraphs

(a) G – e (b) G – a (c) G – b.

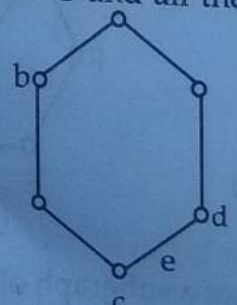


Solution

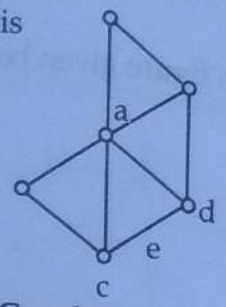
(a) After deleting the edge e = (c, d) from G, we get a subgraph G – e which is



(b) After deleting the vertex a from G and all the edges incident on it, we get a subgraph G – a which is



(c) The subgraph G – b is



Union and Intersection of Graphs

Union

Given two graphs G_1 and G_2, their union will be a graph such that

$$V(G_1 \cup G_2) = V(G_1) \cup V(G_2)$$

and $$E(G_1 \cup G_2) = E(G_1) \cup E(G_2)$$

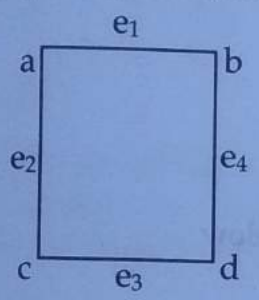
Intersections

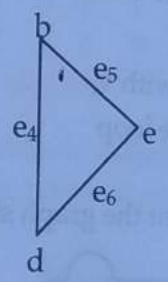
Given two graphs G_1 and G_2, their intersection will be a graph such that

$$V(G_1 \cap G_2) = V(G_1) \cap V(G_2)$$

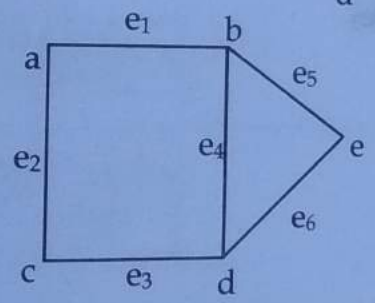
$$E(G_1 \cap G_2) = E(G_1) \cap E(G_2)$$

Consider two graphs G_1 and G_2 as

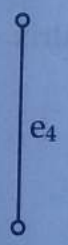




Then $G_1 \cup G_2$



and $G_1 \cap G_2$ is



Representation of Graph

Graph can be represented in many ways. One of the representation method of graph is Matrix representation, based on adjacency of vertices, called adjacency matrix and another is based on incidence of vertices and edges called incidence matrix. The other representation of graph is adjacency list, based on the list of adjacent vertices.

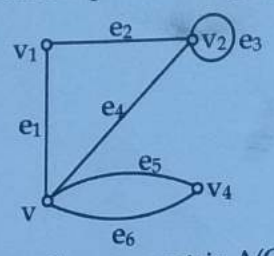
Adjacency Matrix

Let G=(V,E) be a graph with n vertices: $v_1, v_2, v_3, \ldots\ldots v_n$. The adjacency matrix of G with respect to given ordered list of vertices is a n×n matrix denoted by $A(G) = (a_{ij})_{n\times n}$ such that

$$a_{ij} = \begin{cases} 0 \text{ if there is no edge between the vertices } v_i \\ 1 \text{ if there is an edge between the vertices } v_i \\ K \text{ if there are } K(\geq 2) \text{ edges between the vertices } v_i \end{cases}$$

Example

Find the adjacency matrix to represent the graph shown in figure given below.



Solution

Since G has four vertices, adjacence matrix A(G) will be a 4 × 4 matrix.

$$A(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{bmatrix} \end{array}$$

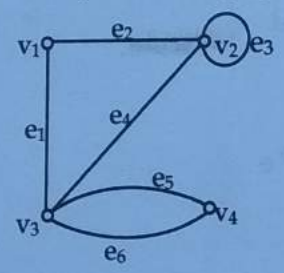
Incidence Matrix

Let G be a graph with vertices $v_1, v_2, \ldots, v_m$ and edges $e_1, e_2, \ldots e_n$. The incidence matrix I(G) of graph G is a m×n matrix with $I(G) = (m_{ij})_{m\times n}$, where

$$m_{ij} = \begin{cases} 1 \text{ if } e_j \text{ is incident with} \\ 0 \text{ if } e_j \text{ is not incident with } v_i \\ 2 \text{ if } v_i \text{ is the end of the loop} \end{cases}$$

Example

Find the incidence matrix to represent the graph shown in figure below



Solution

Since G ahs four vertices and six edges, incidence matrix I(G) will be a 4 × 6 matrix.

$$I(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

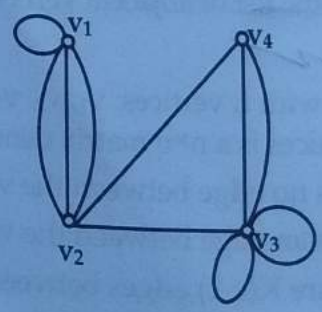
Example

Draw the graph G corresponding to the following adjacency matrix.

$$A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

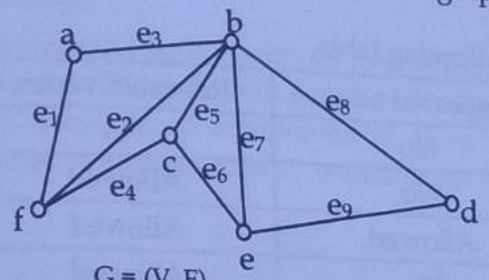
Solution

Since A is a 4 – square matrix, G has four vertices say v_1, v_2, v_3 and v_4. Then G is



Example

Find the adjacency matrix and incidence matrix of the graph given below.



G = (V, E)

Solution

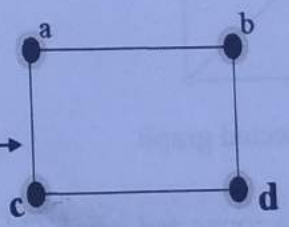
Let the order of the vertices be a, b, c, d, e, f and edges order be $e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9$

$$A(G) = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \end{array} \quad I(G) = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{ccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Adjacency List

One of the ways of representing a graph without multiple edges is by listing its edges. This type of representation is suitable for the undirected graphs without multiple edges, and directed graphs. This representation looks as in the tables below.

Edge List for Simple Graph	
vertex	Adjacent Vertices
a	b,c
b	a,d
c	a,d
d	b,c



Graph Connectivity

Walk

A walk in a graph G is a finite ordered set $W = (v_0, e_1, v_1, e_2, v_2, \ldots v_{k-1}, e_k, v_k)$ whose elements are alternately vertices and edges such that $1 \le i \le k$, the edge e_i has ends v_{i-1} and v_i.

This walk W is a $V_0 - V_K$ walk or walk from V_0 to V_K. The number of edges appearing in the sequence of the path is called its length. If the length of the walk is zero i.e. the walk has no edges, it contains only a single vertex and is called a trivial walk. A walk is closed if it starts and ends at the same point, otherwise the walk is open.

Trail

A walk W(U, V) in which all the edges are distinct, is called a trail.

Path

A walk in which all the vertices and edges are distinct, is called a path.

Circuit

A closed trail which contains at least three edges is called a circuit.

Cycle

A circuit which does not repeat any vertices (except the initial and final vertex) is called a cycle. Thus, a cycle is a non-intersecting circuit and must have length three or more. A cycle of length K is

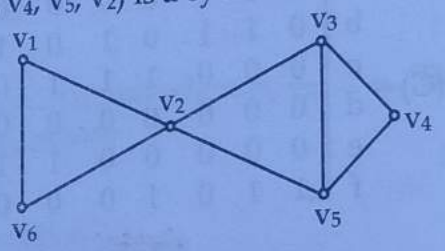
called K-cycle. It should be noted that while every cycle is a circuit, the converse is not always true. A circuit may have repeated vertices other then the end vertices, but in a cycle the only repeated vertices are the first and last.

These definitions are summarized in the following table.

Term	Repeated edge	Repeated vertex
Path	No	No
Trail	No	Allowed
Walk	Allowed	Allowed
Circuit	No	Allowed
Cycle	No	First and last only

Example

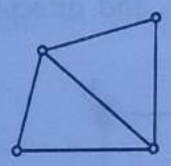
Consider the graph G in figure below, the closed trail ($v_1, v_2, v_3, v_4, v_5, v_2, v_6, v_1$) is a circuit but not a cycle, while the closed trail (v_2, v_3, v_4, v_5, v_2) is a cycle as well as a circuit.



Connected graph

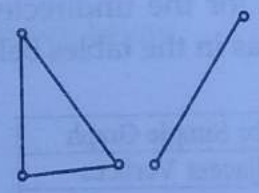
A graph G is said to be connected if there is a path between each possible pair of its vertices; otherwise G is disconnected.

(i)



Connected graph

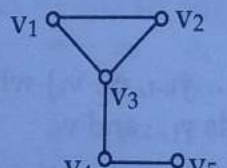
(ii)



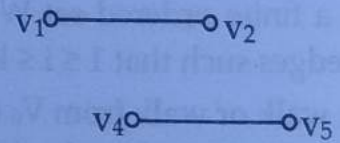
Disconnected graph

Cut-vertex

A vertex v of a connected graph G is called a cut-vertex (or cut-point) if G – v is disconnected. Any vertex in a graph is said to be cut vertex if graph becomes disconnected after removal of this vertex form the graph.



G = (V, E)

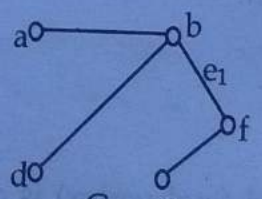


G – v_3

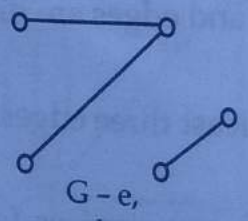
In above figure, after removable of vertex v_3, graph G becomes disconnected. So, v_3 is cut-vertex. Similarly, vertex v_4 also.

Cut-edge or bridge

Any edge in graph after whose removal graphs becomes disconnected, is called bridge or cut edge. An edge e is a bridge for G if G – e is disconnected.



G



G – e,
where e = (b, f)

In above figure, after removable of an edge e = {b, f}, the connected graph G becomes disconnected. So, e = {b, f} is cut-edge.

Connected Component

A graph that is not connected is the union of two or more connected subgraphs, each pair of which has no vertex in common. These disjoint connected subgraphs are called the connected components of G. In other word, a connected component H of an undirected graph G is maximal connected subgraph. By 'maximal' we mean that G contains no other subgraph that is both connected and properly contains H.

Theorem 4:

There is a simple path between every pair of distinct vertices of a connected undirected graph.

Proof:

Suppose a and b are two distinct vertices of the connected undirected graph G = (V, E). we know that G is connected so by definition there is at least one path between a and b. Let $x_0, x_1, \ldots, x_n$, where $x_0 = a$ and $x_n = b$, be the vertex sequence of a path of a least length. Now if this path of the least length is not simple then we have $x_i = x_j$, for some i and j with $0 \le i < j$. This implies that there is a path from a to b of shorter length with the vertex sequence $x_0, x_1, \ldots, x_i, \ldots, x_{j+1}, \ldots, x_n$ obtained by removing the edges corresponding to the vertex sequence $x_{i+1}, \ldots, x_j$. This shows that there is a simple path.

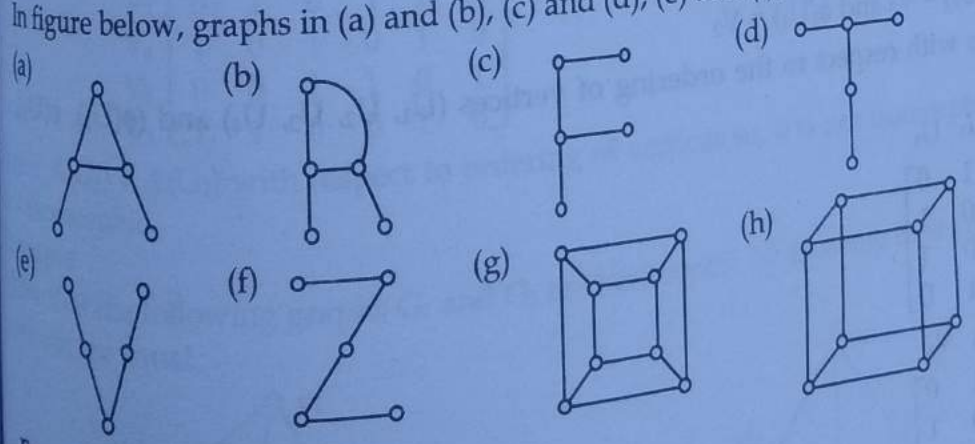
Isomorphism of Graphs

Two graphs $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ are isomorphic if there exists a bijective mapping ϕ between $V_1(G_1)$ and $V_2(G_2)$ such that {u, v} is in E_1 if and only if $\{\phi(u), \phi(v)\}$ is in E_2. The function ϕ is called isomorphism.

if two graph G_1 and G_2 are isomorphic then they must have:

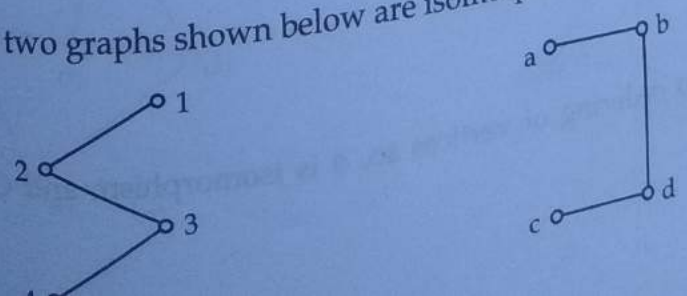
i. same number of vertices i.e. $|V_1| = |V_2|$
ii. same number of edges i.e. $|E_1| = |E_2|$
iii. if {u,v} in E_1 ->$\{\phi(u), \phi(v)\}$ in E_2
iv. if deg(u)=k in G_1 then $\deg(\phi(u)) = k$ in G_2
v. $A(G_1)=A(G_2)$ with respect to orders of vertices $v_1, v_2, v_3, \ldots v_n$ and $\phi(v_1), \phi(v_2), \phi(v_3), \ldots\ldots$ $\phi(v_n)$.

In figure below, graphs in (a) and (b), (c) and (d), (e) and (f), and (g) and (h) are isomorphic graphs.



Example

Show that the two graphs shown below are isomorphic



Solution

Here,

$V(G_1) = \{1, 2, 3, 4\}$, $V(G_2) = \{a, b, c, d\}$

$E(G_1) = \{(1, 2), (2, 3), (3, 4)\}$

$E(G_2) = \{(a, b), (b, d), (c, d)\}$

Define a function $f: V(G_1) \to V(G_2)$ as

$f(1) = a$, $f(2) = b$, $f(3) = d$, $f(4) = c$

Then f is one-to-one onto and

$(1, 2) \in E(G_1)$ and $\{f(1), f(2)\} = (a, b) \in E(G_2)$.

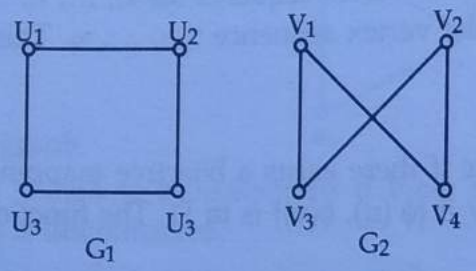
$(2, 3) \in E(G_1)$ and $\{f(2), f(3)\} = (b, d) \in E(G_2)$.

$(3, 4) \in E(G_1)$ and $\{f(3), f(4)\} = (d, c) \in E(G_2)$.

Thus G_1 and G_2 are isomorphic.

Example

Show that the graphs G_1 and G_2 are isomorphic.



Solution

The isomorphic invariants for two graphs are:

No. of vertices in G_1 $|V(G_1)| = 4$

No. of edges in G_1 $|E(G_1)| = 4$

No. of vertices in G_2 $|V(G_2)| = 4$

No. of edges in G_2 $|E(G_2)| = 4$

In graph G_1, there are four vertices each of degree 2 i.e. (2, 2, 2, 2) similar is true in graph G_2 also.

Since both graphs agree so many isomorphic invariants so, it is reasonable to find an isomorphison ϕ.

Let $\phi: V(G_1) \to V(G_2)$ defined by

$\phi(U_1) = V_1$, $\phi(U_2) = V_4$, $\phi(U_3) = V_3$ and $\phi(U_4) = V_2$

Now, adjacency matrices with respect to the ordering of vertices (U_1, U_2, U_3, U_4) and $(\phi(U_1), \phi(U_2), \phi(U_3), \phi(U_4))$ are

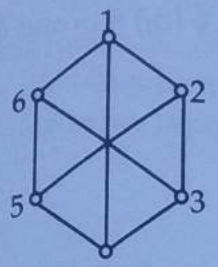
$$A(G_1) = \begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array} \begin{array}{c} \begin{array}{cccc} U_1 & U_2 & U_3 & U_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$$A(G_2) = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \end{array} \begin{array}{c} \begin{array}{cccc} V_1 & V_2 & V_3 & V_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

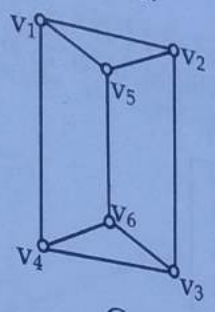
Since: $A(G_1) = A(G_2)$ with respect to ordering of vertices so, ϕ is isomorphism and G_1 and G_2 are isomorphic.

Example

Show that graphs G_1 and G_2 given below are not isomorphic.



G_1



G_2

Solution

The isomorphic invariants of two graphs are

$|V(G_1)| = |V(G_2| = 6$

$|E(G_1)| = |E(G_2)| = 9$

Degree sequence of G_1: (3, 3, 3, 3, 3, 3)

Degree sequence of G_2: (3, 3, 3, 3, 3, 3)

Since both graphs agree so many invariants so, it is reasonable to find an isomorphism ϕ.

Let $\phi : V(G_1) \to V(G_2)$ defined by

$\phi(1) = V_1, \phi(2) = V_2, \phi(3) = V_3, \phi(4) = V_4, \phi(5) = V_6, \phi(6) = V_5$

Now,

Adjacency matrices with respect to ordering of vertices in ϕ are

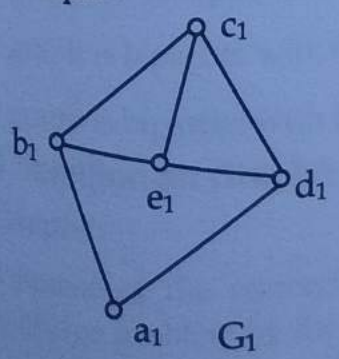
$$A(G_1) = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

$$A(G_2) = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_6 \\ V_5 \end{array} \begin{array}{c} \begin{array}{cccccc} V_1 & V_2 & V_3 & V_4 & V_6 & V_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

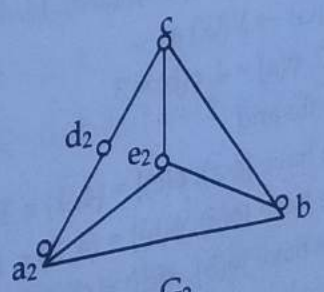
Since: $A(G_1) \neq A(G_2)$ with respect to ordering of vertices so, ϕ is not isomorphism and G_1 and G_2 are not isomorphic.

Example

Show that the following graphs G_1 and G_2 are isomorphic by showing their corresponding adjacency matrices are equal.



G_1



G_2

Solution

Consider the map $\phi: G_1 \to G_2$ defined as $\phi(a_1) = d_2$, $\phi(b_1) = a_2$, $\phi(c_1) = b_2$, $\phi(d_1) = c_2$ and $\phi(e_1) = e_2$. The adjacency matrix of G_1 for the ordering a_1, b_1, c_1, d_1 and e_1 is

$$A(G_1) = \begin{array}{c} \\ a_1 \\ b_1 \\ c_1 \\ d_1 \\ e_1 \end{array} \begin{array}{c} \begin{array}{ccccc} a_1 & b_1 & c_1 & d_1 & e_1 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

The adjacency matrix of G_2 for the ordering d_2, a_2, b_2, c_2 and e_2 is;

$$A(G_2) = \begin{array}{c} \\ d_2 \\ a_2 \\ b_2 \\ c_2 \\ e_2 \end{array} \begin{array}{c} \begin{array}{ccccc} d_2 & a_2 & b_2 & c_2 & e_2 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

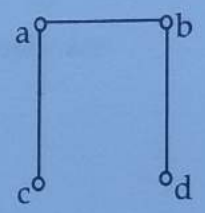
$\therefore$ G_1 and G_2 are isomorphic.

Self-complementary Graph

A graph $G = (V, E)$ is said to be self-complementary if G is isomorphic to its complement graph.

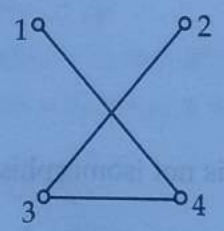
Example

Show that the following graph is self-complementary.



Solution

As we know, a graph is self-complementary if it is isomorphic to its complement, we now find a complement G' of the graph G(given)



Here $V(G) = \{a, b, c, d\}$, $E(G) = \{a, b\}, \{a, c\}, \{b, d\}$

$V(G') = \{1, 2, 3, 4\}$, $E(G') = \{(1, 4), (2, 3), (3, 4)\}$

Define a function $\phi: V(G) \to V(G')$ as

$\phi(c) = 1$, $\phi(d) = 2$, $\phi(a) = 4$, $\phi(b) = 3$

Then ϕ is one-to-one onto and

$(a, c) \in E(G)$ we have $\{\phi(a), \phi(c)\} = (4, 1) \in E(G')$.

$(a, b) \in E(G)$ we have $\{\phi(a), \phi(b)\} = (4, 3) \in E(G')$.

$(b, d) \in E(G)$ we have $\{\phi(b), \phi(d)\} = (3, 2) \in E(G')$.

Since G is isomorphic to its complement G', it is self complementary.

Application of Graph on Local Area Network

In a local area network, there are many computer connected to each other, which form a special geometrical structure, called network topology. To model local area network in the form of topology, graph can be used-in-which computers or devices are represented by vertices and connections between these device are represented by edges.

For example:

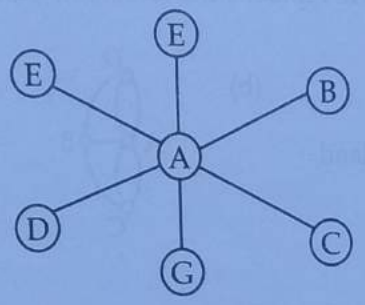


Fig: Stont network.

This topology can be modelled using complete bipontite graph $k_{1,6}$.

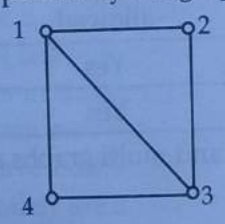
Platonic Graph

The graph formed by the vertices and edges of five regular (platonic) solids - the tetrahedron, octahedron, cube, dodecahedron and icosahedron are called the platonic graphs.

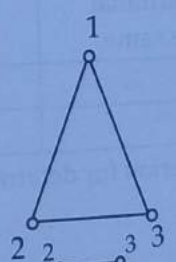
Example

Determine whether or not each of the following graphs is bipartite. In each case, give the partition sets or explain why the graph is not bipartite.

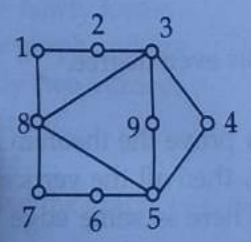
(a)



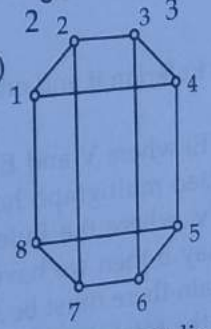
(b)



(c)



(d)



Solution

(a) In this triangle, at least two of the three vertices must lie in one of the bipartite sets and these two are joined by an edge. Hence this graph can not be bipartite.

(b) The graph is not bipartite because it contains two triangles.

(c) The graph is bipartite with the partition sets M = {1, 3, 5, 7} and N = {2, 4, 6, 8, 9}.

(d) The graph is bipartite with the partition sets M = {1, 3, 5, 7} and N = {2, 4, 6, 8}.

Euler and Hamiltonian Graphs

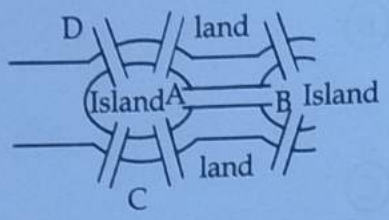
Eulerian Graphs

The development of the concept of the Eulerian graph is due to the solution of the famous Konigsberg bridge problem by the Swiss Mathematician Leonard Euler (1707 - 1783) in 1736.

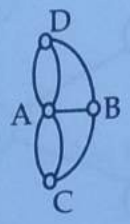
The Konigsberg Bridge Problem

The eighteen century city of Konigsberg included two islands and seven bridges crossing the Pregel river with land areas, denoted by A, B, C and D as shown in figure (a). It was asked whether it would be possible to walk around the city by crossing each of the bridges, exactly once. Euler proved in 1736 that such a walk is impossible. He replaced the land areas and islands by points and the bridges by curves, as shown in figure (b).

(a)



(b)



Eulerian Trail

A trail in a graph G is called an Eulerial trail if it includes every edge of G and then G is called a traversable graph.

Eulerian Circuit

A circuit (closed trail) containing all the edges of a graph G is called an Eulerian circuit.

Eulerian Graph

A graph containing an Eulerian circuit is called an Eulerian graph or simply Eulerian.

We summarize the above definitions using a table as

Term	Initial and terminal vertices the same	Must include every edge	Repeated vertices allowed
Eulerian circuit	Yes	Yes	Yes
Eulerian Trail	No	Yes	Yes

The following two theorems give a criterion for determining which graphs and multi graphs are Eulerian.

Theorem

A connected graph (multi graph) G is Eulerian if and only if each vertex has even degree.

Proof:

Take a connected multigraph G =(V, E) where V and E are finite. We can prove the theorem in two parts. First we prove that if a connected multigraph has an Euler circuit, then all the vertices have even degree. For this, take a vertex v, where the Euler circuit begins. There is some edge that is incident to v and some other vertex say u then we have an edge {v, u}. This edge {v, u} contributes one to the degree of v and u both. Again there must be some edge other than {v,u} that is incident to u and some other vertex. In this case the total degree of the vertex u becomes even, so whenever in the circuit the vertex is met the degree of that vertex is even since every time entering and leaving the vertex gives even degree to all the vertices other than the initial vertex. However since the circuit must terminate in the vertex v and the edge that is terminating the circuit contributes one to the degree of the initial vertex v the total degree of the vertex v is also even. Now we have every time the vertex is entered and left it gives even degree and the initial vertex also gives even degree, we can conclude that if a graph has Euler circuit, then all the vertices have even degree.

Now we try to prove that if all the vertices in the connected multigraph have even degree, then there exist Euler circuit. For this, take a connected multigraph G with all the vertices having even degree. To make a circuit start at arbitrary vertex, say a of G. now start from the vertex a = x_0 and arbitrarily choose other vertex x1 to form and edge $\{x_0, x_1\}$. Continue building the simple path $\{x_0, x1\}$, $\{x_1, x_2\}$, ..., $\{x_{n-1}, x_n\}$. This path terminates since it has a finite number of edges. It begins at a with an edge {a, x} and terminate at a with some edge {y, a}. This is correct since every vertex has even degree in the

graph we are considering, if an edge left some vertex then there must be an edge entering that vertex to make its degree even. Now we have shown that there exists simple circuit in the graph with all the vertices of even degree. If this circuit has all the edges of the graph in it, then the simple circuit is itself an Euler circuit. If all the edges are not in the circuit, then we have next possibility. Now, consider the subgraph, say H that is formed by removing all the edges that are already in the simple circuit formed above and by removing the isolated vertices after edges are removed. Since the original graph G is connected, there must be at least one vertex of H that is common with the circuit we have formed. Let w be such a vertex. Every vertex in H has even degree since it is a subgraph of original graph. In case of w, while forming the circuit pairs of incident edges are used up. So the degree of w is again even. Beginning at w we can build a simple circuit as described above. We can continue this process until all edges have been used. Now if we combine the formed circuit in a way that it makes use of common vertex to make a circuit then we can say that the circuit is an Euler circuit. Hence if every vertices of a connected graph has an even degree then it has an Euler circuit.

Theorem

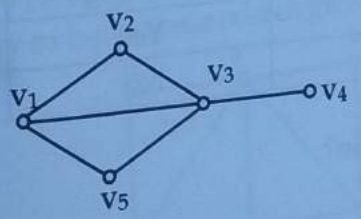
A connected graph G has an Eulerian trail if and only if it has exactly two odd vertices.

Proof:

This fact can be proved if we can prove that first, if the connected multigraph has Euler path exactly two vertices have odd degree and second if the connected multigraph has exactly two vertices of odd degree, then it has Euler path. Now, if the graph (in this proof graph means connected multigraph) has an Euler path say from a to z but not Euler circuit, then it must pass through every edge exactly once. In this scenario the first edge in the path contributes one to the degree of vertex a, and at all other time when other edges pass through vertex a it contributes twice to the degree of a, hence we can say that degree of a is odd. Similarly the last edge in the path coming to z contributes one to the degree of z, all the other edges contributes two one for entering and one for leaving. Here also the degree of last vertex, z is odd. All the other vertices other than a and z must have even degree since the edges in those vertices enter and leave the vertex contributing two to the degree every time the vertices are met. Hence if there is an Euler path but not an Euler circuit, exactly two vertices of the graph have odd degree. Secondly, if exactly two vertices of a graph have odd degree and lets consider they are a and z. Now, consider another graph that adds an edge {a, z} to the original graph, then the newly formed graph will have every vertices of even degree. So there exists Euler circuit in the new graph and the removal of the new edge gives us the Euler path in the original graph. Hence if exactly two vertices of the graph have an odd degree, then the graph has an Euler path but not Euler circuit.

Example

Show that the graph in figure contains an Eulerian trail but no Eulerian circuit.



Solution

Here,

G is connected and

Deg (V1) = 3, deg (V3) = 4

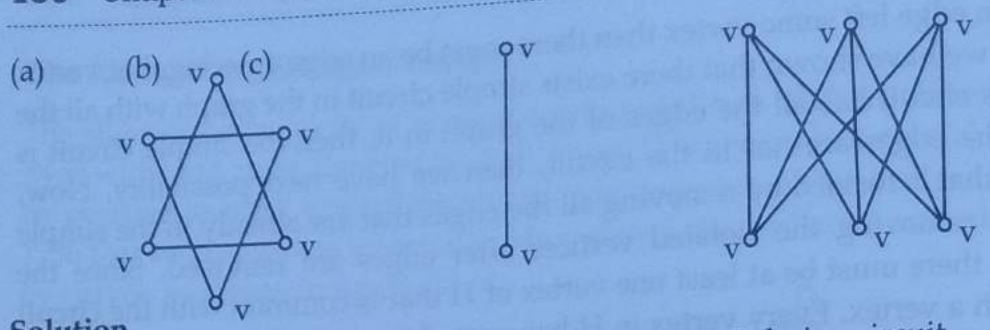
Deg (V2) = deg(V5) = 2

and deg(V4) = 1

Since the graph G has exactly two odd vertices, it contains an Eulerian trail but no Eulerian circuit.

Example

Show that the graphs in figure contain no Eulerian circuit.



Solution

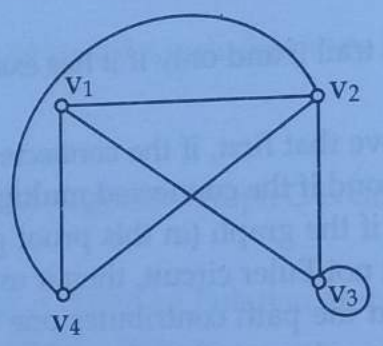
(a) It is not connected, so it does not contain an Eulerian circuit.

(b) It is connected but each degree is odd, so it does not contain an Eulerian circuit.

(c) It is connected but each degree is odd, so it does not contain an Eulerian circuit.

Example

Show the graph shown in figure has no Eulerian circuit but has an Eulerian trail.



Solution

G is connected and

deg(V1) = deg(A4) = 3 and

deg(V2) = deg(V3) = 4

Since it has exactly two odd vertices, it has an Eulerian trail but no Eulerian circuit. Where Eulerian trail can be described as (V1, V2, V4, V1, V3, V3, V2, V4).

Hamiltonian Graphs

Hamiltonian graphs are named after sir Willian Hamilton, an Irish mathematician who introduced the problem of finding a circuit in which all the vertices of a graph appear exactly once.

A cycle that contains every vertex of a graph G exactly once is called Hamiltonian cycle (Hamiltonian circuit).

A graph G is Hamiltonian of it has a Hamiltonian cycle.

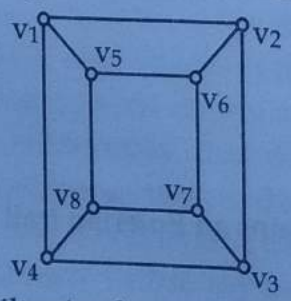
A Hamiltonian path is a simple path that contains all vertices of G.

Now, we summarize two basic concepts of this chapter in the following table:

Term	Initial and terminal vertices the same	Must include every edge	Repeated vertices followed
Eulerian circuit	Yes	Yes	Yes
Hamiltonian cycle	Yes	No	No

Example

Is the graph (cube) given in figure is Hamiltonian?



Solution

The graph in figure is Hamiltonian because it contains a cycle covering all the vertices, is (v5, v1, v2, v6, v7, v3, v4, v8, v5).

Theorem (without proof)

A simple connected graph with $n > 2$ vertices is Hamiltonian if degree of every vertex is at least $n/2$.

(This theorem is known as Dirac's Theorem)

Theorem (without proof)

A connected graph with n vertices is Hamiltonian if for any two non-adjacent vertices u and v, $\deg(u) + \deg(v) \geq n$.

(This theorem is known as Ore's Theorem).

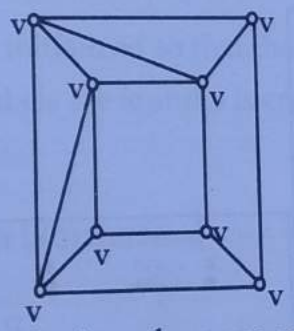
It may be noted that the theorems stated above provide only sufficient criterion. There are no known simple necessary and sufficient criteria for the existence of Hamiltonian cycle nor is there even an efficient algorithm. For finding such a cycle many theorems exist that establish either necessary or sufficient conditions for a connected graph to have Hamiltonian cycle or path.

A few helpful hints for trying to find a Hamiltonian cycle in a graph are given below.

1. If G has a Hamiltonian cycle, then for all $u \in V$, $\deg(u) \geq 2$.
2. If $v \in V$ and $\deg(v) = 2$ then two edges incident with vertex v must appear in every Hamiltonian circuit for G.
3. If $v \in V$ and $\deg(v) > 2$, then we try to build a Hamiltonian cycle, once we pass through vertex v, any unused edges incident with v are deleted from further consideration.
4. In building a Hamiltonian circuit for G, we cannot obtain a circuit for a subgraph of G unless it contains all the vertices of G.

Example

Determine, in graph of figure, if there is an Eulerian circuit and/or a Hamiltonian cycle.



Solution

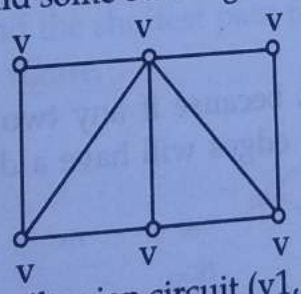
Clearly there is no Eulerian circuit since there are some odd vertices, but the graph has Hamiltonian cycle (v1, v2, v4, v6, v8, v7, v5, v3, v1).

Example

Give an example of a graph with six vertices which is Hamiltonian but not Eulerian and vice-versa.

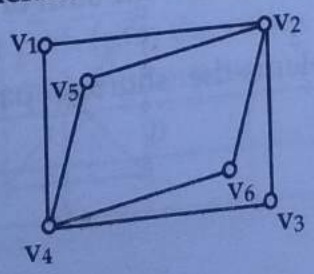
Solution

Here, we need to be very clever since for a graph to not be Eulerian means that not all the vertices are of even degree. So we try to build some odd degrees in that graph as shown in figure.



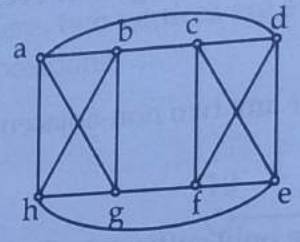
The graph above contains a Hamiltonian circuit (v1, v2, v3, v4, v5, v6, v1) but no Eulerian circuit.

The graph shown in figure is Eulerian but not Hamiltonian.



Example

Is the graph in figure is Hamiltonian?



Solution

The graph shown in figure above is Hamiltonian (by Dirac's theorem) because it has 8 vertices such that each vertex has degree $\frac{8}{2} = 4$. So the Hamiltonian cycle (circuit) is (a, b, g, h, e, f, c, d, a).

A matching graph is a subgraph of a graph where there are no edges adjacent to each other. Simply, there should not be any common vertex between any two edges.

Matching

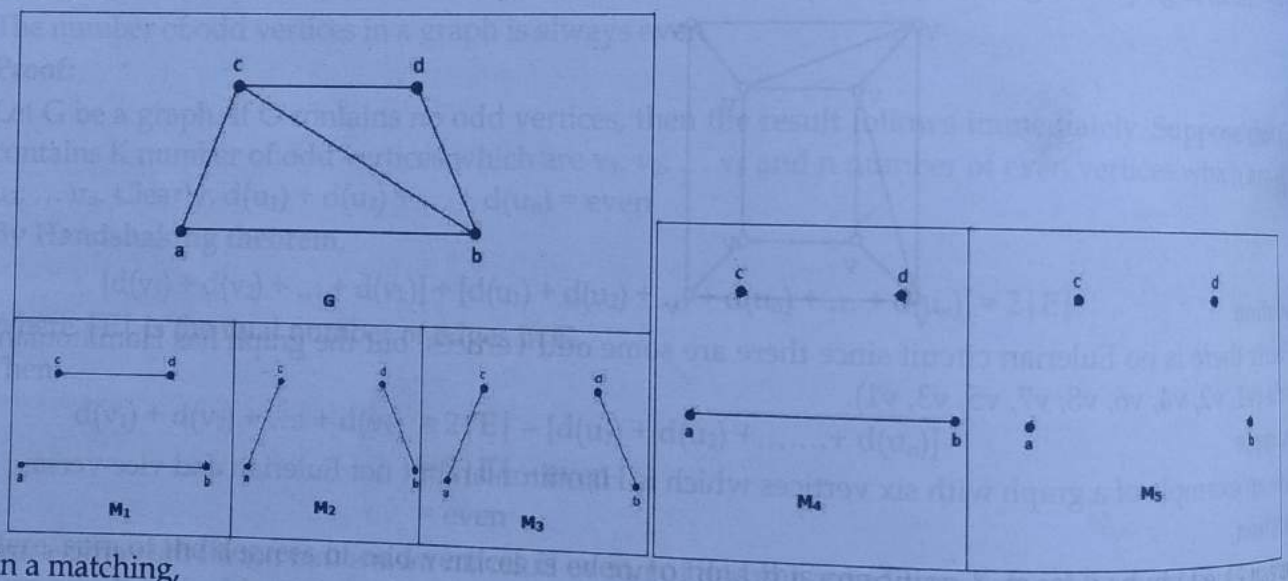
Let 'G' = (V, E) be a graph. A subgraph is called a matching M(G), if each vertex of G is incident with at most one edge in M, i.e.,

$\deg(V) \leq 1 \ \forall \ V \in G$

which means in the matching graph M(G), the vertices should have a degree of 1 or 0, where the edges should be incident from the graph G.

Notation – M(G)

Example



In a matching,

if deg(V) = 1, then (V) is said to be matched

if deg(V) = 0, then (V) is not matched.

In a matching, no two edges are adjacent. It is because if any two edges are adjacent, then the degree of the vertex which is joining those two edges will have a degree of 2 which violates the matching rule.

Weighted Graph or Labelled Graph

A weighted graph is a graph G, in which each edge, e, is assigned a non-negative real number, w(e), called the weight of e. The weight of a subgraph H of G is the sum of the weights of the edges of the subgraph H.

Now we discuss two famous network problems-the shortest path problem and the Chinese postman problem.

The Shortest Path Algorithm

Consider a weighted graph G. The length of a path in a weighted graph is the sum of the weights of the edges of this path and the shortest path between the two vertices is the minimum length of the path. There are several different algorithms to find the shortest path between two vertices in a weighted graph. We discuss here one discovered by E.W. Dijkstra.

Dijkstra's Algorithm

Step 1 : Label the initial vertex of the graph with weight zero.

Step 2 : Calculate the weights of all vertices adjacent to the initial vertex corresponding to the weights of the edges incident on the initial vertex.

Step 3 : Label these vertices with smallest possible value of their weights.

Step 4 : Calculate the weights of all those vertices which are adjacent to the vertices with minimum weights determined in step 3.

Step 5 : Label these vertices with minimum weight.

Step 6 : Continue this process until all the vertices of weighted graph are labeled.

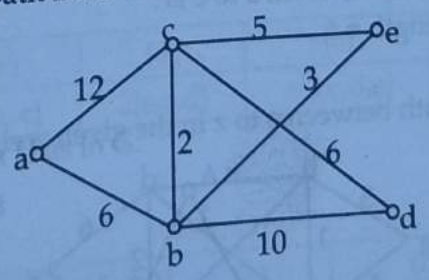
Step 7 : Trace the path of cumulative minimum weight from the initial vertex to desire vertex.

Pseudo code for Dijkstra's algorithm

```
DijkstraSP(G: Weighted connected simple graph with all weights positive)
{
    for i=1 to n
        L(vi)=∞
    L(a)=0
    S=ϕ //the labels are now initialized so that the label of a is 0
                and all other labels are ∞ and S is empty set}
    while Z ∉ S
    begin
        u=a vertex not in S with L(u) minimal
        S=SU{u}
        for all vertices v not in S
        if L(u)+w(u,v)<L(v) then L(v)=L(u)+w(u,v)
    // this ads a vertex          in S with minimal label and updates the label of    vertices not in
S
    end // L(z)=length of a shortest path from a to z.
}
```

Example

Apply Dijkstra's algorithm to find the shortest path from the vertex a to each of the other vertices of the following weighted graph in figure.



Solution

Since we have to find the shortest path from the vertex a to each of the other vertices, then we assign weight 0 to vertex a and ∞ to all remaining vertices.

Vertex	(a)	b	c	d	e
Label	0	∞	∞	∞	∞

Now, The vertices adjacent a are b & c, we ... them with minimum weight.

wt (b) = wt (a) + wt (a,b), = 0 + 6 = 6

wt (c) = wt (a) + wt (a,c) = 0 + 1 = 1

Since, c has minimum weight so, we select it

Vertex	(a)	b	c	d	e
Label	0	6	1	∞	∞

Now the vertices adjacent to c are b, e & d

wt (b) = wt (c) + wt (c,b) = 1+2 = 3

wt (e) = wt (c) + wt(c,e) = 1+5 = 6

wt (d) = wt (c) + wt(c,d) = 1+6 = 7

Since, b has smallest weight we select it & replace previous wt of b by new weight.

Vertex	(a)	(b)	(c)	d	e
Label	0	3	1	7	6

Now, the vertices adjacent 'b' are 'e' and 'd'

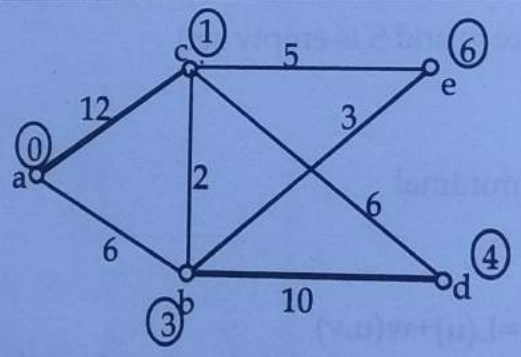
So,

wt (e) = wt (b) + wt(b,e) = 3+3 = 6

wt (d) = wt(b) + wt(b,d) = 3+1 = 4

Since, 'd' has minimum weight so, we select 'd' and replace it's pervious weight by new.

Vertex	(a)	(b)	(c)	(d)	(e)
Label	0	3	1	4	6



∴ The shortest path from a to c is a – c length = 1

The shortest path from a to b is :

a – c – b, length = 3

The length of shortest path from a to d is :

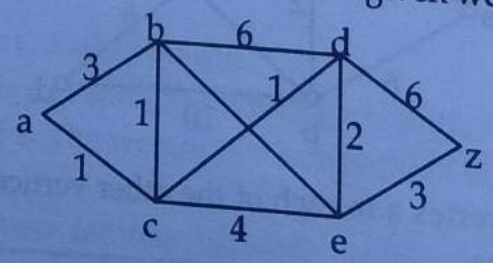
a – c – b – d length = 4

The length of shortest path from a to e is :

a – c – e length = 6

Example

Find the shortest path between a to z in the given weighted graphs.



Solution

Since we have to find the shortest path from vertex a to z. So, we assign weight 0 to a and ∞ t remaining vertices.

Vertex	(a)	b	c	d	e	z
Label	0	∞	∞	∞	∞	∞

The vertices adjacent to a are b and c, we calculate weights of b and c and label them with minimum weight.

$wt(b) = \min(wt(b), wt(a) + wt(a, b))$
$= \min(\infty, 0 + 3) = \min(\infty, 3) = 3$

$wt(c) = \min(wt(c), wt(a) + w + (a, c))$
$= \min(\infty, 0 + 1) = \min(\infty, 1) = 1$

Since c has minimum weight so we select it

Vertex	(a)	b	(c)	d	e	z
Label	0	3	1{a, c}	∞	∞	∞

The vertices adjacent to c are b, d, and e

$\therefore$ $wt(b) = \min(wt(b), wt(c) + wt(c, b))$
$= \min(3, 1 + 1) = \min(3, 2) = 2$

$wt(d) = \min(wt(d), wt(c) + t(c, d))$
$= \min(\infty, 1 + 1) = \min(\infty, 2) = 2$

$wt(e) = \min(wt(e), wt(c) + wt(c, e))$
$= \min(\infty, 1 + 4) = \min(\infty, 5) = 5$

Since b and d has equal wt so we randomly select b.

Vertex	(a)	(b)	(c)	d	e	z
Label	0	2{a,c,b}	1{a, c}	2	5	∞

The vertex adj. to b still unmarked is d.

So, $wt(d) = \min(wt(d), wt(b) + wt(b, d))$
$= \min(2, 2 + 6) = \min(2, 8) = 2$

Now we select d

Vertex	(a)	(b)	(c)	(d)	e	z
Label	0	2{a,c,b}	1{a, c}	2{a,c,d}	5	∞

The vertices adj. to d still unmarked are: e & z

$\therefore$ $wt(e) = \min(wt(e), wt(d) + wt(d, e))$
$= \min(5, 2 + 2) = \min(5, 4) = 4$

$wt(z) = \min(wt(z), wt(d) + wt(d, z))$
$= \min(\infty, 2 + 6) = \min(\infty, 8) = 8$

Since e has minimum weight so we select it.

Vertex	(a)	(b)	(c)	(d)	(e)	z
Label	0	2(a,c,b}	1{a, c}	2{a,c,d}	4{a,c,d,e}	8

The vertex adjacent to e is z

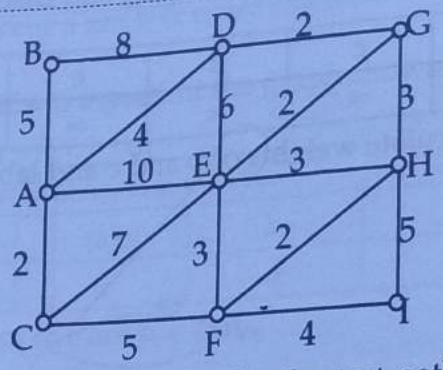
So, $wt(z) = \min(wt(z), wt(e) + wt(e, z))$
$= \min(8, 4 + 3) = \min(8, 7) = 7$

Vertex	(a)	(b)	(c)	(d)	(e)	(z)
Label	0	2{a,c,b}	1{a,c}	2{a,c,d}	4{a,c,d,e}	7{a,c,d,e,z}

$\therefore$ Shortest path from a to z is a - c - d - e - z and weight is 7.

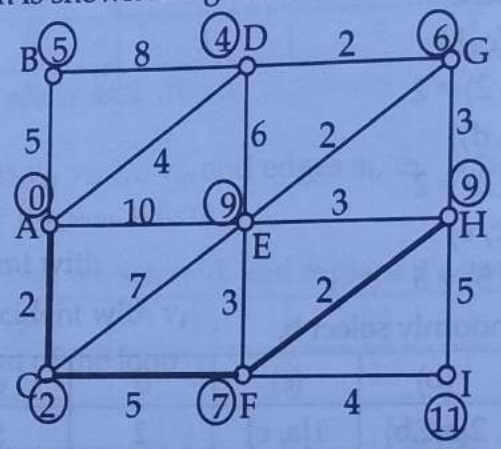
Example

Apply Dijkstra's Algorithm to find the shortest path from the vertex A to the vertex H in figure.



Solution

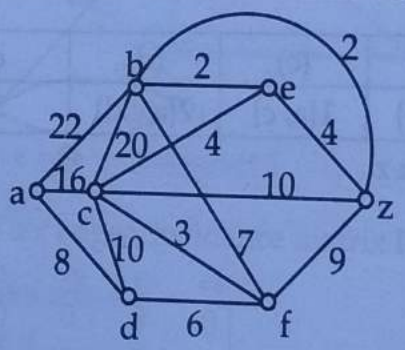
In the graph of figure, we have to find the shortest path from the vertex A to H, so we label initial vertex A with weight zero. Then we calculate the weights of all vertices adjacent to the vertex A and label them with minimum weight. We continue this process until all the vertices of the graph are labelled with minimum weight and then we trace the shortest path of cumulative minimum weight from the vertex A to H, which is shown in figure below.



The length of the shortest path is 9 and the shortest path is (A, C, F, H).

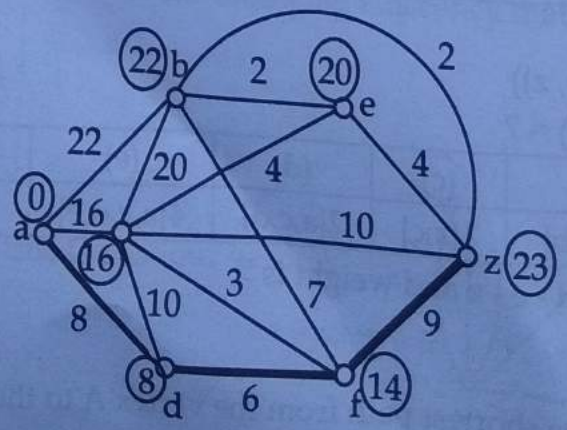
Example

Determine the shortest path from the vertex a to z in the graph of figure below by using Dijkstra's algorithm.



Solution

To find the shortest path from the vertex a to z, we label the vertex a with zero. Then we calculate the weights of all adjacent vertices to the vertex a and label them with minimum weight. We continue this process until all the vertices are labeled with minimum weight. Then we find the shortest path from the vertex a to z, is shown in figure below.



Example

The complete graph K_n is Hamiltonian for all $n > 2$.

Solution

Dirac's theorem tells us that a connected graph with n(>2) vertices is Hamiltonian if $d(v) \geq \frac{n}{2}$, for every vertex in G.

Since K_n is a complete graph with n(> 2) vertices and $d(v) = n - 1$, for every vertex in K_n. Therefore to show K_n is Hamiltonian, we show

$$d(v) \geq \frac{n}{2}, \text{ for every vertex } v \in K_n.$$

Since $n > 2$ (given)

or $\frac{n}{2} > 1$

or $\frac{n}{2} - 1 > 0$

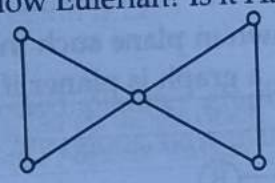
or $n - \frac{n}{2} - 1 > 0$

or $n - 1 > \frac{n}{2}$

Thus, K_n is Hamiltonian.

Example

Is the graph given below Eulerian? Is it Hamiltonian?



Solution

Yes, the graph is Eulerian but not Hamiltonian.

Traveling Sales Man Problem (TSP)

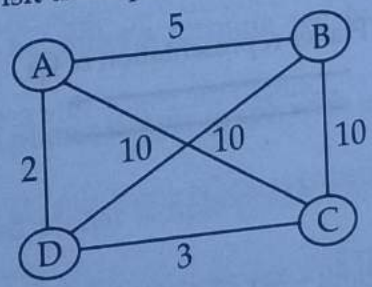
This problem was first formulated in 1930 and is one of the most intensively studied problem in graph theory and optimization. The general - TSP problem can be formulated as follows:

given a list of cities (represented by vertex of graph) and distance between each pair of cities, the problem is to find out the shortest possible route or path that usual each city exactly once and returns to the origin or starting point (city).

The name "traveling salesman problem" is given as it is analogous to the problem like a salesman want to visit each of n-city exactly once to sale his business and finally returns to his horse at the end of journey.

Example

Let a travelling salesman want to visit places. A, B, C, D, as shown in figure below. Now the problem is: in which order should be visit these places to travel minimum total distance.



To solve this problem, let us assume that salesman start as A then we can examine all possible way for him to visit other places and then return to A.

Route	Total distance
$A \to B \to C \to D \to A$	$5 + 10 + 3 + 2 = 20$
$A \to C \to B \to D \to A$	$10 + 10 + 10 + 2 = 32$
$A \to D \to B \to C \to A$	$2 + 10 + 10 + 10 = 32$

From the table above, the minimum distance a travel salesman has to travel to cover all the fan cities and return to his home 'A' is equals to 20.

The most straightforward solution to TSP is to examine all possible Hamilton circuit and select the circuit with minimum length. Now, the issue is how many such circuit exist with vertex 'n'?

There are (n - 1)! such different hamilton circuit as there are (n - 1) choice for selection first vertex (n - 2) for second and so on.

Since hamilton circuit can be travelled in reverse order, we only need to examine (n - 1)!/2 Hamilton circuit.

For example,

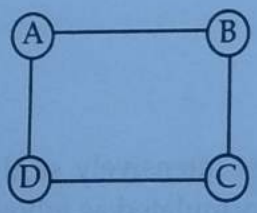
In the previous figure, there are four vertices. So n = 4 and the total possible route = (n - 1)!/2 = (4 - 1)!/2 = 6/2 = 3.

The complexity (n - 1)!/2 grows rapidly it is impossible to solve TSP when n is large. For example, when n = 25 then total number of possible path 24!/2 which is approximately 3.1×10^{23} = path. It will take approximately many million year to find a minimum length path.

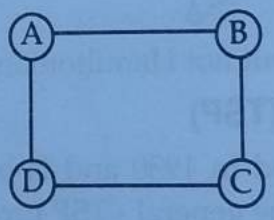
Planer Graph

A graph G = (V, E) is said to be planer graph if it can be drawn in plane such that no-intersection of edges exist at a point other then their common end point i.e. a graph is planer if it is drawn without crossing the edge.

Example

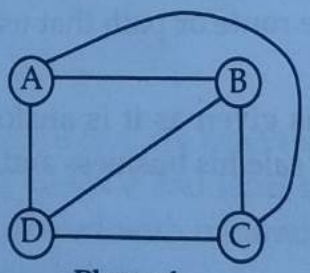


Planer graph



Planer graph

The planner representation of k_4 is



Planer k_4

The cube graph Q_3 is

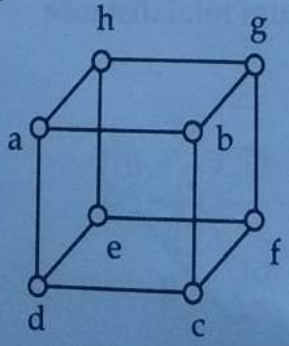
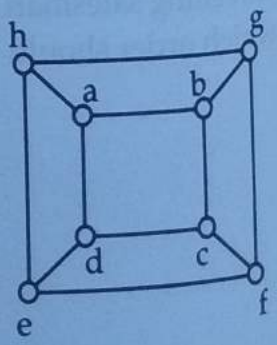


Fig. Q_3

Planer representation of Q_3



Euler's Formula

Theorem:

Let G = (V, E) be a connected planer simple graph with V vertices, e edges and r be number of regions in planar representation then r = e–V + 2.

Example

Suppose that a connected planer simple graph has 20 vertices, each of degree 4. Into how many regions does a representation of this planner graph split the plane?

Solution

The graph has 20 vertices, each of degree 4.

Therefore, V = 20

Sum of degree of vertices = 4×20 = 80

Since, sum of degree of vertices is equal to twice the number of edges.

$\therefore \quad 80 = 2\times e$

or, $\quad e = \frac{80}{2} = 40$

Now,

Using Euler's formula

$r = e - V + 2$

$= 40 - 20 + 2$

$= 22$

Therefore, number of region is 22.

Example

Suppose that a connected planner graph has 30 edge. If a planner representation of this graph divides the plane into 20 regions, how many vertices does this graph have?

Solution

Here, the number of edge is the graph e = 30

The number of region in the planer graph r = 20

Now, we know that the ruler's theorem state the relation

$r = e - v + 2$

$v = e - r + 2$

$= 30 - 20 + 2$

$v = 12$

$\therefore$ The total number of vertices (v) = 12.

Example

Suppose that a connected planar graph has 30 edges. If a planar representation of this graph divides the plane into 20 regions, how many vertices does this graph have?

Solution

We have, r = 20, e = 30, so by Euler's formula we have v = e – r + 2 = 30 – 20 + 2 = 12. So the number of vertices is 12.

Corollary 1: If G is a connected planar simple graph with e edges and v vertices where $v \geq 3$, then $e \leq 3v - 6$.

Corollary 2: If G is a connected planar simple graph, then G has a vertex of degree not exceeding five.

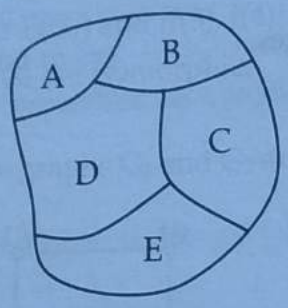
Corollary 3: If a connected planar simple graph has e edges and v vertices with $v \geq 3$ and no circuits of length three, then $e \leq 2v - 4$.

Graph Coloring

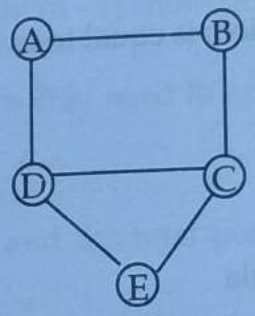
The map of the world consist of many region. To designers one region with its adjacent another region, different colors are used. One way to ensure that two adjacent regions never have the same color is to use a different on maps with many regions it would be hard to distinguish similar colors. Instead, a small number of color should be used whenever possible. For this, we some method to determine least no. of color for coloring map.

Each map in the plane can be represented by a graph. Each region of the map is represented by a vertex. Edge connects two vertices if the region represented by vertices have a common order. The graph made in this way is known as dual graph.

A coloring of a simple graph is the assignment of a color to each vertex of the graph so that no two adjacent vertices are assigned the same color.



Map

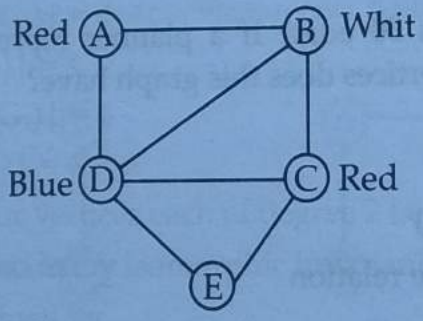


Equivalent graph of map.

A graph can be coloured by assigning different color to each vertex but it is inefficient of the num of vertex one very large. We can color graph with less number of color-than number of vertex.

The least number of colors needed for coloring a graph is known as chromatic number.

Example



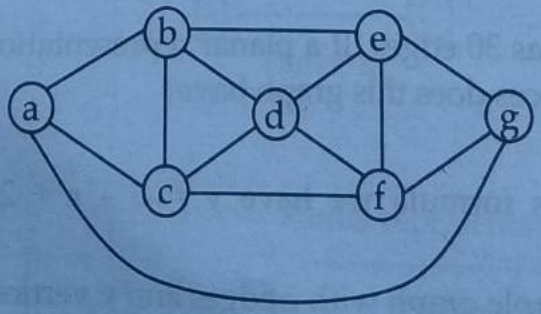
White

Here, chromatic number of this graph = 3.

Theorem: (Four color Theorem): The chromatic number of a planner graph is no greater than fo

Example

What is the chromatic no. of given graph?



Solution

Here, let us choose first vertex 'a' and colour *l* with 'red' i.e. col(a) = Red.

Now, adjacent vertex of 'a' can't have red color so we need different color for vertex 'b'. So let

col (b) = blue

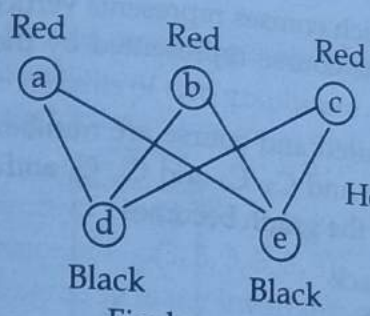
Example

What is the chromatic number of $k_{m,n}$?

Solution

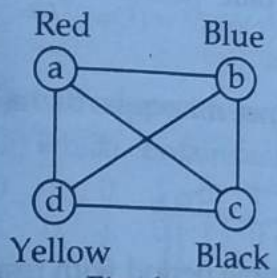
In complete bipatrate graph $k_{m,n}$, every verties of first position set are adjacent to each 'n' vertices of another - partition set. Each vertices of first position set can be colored with single color as the vertices in the same position are upon adjacent to each other. Similarly, all vertices of second position can be colored with another single color. Hence, chromatic number of $k_{m,n}$ is equals to 2.

i.e. $|k_{m,n}| = 2$



Here, chromatic number = 2.

Fig: $k_{3,2}$



Here, chromatic number = 4

Fig.: k_4

Since 'c' is adjacent vertex of both a and b, so it requires different color then a and b. Let

col (c) = black

Next let us choose vertex 'd' since 'd' is adjacent to previous (processed) vertices b and c but non-adjacent to a. It need different color then the color of vertex b and c but similarly to a. Therefore,

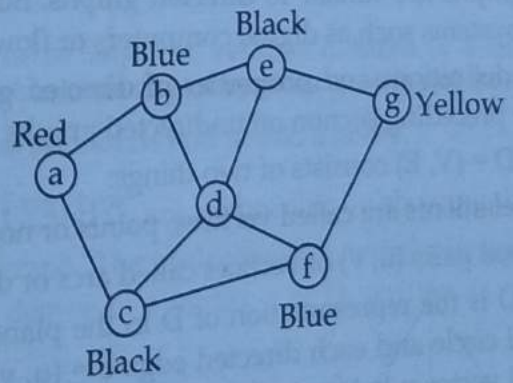
col (d) = red

Similarly, we can process other vertices and get the following graph with color.

col (e) = black

col (f) = blue

col (g) = yellow



Graph with color

Example

What is the chromatic number of k_n?

Solution

In complete graph k_n, there exist an edge between each possible pair of vertices, so no two vertices can be assigned the same color. Hence, chromatic number of $k_n = n$ (each vertex has different color).

Application of graph coloring

The problems involving scheduling assignments of resour, can be solved by using concept of graph coloring.

(a) Scheduling Final Exam

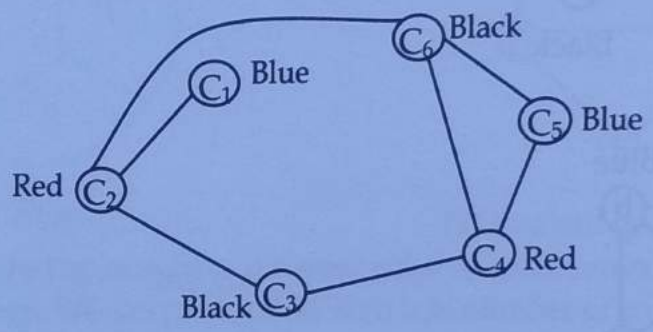
Problem:

How can the final exams at a university be scheduled so that no students has two exam at the same time?

Solution

This problem can be solved using a graph model in which comses represents vertices and there is an edge between two vertices if a common students in the course represented by these vertices. Each time slot for final exam is represented by different color.

For example, let there are six finals course to be scheduled and course are numbered from C_1 to C_6 suppose that the course number C_1 & C_2. C_1 and C_3, C_2 and C_3, C_3 and C_4, C_4 and C_5, C_4 and C_6, C_5 and C_6, C_2 and C_6 has common students for exam. Then the graph becomes



Now, scheduling of exam is determined by coloring this graph.

Therefore, the exam schedule is determined with save color as time period with respective course.

Time period	Course
I	C_1, C_5 (Blue color)
II	C_3, C_6 (Black color)
III	C_2, C_4 (Red color)

Directed Graph

The theory of graphs studied so far is concerned with undirected graphs. Most of the concepts and terminology of undirected graphs are similar to directed graphs. Such graphs are frequently more useful in various dynamical systems such as digital computers or flow systems.

This section gives the basic definitions and properties of directed graphs. Many of the definitions will be similar to those in the preceding section on undirected graphs.

A directed graph or digraph D = (V, E) consists of two things:

(i) A set V = V(D) whose elements are called vertices, points or nodes of D.

(ii) A set E = E(D) of ordered pairs (u, v) of vertices called arcs or directed edges or simply edges.

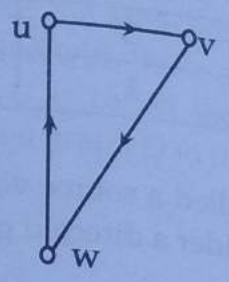
A picture of directed graph D is the representation of D in the plane. That is, each vertex v of D is represented by a dot or small circle and each directed edge e = (u, v) is represented by an arrow or directed curve from the initial vertex u to terminal vertex v.

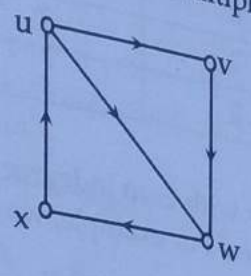
If edges and /or vertices of a directed graph D are labeled with some type of data, then D is called a labeled directed graph.

A directed graph D=(V, E) is said to be finite if its set V of vertices and its set E of edges are finite.

Simple digraphs

A directed graph D=(V, E) which has neither loops nor multiple edges is called simple directed graph

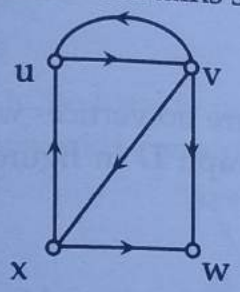




Multiple digraphs

In any diagraph, two or more edges are said to be parallel if they have same initial and terminal vertex with same orientation.

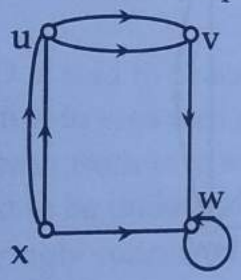
A digraph D=(V,E) which contains some multiple edges is called a multiple directed graph.



Pseudo digraph

In any digraph, an arc or edge with same initial and terminal vertex, is called self loop.

A digraph D = (V, E) which contains self loop is called a pseudo digraph.



Subgraphs

Let H be a directed graph with vertex set V(H) and edge set E(H). Similarly let G be a directed graph with vertex set V(G) and edge set E(G). Then H is said to be subgraph of G, written as $H \subseteq G$, if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

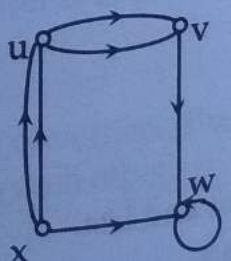
Adjacent Vertices

The vertices u and v are said to be adjacent vertices if there is a directed edge e = (u, v) or e = (v, u). Note that the edges (u, v) and (v, u) are different in a directed graph.

The edge e is said to be incident on each of its end points u and v.

In degree and out degree of vertex

Suppose D = (V, E) is a directed graph. The in-degree of v, written indeg(v), is the number of edges incident towards v and the out degree of a vertex v of D, written as outdeg(v), is the number of edges directed away from v.

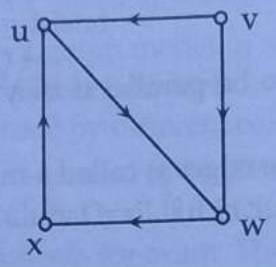


Here,

Vertex	u	v	w	x
In degree	2	2	3	0
Out degree	2	1	1	3

Source and Sink vertex

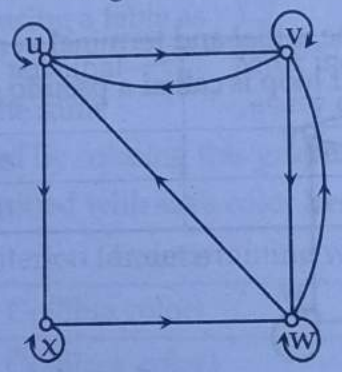
In a digraph D = (V, E), a vertex v with zero indegree is called a source vertex, and a vertex v with zero outdegree is called a sink vertex. For example, we consider a directed graph D of four vertices u, v, w and x in figure below.



In figure, the vertex v has indegree 0, so it is a source and there are no vertices with outdegree zero, so there are no sinks. The indegree sequence of the directed graph D in figure is (2, 2, 1, 0) and outdegree sequence of D is (2, 1, 1, 1).

Example

Determine whether the directed graph D in figure is a reflexive, symmetric and transitive digraph.



Solution

Here in directed graph D,

V(D) = {u, v, w, x} and

E(D) = {(u, u), (u, v), (v, u), (v, v), (v, w), (w, v), (w, w), (w, u), (x, w), (x, x), (u, x)}

Digraph D is reflexive since for all vertex a ∈ V(D), we have (a, a) ∈ D.

Digraph D is not symmetric since there is no directed edge (a, b) for all directed edge (b, a) in D.

Digraph D is not transitive since for (a, b) and (b, c) in D, there is no directed edge (a, c) in D. for example, (u, v) and (v, w) does not imply (u, w) in D.

Paths

Let D be a directed graph. The concepts of paths, simple paths, trials and cycles carry over from non-directed graphs G except that the directions of the edges must agree with the direction of the path. Specifically:

(i) A (directed) path in D is an alternating sequence of vertices and directed edges, say,
$P = (v_0, e_1, v_1, e_2, v_2, \ldots, v_n)$
such that each edge e_i begins at v_{i-1} and ends at v_i.

(ii) The length of the path P is n, its number of edges.

(iii) A simple path is a path with distinct vertices.

(iv) A trial is a path with distinct edges.

(v) A closed path has the same first and last vertices.

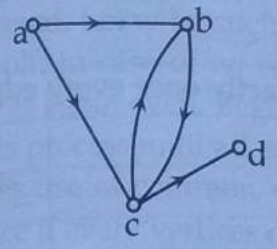
(vi) A spanning path contains all the vertices of D.

(vii) A cycle is a closed path with distinct vertices except first and last.

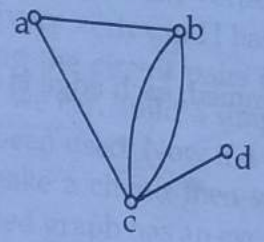
(viii) A circuit is a closed path containing at least three edges.

Underlying Graph

Given a digraph D, we can obtain a graph G from D by removing all the arrows or directions from the edges. If the graph G has the same vertex set as that of the digraph D and corresponding to each directed edge in D associated with the ordered pair of vertices (a, b), there is an edge in G associated with the pair (a, b) then G is called the underlying graph of D. For example, figure (b) is the underlying graph of directed graph D in figure (a).



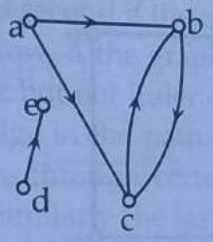
(a)



(b)

Weakly Connected

A digraph D is said to be weakly connected if its underlying graph is connected. For example, the digraph D in figure is weakly connected but the digraph D in figure is not weakly connected.



Strongly Connected

A directed graph or digraph D is said to be strongly connected if for any pair of vertices v_i and v_j in D, there is a directed path form v_i to v_j as well as a directed path from v_j to v_i.

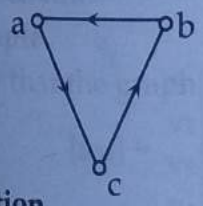
In case, if there is a directed path from v_i to v_j or from v_j to v_i (not necessarily both) for any pair of vertices v_i and v_j, then D is said to be unilaterally connected.

Clearly, a digraph which is strongly connected is also unilaterally connected.

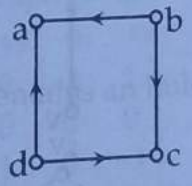
Example

Determine which of the digraphs in figure is strongly connected and unilaterally connected?

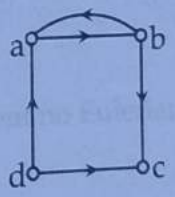
(i)



(ii)



(iii)



Solution

The digraph D in figure (i) is strongly connected, so it is unilaterally connected also.

The digraph D in figure (ii) is not strongly connected since there is no path from a to b. This digraph D is not unilaterally connected as well, since there is no directed path from b to d or from the vertex d to b.

The digraph D in figure (iii) is not strongly connected since there is not a directed path from the vertex c to b but this digraph D is unilaterally connected since there is a directed path between any two vertices.

Theorem

The sum of the outdegrees of vertices, the sum of indegrees of vertices and the number of edges in a directed graph are equal to each other.

OR,

If D is a directed graph with vertices $v_1, v_2, \ldots v_n$ and q is the number of directed edges in D, then

$$\sum_{i=1}^{n} \text{in-deg}(v_i) = \sum_{i=1}^{n} \text{out-deg}(v_i) = q$$

Proof: When the in-degrees of the vertices are summed, each edge is counted exactly once since every edge goes to exactly one vertex. Thus

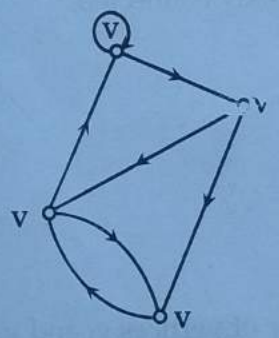
$$\sum_{i=1}^{n} \text{in-deg}(v_i) = q$$

Similarly, when the outdegrees are summed, each edge is counted exactly once every edge goes out of exactly one vertex. Then

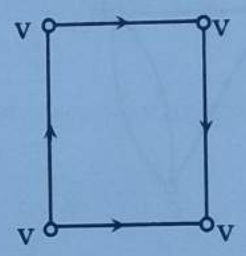
$$\sum_{i=1}^{n} \text{out-deg}(v_i) = q$$

Thus, $$\sum_{i=1}^{n} \text{in-deg}(v_i) = \sum_{i=1}^{n} \text{out-deg}(v_i) = q$$

(i)

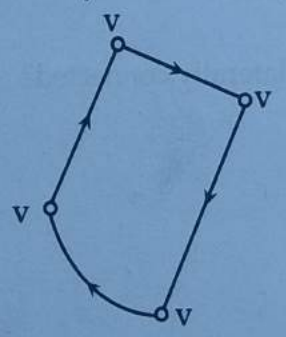


(ii)

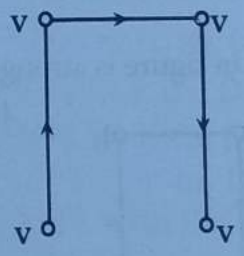


In figure (i), we can clearly get a closed spanning path, which is shown in figure, so it is strongly connected. Since (i) is strongly connected it is unilaterally connected as well. The digraph (ii) has no closed spanning paths, hence it is not strongly connected but it has a spanning path (v_4, v_1, v_2, v_3), so it is unilaterally connected. Figure shows this spanning path.

(i)



(ii)



Representation of Digraph

(i) Adjacency Matrix:

Let D = (V, E) be a digraph with vertices $v_1, v_2, \ldots, v_n$. Then the adjacency matrix of D with respect to given order of vertices is $n \times n$ matrix $A(D) = [a_{ij}]_{n\times n}$ is defined as follows:

$$a_{ij} = \begin{cases} 1 \text{ if there is an edge } (v_i, v_j) \\ 0 \text{ if there is an edge } (v_i, v_j) \\ k \text{ if there are k number of arc from } v_i \text{ to } v_j \end{cases}$$

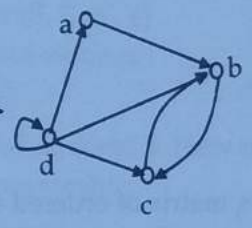
(ii) Incidence Matrix:

Let D =(V,E) be a digraph with vertices $v_1, v_2, \ldots, v_m$ and directed edges $e_1, e_2, \ldots, e_n$. Then incidence matrix of D, $[m_{ij}]_{m\times n}$, is defined as follows:

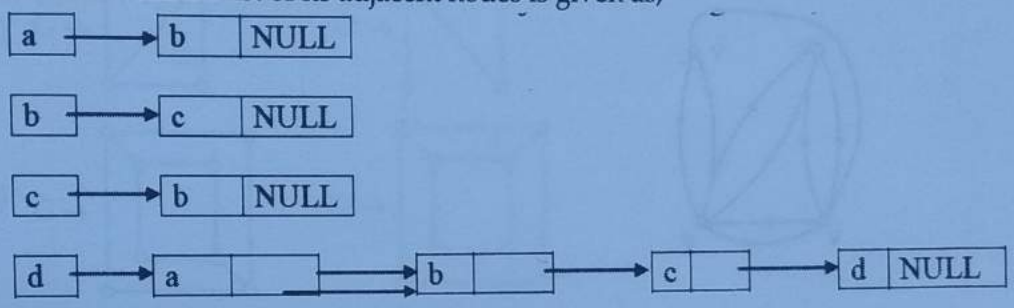
$$m_{ij} = \begin{cases} 1 \text{ of edge } e_j \text{ is directed away from a vertex } v_i \\ -1 \text{ if edge } e_j \text{ is directed towards vertex } v_i \\ 0 \text{ otherwise} \end{cases}$$

(iii) Adjacency List (Linked list)

Edge List for Simple Graph	
Vertex	Adjacent Vertices
a	b
b	c
c	b
d	a, b, c, d

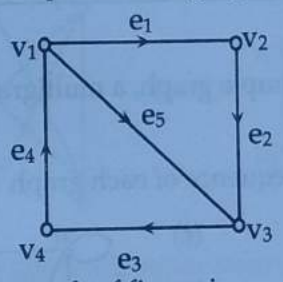


And for each node a linked list of its adjacent nodes is given as;



Example

Find the incidence matrix to represent the graph shown in figure



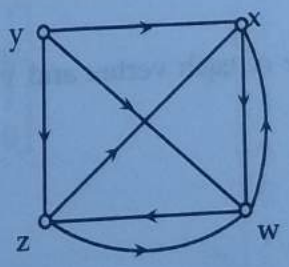
Solution

The incidence matrix of the graph of figure is

$$[m_{ij}] = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 \end{bmatrix}_{4 \times 5} \end{array}$$

Example

Find the adjacency matrix to represent the directed graph shown in figure, where vertices are ordered as $v_1 = x$, $v_2 = y$, $v_3 = z$ and $v_4 = w$.



Solution

The adjacency matrix of the directed graph of fig. 6.64 is

$$A = \begin{array}{c} \\ x \\ y \\ z \\ w \end{array} \begin{array}{c} \begin{array}{cccc} x & y & z & w \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

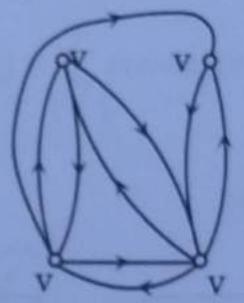
Example

Draw the digraph D corresponding to the adjacency matrix A, where A is given as,

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

Solution

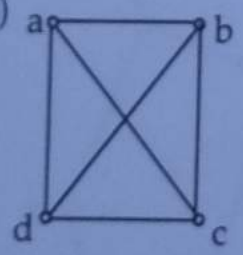
Since the given matrix is a square matrix of ordered 4, the digraph D has 4 vertices, say v_1, v_2, v_3 and v_4. Draw a directed edge from v_i to v_j where $a_{ij} = 1$. The required digraph D is shown in figure below.



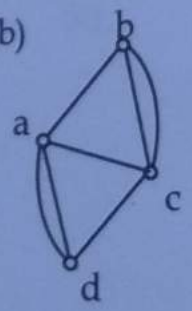
Exercise

1. Considering the following graphs, determine
   (i) whether each of the graphs shown is a simple graph, a multigraph, a Pseudograph
   (ii) vertex set (iii) edge set
   (iv) degree of each vertex (v) degree sequence of each graph

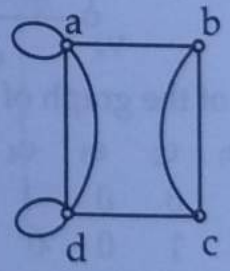
(a)



(b)

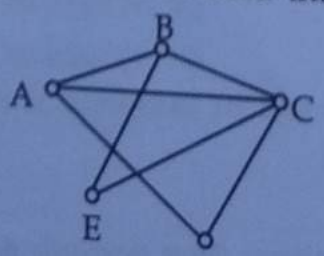


(c)



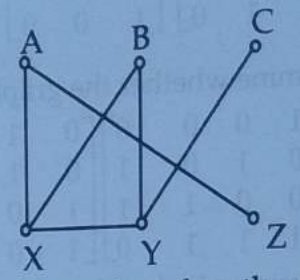
2. Draw the following graphs:
   (i) two 3-regular graphs with six vertices.
   (ii) two 3-regular graphs with eight vertices.
   (iii) if possible, a 3-regular graph with nine vertices. If it is not possible, explain why?
   (iv) the complete bipartite graph $K_{3,5}$.

3. Consider a graph given below. Find the degree of each vertex and verify the Handshakin theorem.



4. Draw a graph with five vertices v_1, v_2, v_3, v_4, v_5, such that deg $(v_1) = 3$, v_2 is an odd vertex, deg $(v_3) = 2$, and v_4 and v_5 are adjacent.

5. Consider the graph G in question no.3 and find
   (a) all simple paths from A to C.
   (b) all cycles

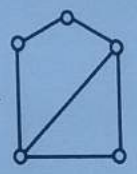


6. Consider the graph given below and find the following
   (a) Subgraph H of G induced by V(H) = {B, C, X, Y}
   (b) G – Y
   (c) all cut-vertices
   (d) all bridges

7. Suppose a graph has vertices of degree 0, 2, 2, 3 and 9. How many edges does the graph has?

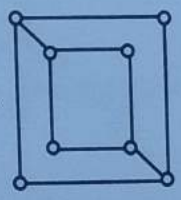
8. Show that the following graphs are not isomorphic.

(a) G →

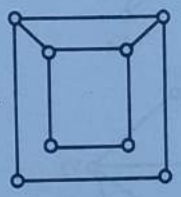


G' →

(c) G →

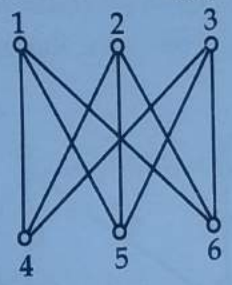


G' →

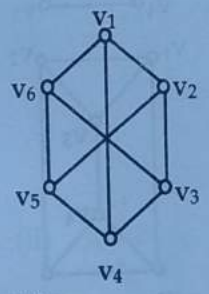


9. Show that the following graphs are isomorphic.

G →



G' →



10. Draw a graph with given adjacency matrices

(a) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ (d) $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 0 & 4 \\ 3 & 4 & 0 \end{bmatrix}$

(e) $\begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ (f) $\begin{bmatrix} 0 & 1 & 3 & 0 & 4 \\ 1 & 2 & 1 & 3 & 0 \\ 3 & 1 & 1 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$

(g) $\begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 2 \\ 1 & 2 & 2 \end{bmatrix}$ (h) $\begin{bmatrix} 0 & 2 & 3 & 0 \\ 2 & 2 & 2 & 1 \\ 3 & 2 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{bmatrix}$

11. Are the simple graphs with the following adjacency matrices isomorphic?

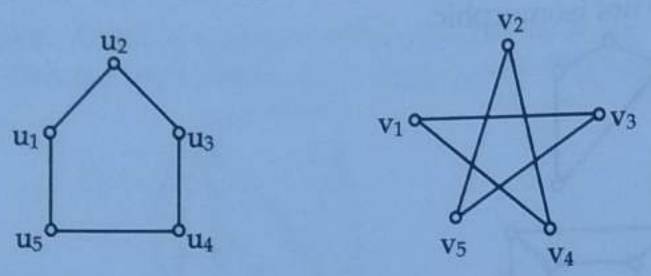
(a) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

12. Determine whether the graphs with these incidence matrices are isomorphic.

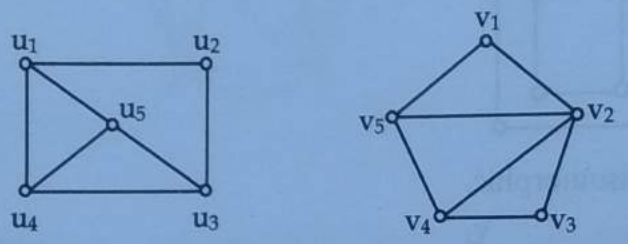
$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

13. Determine whether the given pair of graph is isomorphic.

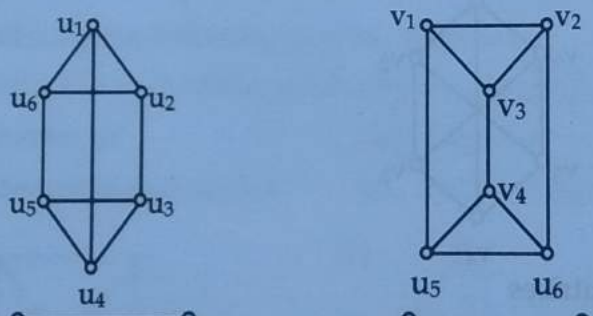
(i)



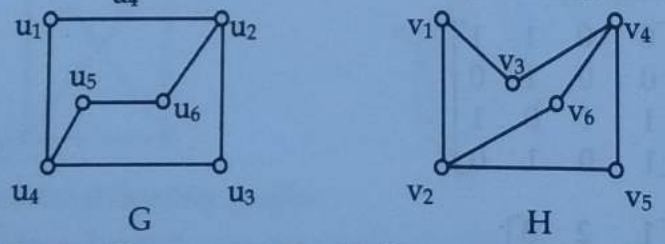
(ii)



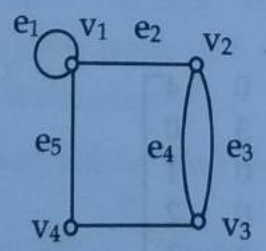
(iii)



(iv)



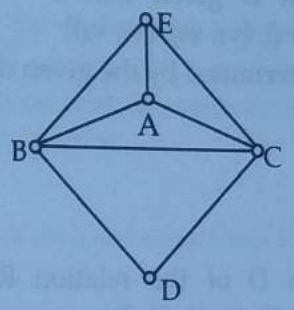
14. Find the incidence matrix and adjacency matrix of the graph given below.



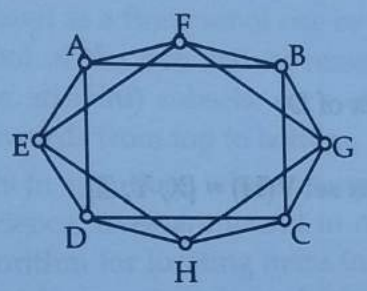
15. Draw the graph G corresponding to the following adjacency matrix.

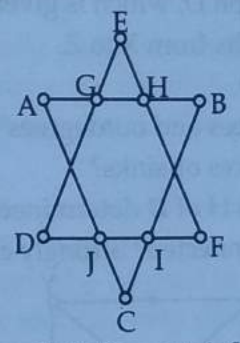
$$A = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 2 & 0 & 2 & 2 \end{bmatrix}$$

16. Test each of the following graphs for Eulerian circuits and Hamiltonian cycles
    (i) K_4 (ii) K_5 (iii) $K_{3,5}$
17. From the graph in fig below, state that
    (i) Is the graph Hamiltonian?
    (ii) Is there a Hamiltonian path?
    (iii) Is it Eulerian?
    (iv) Is there an Eulerian trail?

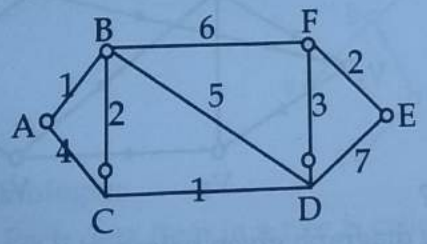


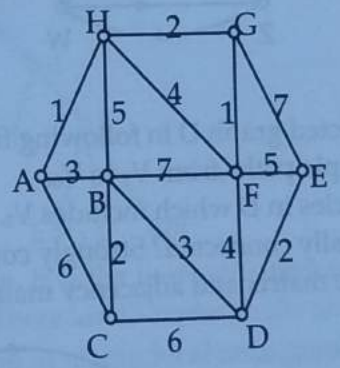
18. In each case, explain why the graph is Eulerian and find an Eulerian circuit.

(i)


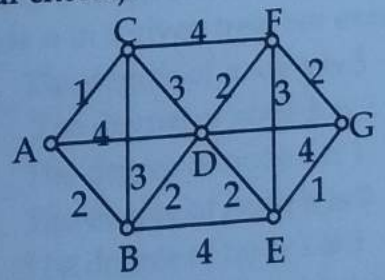
(ii)


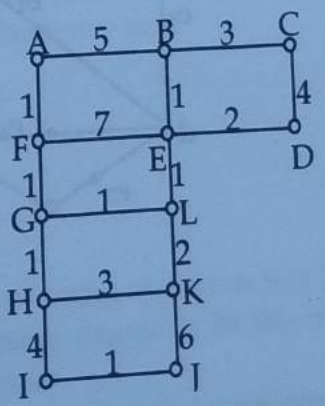
19. (a) How many edges must a Hamiltonian cycle in K_n contain?
    (b) How many Hamiltonian cycles does K_n have?
20. Use Dijkstra's algorithm to find the shortest path from A to E in the following weighted graphs.

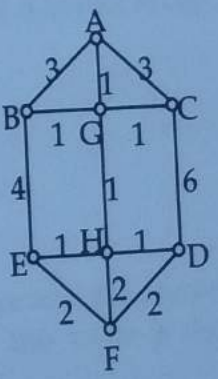
(i)


(ii)


21. Solve the shortest path problem for following graphs (Choose source and destination vertex as your choice).

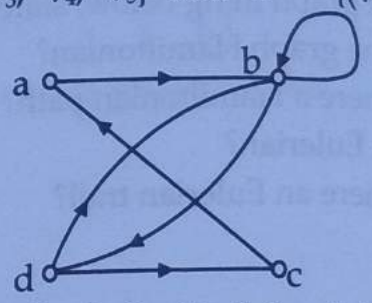
(i)


(ii)


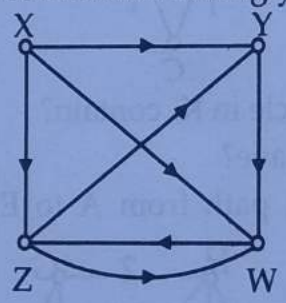
(iii)


22. Suppose that a connected planner simple graph has 20 vertices, each of degree 3. Into how may regions does a representation of this planar split a plane?
23. What is Euler's formula for planar graph? How can Euler's formula for planar graph can be used to show that simple graph is non-planar.

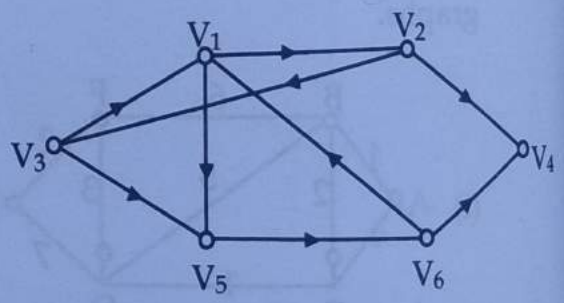
24. Which of the undirected graph in the following figure have an Euler circuit? Explain.
25. What is chromatic number of $k_{m,n}$ and k_n.
26. Draw the diagraph D given that $V = \{v_1, v_2, v_3, v_4, v_5\}$ and $E = \{(v_1, v_2), (v_1, v_3), (v_2, v_3), (v_2, v_4), (v_2, v_4), (v_3, v_3), (v_4, v_2)\}$
27. Find the relation determined by the given diagraph.



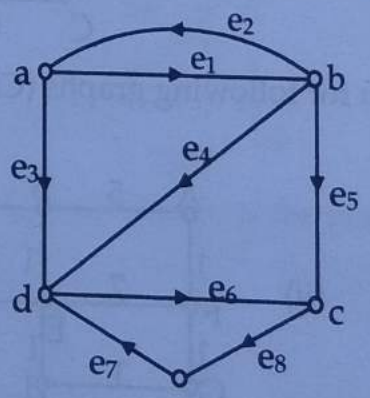
28. Draw the diagraph D of the relation R on $V = \{1, 2, 3, 4\}$ defined by $R = \{(1, 2), (2, 2), (2, 4), (3, 2), (3, 4), (4, 1), (4, 3)\}$.
29. Consider a directed graph D, which is given below
    (a) Find all simple paths from X to Z.
    (b) Find all cycles in D.
    (c) Find all the indegrees and outdegrees of each vertex of D.
    (d) Are there any sources or sinks?
    (e) Find the subgraphs H of D determined by the vertex set $V(H) = \{X, Y, Z\}$.
    (f) Is D unilaterally connected? Strongly connected?



30. Consider the directed graph D in following figure.
    (a) Find the simple paths from V_1 to V_6.
    (b) Find four cycles in D which includes V_3.
    (c) Is D unilaterally connected? Strongly connected?



31. Find the incidence matrix and adjacency matrix of the diagraph given below.



6.3 Tree

Introduction

A tree is a collection of nodes connected by directed (or undirected) edges. A tree is a nonlinear data structure, compared to arrays, linked lists, stacks and queues which are linear data structures. A tree can be empty with no nodes or a tree is a structure consisting of one node called the root and zero or one or more subtrees. A tree has following general properties:

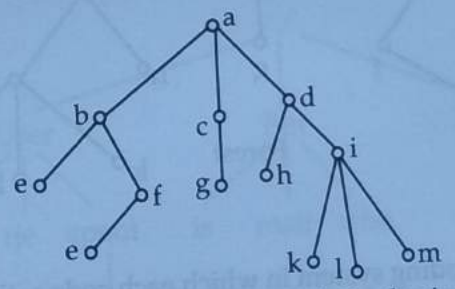
- One node is distinguished as a **root**;
- Every node (exclude a root) is connected by a directed edge from exactly one other node; A direction is: parent -> children

A tree is a non-linear data structure in which items are arranged in a sequence. It is used to represent hierarchical relationship existing among several data items.

A tree is defined as a finite set of one or more data items (nodes) such that there is a special data item called the root of the tree and its remaining data items are partitioned into a number of mutually exclusive (i.e. disjoint) subsets, each of which itself is a tree (called sub trees).Tree data structure grows downwards from top to bottom.

A tree occurs in situations where many elements are to be organized into some sort of hierarchy. In computer science, trees are useful in organizing and storing data in a database, used to construct efficient algorithm for locating items in a list. They can also be used in algorithms, such as Huffman coding, to study games such as checkers and chess and can help determine winning strategies for playing those games.

The tree consisting of a single vertex with no edges is called the trivial tree or the degenerate tree.

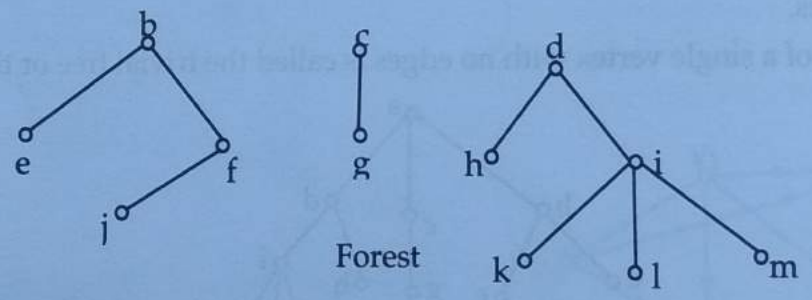


Tree Terminologies

- **Node:** Each data item in a tree is called a node. It is the basic structure in a tree. It specifies the data and links (branches) to other data items. There are 13 nodes in the above tree.
- **Root:** It is the first data item (or node) lies at top in hierarchical arrangement of data items. In the above tree, **a** is the root item.
- **Degree of a node:** It is the number of sub trees (the no of trees which have node **n** as root node) of a node **n** in a given tree. For example, in the above tree,
  - The degree of node **a** is 3
  - The degree of node **b** is 2
  - The degree of node **c** is 1
  - The degree of node **h** is 0
  - The degree of node **i** is 3
- **Degree of a tree:** It is the maximum degree of nodes in a given tree. In the above tree, the degree of node a is 3 and another node i also have degree 4. In the whole tree, this value is the maximum. So, the degree of the above tree is 4.
- **Terminal node(s):** A node with out degree zero is called a **terminal node** or **leaf node**. In the above tree, there are 7 terminal nodes: **e, j, g, h, k, l** and **m**.
- **Non-terminal node(s):** Any node (except the root node) whose out degree is not zero is called **non-terminal node**. **Non-terminal nodes** are the intermediate nodes in traversing the given tree

from its root node to the terminal nodes (leaves). In the above tree, there are 5 **non-terminal nodes**: **b, c, d, f** and **i**.

- **Siblings:** The children nodes of a given parent node are called siblings. They are also called **brothers**. In the above tree,
  - **e** and **f** are siblings.
  - **k, l** and **m** are siblings of parent node **i**
- **Level/Depth:** The number of edges that need to be followed while traversing a tree from root to that node is called depth of node. The entire tree structure is leveled in such a way that the root node is always at level 0. Then its immediate children are at level 1 and their immediate children are at level 2 and so on up to the terminal nodes. In general, if a node is at level n, then its children are at level n+1. In the above tree, there are four levels from level 0 to level 3.
- **Edge:** It is a connecting line of two nodes or relation between two nodes of tree.
- **Path:** Path in a tree is the sequence of consecutive edges from the source to the destination node of tree. In the above tree, the **path** between **a** and **j** is given by the node pairs: **(a, b)**, **(b, f)** and **(f, j)**.
- **Depth:** It is the maximum level of any leaf in a given tree. This equals the length of the longest path from root to the terminal nodes (leaves). The term **height** is also used to denote the depth. The **depth** of the above tree is 3.
- **Forest:** It is a set of disjoint trees. In a given tree, if we remove its root, then it becomes a forest. In the above tree, there is forest with three trees if we remove the root node.



Applications of Tree

Prefix codes

A prefix code is a special type of coding system in which each code satisfy a "prefix property".

Prefix property means there is no code were in the system that is prefix of any other code word in the system.

Example

A code with codings (code word) {0, 10, 11} is a prefix code. But the coding system with code words {0, 01, 011} is not a prifix code since 0 is prefix of second code word (01) and 01 is prefix of third code word.

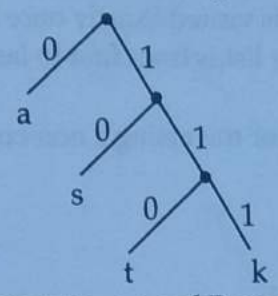
A prefix code can be represented using binary tree where the symbols are leaf node and edges are labeled with code words.

Character
e
a
t
n
s

The edges of the tree are labeled so that an edge leading to a left child is assigned a '0' and an edge leading to a might child is assigned a bit 'i'. Now the bit string used to encode a character is the sequence of edges in the unique path from the root to that leaf node with specific character.

Example

Let us draw a tree as follows (by maintaining rule of prefix tree as explained below):

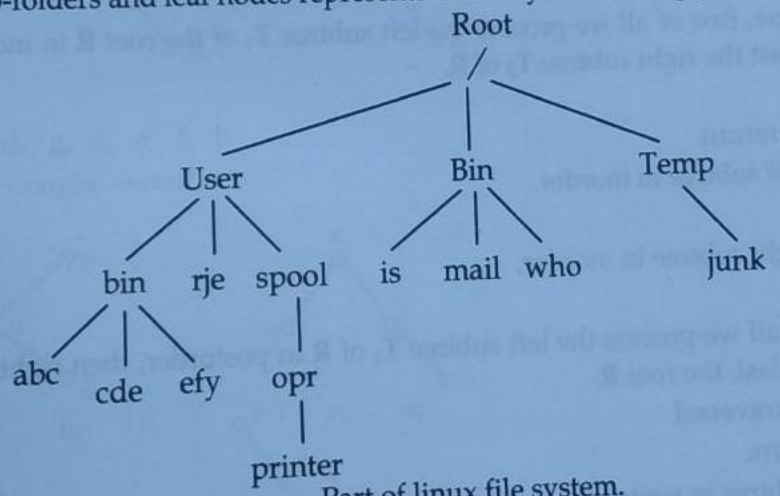


Now, the prefix for the character a, s, t and R can be written as

Character	Code
a	0
s	10
t	110
k	111

Tree as models in computer File System

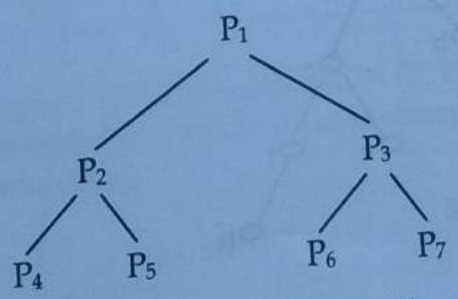
Files in computer memory can be organized into directories or folder in which folder contains both files and sub-folders. In file system, root directory or folder contains files in the system. So a file system can be represented by a rooted tree, where the root represents main folder, internal vertices represents sub-folders and leaf nodes represents ordinary files or empty folders.



Part of linux file system.

Tree as a model for parallel processing

A parallel processing system consists of many processing devices (CPU). These processor are interconnected with each other to complete a task in parallel computing fashion. Tree can be used to represent the connection between these processor. Here, a processor is represented by vertex and the edges between these vertices are used to represent connection between them. A tree connected network for seven processors is as shown in figure.



A tree connected network.

Tree Traversal

Tree traversal is one of the most common operations performed on tree data structures. Traversing a binary tree is a way in which each node in the tree is visited exactly once in a systematic manner. We know that the order of traversal of nodes in a linear list is from first to last, however there is no such "natural" linear order for the nodes of a tree.

We have the following three orderings or methods for traversing a non-empty binary tree:

- Preorder (Depth-first order) Traversal
- Inorder (Symmetric order) Traversal
- Postorder Traversal

All theses traversal techniques are defined recursively.

Preorder Traversal

In this technique, first of all we process the root **R** of the binary tree **T**. Then, we traverse the left subtree T_1 of **R** in preorder (which means that we traverse root of subtree T_1 first and then its left subtree). After visiting left subtree of **R**, then we take over right subtree T_2 of **R** and process all the nodes in preorder.

Steps

1. If root=NULL, return.
2. Visit the root.
3. Traverse the left subtree in preorder.
4. Traverse the right subtree in preorder.

Inorder Traversal

In this traversal technique, first of all we process the left subtree T_1 of the root **R** in inorder, then we process the root and at last the right subtree T_2 of **R**.

Steps

1. If root=NULL, return.
2. Traverse the left subtree in inorder.
3. Visit the root.
4. Traverse the right subtree in inorder.

Postorder Traversal

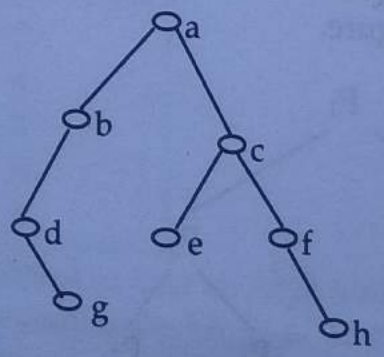
In this technique, first of all we process the left subtree T_1 of **R** in postorder, then right subtree T_2 of **R** in postorder and at the last, the root **R**.

Algorithm for postorder traversal

1. If root=NULL, return.
2. Traverse the left subtree in postorder.
3. Traverse the right subtree in postorder.
4. Visit the root.

Example

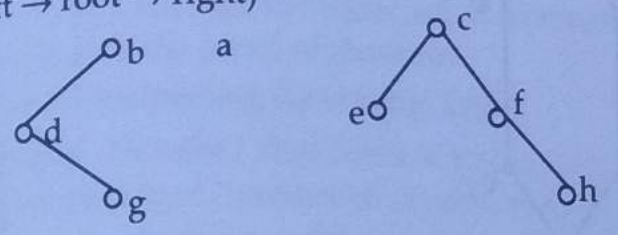
Find the preorder, in-order and post-order traversal of following tree.



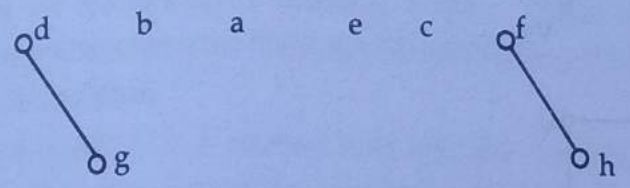
Solution

In order (left → root → right)

Step 1:



Step 2:

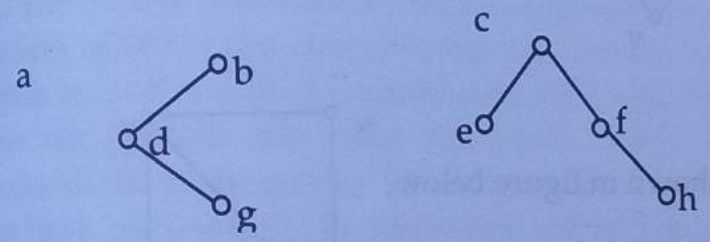


Step 3:

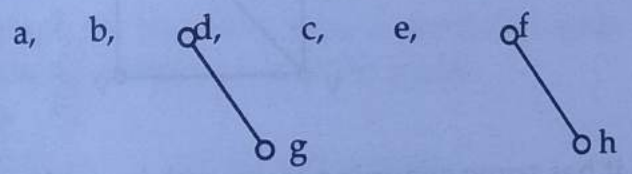
d, g, b, a , e, c, f, h

Pre-order (root → left → right)

Step 1:



Step 2:

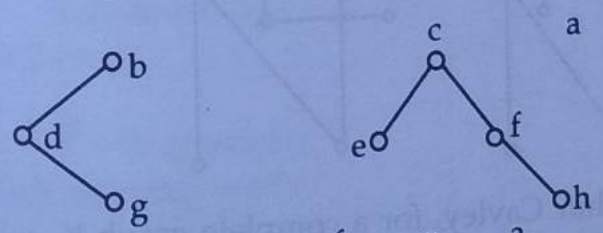


Step 3:

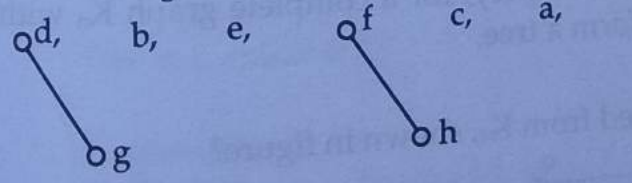
a, b, d, g, c, e, f, h

Post order (left → right → root)

Step 1:



Step 2:



Step 3:

d, g, b, e, h, f, c, a

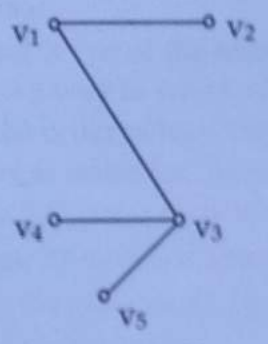
Therefore,

Preorder	a	b	d	g	c	e	f	h
In oder	d	g	b	a	e	c	f	h
Postorder	g	d	b	e	h	f	c	a

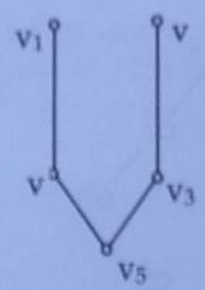
Spanning Tree

Let G = (V, E) be any connected graph then any subgraph T= (V, E') of given graph G consist of all the vertices in G, which is still connected and acyclic is called spanning tree of given graph. In figure (i), (ii) and (iii) are the spanning tree of (iv).

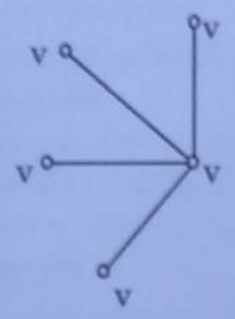
(i)



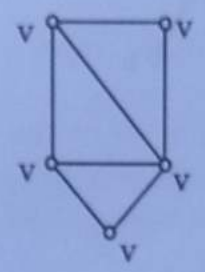
(ii)



(iii)

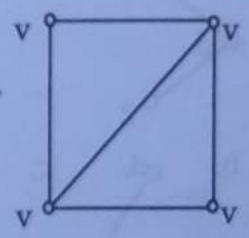


(iv)



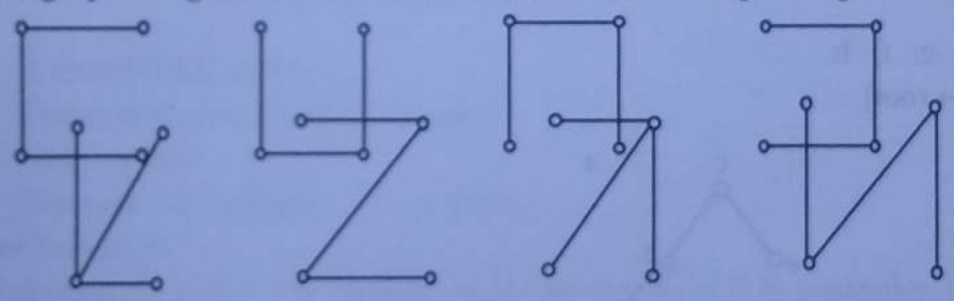
Example

Write all the spanning trees of the graph G shown in figure below.



Solution

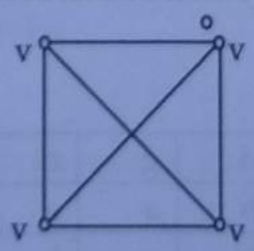
Since the graph in figure below is connected, so it has some spanning trees which are shown below:



Note: According to English mathematician Arthur Cayley, for a complete graph K_n with n vertices there are n^{n-2} different ways of joining them to form a tree.

Example:

How many different spanning trees can be formed from K_4, shown in figure?



K_4 or 3 – regular graph

Solution

Since, K_4 consists of n = 4 vertices, there are $(4)^{4-2} = 16$ different ways of joining them to form a spanning tree. This means 16 different trees can be formed.

Theorem

A simple graph is connected if and only if it has a spanning tree.

Proof

If a graph G has a spanning tree than by definition of spanning tree it is connected.

Conversely, let G be a connected graph, if G has no cycles, then G is itself a tree. Hence, in the case, G itself is a spanning tree. Now suppose that G has at least one cycle. If we delete an edge of the cycle

of G, the resulting graph G_1 is connected and has the same set of vertices as G. If G_1 has a cycle then we delete an edge of a cycle of G_1 and so on. In this way, we ultimately arrive at a connected graph H which has no cycles and has the same set of vertices of G. Hence, by definitions H is a spanning tree of G which complete the proof of theorem.

Algorithms for Constructing Spanning Trees

We have already discussed that from a given connected graph G to construct a spanning tree we delete one or more edges. Instead of constructing spanning trees by removing edges, spanning trees can be built by successively adding edges. There are two algorithms based on this principle for finding a spanning tree and they are Breadth-first search (BFS) and Depth-first search (DFS).

(a) BFS Algorithm

In this algorithm a rooted tree will be constructed, and the underlying undirected graphs of this rooted tree forms the spanning tree. The idea of BFS is to visit all vertices on a given level before going into the next level.

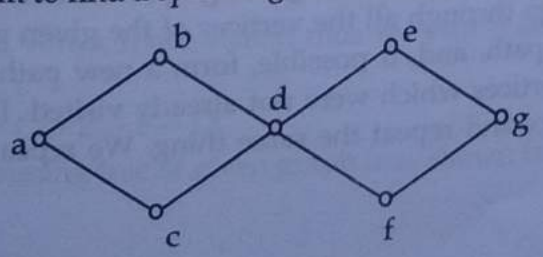
Procedure: Arbitrarily choose a vertex and designate it as the root. Then add all the edges incident to this vertex such that the addition of edges does not produce any cycle. The new vertices added at this stage become the vertices at level 1 in the spanning tree. Next, for each vertex at level 1, visited in order, add each edge incident to this vertex to the tree as long as it does not produce any cycle. Arbitrarily order the children of each vertex at level 1. This produces the vertices at the level 2 in the tree. Continue this process until all the vertices in the tree have been added. The procedure will end since, there are only a finite number of edges in the graph. A spanning tree is produced since we have produced a tree without a cycle but containing every vertex of the graph.

Pseudocode

```
BFS (G,s)        /*s is start vertex*/
{
        T={s};
        L=ϕ;                /*an empty queue*/
        Enqueue (L,s);
While (L!= ϕ)
{
        V = Dequeue(L);
For each neighbor w to v
{
        If(w ∉ L and w ∉ T)
{
        Enqueue(L,w);
        T=T U {w}           /*put edge {v,w}Also*/
}
}
}
}
```

Example

Use BFS algorithm to find a spanning tree of graph G of figure.



Solution

(i) Choose the vertex a to be root.

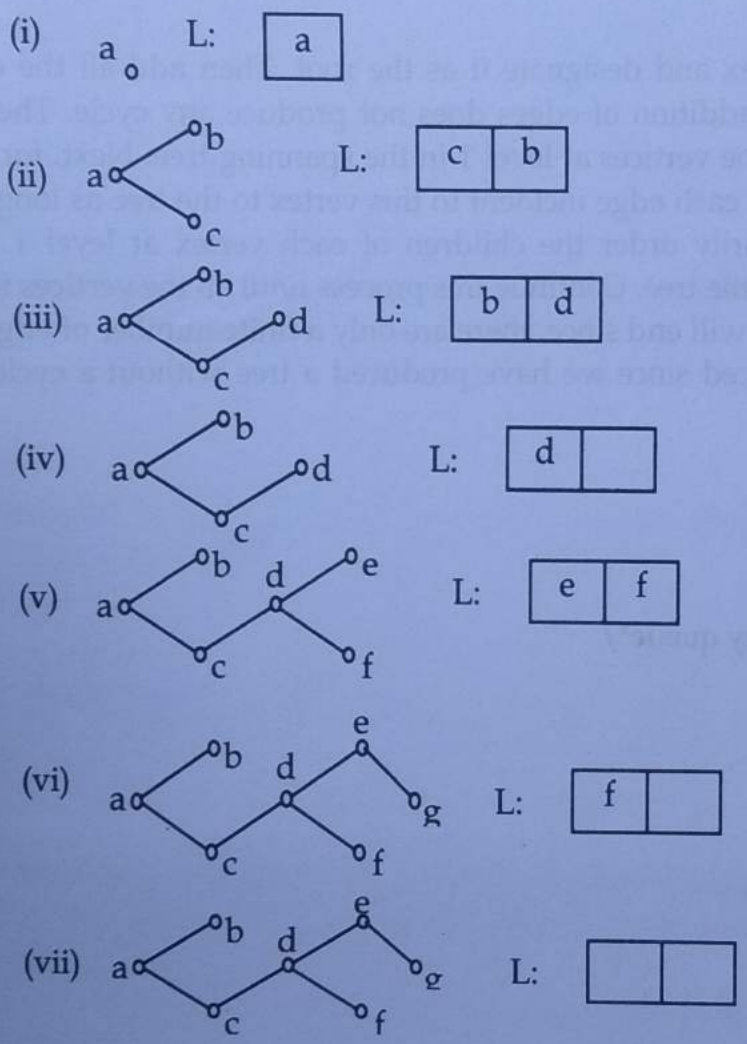
(ii) Add edges from the vertex a to all adjacent vertices on it. Then the edges {a, b}, {a, c} are added.

(iii) Add edges from these vertices at level 1 to adjacent vertices which are not already joined in the tree. Hence the edge {c, d} is added. The vertex d is at level 2.

(iv) Add edges from d in level 2 to adjacent vertices not already in the tree. The edges {d, e} and {d, f} are added. Hence e and g are at level 3.

(v) Add edge from e at level 3 to adjacent vertices which are not already in the tree and hence {e, g} is added.

The steps of BFS are shown in figure below



(b) DFS Algorithm

An alternative to BFS is DFS which proceeds to successive levels in a tree at the earliest possible opportunity. DFS is also called back tracking.

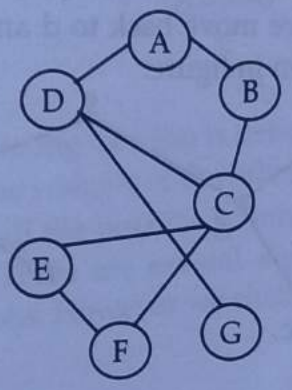
Procedure: Arbitrarily choose a vertex and designate it as the root. Form a path starting from the root 'a' by successively adding edges as long as possible so that the edges do not produce any cycle. If the path goes through all the vertices of the given graph, the tree with this path is a spanning tree. If the path does not go through all the vertices of the given graph, we move back to the next to last vertex in the path, and, if possible, form a new path starting at this vertex which passes through those vertices which were not already visited. If this cannot be done, we move back to another vertex and repeat the same thing. We repeat the procedure until all the vertices are visited.

Pseudocode

```
DFS(G,s)
{
    T={s};
    Traverse(s);
}
Traverse(v)
{
    for each w adjacent to v  and not yet in T
    {
        T= T U {w};        /*put edge {v,w} also*/
        Traverse(w);
    }
}
```

Illustration of above algorithms

A	B	D		
B	A	C		
C	B	D	E	F
D	A	C	G	
E	C	F		
F	C	E		
G	D			



Edge table (adjacent table)

In order to do a DFS is to follow the chain of edges as far as we can into graph before we back track to pick u other vertices. As we visit each vertex we cross it off everywhere it appears in the edge table. Since we are starting with A, cross it off every where it appears.

~~A~~	B	D		
B	~~A~~	C		
C	B	D	E	F
D	~~A~~	C	G	
E	C	F		
F	C	E		
G	D			

A → B → C

A → B → C → D → G

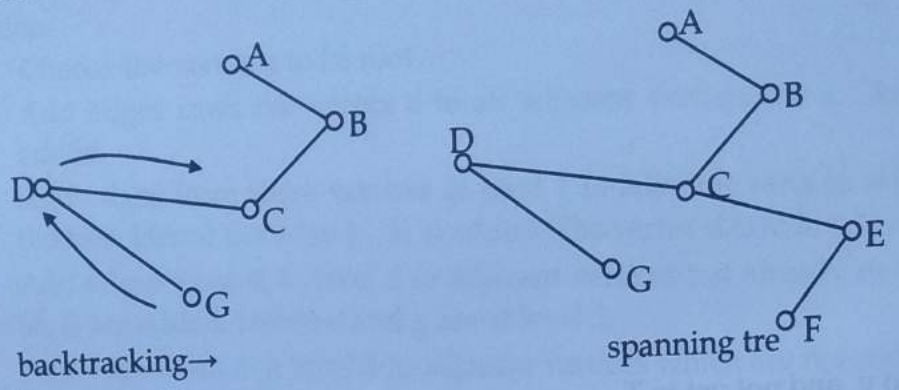
Hence we have seen that while traversing we start at A and got B and moved to vertex B, then start traversing and found C then to vertex D. from first row. In that row A and C are already visited and next found G which send us to 7th row from where there is no any other vertex to traverse. Now we have not visited E and F, to visit E and F we back track

G → D → C.

Hence, we found vertex E not visited thus we visit E and then F from 6th row Hence final traverse list will be

A → B → C → D → G → E → F → Q.

Therefore the spanning tree of given graph is as shown below:

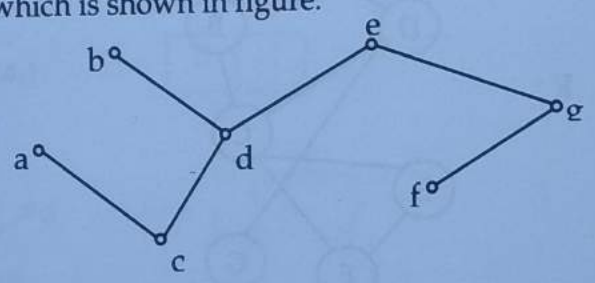


Example

Find a spanning tree of the graph of figure using DFS algorithm.

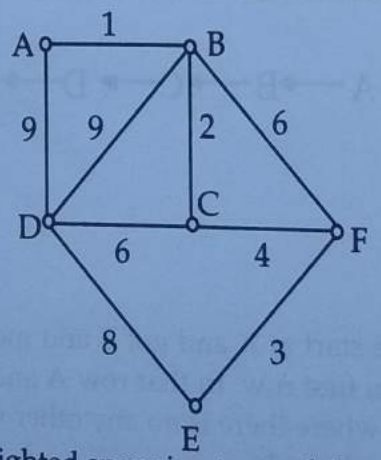
Solution

Choose the vertex a to be the root. Form a path starting from the vertex a by successively adding edges incident with vertices which are not already in the path as long as possible. This produces the path a – c – d – e – g – f. since this path does not include the vertex b, so we move back to g. There is no path beginning at g containing those vertices which are not already visited. Similarly we move back to e, there is no new path. So we move back to d and form the path d – b. This produces the required spanning tree which is shown in figure.



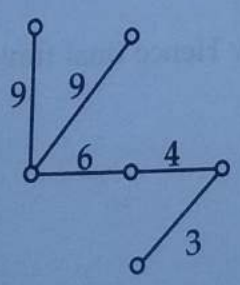
Minimal Spanning Trees

Let G be a connected weighted graph. The weight of a spanning tree of G is the sum of the weights of the edges which are included on that spanning tree. Thus, a minimal spanning tree of G is a spanning tree of G with minimum possible weight among all possible spanning trees of that graph. Consider figure which shows six cities and cost of lying railway links between certain pair of cities. We want to set up railway links between the cities at minimum costs.

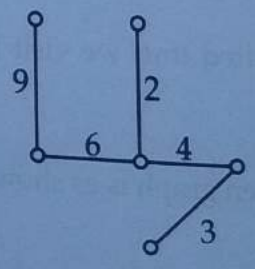


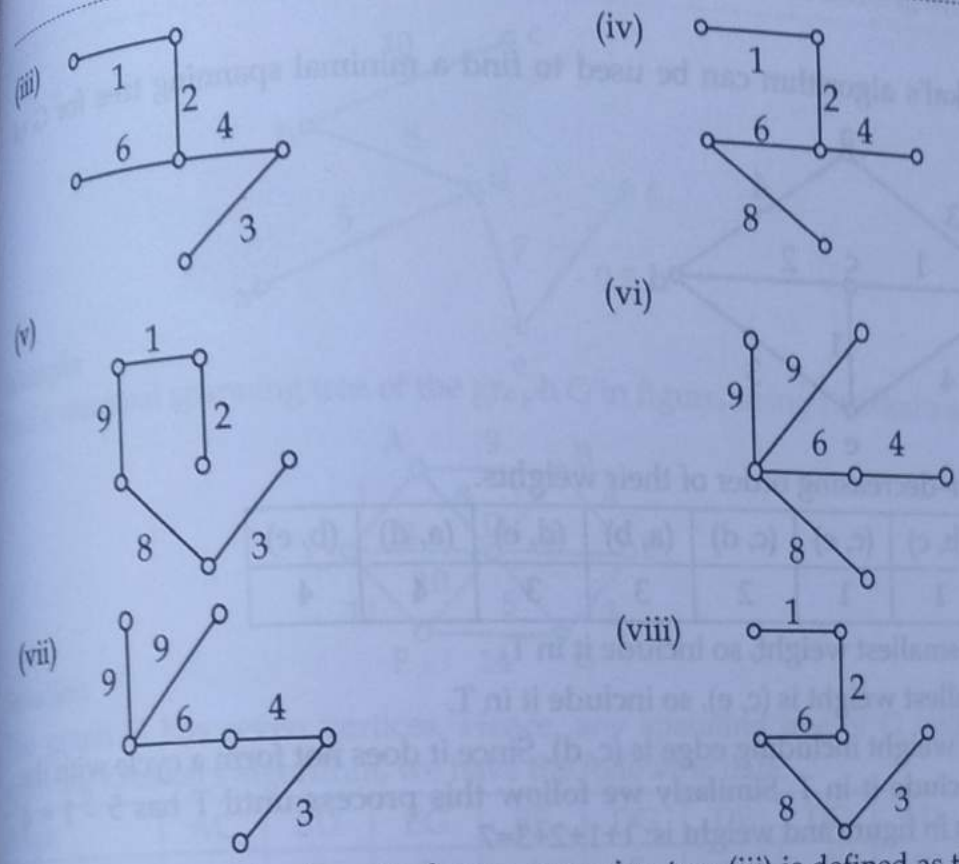
Now, we consider some weighted spanning trees of the weighted graph of figure given below.

(i)



(ii)





Among the spanning trees in figure, spanning tree (iii) is defined as the minimal spanning tree since its weight is minimum as compared to the weights of the other spanning trees.

It is unnecessary to find the weights of all the possible spanning trees of a given weighted graph to determine its minimal spanning tree. There are several algorithms for determining the minimal spanning tree of the given weighed graphs. However we shall discuss only two algorithms here.

Kruskal's Algorithm

The algorithm involves the following steps:

Step 1: List all the edges of G with non-decreasing order of their weights.

Step 2: Select an edge of minimum weight (if there are more then one edge of minimum weight, arbitrarily choose one of them). This will be the first edge of T.

Step 3: At each stage, select an edge of minimum weight from all the remaining edges of G if it does not form a cycle with the previously selected edges in T. Then add the edge to T.

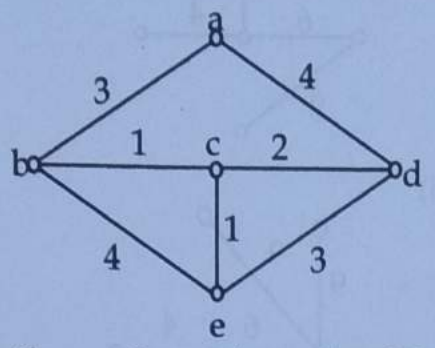
Step 4: Repeat step 3 until n -1 edges have been selected.

Pseudo-code for kurskal's Algorithm

```
KruskalMST(G)
{
    T={V}// Set of vertices
    E= Set of edges sorted in non-decreasing order of their weight
    while(|T| <n-1 and E!=NULL)
    {
        select(u,v) from the E in order
        remove (u,v) from E
        if(u,v) does not create cycle in T
        T=TU{(u,v)
    }
}
```

Example

Show step by step, how Kruskal's algorithm can be used to find a minimal spanning tree for G of figure.



Solution

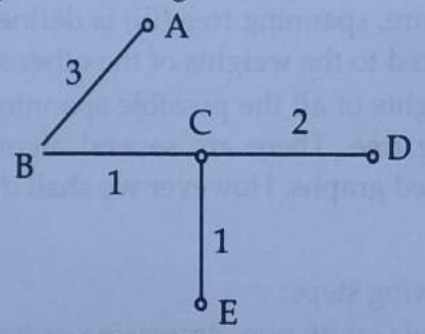
Step 1: List the edges with non-decreasing order of their weights.

Edge	(b, c)	(c, e)	(c, d)	(a, b)	(d, e)	(a, d)	(b, e)
Weight	1	1	2	3	3	4	4

Step 2: The edge (b, c) has the smallest weight, so include it in T.

Step 3: An edge with next smallest weight is (c, e), so include it in T.

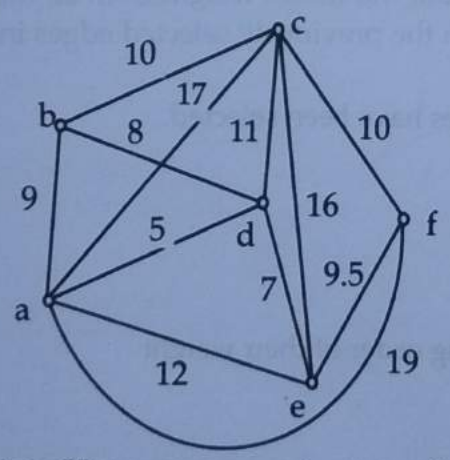
Step 4: Similarly next smallest weight including edge is (c, d). Since it does not form a cycle with the existing edges in T, include it in T. Similarly we follow this process until T has 5 - 1 = 4 edges which are shown in figure and weight is: 1+1+2+3=7



T = (V, E)

Example

Find a minimal spanning tree of weighted graph G in figure, using Kruskal's algorithm.

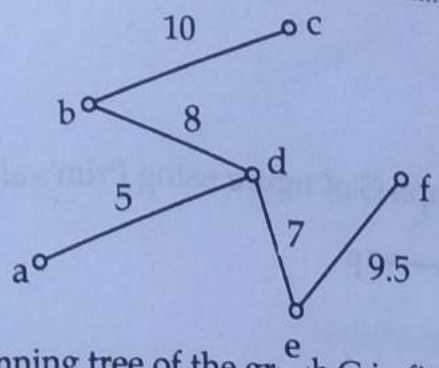


Solution

The graph G has six vertices. Hence, any spanning tree of G will have (6 – 1) = 5 edges.

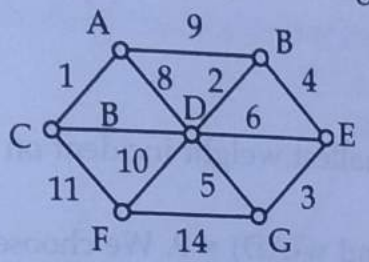
Edges	(a,d)	(d, e)	(b,d)	(a, b)	(e, f)	(b, c)	(c, f)	(d, c)	(a, e)	(c,e)	(a, c)	(a, f)
Weight	5	7	8	9	9.5	10	10	11	12	16	17	19
Select	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No

Thus, the minimal spanning tree of G contains the edges {(a, d), (d, e), (b, d), (e, f), (b, c)}. This minimal spanning tree of weight 39.5 is shown in figure.



Example

Find a minimal spanning tree of the graph G in figure, using Kruskal's algorithm.

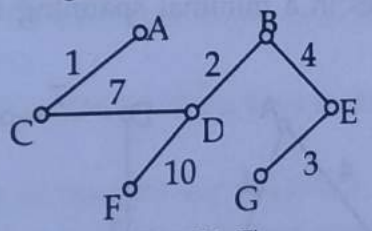


Solution

The graph G has seven vertices. Hence, any spanning tree of G will have (7 - 1) = 6 edges. By applying Kruskal's algorithm, we have the following data:

Edge	AC	BD	EG	BE	DG	DE	DC	AD	AB	DF	CF	FG
Weight	1	2	3	4	5	6	7	8	9	10	11	12
Select	Yes	Yes	Yes	Yes	No	No	Yes	No	No	Yes	No	No

Thus, the minimal spanning tree of G contains the edges (AC, BD, EG, BE, DC, DF). This minimal spanning tree of weight 27 is shown in figure.



T = (V, E)

Prim's Algorithm

This algorithm involves the following steps:

Step 1: Select any vertex in G. Among all the edges which are incident to it, choose an edge of minimum weight. Include it in T.

Step 2: At each stage, choose an edge of smallest weight joining a vertex which is already included in T and a vertex which is not included yet so that it does not form a circuit. Then include it in T.

Step 3: Repeat until all the vertices of G are included with n - 1 edges.

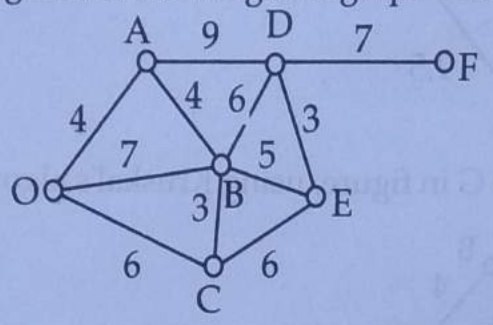
The pseudo-code for prim's algorithm

```
primsMST(G)
{
        T={ }       //set of edges of MST
        S={s}       //s is the randomly chosen vertex
        while(S!=V)
        {
          e={u,v} //an edge of miimum weight incident to vertices in s and not forming a
        simple cycle in T.
        T=T U{u,v}
        S=SU{v}
```

```
        }
    }
```

Example

Find the minimal spanning tree of the weighted graph G of figure using Prim's algorithm.



Solution

Step 1: We choose a vertex O. Now edge with smallest weight incident on O is OA. So we include OA in T.

Step 2: Now w(OB) = 7, w(OC) = 6, w(AB) = 4 and w(AD) = 9. We choose the edge AB since it is minimum. Then we include it in T.

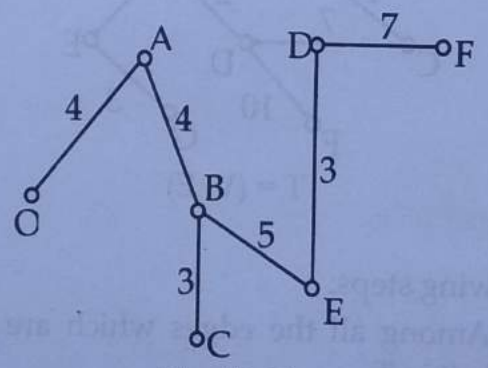
Step 3: Now w(BD) = 6, w(BE) = 5, w(BC) = 3, w(AD) = 9, w(OC) = 6. So we choose B and include it in T.

Step 4: Again w(OC) = 6, w(CE) = 6, w(BE) = 5. So we choose BE and include it in T.

Step 5: Since w(ED) = 3, we include it in T.

Step 6: Now w(DF) = 7, and further we have no choice since if we choose any remaining edge whose weight is less or equal to seven, it forms a circuit. So we include DF in T.

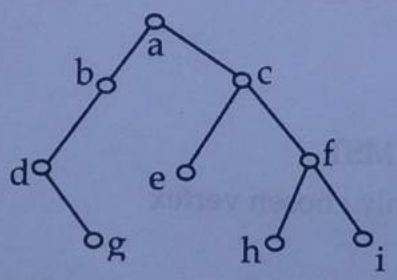
So we have (7 – 1) = 6 edges in a minimal spanning tree, which is shown in figure and weight is: 3+3+4+4+5+7=26



T = (V, E)

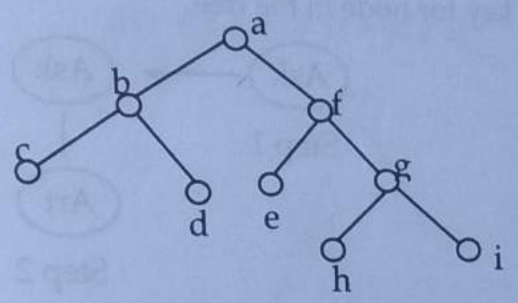
Binary Tree

A binary tree is a finite set of elements that is either empty or partitioned into three disjoint subsets. the first subset contains the single elements called root of the tree, the other subsets are called left and right sub tree of original tree. The binary tree is so named because each node can have at most two descendants.



Strictly Binary Tree

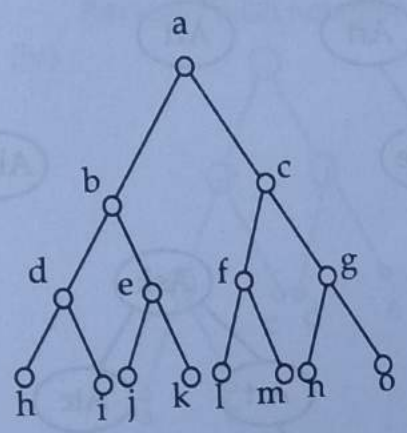
A binary tree is called strictly binary tree if every non-leaf node in a binary tree has non-empty left and right sub-tree.



Strictly binary Tree

Complete (Full) Binary Tree

A strictly binary tree in which all the leaf nodes lies on same level is called complete binary tree.

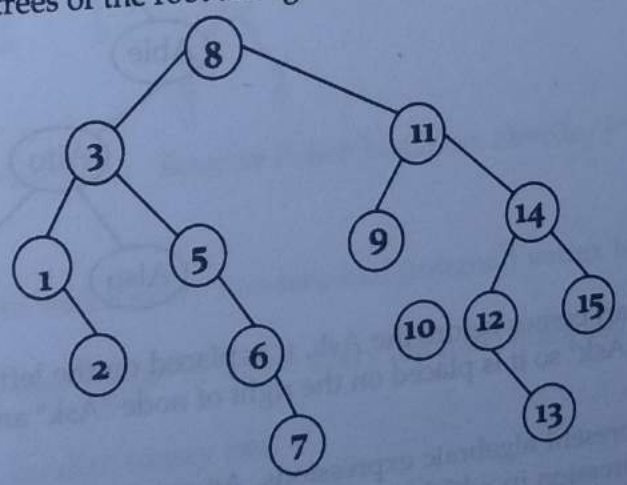


Complete Binary Tree

Binary Search Trees

A binary search tree is a binary tree that is either empty or in which each node possesses a key that satisfies the following three conditions:

- For every node X in the tree, the values of all the keys in its left subtree are smaller than the key value in X.
- Keys in its right subtree are greater than the key value in X.
- The left and right subtrees of the root are again binary search trees.



A Binary Search Tree

Example

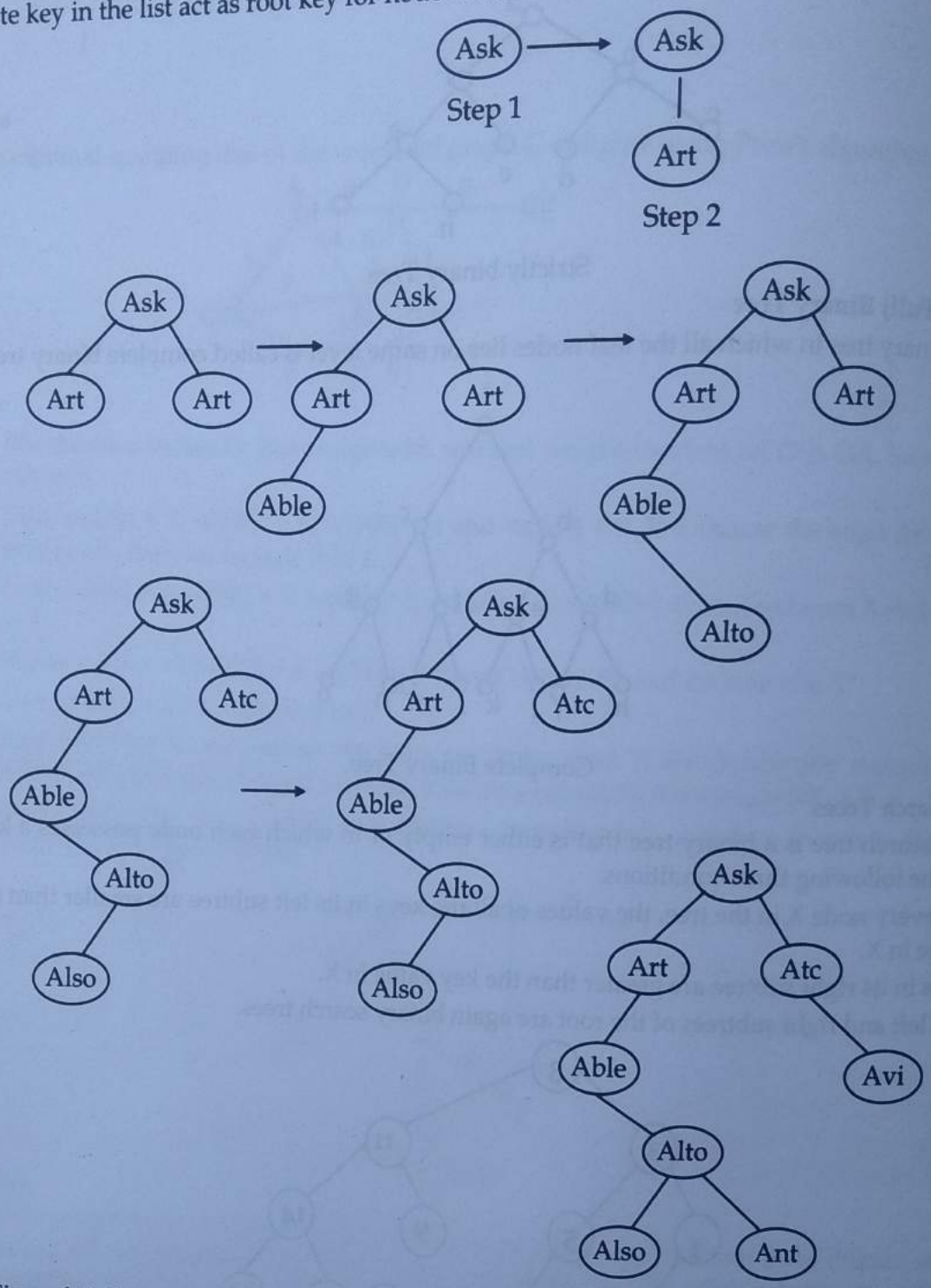
Draw a BST for the flowing words: ask, art, atc, able, alto, also, avid, ant.

Solution

Given list of key is

ask, art, ate, able, alto, also, avid, ant

The finite key in the list act as root key for node in the tree.



[Note: Since alphabetically art comes before the Ask, it is placed on the left of node "Ask". Similarly, "Ate" curve after the word "Ask" so it is placed on the right of node "Ask" and so on].

Algebraic Expression Tree

Binary trees are used to represent algebraic expressions. An expression tree is a binary tree used to represent mathematical expression in which all the leaf node contains operands such as constant or variables and non leaf node contains mathematical operators. Operations such as +, –, ×, ÷, ↑, /, etc. can only be assigned to the internal nodes. This particular tree happens to be binary because all of the operations are binary.

Example

Use a binary tree to represent the expressions

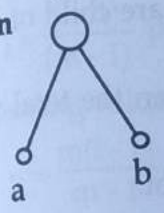
(i) a – b (ii) (a + b) ∗ c

(iii) $(a + b) * (c - d)$ (iv) $((a + b) * c) + (d / e)$

(v) $(a + b) * (c + (d / e))$

Solution

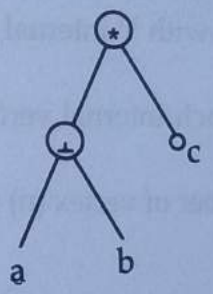
(i)



Polish Notation: -ab

Reverse Polish Notation: ab-

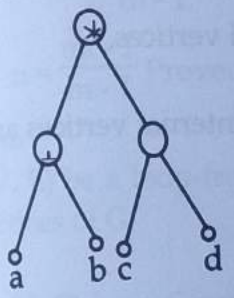
(ii)



Polish notation: *+abc

Reverse Polish notation: ab+c*

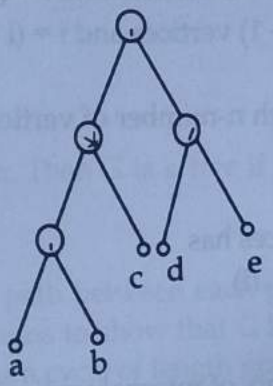
(iii)



Polish Notation: *+ab-cd

reverse Polish Notation: ab+cd-*

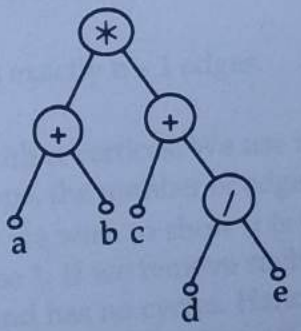
(iv)



Polish Notation: +*+abc/de

Reverse Polish Notation: ab+c*de/+

(v)



Polish Notation: *+ab+c/de Reverse Polish Notation: ab+cde/+*

m-ary tree

A rooted tree T = (V, E) in which every non-terminal (internal) vertex has no more then m-children, is called m-ary tree.

Full m-ary tree: A m-ary tree T = (V, E) where every internal vertex has exactly on children, is called full m-ary tree.

An m-ary tree with m=2 is called binary tree.

Example

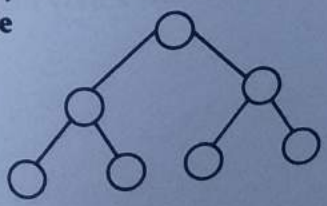


Fig.: Full 2-ary tree

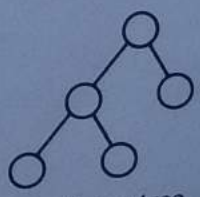


Fig.: 2-ary tree

Theorem:

A full m-ary tree with 'i' internal vertices contain $n = mi + 1$ vertices.

Proof: Let T = (V, E) is a full m-ary tree with 'i' internal vertices except the root are child of internal vertices.

Since, by defination of full m-ary tree each internal vertex has exactly on-children the total vertices except root is equal to $m \times i$.

Hence, A full m-ary tree T has total number of vertex (n) = $m \times i + 1$, including root.

Theorem:

A full m-ary tree with

(i) n vertices has $i = (n - 1)/m$ internal vertices and $l = [(m - 1) \times n + 1)]/m$ leaves.

(ii) i internal vertices has $n = mi + 1$ vertices and $l = (m - 1) \times i + 1$ leaves

(iii) l leaves has $n = (ml - 1)/(m - 1)$ vertices and $i = (l - 1)/(m - 1)$ internal vertices.

Proof:

Let T = (V, E) be a full m-ary tree with n-number of vertices, i be number of internal vertices and l-be number of leaves.

Since,

A full m-ary free with i internal vertices has

$$n = mi + 1 \text{ vertices} \quad .....(i)$$

and

$$n = i + l \quad [\because \text{ total vertices = no. of internal vertices + leaf vertices})$$

From eq^n. (i)

$$n = mi + 1$$

or, $mi = n - 1$

or, $i = (n - 1)/m$ Proved.

Again, putting value of i in equation (ii) we get,

$$n = (n - 1)/m + l$$

or, $$n - \frac{(n-1)}{m} = l$$

or, $$\frac{m * n - n + 1}{m} = l$$

or, $$\frac{n(m-1) + 1}{m} = l$$

i.e. $$l = \frac{n(m-1) + 1}{m}$$

(ii) We know that

$$n = mi + 1 \quad .....(i)$$

and $n = i + l$

Now, putting value of n from (i) to (ii), we get

$$mi + 1 = i + l$$

$$mi + 1 - i = l$$

i.e. $l = i(m - 1) + 1$

(iii) We know that

$$n = mi + 1 \quad .....(1)$$

and $n = l + i \quad .....(2)$

Solving (1) and (2)

$$mi + 1 = l + i$$

$$mi - i = l - 1$$

$$i(m - 1) = l - 1$$

$$i = \frac{(l - 1)}{(m - 1)} \text{ Proved.}$$

Again, putting value of (i) in (1)

$$n = \frac{m(l - 1)}{m - 1} + 1$$

(iv) $$n = \frac{m(l - 1) + m.1}{m - 1}$$

$$n = \frac{ml - m + m - 1}{m - 1}$$

$$n = \frac{ml - 1}{m - 1} \text{ Proved.}$$

Theorem

Let G(V, E) be a loop-free undirected graph. Then G is a tree if there is a unique path between any two vertices of G.

Proof

Let G=(V, E) be a Graph. Since there is a path between each pair of vertices u and v, G must be connected. Thus, to show G is a tree it remains to show that G has no cycles. Since G is loop-free, it has no cycles of length 1. Suppose that G has a cycle of length greater than one, say

$$C = (v_1, v_2, \ldots\ldots, v_n, v_1).$$

Then any two distinct vertices of the cycle C are joined by two paths, which contradict the fact that there is an unique path between any two vertices of G. Hence, G has no cycles and so it is a tree.

Theorem

A tree with n vertices has exactly n – 1 edges.

Proof

Let G= (V, E) be a tree with n vertices. We use induction method to prove it. Let n = 1 i.e. G has one vertex, since it has no loops, the number of edges in G is 0. This establishes that it is true for n = 1. Let it be true for n. Now we wish to show it is true for n + 1. Let G be a tree with n + 1 vertices and let u be a vertex of degree 1. If we remove such a vertex and the edge incident on it, then sub graph G – u is still connected and has no cycles. Hence G – u is a tree. However G – u has n vertices, so by induction it has n – 1 edge. Since G – u has exactly one edge less than that of G, it follows that G has n edges. So assuming n + 1 vertices of G we got n edges. This completes the proof.

Theorem

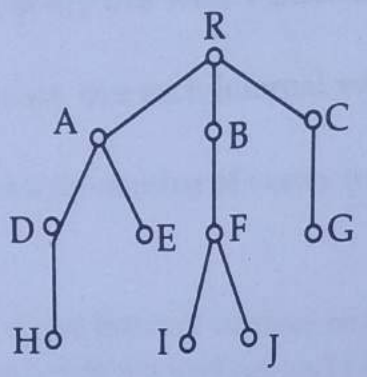
In any tree G, there are at least two pendant vertices.

Proof

Let G= (V, E) be a tree and v_1 be a vertex of degree 1. If there is a vertex v_2 adjacent to v_1 with degree 1 then we are done. If not, we select v_3 adjacent to v_2. Continuing in this way, we get a sequence of vertices $v_1, v_2, \ldots\ldots v_k$. Since a tree has no cycle, this sequence terminates for some K i.e. there exists an adjacent vertex with degree 1. Thus v_1 and v_k are our desired vertices each of degree 1.

Exercise

1. Consider the tree with root R, shown below:



(a) Identify the path from the root R to each of the following vertices and find the level number of the vertex:
(i) D (ii) J (iii) G

(b) Find the leaves of T (tree).

(c) Assuming T is an ordered rooted tree, find the universal address of each leaf of the tree.

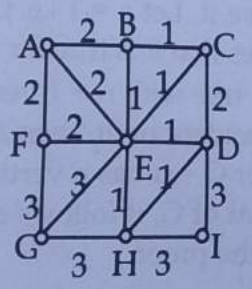
2. Obtain the rooted tree with 'a' as the root from the graph G(V, E) where V = {a, b, c, d, e, f, g, h, I, j, k, l, m} and E = {(c, d), (b, c), (a, b), (a, g), (g, h), (h, k), (a, l), (c, e), (g, i), (g, j), (j, m), (j, f)}. Also find i) ancestors of e, ii) siblings of h, iii) height of tree.

3. If D(V, A) be a directed graph, where the vertices set V = { a, b, c, d, e, f, g, h, i} and the directed edges set A = {(b, c), (b, a) , (d, e), (d, f), (e, h), (f, g), (d, b), (g, i), (g, j)}. Show that D (V, A) is a rooted tree and identify the root and leaves. Also find the height of the tree.

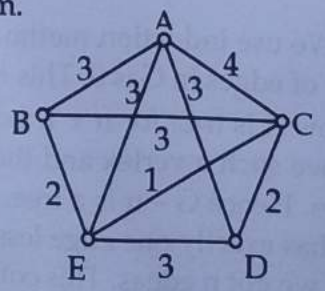
5. Obtain the rooted tree with 'a' as the root from the graph G(v, E), where v={a, b, c, d, e, f, g, h, i, j, k, l, m} and E={(c, d), (b, c), (a, b), (a, g), (g, h) (h, k), (a, l), (c, e), (g, i), (g, j), (j, m), (j, l). Also, find (i) level of each vertices (ii) siblings of h (iii) ancestors of e (iv) height of tree.

6. Find a minimal spanning tree in the weighted graphs shown below by using both Kruskal's algorithm and Prim's algorithm.

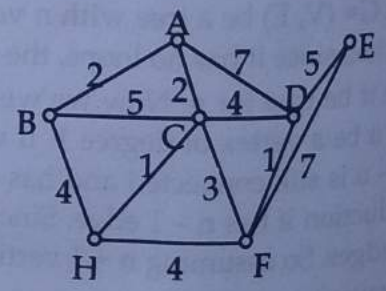
(a)



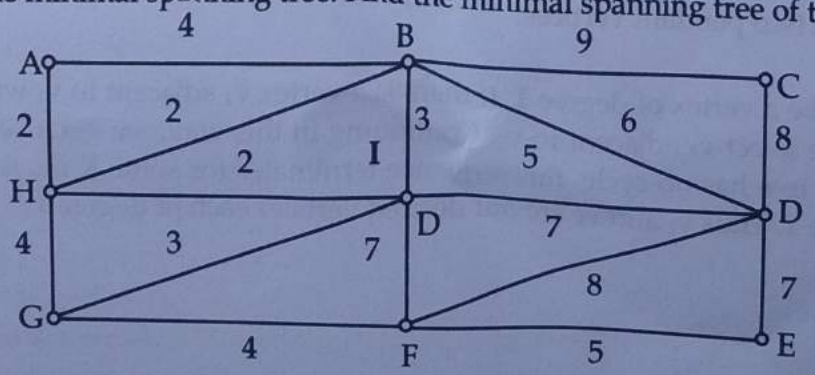
(b)



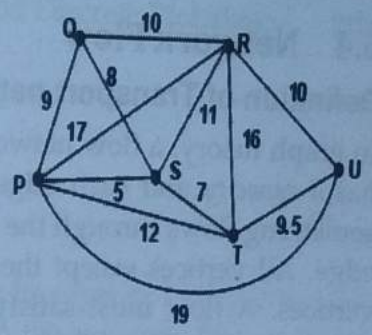
(c)



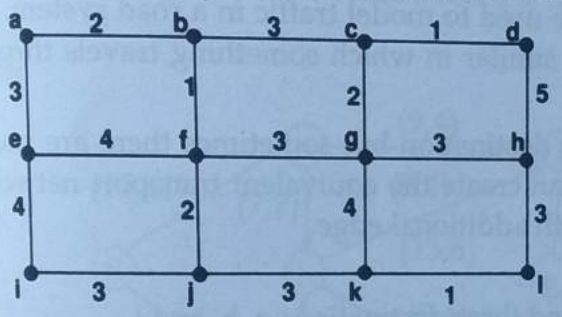
7. Define minimal spanning tree. Find the minimal spanning tree of the following weighted graph.



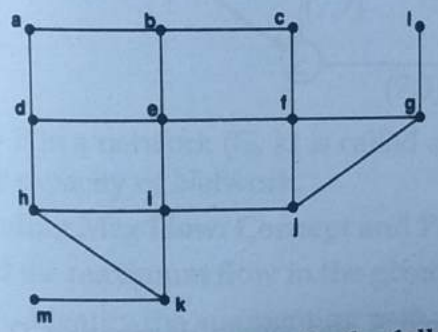
8. Find a minimal spanning tree of the given graph by using Kruskal' algorithm.



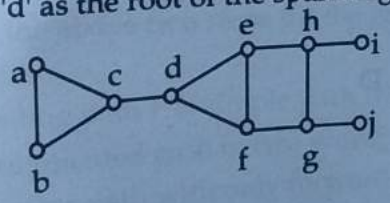
9. Use kruskal's algorithm to find a minimum spanning tree of the graph shown below.



10. Use breadth first search to find a spanning tree for the graph.



11. Find a spanning tree in the following graphs using depth first search and breadth-first search. Choose 'd' as the root of the spanning tree.



6.4 Network Flow

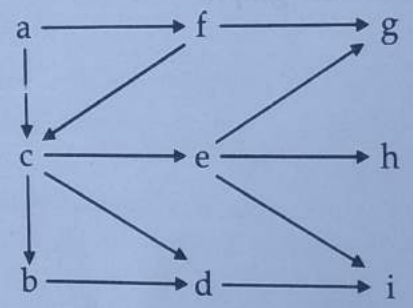
Definition of Transport network

In graph theory, a flow network (also called transport network) is a directed graph where each edge has *a capacity* and each edge receives *a flow*. Here, capacity implies the maximum rate at which something flows through the edge. The amount of flow on an edge cannot exceed the capacity of the edge. All vertices except the source denoted by S and sink denoted by D are called intermediate vertices. A flow must satisfy the restriction that the amount of flow into an intermediate vertex equals the amount of flow out of it, unless it is a source S, which has only outgoing flow, or sink D, which has only incoming flow. A flow network can be used to model traffic in a road system, fluids in pipes, currents in an electrical circuit, or anything similar in which something travels through a network of nodes.

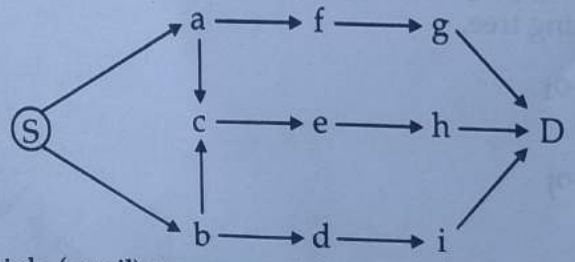
Note: In most cases, there is single source and single destination but sometimes there are multiple sources and multiple destinations. In such case, we can create the equivalent transport network by combining there multiple source auto single source with additional edge.

Example

In the following figure, there are two sources *a* and *b* and three destinations g, h, and i.



Then, the equivalent transportation network with single source *S* and single destination *D* is as shown in figure.



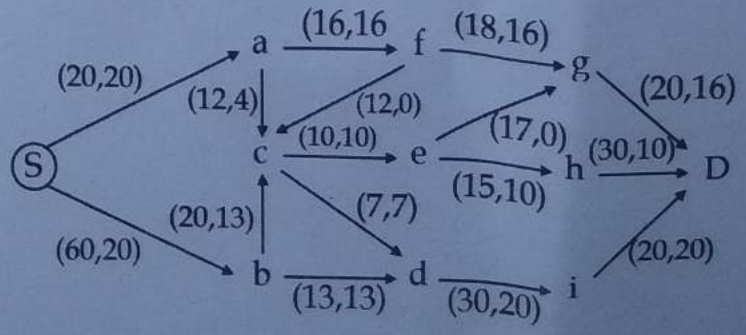
Flows: The materials (or oil) transport along any edge is known as flow.

Let us label edges with two no. first label represents the capacity of edge and second represent the amount of flow through that edge. The two criteria are:

(i) The amount of flow can't exceed the capacity of that edge.

(ii) For every node (except S & D), the amount of flow flowing into vertex v (Incoming flow) must be equal to the account of flow flowing out of vertex v.

Example



Σ Incoming flow at C = 13+4=17

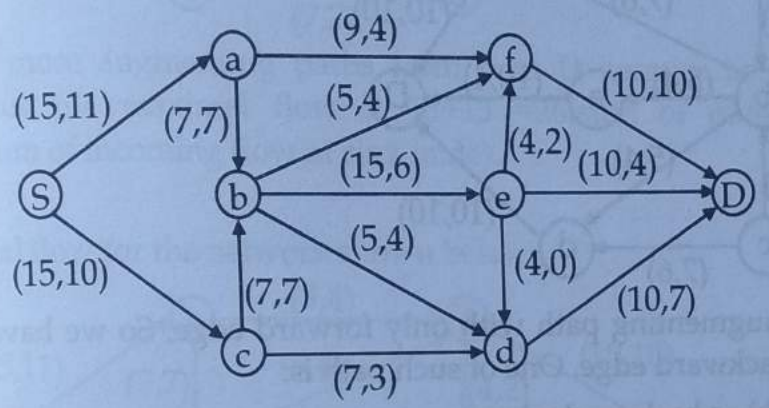
Σ Outgoing flow at C = 10+7=17

[Remarks: Total flow leaving at S = Total flow arriving at D]

Network Flow Problem

Given a transport graph G = (V, E) where each edge *e* is associated with its capacity C(e) > 0 and the two special node: source node *S* and sink or destination node *D* then the network flow problem states that *what is the maximum total amount of flow possible to carry on from Source node S to Destination node D.*

Example



A flow F in a network (G, k) is called a maximal flow if |F| ≥ |F'| for every flow F' in (G, k), Where k is the capacity of Network.

Computing Max Flow: Concept and Process

To find the maximum flow in the given transport network (G,k), the following steps are necessary.

- Identify the augmenting path
- Increase flow along that path
- Repeat the above two steps till the maximum flow is obtained.

Augmenting path

- An augmenting path P is simple path from S to D with unsaturated edge.
- We build augmented path in two ways:

(1) Augmenting path with only forward unsaturated edge.

(2) Augmenting path with some backward edge.

In backward edged Augmenting Path (A.P), the backward edge must have positive flow and of course, the forward edge must be unsaturated.

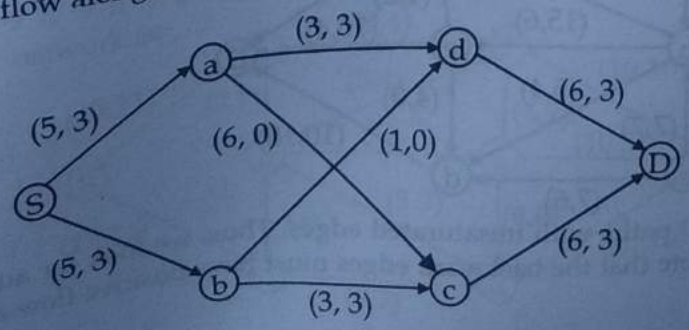
When an edge (eg. d→c) is taken in opposite direction (eg. c→d), is called backward edge

Two Basic Ways to Increase the Value of Flows

(1) If an edge is not being used to capacity, try to send more flow through it.

(2) If an edge is working against us by sending some flow back toward the source, we could try to reduce the flow along this edge and redirect in a more practical direction.

Example



Here, we increase *flow* along path S →a→d→D.

Now,

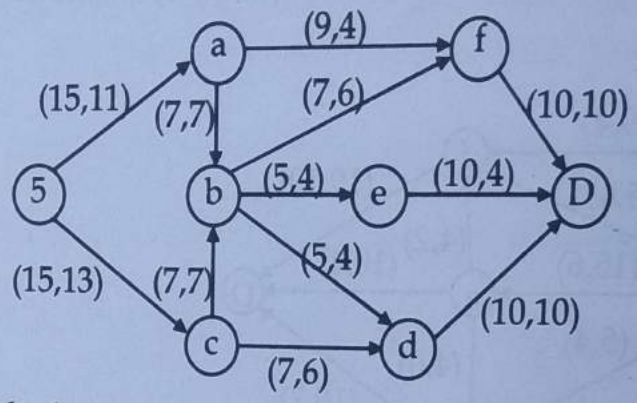
k(S, a) - F(S, a) = 5 - 3 = 2

k(a, d) - F(a, d) = 6 - 0 = 6

k(d, D) - F(d, D) = 6 - 3 = 3

∵ Min. {2, 6, 3} = 2, increase flow by 2.

Example



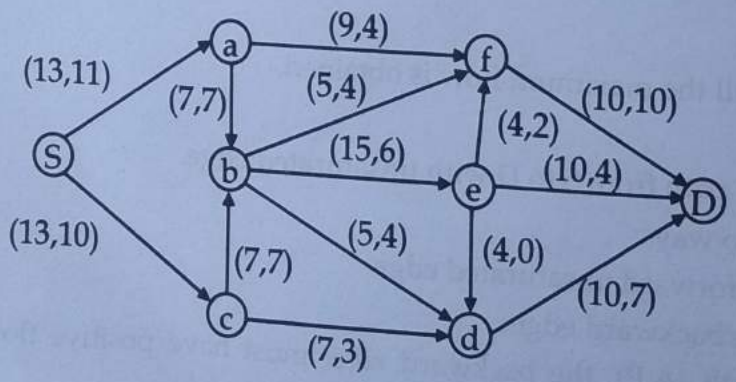
In the given network, there is no augmenting path with only forward edge. So we have to find (if any) augmenting path with some backward edge. One of such path is:

S→ c→ d→ b→ e→ D with (d,b) as backward edge.

This is an augmenting path since we can increase flow by 1 along the path. Note: - in backward edge, we will subtract the flow by 1, to maintain the rule of flow conservation)

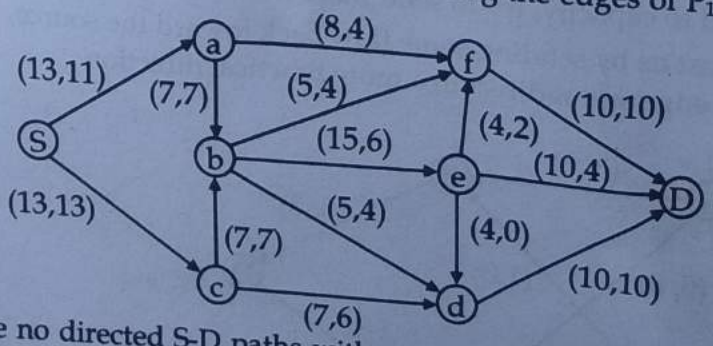
Example

Find a maximal flow for the network below:



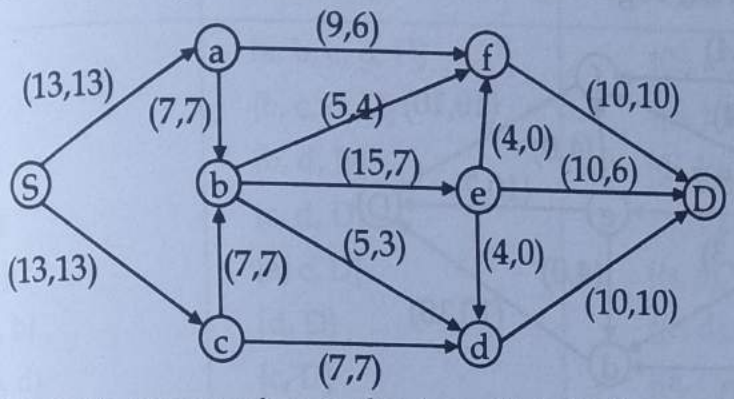
Solution

Here, first we look for an augmenting path where, if possible, all edges are forward edges (and they have to be unsaturated). The path P_1 : s → c → d→D is such a path. The minimum slack of the edges along P_1 is 3. By increasing the flow by 3 with along the edges of P_1, we obtain the flow F_1 as shown below.



Now, there are no directed S-D paths with unsaturated edges. Thus, we look for augmenting paths with some backward edges. Note that the backward edges must have
edges must be unsaturated.

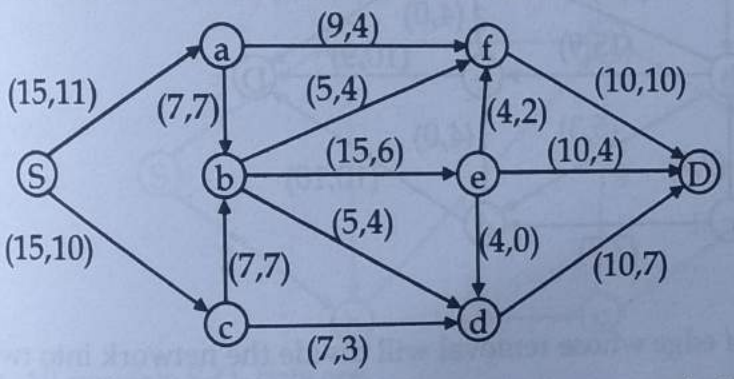
Now, we augment the flow by 2 along the path S → a → f → e → D (with backward edge from *f to e*) to obtain the flow as in figure below:



There are no more augmenting paths from S to D because both edge (S, a) and (S,c) become saturated. Thus the maximal flow is 13+13 =26(sum of outgoing flow at source node) or 10+6+10=26(sum of incoming flow at sink node).

Example

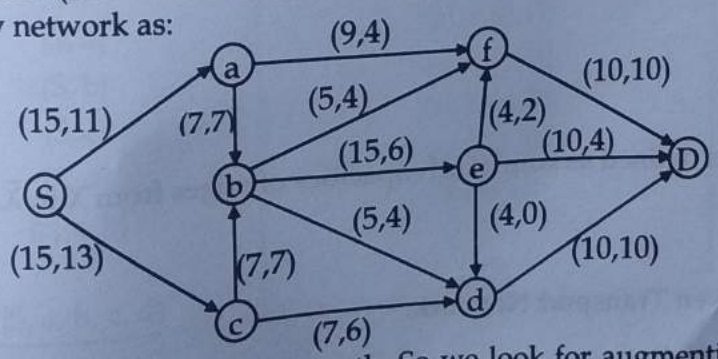
Find a maximal flow for the network shown below:



Solution

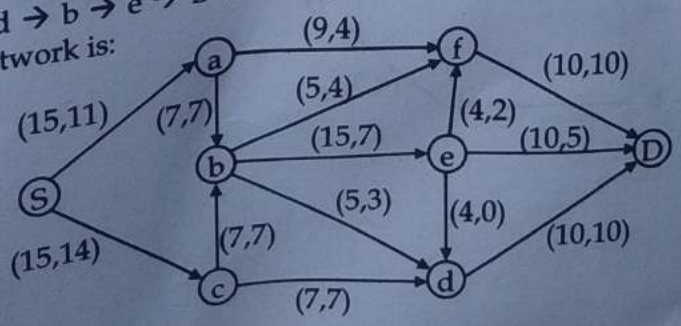
First we try to find out the augmenting path with all forward edge if possible the path: $P_1 = S \to c \to d \to D$ is such path.

The minimum slack (the value that can be augmented /added) along P_1 is 3. After increasing by 3, we have the flow network as:

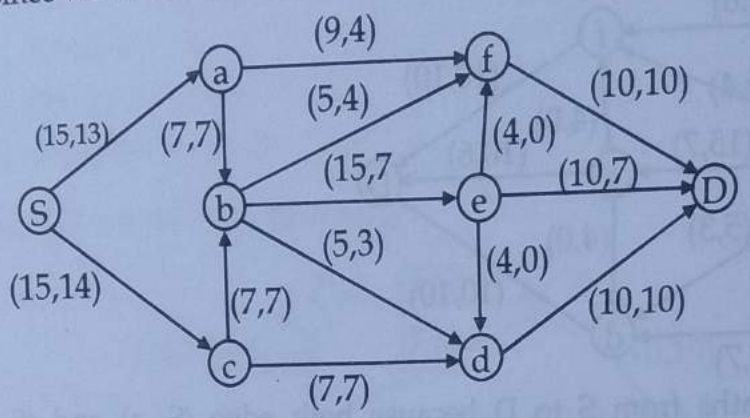


Now, there is no directed augmenting path. So we look for augmenting path with some backward edge.

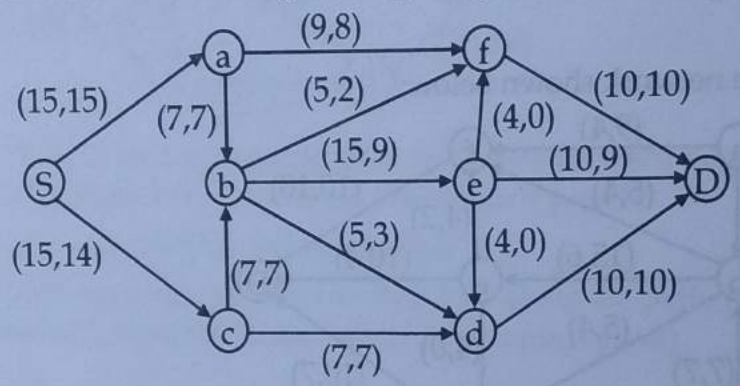
The path: P_2: S → c → d → b → e → D is such path with minimum slack. So after augmenting this path with flow 1, the network is:



Now, another augmenting path with backward edge is P_3: $S \to a \to f \to e \to D$, where the minimum slack is 2 (since we can't make backward edge -ve), the flow network is



Now, another augmenting path with backward edge is P_4 : $S \to a \to f \to b \to e \to D$, where the minimum slack is 2, the flow network augmenting this path.



S - D Cut or Cut

A cut of transport network is a set of edge whose removal will divide the network into two halves X and $\bar{X}$ where:

- Source vertex $S \in X$
- Sink vertex $D \in \bar{X}$

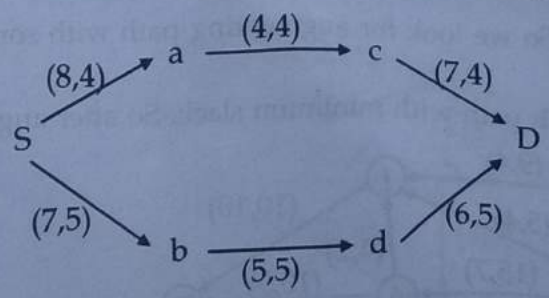
It is denoted by $(X, \bar{X})$

Capacity of Cut

The capacity of S-D cut $(X, \bar{X})$ is defined as sum of all capacities of edges from X to $\bar{X}$. It is denoted by $K(X, \bar{X})$.

Example

Find all the S-D cuts in the given Transport Network.



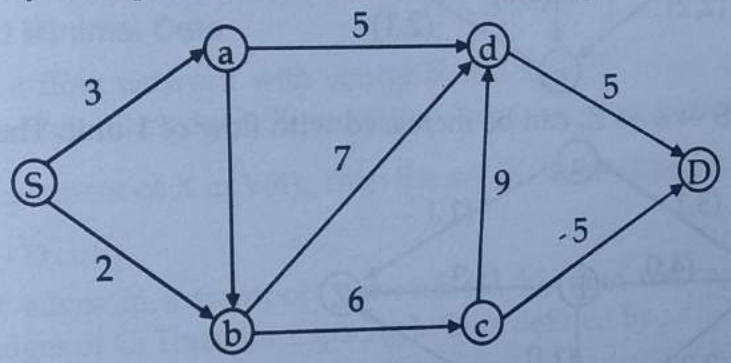
Solutions: All possible S-D cuts are:

X	$\bar{X}$	Cuts $(X, \bar{X})$	$K(X, \bar{X})$
S	{a, b, c, d, D}	{(S, a), (s, b)}	15
{S, a}	{b, c, d, D}	{(S, b), (a, c)}	11
{S, a, c}	{b, d, D}	{(S, b), (c, D)}	14
{S, a, b}	{c, d, D}	{(a, c), (b, d)}	9
{S, b, d}	{a, c, D}	{(s, a), (d, D)}	14
{S, a, c, b}	{d, D}	{(c, d), (b, d)}	13
{S, a, b, d}	{c, D}	{(a, c), (d, D)}	10
{S, a, c, b, d}	{D}	{(c, d), (d, D)}	13

The capacity of minimal cut is 9.

Example

Calculate the capacity of all possible S-D cuts in the following flow network.



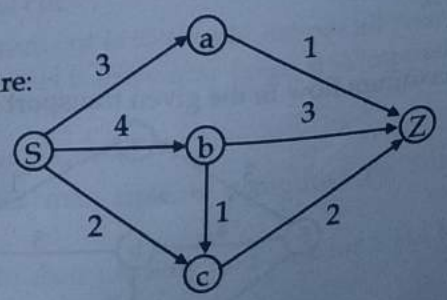
Solution. All possible S-D- cuts are:

X	$\bar{X}$	$K(X, \bar{X})$
{S}	{a, b, c, d, D}	3 + 2 = 5
{S, a}	{b, c, d, D}	2 + 4 + 5 = 11
{S, b}	{a, c, d, D}	3 + 7 = 10
{S, c}	{a, b, d, D}	3 + 2 + 6 + 5 = 16
{S, d}	{a, b, c, D}	3 + 2 + 9 + 5 = 19
{S, a, b}	{c, d, D}	5 + 7 = 12
...	...	...
{S, a, b, c, d}	{D}	5 + 5 = 10

∴ Minimal cut = 5

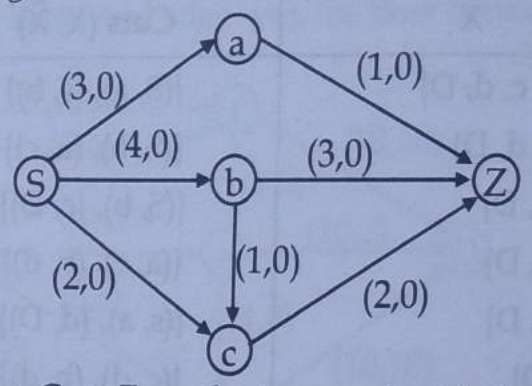
Example

Find the maximum flow in the network shown in figure:

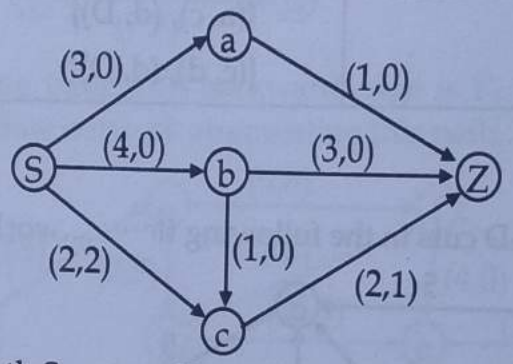


Solution:

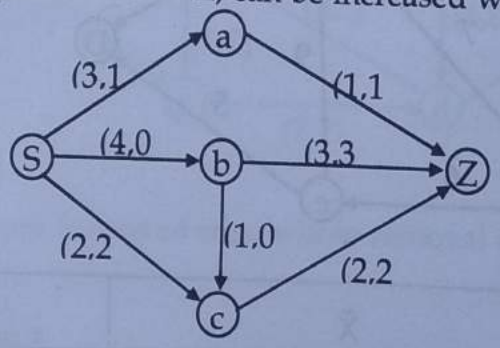
Since, there is no initial flow given in the network, we initialize all flow equal to zero as shown below:



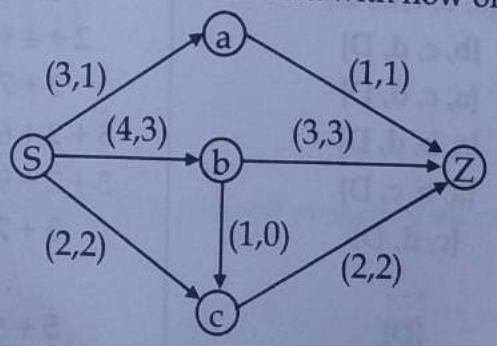
Now, the augmenting path S → C → Z can be increased with the flow of 2 unit and the resulting network is



Again, the augmenting path S → a → Z, can be increased with flow of 1 unit. The resulting network is



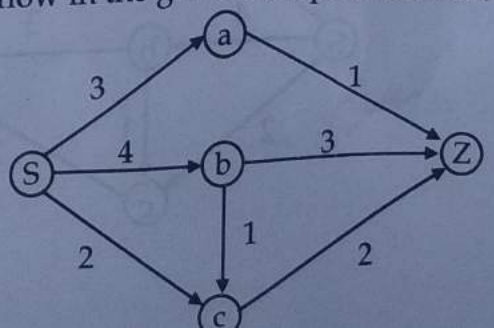
Again, the path S → b → Z can be increased with flow of 3 unit and the resulting network is



Since, there is no more augmenting path (all path are saturated), the maximum flow in the given network is: 6.

Example:

Find the maximum flow in the given transport network using S-D cut method.



Solution: The possible S-D cut for the given network are tabulated below.

X	$\bar{X}$	$(X, \bar{X})$	$K(X, \bar{X})$
{S}	{a, b, c, Z}	{(s, a), (s, b), (s, c)}	9
{S, a}	{b, c, z}	{(s, b), (S, c), (a, Z)}	6
{S, b}	{a, c, Z}	{(s, a), (S, c), (b, c), (b, Z)}	9
{S, c}	{a, b, Z}	{(S, a), (S, b), (c, Z)}	9
{S, a, b}	{c, z}	{(S, c), (b, c), (b, Z), (a, Z)}	7
{S, a, c}	{b, Z}	{(S, b), (a, Z), (c, Z)}	7
{S, b, c}	{a, z}	{(S, a), (b, Z), (c, Z)}	8
{S, a, b, c}	{Z}	{(a, Z), (b, Z), (c, Z)}	6

$\therefore$ The capacity of minimum cut = 6.

By max-flow, min-cut theorem, the max flow in network = 6.

Maximal Flow and Minimal Cuts

Suppose (G, k) in a flow network with source S and sink D, where G represents the graph and k represents the capacity of the edges. Suppose that X in a set of vertices such that $S \in X$, but $D \notin X$. Let $\bar{X}$ denotes the complement of X in V(4). Then the set $(X, \bar{X})$ of all edges from a vertex in X to a vertex in $\bar{X}$ is called an S - D cut.

If C is any set of edges in a transport network (G, k), then the capacity of C is the sum of the capacities of the edges of C. Thus, the capacity k(C) in defined by :

$$k(C) = \sum_{e \in C} k(e)$$

The capacity of an S-D cut, $k(X, \bar{X})$ in the sum of all capacities of edges from X to $\bar{X}$. There may be edges from $\bar{X}$ to X but are not exerted into the computation of $k(X, \bar{X})$. We call an S-D cut $(X, \bar{X})$ a minimal cut if there is no S-D cut $(Y, \bar{Y})$ such that

$$k(Y, \bar{Y}) < k(X, \bar{X})$$

Computing Minimal Cut from Max Flow

Let V_S be the set of verties reached by augmenting path from the source S, and v_D is the set of remaining vertices, then the cut (v_S, v_D) is the minimal cut.

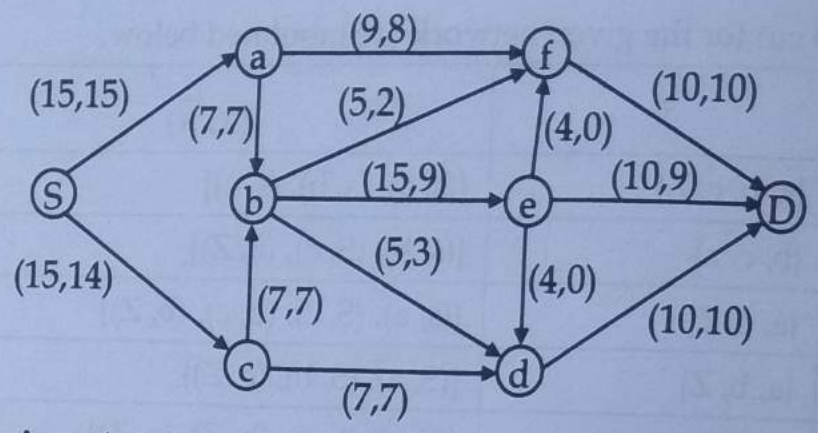
One very *simple* but *inefficient* way to find the minimum cut is to simply list out all possible cuts and select the smallest. However, the number of possible cuts is extremely large, it is impossible to list all possible cuts in a network.

A better approach is to make use of ***max flow min-cut theorem.***

The minimum cut is actually simple to find after max flow is computed by Ford-Folkerson algorithm.

Simply mark the edges that carrying a flow equal to their capacity and look for a cut that consists only of marked edge and no other edges.

Example



Theorem (Max. flow min cut)

Statement: In any flow (transport) network, the value of any maximal flow is equal to the capacity of a minimal cut.

Proof:

We know that for a given flow network with flow F and capacity of cut K, we have

Value of F ≤ capacity of k.

Now, optimizing this flow network such that there are no F-augmenting paths, we have

value of F = capacity of cut k

Let F* be maximum flow and k* be minimum cut for the network. Then for some flow F and cut k, we have

capacity of k = value of F ≤ capacity of k*

But no cut can have capacity less than minimum cut, we have

value of F = capacity of k*

Also, we have

value of F* ≤ capacity of k* = value of F

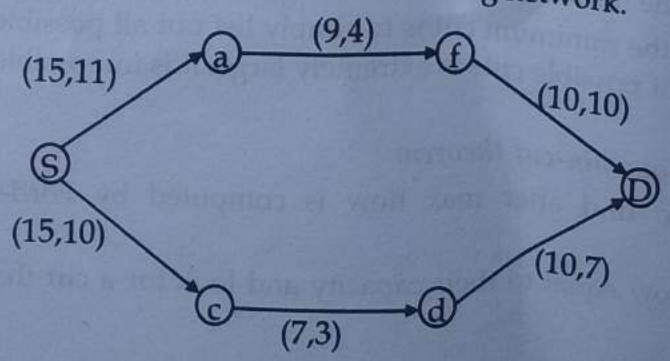
But no flow can be greater than the maximum flow.

∴ Value of F* = Capacity of k*.

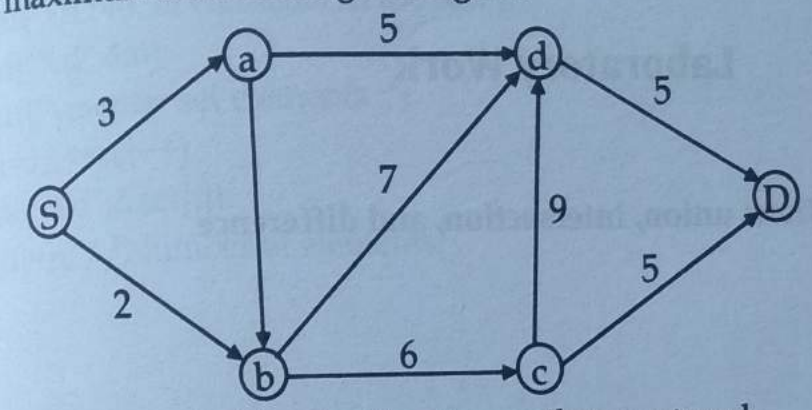
Hence proved.

Exercise

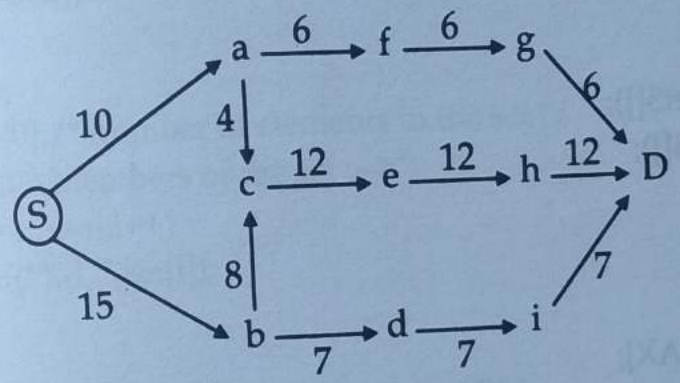
1. Define cut and capacity of cut.
2. Define maximum flow for the transport network.
3. What is augmenting path?
4. What is maximum flow problem? Illustrate it with suitable example.
5. Find all possible S-D cut for the following network.



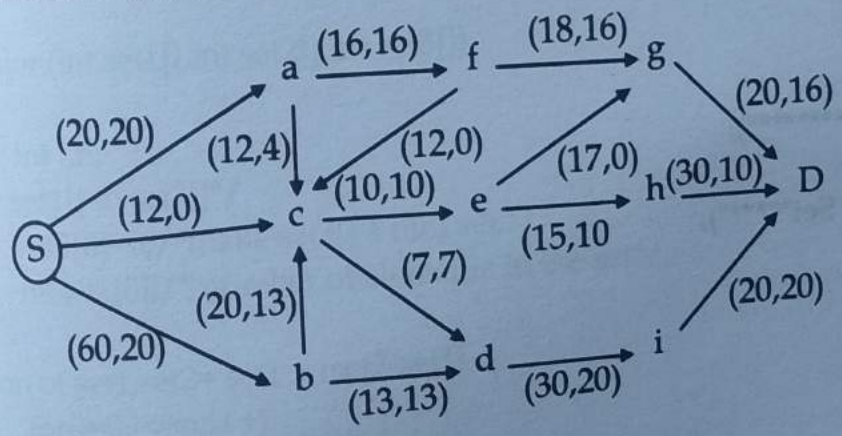
Find the maximum flow in the given figure.



7. Find the maximum flow for the given railway network.



8. Find the maximum flow for the given network.



Model Question

Section A

Long Answer Questions

Attempt any 2 questions. **[2×10=20]**

1. Why breaking down of large integer into set of small integers is preferred while performing integer arithmetic? Find sum of numbers 123,684 and 413,456 by representing the numbers as 4-tuple by using reminders modulo of pair-wise relatively prime numbers less than 100. {2+8}
2. Define linear homogeneous recurrence relation. Solve the recurrence relation $a_n = a_{n/2} + n + 1$ with $a_1 = 1$. Also discuss about probabilistic primility testing with example. {2+4+4}
3. How Zero-one matrix and diagraphs can be used to represent a relation? Explain the process of identifying whether the graph is reflexive, symmetric, or anti-symmetric by using matrix or diagraph with suitable example. {4+6}

Section B

Short Answer Questions

Attempt any 8 questions. **[8×5=40]**

4. Prove that $\overline{A \cap B} = A \cup B$ by using set builder notation. How sets are represented by using bit string? Why it is preferred over unordered representation of sets? {3+2}
5. How can you relate domain and co-domain of functions with functions in programming language? Discuss composite and inverse of function with suitable examples. {2+3}
6. State Euclidean and extended Euclidean theorem. Write down extended Euclidean algorithm and illustrate it with example. {1+4}
7. State and prove generalized pigeonhole principle? How many cards should be selected from a deck of 52 cards to guarantee at least three cards of same suit? {2.5+ 2.5}
8. Represent the argument "If it does not rain or if is not foggy then the sailing race will be held and the lifesaving demonstration will go on. If sailing race is held then trophy will be awarded. The trophy was not awarded. Therefore it not rained" in propositional logic and prove the conclusion by using rules of inferences. {2+3}
9. Discuss common mistakes in proof briefly. Show that n is even if $n^3 + 5$ is odd by using indirect proof. {2+3}
10. How mathematical induction differs from strong induction? Prove that $1^2 + 2^2 + 3^2 + ... n^2 = n(n + 1)(2n + 1)/6$ by using strong induction. {1+4}
11. Write down recursive algorithm for computing a^n. Argue that your algorithm is correct by using induction. {2.5+2.5}
12. What is meant by chromatic number? How can you use graph coloring to schedule exams? Justify by using 10 subjects assuming that the pairs {(1,2), (1,5), (1,8), (2,4), (2,9), (2,7), (3,6), (3,7), (3,10), (4,8), (4,3), (4,10), (5,6), (5,7)} of subjects have common students. {1+4}

Guideline for Question Setter

→ There must be at least one question from each unit

→ There should not be more than one question from a sub-unit