



Propositional Logic

Introduction:

It has a large amount of applications in mathematics. It is used to prove theorems. Every theorem consists of various statements which ultimately reach a conclusion. To check the validation of these statements, logic is required. Mathematical logic tells us whether the statement is valid or not. Now, the question that may arise is, from where do all these statements come from? So, all these statements come from a set of all English statements.

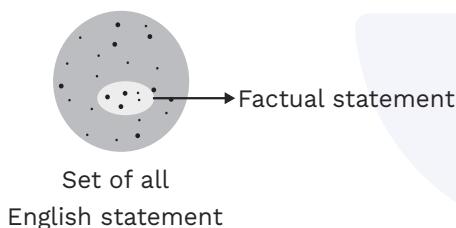


Fig. 1.1

Definition



Proposition: Proposition is a logical statement which can be true or false but not both.

- e.g: 1. $2 + 2 = 4$
- 2. 'C' is a vowel

Note:

- Factual statements are part of the “set of all English statements” which is used to conclude something. These factual statements in mathematical logic are called propositional logic.
- Factual statements are facts which have only two cases yes(true)/no(false)
- Any **question, command, exclamation, vague reference** will never be a proposition.

1. Which of the following is/are not proposition?
 - (A) $x + 2 = 5$
 - (B) He is tall
 - (C) Today is Monday
 - (D) Tomorrow will be rain

Solution: (A), (B), (C), (D)



Rack Your Brain

Is “Read this carefully” a proposition?

Atomic and compound proposition:

The Propositional statement is of two types

1. Compound propositional statement
2. Atomic propositional statement

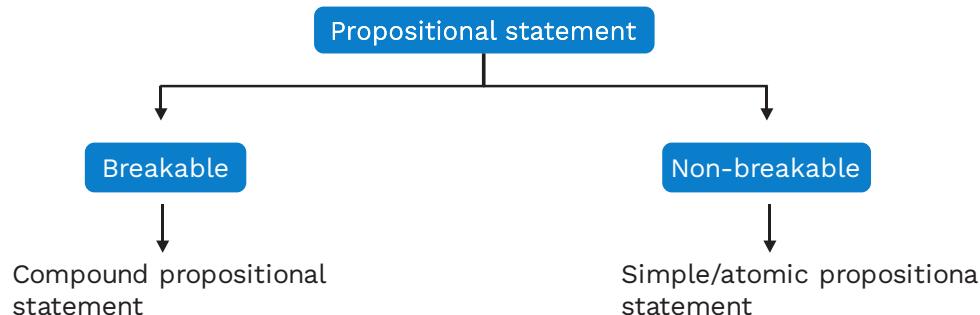


Fig. 1.2



Statements that are constructed by combining one or more factual statements, to form a new proposition is called a compound proposition.

- e.g: 1. $5 > 3$: non-breakable, \therefore atomic
 2. $5 \geq 3$: This statement can be broken into
 a) $5 > 3$
 b) $5 = 3$
 \therefore Compound statement

Propositional variable:

A variable is used to represent the proposition.

Simple proposition represented by $p, q, r\dots$

Compound proposition represented by $P, Q, R\dots$

Single propositions have 2 possible truth combinations.

p
T
F

Two propositional variables have $2^2 = 4$ truth combinations.

f	g
0	1
1	0
1	1
0	0

3 propositions variables - 8 truth combinations

⋮

n propositions variables - 2^n truth combination

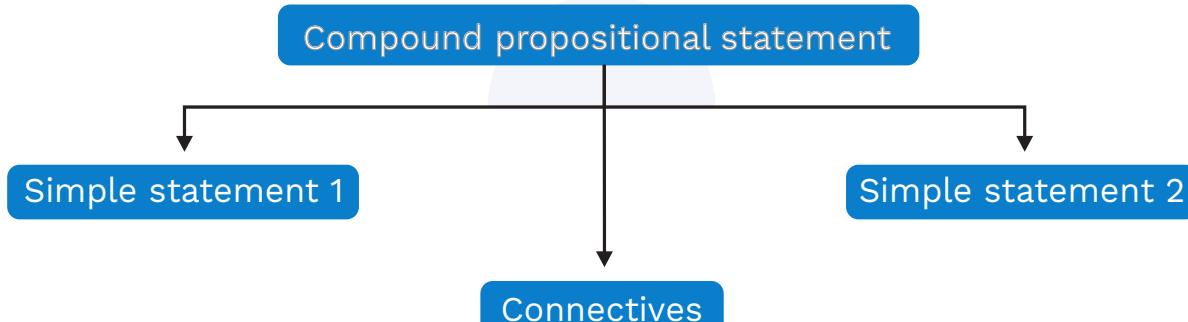
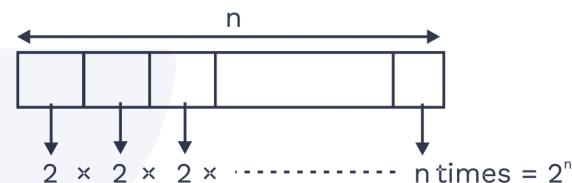


Fig. 1.3

A compound statement is breakable into simple statements while breaking it; it is breakable at the breaking point / weak point called connectives. That weak point is called connectives.

In mathematics, there are 4 types of connectives:

- | | |
|--|--|
| <ul style="list-style-type: none"> • Conjunction / AND • Disjunction / OR • Implication • Bi implication | <p>Representation</p> <ul style="list-style-type: none"> (\wedge) (\vee) (\rightarrow/\Rightarrow) ($\Leftrightarrow/\leftrightarrow$) |
|--|--|

Note:

There is 1 more type of connective called "modifiers (negation)".



Boolean logic:

1. Negation:

It is a unary operation and can be denoted in the following ways:

- a) $\neg p$
- b) $\sim p$
- c) p'
- d) \bar{p}

Note:

A unary operation is an operation which can be implemented on single proposition.

Definition

Negation: Let p be a proposition. The “negation of p ”, denoted by $\neg p$ (also by \bar{p}),

is the statement “It is not the case that p ”. The proposition \bar{p} is read as “not p ”.

The truth value of \bar{p} is the opposite of the truth value of p .

e.g: Let a proposition $p =$ I am Michel.

The negation of $p(\bar{p}) =$ I am not Michel.

p	\bar{p}
T	F
F	T

Table 1 The Truth Table for the Negation of a Proposition

2. Conjunction:

It is basically AND operator and is represented by “ \wedge ”.

Definition

Conjunction: Conjunction is similar to performing AND operation between two variables. Conjunction between two proposition will be true only when both the propositions are true otherwise it will always be false.

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

Table 2 The Truth Table for Conjunction of Proposition

Note:

In the truth table, we mention the cases. As we all know, the compound statement is nothing but a group of some atomic/simple statements. We generate cases out of these atomic statements to reach the conclusion of the compound statement.



Rack Your Brain

Find the conjunction of the proposition p & q where p is the proposition “It is raining today”, and q is the proposition “I will not go to the school”.

3. Disjunction:

Disjunction is an “OR” case.

OR is of two types:

- a) Inclusive OR (\vee)
- b) Exclusive OR (\oplus)

Note:

In mathematics, we always use (\vee) inclusive OR, until and unless it is mentioned as \oplus



Inclusive OR:

If any of the simple propositions are true, the conclusion will be true and the conclusion will be false otherwise.

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

Table 3 Table for Disjunction Using Inclusive OR

For example,

“Students who have taken calculus or computer science can take this class”.

With this statement, we mean that those students who have taken either calculus or computer science can take the class also, the students who have taken both can take the class.

Exclusive OR:

Using exclusive OR, we can reframe the sentence as

“Students who have taken calculus or computer science, but not both can take the class”.

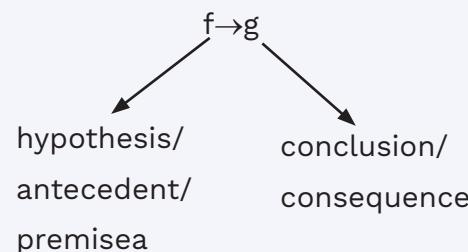
q	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Table 4 Table for Disjunction Using Exclusive OR

Conditional statement/implication:

Definition

Let f and g be two propositions, and the conditional statement $f \rightarrow g$ is the proposition, “if f then g ”. The conditional statement $f \rightarrow g$ is false when f is true and g is false, and true otherwise.



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

Table 5 The Truth Table for the Conditional Statement $p \rightarrow q$

Different forms of Implication (\rightarrow):

$p \rightarrow q$ can be written as:

- p implies q
- if p then q
- if p , q
- q if p
- q when p
- q whenever p
- q unless p
- p only if q
- a sufficient condition for q is p
- q whenever p
- q is necessary for p
- q follows from p



Rack Your Brain

Convert the given statement into propositional logic form

p: I stay

q: you go

1. I stay if you go
2. I stay only if you go
3. I stay unless you go
4. you go when I stay

1. If you win, I will give you pizza.

Solution:

The statement can be interpreted as: if you win the match, then I will give you pizza.

Case 1: Let p be the proposition “If you win” (hypotheses) and q be conclusion “I will give you pizza”.

Case 1 says p and q both are true, means “If you win, I will give you pizza” which is true.

$$\therefore p \rightarrow q = \text{True.}$$

Case 2: p = True = If you win

q = False = I will not give you a pizza

which means, If you win, I will not give you pizza, which is false.

$$\therefore p \rightarrow q = \text{False.}$$

Case 3: Similarly, In case 3 the conclusion is “If you do not win, I will give you pizza” is True. As this condition can not be interpreted from the given statement.

$$\therefore p \rightarrow q = \text{True}$$

Case 4: Thus case says, “If you do not win, I will not give you pizza” Which is true

$$\therefore p \rightarrow q = \text{True.}$$



Rack Your Brain

Let p be the statement “Maria learns discrete mathematics” and q be the statement “Maria will find a good job”. Express the statement $p \rightarrow q$ as a statement in English.

Converse, contrapositive, and inverse:

These are different types of conditional statements.

Let us consider an implication $p \rightarrow q$

- **Contrapositive** $\sim q \rightarrow \sim p$
- **Converse** $q \rightarrow p$
- **Inverse** $\sim p \rightarrow \sim q$

Law of contrapositive:

Implication and its contrapositive are equivalent

$$p \rightarrow q \equiv \sim q \rightarrow \sim p$$

Converse and Inverse are equivalent.

$$q \rightarrow p \equiv \sim p \rightarrow \sim q$$



Rack Your Brain

What is the inverse of “The home team wins whenever it is raining”.

Bi-conditionals:

It is represented by (\leftrightarrow)

Definition



Let p and q be propositions. The biconditional statement $p \leftrightarrow q$, is the proposition “p if and only if q” or “p if q”. Biconditional statement between two propositions will be true only when both the propositions have same values (True or false) in all the other cases it will give false output.



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

Table 6 Truth Table for the Biconditional $p \leftrightarrow q$.

e.g., Let p be the statement “you can take the flight” and q be the statement “you buy a ticket”. $p \leftrightarrow q$ will be, “you can take the flight if and only if you buy a ticket”.

Precedence of logical operator:

Generally, we use parenthesis to define the precedence of a logical operator.

- Negation operator has the highest priority. For example, let us consider a proposition $\neg p \wedge q$. This proposition will be considered as the conjunction of $(\neg p)$ and q and not the negation of the conjunction of p and q .
- Conjunction operator’s precedence is greater than the disjunction operator’s precedence.
- The conditional and biconditional operator has the lowest precedence among all operators.

Operator	Precedence
\neg	1
\wedge	2
\vee	3
\rightarrow	4
\leftrightarrow	5

Table 7 Precedence of Logical Operators

Compound propositions:

We have already studied connectives, i.e., conjunction, disjunction, conditional, bi-

conditional statements and negations. Now, we can use all these connectives to forms compound propositions with ‘n’ number of variables.

Construct a truth table for: $(p \vee \neg q) \rightarrow (p \wedge q)$

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

Table 8 Example for Truth Table for Compound Propositions



Rack Your Brain

How many rows appear in a truth table for the following compound statements

- (A) $p \rightarrow \neg p$
(B) $(p \vee \neg r) \wedge (q \vee \neg r)$

Generally, we use 1 to represent true and 0 to represent false.

A Boolean variable is a variable that has a value of either 0 or 1.

p	q	$p \vee q$	$p \wedge q$	$p \oplus q$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Table 9 Table for Bit Operators: OR, AND and XOR



Rack Your Brain

Find the bitwise OR, bitwise AND and bitwise XOR for the following pair of strings 11110000, 10101010



Application of propositional logic:

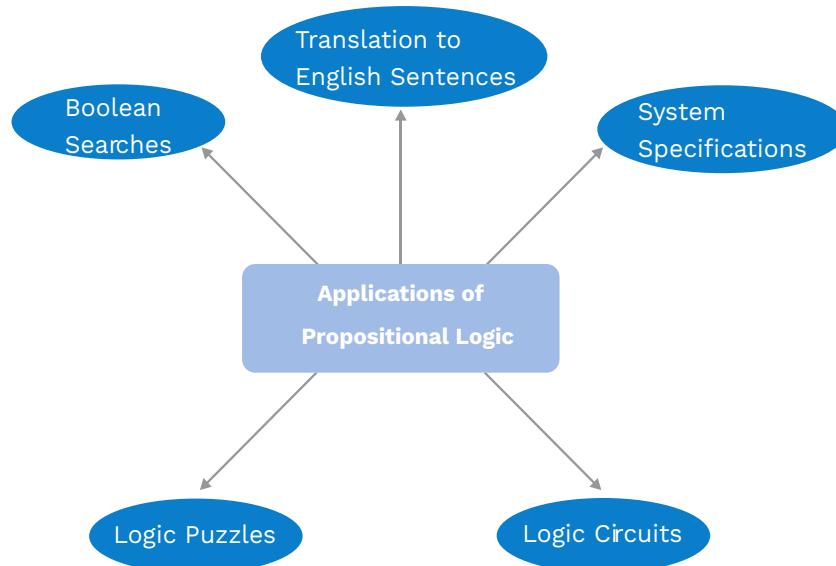


Fig. 1.4

Mathematical logic has a vast number of applications. Some of them we have already mentioned. But we will limit our discussion to only two applications i.e.

- (i) Translating English sentences
- (ii) Logic circuits

- **Translating English sentences:**

English is very ambiguous; to resolve that ambiguity, we translate these sentences into compound statements.

- **Example:**

Convert given sentence into a logical form:

“You can not ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old.”

- **Solution:**

Let p , q , r represent “You can ride the roller coaster,” “you are under 4 feet tall”; and “you are older than 16 years old”.

\therefore The sentence can be translated to

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

- **Logic circuits:** Logic is also used to design hardware, which takes the input signal and produces output signals. As we use connectives negation etc., to form compound statements, similarly,

in the hardware, we use basic circuits called gates to form the combinational circuit.

- **(A) AND gate:** It takes two signals as input and produces $(p \wedge q)$ signal as output.



Fig. 1.5

- **(B) Or gate:** It takes two signals as input and gives $(p \vee q)$ signal as output.

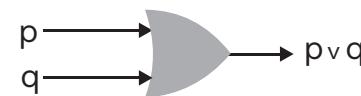


Fig. 1.6

- **(C) Not gate/inverters:**

It takes p as input and produces (\bar{p}) as output.



Fig. 1.7

- **Combinatorial circuit:**

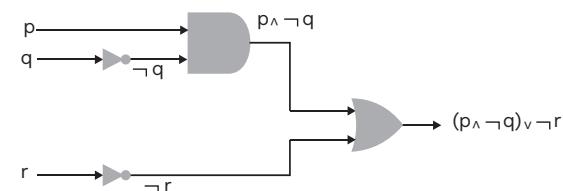


Fig. 1.8



Logically equivalent:

- Two propositions are said to be logically equivalent if and only if they have same truth table.
- Two propositions are said to be logically equivalent if $p \leftrightarrow Q$ is a tautology.
- The Equivalency of two propositions is represented by (\equiv)

Example 1: Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

p	q	$p \rightarrow q$	$\neg p \vee q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Table 1.10

Now, $p \rightarrow q$ and $\neg p \vee q$ are precisely same.

\therefore Both boolean expressions are logically equivalent.

Tautology:

If a given proposition turns out to be always true, then it is called a tautology.

Example:

$$p \vee \sim p$$

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

Contradiction:

If a given proposition turns out to be always false, then that proposition is a contradiction.

Example:

$$p \wedge \sim p$$

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	T

Contingency:

Given proposition turns out to be either true or false, then that proposition is contingency.

Example:

$$(p \wedge q) \rightarrow s$$

p	q	s	$p \wedge p \sim s$
T	T	T	F
T	T	F	T

Note:

Contradiction is also known as fallacy or invalid.

Satisfiable:

A proposition that is either a tautology or a contingency is called satisfiable.

Example:

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

q	r	s	$(p \wedge q \wedge r) \rightarrow s$
T	T	T	F
T	T	F	T

Contingency so satisfiable

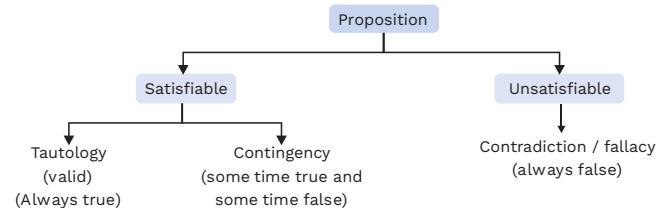


Fig. 1.9



Rack Your Brain

Choose the correct option:

- All valids are satisfiable
- All contingency are satisfiable
- All satisfiable are contingency
- None



2. Which of the following option/s are satisfiable compound propositions?
- $(p \vee \neg q) \wedge (\neg p \wedge q) \wedge (\neg p \vee \neg q)$
 - $(p \rightarrow q) \wedge (p \wedge \neg q) \wedge (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$
 - $(p \leftrightarrow q) \wedge (\neg p \leftrightarrow q)$
 - None of the above

Solution:

$$\begin{aligned}
 (A) &= (p \vee \neg q) \wedge (\neg p \wedge q) \wedge (\neg p \vee \neg q) \\
 &= (p + \neg q) (\neg p + q) (\neg p + \neg q) \\
 &= (p \cdot \neg p + p \cdot q + \neg p \cdot \neg q) (\neg p + \neg q) \\
 &= (p \cdot q + \neg p \cdot \neg q) (\neg p + \neg q) \\
 &= (\neg p \cdot \neg q + \neg p \cdot \neg q) \\
 &= (\neg p \cdot \neg q)
 \end{aligned}$$

As given preposition depend on the value of 'p' and 'q' thus it can be true or false therefore satisfiable.

$$\begin{aligned}
 (B) &= (p \rightarrow q) \wedge (p \rightarrow \neg q) \wedge (\neg p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \\
 &= (\neg p + q) (\neg p + \neg q) (p + q) (p + \neg q) \\
 &= ((p + q) (\neg p + \neg q)) ((p + \neg q) (\neg p + q)) \\
 &= 0
 \end{aligned}$$

Given preposition is contradiction thus not satisfiable.

$$\begin{aligned}
 (C) &= (p \leftrightarrow q) \wedge (\neg p \leftrightarrow q) \\
 &= (p \rightarrow q) \wedge (q \rightarrow p) \wedge (\neg p \rightarrow q) \wedge (\neg q \rightarrow \neg p) \\
 &= ((\neg p + q) (\neg q + p)) ((p + q) (\neg q + \neg p)) \\
 &= 0
 \end{aligned}$$

It is also not satisfiable.

3. The predicate statement $\forall z[p(z) \rightarrow (\neg q(z) \rightarrow p(z))]$ is:
- Satisfiable
 - Tautology
 - Contradiction
 - None of these

Solution:

$$\begin{aligned}
 &\forall z[p(z) \rightarrow (\neg q(z) \rightarrow p(z))] \\
 &\equiv \neg \exists z[\neg p(z) \vee q(z) \vee p(z)] \\
 &\equiv \neg \forall z[T \vee q(z)] \\
 &\equiv \neg T \\
 &\equiv F
 \end{aligned}$$



Previous Years' Questions

Choose the correct choice regarding the following propositional logic assertion S:

[GATE CSE 2021 Set-2]

- S: $((P \wedge Q) \rightarrow R) \rightarrow (((P \wedge Q) \rightarrow (Q \rightarrow R))$
- S is neither a tautology nor a contradiction
 - S is a tautology
 - S is a contradiction
 - The antecedent of S is logically equivalent to the consequent of S.

Solution: (B), (D)

Applications of satisfiability:

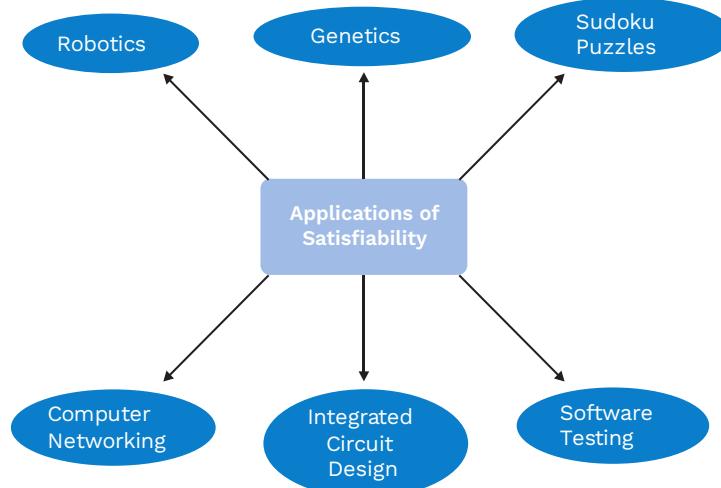


Fig. 1.10



Rack Your Brain

Which of the compound propositions are satisfiable.

- (A) $(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg s)$
- (B) $(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg s) \wedge (p \vee \neg q \vee \neg s) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg r \vee \neg s)$

Logical equivalence:

Equivalences (laws):

T = Compound statement that is always true.
F = Compound statement that is always false.

Equivalence	Name
$F \wedge T \equiv F$	
$F \vee F \equiv F$	Identity laws
$F \vee T \equiv T$	
$F \wedge F \equiv F$	Domination laws
$F \vee F \equiv F$	
$F \wedge F \equiv F$	Idempotent laws
$\neg(\neg F) \equiv F$	Double negation law
$F \vee s \equiv s \vee F$	Commutative laws
$F \wedge s \equiv s \wedge F$	
$(F \vee s) \vee r \equiv F \vee (s \vee r)$	Associative laws
$(F \wedge s) \wedge r \equiv F \wedge (s \wedge r)$	
$F \vee (s \wedge r) \equiv (F \vee s) \wedge (s \vee r)$	Distributive laws
$F \wedge (s \vee r) \equiv (F \wedge s) \vee (s \wedge r)$	
$\neg(F \wedge s) \equiv \neg F \vee \neg s$	De Morgan's laws
$\neg(F \vee s) \equiv \neg F \wedge \neg s$	
$F \vee (F \wedge s) \equiv F$	Absorption laws
$F \wedge (F \vee s) \equiv F$	
$F \vee \neg s \equiv T$	Negation laws
$F \wedge \neg s \equiv F$	

Table 11 The Special Case of Boolean Algebra Identities

These laws help to make complicated-looking boolean expressions simple.

"Bitty bought a butter, but the butter was bitter, so bitty bought another butter to make bitter butter, better butter."

- As, the above statement seems a little complicated, but it can be made simpler using English.
- Similarly, in mathematical logic, complicated boolean expressions can be made simpler with the laws stated above in table 11.

Equivalences involving implication:

$f \rightarrow s$	\equiv	$\neg f \vee s$
$f \rightarrow s$	\equiv	$\neg s \rightarrow \neg f$
$f \vee s$	\equiv	$\neg f \rightarrow s$
$\neg(f \rightarrow s)$	\equiv	$f \wedge \neg s$
$(f \rightarrow s) \wedge (f \rightarrow r)$	\equiv	$f \rightarrow (s \wedge r)$
$(f \rightarrow r) \wedge (s \rightarrow r)$	\equiv	$(f \vee s) \rightarrow r$
$(f \rightarrow s) \vee (f \rightarrow r)$	\equiv	$f \rightarrow (s \vee r)$
$(f \rightarrow r) \vee (s \rightarrow r)$	\equiv	$(f \vee s) \rightarrow r$

Table 12 Logical Equivalences Involving Conditional Statements

$f \leftrightarrow s$	\equiv	$(f \rightarrow s) \wedge (s \rightarrow f)$
$f \leftrightarrow s$	\equiv	$\neg f \leftrightarrow \neg s$
$f \leftrightarrow s$	\equiv	$(f \wedge s) \vee (\neg f \vee \neg s)$
$\neg(f \leftrightarrow s)$	\equiv	$f \leftrightarrow \neg s$

Table 13 Logical Equivalence Involving Biconditional Statements

De Morgan's laws:

As we have already seen that De Morgan's laws state:

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

Note:

When using De Morgan's laws, remember to change the logical connective after you negate.

It states that negation of conjunction/disjunction is formed by disjunction/conjunction.

conjunction of negation of the component propositions.

4. Use De Morgan's law to express the negation of "Maya will go to fare or Abdul will go to fare".

Solution:

\Rightarrow Let p = Maya will go to fare
 q = Abdul will go to fare
 Can be represented by $p \vee q$
 Now, the negation of $p \vee q = \neg(p \vee q)$
 According to De Morgan's law $\neg(p \vee q) = \neg p \wedge \neg q$
 Which states that Maya will not go to fare and Abdul will not go to the fare.

5. Use De-Morgan's law, to show $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logical equivalent.

Solution:

$\neg(p \vee (\neg p \wedge q))$ [using De Morgan law]
 $\neg p \wedge \neg(\neg p \wedge q)$
 $\neg p \wedge [\neg(\neg p) \vee \neg q]$
 $\neg p \wedge (p \vee \neg q)$ [Using distributive law]
 $(\neg p \wedge p) \vee (\neg p \wedge \neg q)$
 $F \vee (\neg p \wedge \neg q) \quad (\because \neg p \wedge p \equiv F)$
 $\neg p \wedge \neg q$ [using commutative law of disjunction]
 Hence, proved, $\neg(p \vee (\neg p \wedge q))$ is logically equivalent to $\neg p \wedge \neg q$.

The general form of an argument: (Inference)

The process of deriving the conclusion based on assumption is called an **argument**.

The conjunction of premises implies a conclusion.

$$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow q$$

An inference which is **tautology** called **valid inference** otherwise invalid inference.

Rule of inference:

Any valid inference is the rule of inference.

Name	Rule of Inference	Tautology
Addition	$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$
Conjunction	$\frac{q}{\therefore p \wedge q}$	$([p] \wedge [q]) \rightarrow (p \wedge q)$
Simplification	$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$
Modus ponens	$\frac{\begin{array}{l} p \rightarrow q \\ p \end{array}}{\therefore q}$	$(p \wedge [P \rightarrow q]) \rightarrow q$
Hypothetical syllogism	$\frac{\begin{array}{l} p \rightarrow q \\ q \rightarrow r \end{array}}{\therefore p \rightarrow r}$	$([p \rightarrow q] \wedge [q \rightarrow r]) \rightarrow (p \rightarrow r)$
Disjunctive syllogism	$\frac{\begin{array}{l} p \vee q \\ \neg p \end{array}}{\therefore q}$	$([p \vee q] \wedge \neg p) \rightarrow q$
Modus tollens	$\frac{\begin{array}{l} p \rightarrow q \\ \neg q \end{array}}{\therefore \neg p}$	$(\neg q \wedge [p \rightarrow q]) \rightarrow \neg p$
Resolution	$\frac{\begin{array}{l} p \vee q \\ \neg p \vee r \end{array}}{\therefore q \vee r}$	$([p \vee q] \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

Table 14 Rules of Inference

6. "If Vinay comes to the ceremony, Atul will not come to the ceremony. If Atul doesn't come to the ceremony, Siddhu will come to the ceremony."

Solution:

Let the propositions be as follows:

p : Vinay comes to the ceremony.



q: Atul does not come to the ceremony.

r: Siddhu comes to the ceremony.

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

This argument is a hypothetical syllogism.

Functional completeness: If any boolean function can be expressed using a given set of boolean functions, then that set of boolean functions is functionally complete.

For example, The set $\{\wedge, \vee, \neg\}$ is clearly functionally complete.

Note:

With n variable, $2^{(2^n)}$ boolean functions can be represented.

- The set $\{\wedge, \neg\}$ is said to be functionally complete or minimal functionally complete set.
- The set $\{\vee, \neg\}$ is also functionally complete.
- The set $\{\wedge, \vee\}$ is not functionally complete as we can not generate "not" with the of "AND" and "OR".

Note:

A set is said to be functionally complete if we can derive a set which is already functionally complete.

Minimally functionally complete set: A set is said to be minimally functionally complete if:

- It is functionally complete

- No subset of the given set is functionally complete.

For example:

- $\{\wedge, \vee, \neg\}$ is not minimally functionally complete.
- $\{\wedge, \neg\}, \{\vee, \neg\}$ are minimally functionally complete.

E.g., with \uparrow we can generate "NOT", "AND", and "OR".

Note:

$\{\uparrow\}$ and $\{\downarrow\}$ are smallest functionally complete sets.

Normal forms: The method of reducing a given formula to an equivalent form is called 'normal form'.

There are two types of standard normal forms:

- PDNF (Principal disjunctive normal form)
- PCNF (Principal conjunctive normal form)

Considering m for minterm and M for maxterm.

Note:

Number of terms in PDNF + Number of terms in PCNF = 2^n

After solving the boolean function.

If the conclusion is '1' then it'll be considered in minterms maxterm otherwise.

PDNF: Disjunction of min terms

PCNF: Conjunction of max terms

E.g., $p \leftrightarrow (q \rightarrow r')$

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

p	q	r	$q \rightarrow r'$	$p \leftrightarrow (q \rightarrow r')$	Min Terms	Max Terms
0	0	0	1	0	m_0	$M_0 = p \vee q \vee r$
0	0	1	1	0	m_1	$M_1 = p \vee q \vee r'$
0	1	0	1	0	m_2	$M_2 = p \vee q' \vee r$



0	1	1	0	1	$m_3 = p' \wedge q \wedge r$	M_3
1	0	0	1	1	$m_4 = p \wedge q' \wedge r'$	M_4
1	0	1	1	1	$m_5 = p \wedge q' \wedge r'$	M_5
1	1	0	1	1	$m_6 = p \wedge q \wedge r'$	M_6
1	1	1	0	0	m_7	$M_7 = p' \vee q' \vee r'$

Table 15

Predicates and Quantifiers

The meaning of the English statement may not always be possible to express in the form of propositional logic.

For e.g., “Every computer science student in the university is intelligent.”

Now, with the help of propositional logic, we in no way can prove Sanya is intelligent.

Where Sanya is one of the computer science students at the university.

Place where propositional logic can not work, predicate logic comes into the picture. To understand predicate logic, let's first learn about predicate properly.

Predicates:

Consider statement, “x is greater than 5”.

- The subject part: Variable itself
 - The predicate part: Is greater than 5
- so we can denote this statement as $P(x)$, where P is the predicate part and x is variable. When the value is assigned to the variable predicate is converted to propositional logic.



Rack Your Brain

Let $p(x)$ denotes the statement “ $x \leq 4$ ”.

What are these truth values?

- (A) $p(0)$
- (B) $p(4)$
- (C) $p(6)$

Pre conditions and post conditions:

Statements that describe valid input are known as **pre-conditions**, and the condition that the output should satisfy when the program has run is called **post-conditions**.

Quantifiers:

Quantification is a way to create a proposition from a propositional function.

Note:

The area of logic that deals with predicate and quantifiers is called predicate logic.

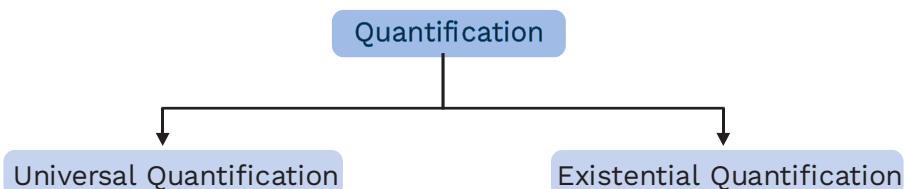


Fig. 1.11



Universal quantifier:

- It tells us the predicate is true for every element under consideration.
- To understand universal quantifier; first we need to understand the term domain of discourse/universe of discourse/domain: When all the values of a variable in a particular domain are true, then a property is called true, that particular domain is called the domain of discourse/universe of discourse/domain.
These types of statements are expressed using universal quantification.

Definition

These universal Quantification of $P(x)$ is the statement.

“ $P(x)$ for all values of x in the domain”
The notation $\forall xP(x)$, denotes the universal Quantification of $P(x)$. Here $\forall x$ is called the universal Quantifier. We read $\forall xP(x)$ as “for all $xP(x)$ ” or “for every $xP(x)$ ”. An element for which $P(x)$ is false is called a counter example of $\forall xP(x)$.

Quantifiers		
Statement	When True	When False
$\forall xP(x)$	$P(x)$ is true for every x .	There is an x for which $P(x)$ is false.
$\exists xP(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x .

Table 16

Existential quantifier:

- By existential quantifier we know that there is atleast one value for which predicate is true.
- In existential quantification, a proposition is formed that is true if and only if $P(x)$ is true for at least one value of x in the domain.

Note:

Truth value of $xP(x)$ depends on the domain.

The uniqueness quantifier:

There is one more type of quantifier called “uniqueness quantifier” denoted by $\exists!$ or \exists_1 .

The notation $\exists!xP(x)$ or $\exists_1xP(x)$ states, “There exists a unique x such that $P(x)$ is true”.

Note:

The truth value of $xP(x)$ depends on the domain.

Logical equivalences involving quantifiers:

Standard definition:

Definition

If two statements have same truth table, then both statements are logically equivalent that two statements S and T involving predicates and quantifiers are logically equivalent.

7. Consider the following statements:
I. $p \wedge q \wedge p \vee q$ is logically equivalent.
II. $p \wedge q \wedge (p \vee q) \wedge (q \vee p)$ is logically equivalent.
Which of the following options are correct?
(A) Only I is true.
(B) Only II is true.
(C) Both are true.
(D) None of the above.

Solution: (C)

I.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Table 1.17

p	q	$\neg p$	$\neg p \vee q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

Table 1.18

Now, $p \rightarrow q$ and $\neg p \vee q$ are precisely the same.
 \therefore Both boolean expressions are logically equivalent.

II.

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Table 1.19

p	q	$\neg p$	$\neg q$	$(p \wedge q) (\neg p \neg q)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	1

Table 1.20

We can clearly see the column $p \leftrightarrow q$ and $(p \wedge q) \vee (\neg p \wedge \neg q)$ have same values, which means these two expressions are logically equivalent.

Note:

- The quantifiers \forall and \exists have a higher precedence than all logical operators.
- When a quantifier is used on the variable x , this occurrence of a variable is Bound.
- The part of the logical expression to which quantifier is applied is called scope.

De Morgan's Laws for Quantifiers

Negation	Equivalent Statement	Why True	Why False
$\neg \exists x P(x)$	$\forall x \neg P(x)$	For every x , $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x .

Table 1.21 De Morgan's laws for Quantifiers

Aristotle form:

- All p 's are Q 's $\forall x[p(x) \rightarrow Q(x)]$
- Some p 's are Q 's $\exists x[p(x) \wedge Q(x)]$
- Not all p 's are Q 's $\sim \forall x[p(x) \rightarrow Q(x)]$
 $\equiv \exists x[p(x) \wedge \sim Q(x)]$
 \equiv Some p 's are not Q 's
- No p 's are Q 's $\sim \exists x[p(x) \wedge Q(x)]$
 $\equiv \forall x[p(x) \rightarrow \sim Q(x)]$
All p 's are not Q 's

Note:

\forall follow implication (\rightarrow)
 \exists follow and (\wedge).



Rack Your Brain

Some real no's are not rational.

- $\exists x[\text{real}(x) \vee \text{rational}(x)]$
- $\exists x(\text{real}(x) \rightarrow \text{rational}(x))$
- $\sim \forall x[\text{real}(x) \wedge \sim \text{rational}(x)]$
- $\exists x[\text{rational}(x) \rightarrow \text{real}(x)]$



8. Match List I and List II
- List I
- Everyone loves Obama
 - Everyone loves someone
 - There is someone whom everyone loves
 - There is someone whom no one loves
- List II
- $\text{loves}(x, \text{Obama})$
 - $\text{y loves}(x,y)$
 - $\text{y loves}(x,y)$
 - $\text{y loves}(x,y)$
- | A | B | C | D |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | 3 | 2 | 4 |
| 1 | 4 | 3 | 2 |
| 1 | 2 | 4 | 3 |

Solution:

- Everyone loves Obama : $\forall x \text{loves}(x, \text{Obama})$
- Everyone loves someone : $\forall x \exists y \text{loves}(x,y)$

There is someone whom everyone loves : $\exists y \forall x \text{loves}(x,y)$

There is someone whom no one loves : $\exists y \forall x \neg \text{loves}(x,y)$



Previous Years' Questions

Choose the correct translation of given statement:
[GATE IT 2013]

"None of my friends are perfect".

- (A) $\forall x(F(x) \neg p(x))$ (B) $\forall x(F(x) p(x))$
 (C) $\exists x(F(x) \neg p(x))$ (D) $\exists x(F(x) p(x))$

Solution: (D)

Nested quantifiers:

We use quantifiers to express mathematical statements such as "The sum of two positive integers is always positive".

Note:

Be careful with the order of existential and universal quantifier.

Statement	When True	When False
$\forall x \forall y P(x, y)$	$P(x, y)$ is true for every pair x, y .	There is a pair x, y for which $P(x, y)$ is false.
$\forall y \forall x P(x, y)$		
$\forall x \exists y P(x, y)$	For every x , there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y .
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y .	For every x , there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y .
$\exists y \exists x P(x, y)$		

Table 1.22 Quantification of Two Variables

9. Translate the statement

$$\forall x(C(x) \vee \exists y(C(y) \wedge F(x,y)))$$

In English, where $P(x)$ is "x has a pentab", $C(x,y)$ is "x and y are colleagues" and the domain for both x and y consists of all the teachers in a college.

Solution:

The statement says that for every teacher x in the college, x has a pentab or there is a teacher y such that y has a pentab and x

and y are colleagues. In other words, every teacher in the college has a pentab or has a colleague who has a pentab.

10. Which of the following options is the correct expression in predicates and quantifiers "A student must take at least 60 hours course or at least 45 hours course and write a master's thesis, and receive a grade not lower than

'B' in all required courses, to receive master's degree".

- (A) $M \rightarrow ((H(60) \wedge H(45)) \wedge T) \vee \forall y G(B,y)$
- (B) $M \rightarrow ((H(60) \vee H(45)) \wedge T) \vee \forall y G(B,y)$
- (C) $M \rightarrow ((H(60) \wedge H(45)) \vee T) \vee \forall y G(B,y)$
- (D) $M \rightarrow ((H(60) \wedge H(45)) \vee T) \vee \forall y G(B,y)$

Solution: (B)

$$M \rightarrow ((H(60) \vee H(45)) \wedge T) \vee \forall y G(B,y)$$

Where M is the proposition "The student receiver master's degree".

$H(x)$ is "The student took at least x hours course".

T is the proposition "The student wrote a thesis".

$G(x, y)$ is "The person got grade x or higher in Course G".

Previous Years' Questions

Which of the following is negation of:

[GATE CSE 2008]

- $[\forall x, \alpha \rightarrow (\exists y, \beta \rightarrow (\forall u, \exists v, y))]$
- (A) $[\exists x, \alpha \rightarrow (\forall y, \beta \rightarrow (\exists u, \forall v, y))]$
- (B) $[\exists x, \alpha \rightarrow (\forall y, \beta \rightarrow (\exists u, \forall v, \neg y))]$
- (C) $[\forall x, \neg \alpha \rightarrow (\exists y, \neg \beta \rightarrow (\forall u, \exists v, \neg y))]$
- (D) $[\exists x, \alpha \wedge (\forall y, \beta \wedge (\exists u, \forall v, \neg y))]$

Solution: (D)

Previous Years' Questions

Consider the following formula and its two interpretations I_1 and I_2 .

[GATE CSE 2003]

$$\alpha: (\forall x) [P_x \leftrightarrow (\forall y) [Q_{xy} \leftrightarrow Q_{yy}]] \rightarrow (\forall x) [\neg P_x]$$

I_1 : Domain: The set of natural numbers.

P_x \equiv x is a prime number

Q_{xy} \equiv y divides x

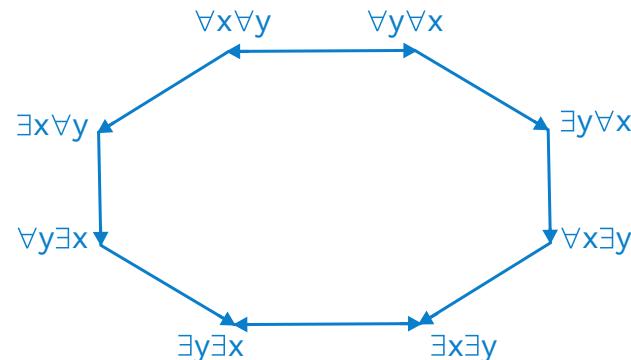
I_2 : same as I_1 except that $P_x = x$ is a composite number.

Which of the following is true?

- (A) I_1 satisfies, I_2 does not
- (B) I_1 satisfies, I_2 does not
- (C) Neither I_1 nor I_2 satisfies
- (D) Both I_1 and I_2 satisfies

Solution: (D)

Relation between two-place predicate:



From the above diagram, we can define the following predicate property and many more according to direction.

1. $\forall x \forall y p(x,y) \equiv \forall y \forall x p(x,y)$
2. $\forall x \forall y p(x,y) \rightarrow \exists x \forall y p(x,y)$
3. $\exists x \forall y p(x,y) \rightarrow \forall y \exists x p(x,y)$
4. $\forall x \forall y p(x,y) \rightarrow \exists y \forall x p(x,y)$
5. $\exists y \forall x p(x,y) \rightarrow \forall x \exists y p(x,y)$
6. $\forall x \exists y p(x,y) \rightarrow \exists y \exists x p(x,y)$
7. $\forall y \forall x p(x,y) \rightarrow \exists x \forall y p(x,y)$
8. $\forall y \exists x p(x,y) \rightarrow \exists y \exists x p(x,y)$
9. $\forall y \exists x p(x,y) \rightarrow \exists x \exists y p(x,y)$
10. $\exists y \exists x p(x,y) \equiv \exists x \exists y p(x,y)$

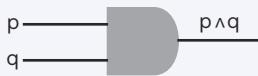
Quantifiers property:

1. $\forall x [p(x) \wedge Q(x)] \equiv \forall x p(x) \wedge \forall x Q(x)$
2. $\exists x [p(x) \vee Q(x)] \equiv \exists x p(x) \vee \exists x Q(x)$
3. $\forall x p(x) \vee \forall x Q(x) \rightarrow \forall x [p(x) \vee Q(x)]$
4. $\exists x [p(x) \wedge Q(x)] \rightarrow \exists x p(x) \wedge \exists x Q(x)$
5. $\forall x [p(x) \wedge Q] \equiv \forall x p(x) \wedge Q$
6. $\forall x [p(x) \vee Q] \equiv \forall x p(x) \vee Q$
7. $\exists x [p(x) \vee Q] \equiv \exists x p(x) \vee Q$
8. $\exists x [p(x) \wedge Q] \equiv \exists x p(x) \wedge Q$
9. $\forall x [p \rightarrow Q(x)] \equiv p \rightarrow \forall x Q(x)$
10. $\exists x [p \rightarrow Q(x)] \equiv p \rightarrow \exists x Q(x)$
11. $\forall x [p(x) \rightarrow Q] \equiv \exists p(x) \rightarrow Q$
12. $\exists x [p(x) \rightarrow Q] \equiv \forall x p(x) \rightarrow Q$



Chapter Summary



- Propositional logic is a declarative statement which results in either true or false.
- There are two types of propositions:
 - Atomic proposition
 - Compound proposition
- Connectives: The weak point at which a compound statement is breakable is called connective.
- There are four types of connectives:
 - Conjunction (\wedge)
 - Disjunction (\vee/\oplus)
 - Simple implication (\rightarrow)
 - Double implication (\leftrightarrow)
- AND gate:

- OR gate:

- NOT gate:

- \forall is called as universal quantifier.
- \exists is called as existential quantifier.
- There are two types of argument:
 - Valid
 - Invalid
- A proposition is valid if each disjunctive clause in any CNF representation of proposition contains a pair of complementary literals.
- PCNF and PDNF are unique.
- If $a = b$, then PDNF of a and b will be same, and PCNF will also be same.

2 Set Theory



Set

Sets are used to group objects together having similar properties.

Definition



Any collection of well defined and distinct object is called a set.

Example: Collection of even positive natural number less than 12

$$A = \{2, 4, 6, 8, 10\}$$

Set notations:

Sets are usually denoted by capital letters of the english alphabet A, B, C, D, ..., etc.

Elements are denoted by small letters a, b, c, d, ..., etc.

Symbol ' \in ' (read as 'belong to' or 'is a member of').

Symbol ' \notin ' (read as 'does not belong' or 'is not a member of').

Methods of depiction of sets:

A set can be represented by two methods:

1. Roster form or Tabular form
2. Set builder form or Rule method

Roster form or tabular form:

In this representation, all the elements/members of a set are listed, separated by a comma and then enclosed within the pair of curly brackets {}.

Set builder form or rule method:

In this form, we choose a variable say 'x', which represents each element of the set satisfying a particular property.

Example: Set of prime number less than 7

$$A = \{x \mid x \text{ is prime number less than } 7\}$$



Rack Your Brain

Which of the following is set?

1. Collection of intelligent students in Prepladder.
2. The collection of rich persons in India.
3. Collection of beautiful women in India.
4. Collection of solution of the equation $x^2 - 9x + 18 = 0$

Note:

Order of elements are immaterial (The order in which elements of a set are listed does not matter).

No element is repeated (It does not matter if an element of a set is listed more than once).

Example: {1, 1, 3, 3, 3, 5} is same as that of {1, 3, 5} because they have same elements.

Some sets in discrete mathematics are denoted using specific letters.

N	Set of natural numbers
Z	Set of integers
Z^+	Set of positive integers
Q	Set of rational numbers



R	Set of real numbers
R^+	Set of positive real numbers
C	Set of complex numbers

Types of sets:

1. Null set/empty set/void set:

The set with 0 elements is called an empty set and is represented by ϕ or $\{\}$.

2. Singleton set:

A set having a single element is called a singleton set. E.g., $\{1\}$.

3. Finite set:

A finite set is one with a countable number of elements.

Example: $A = \{1, 3, 5, 7, 9\}$;

$A = \{x \mid x \text{ is between } 1 \text{ and } 5\}$

4. Infinite set:

The term “infinite set” refers to a set with an infinite number of elements.

Example: $A = \{1, 2, 3 \dots\}$

5. Equivalent sets:

Two sets having an equal number of elements.

Example: $X = \{11, 12, 13\}$, $Y = \{p, y, q\}$ here X and Y are equivalent.

6. Equal sets:

When two sets A and B have the same elements, they are said to be equal sets. And every equal sets are also equivalent sets.

Example: $A = \{11, 12, 13\}$, $B = \{13, 12, 11\}$ here A and B are equal sets as well as equivalent sets.

Subsets, Universal Sets, Power Sets:

Subset:

Definition

The set A is a subset of B if and only if every element of A is also an element of B.

We use the notation $A \subseteq B$ to indicate that A is a subset of the set B.

Using quantifier subset can be defined as $\forall x(x \in A \rightarrow x \in B)$.

Example:

$A = \{a, e, i, o, u\}$

$B = \{x \mid x \text{ is a letter of english alphabets}\}$

A is a subset of B (because every element of A belongs to B).

Properties:

For every set S,

- $\emptyset \subseteq S$
- $S \subseteq S$
- $S \subseteq U$



Rack Your Brain

Is null set is a finite set?

Is equal sets are equivalent sets?



Previous Years' Questions

Let S be a set consisting of 10 elements. The number of tuples of the form (A, B) such that A and B are subsets of S, and $A \subseteq B$ is:



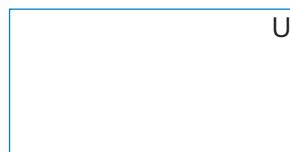
Solution: 59049



Universal set:

Set of all elements that we care about in a given context.

Universal set is represented by: U
Venn Diagram is represented by "rectangle"



Power set:

The power set of A, indicated by $P(A)$, is the set of all possible subsets of set A.

Example: If $A = \{1\}$

$$P(A) = \{\emptyset, \{1\}\}$$

Cardinality of a finite set:

The cardinality of a set A is the number of different elements in a finite set A. and it is denoted by $n(A)$ or $|A|$.

Example 1: Set of even numbers less than 10.

$$A = \{2, 4, 6, 8\}$$

$$\text{Then } |A| = 4$$

Solution: 4

Definition



Let S be a set. If there are exactly n distinct elements in S where n is a non-negative integer, we say that S is a finite set and that n is the cardinality of S. The cardinality of S is denoted by $|S|$.

Note:

The term cardinality comes from the common usage of the term cardinal numbers as the size of finite sets.

Previous Years' Questions



The cardinality of the power set of $\{0, 1, 2, \dots, 10\}$ is _____.

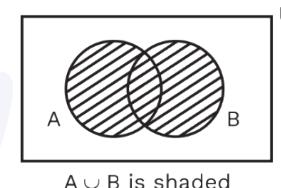
Solution: 2048

Set operations:

Various operations can be performed on two or more than two sets. Some of operations we will be discussing here:

1. Union:

The set denoted by $A \cup B$ contains elements that are either in A or B or in both.

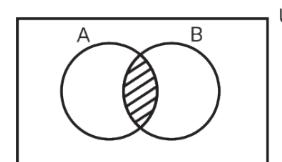


$A \cup B$ is shaded

Fig. 2.1

2. Intersection:

The set containing those elements in both sets A and B is denoted by $A \cap B$, which is the intersection of A and B.



$A \cap B$ is shaded

Fig. 2.2

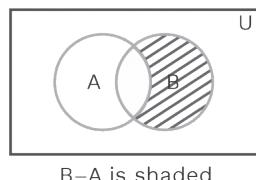
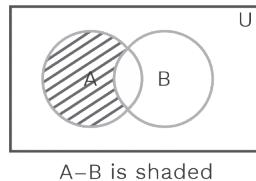
Note:

Two sets are called disjoint if their intersection is empty set.

3. Set-difference:

If and only if $x \in A$ and $x \notin B$, an element x belongs to the difference of A and B.

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



Definition

Let A and B be sets, the difference of A and B, denoted by $A-B$, is the set containing those elements that are in A but not in B. The difference of A and B is also known as complement of B with respect to A.



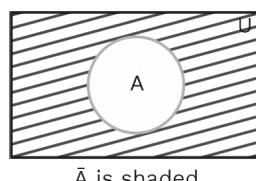
Rack Your Brain



The difference of sets $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and $B = \{1, 3, 5, 6, 7, 8, 9\}$ is?

4. Complement:

An element belongs to \bar{A} if and only if $x \notin A$.
 $\bar{A} = \{x \mid x \notin A\}$



Definition



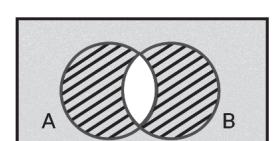
Let U be the universal set. The complement of the set A, denoted by \bar{A} is the complement of A with respect U . In other words, the complement of the set A is $U-A$.

Example 1:

Let A be a set of all positive integers greater than 5.

Then $\bar{A} = \{1, 2, 3, 4, 5\}$

5. Symmetric difference:



$A \oplus B$ is shaded

Fig. 2.3

$A \Delta B = A \oplus B = \{x \mid x \in A \text{ or } x \in B \text{ and } x \notin A \cap B\}$



Rack Your Brain

If A, B, C and D are sets, does it follow that $(A \oplus B) \oplus (C \oplus D) = (A \oplus D) \oplus (B \oplus C)$?

Grey Matter Alert!

$|A| + |B|$ counts each element in A but not in B or in B but not in A exactly once, and each element that is in both A and B exactly twice. Thus, if the number of elements that are in both A and B is subtracted from $|A| + |B|$, elements in $A \cap B$ will be counted only once. Hence,
 $|A \cup B| = |A| + |B| - |A \cap B|$

Note:

The union of arbitrary number of sets is called principle of inclusion - exclusion.

- Let X and V are two sets. The symmetric difference is defined as $A \oplus B = (A-B) \cup (B-A)$. Which of the following is false?

- (A) $A \oplus B = B \oplus A$
 (B) $A \oplus \emptyset = A$
 (C) $A \oplus A = \emptyset$
 (D) $A \oplus B = (A \cap B') \cup (B \cap A')$

Solution: (D)

Let us understand this using Venn diagram.

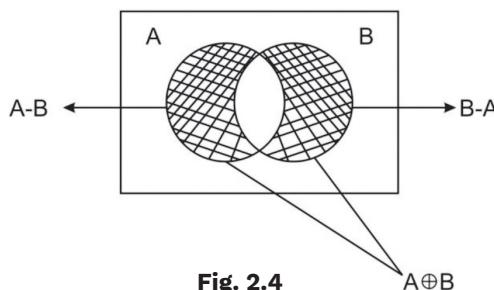


Fig. 2.4

- (A) Given: $A \oplus B = (A - B) \cup (B - A)$
 $B \oplus A = (B - A) \cup (A - B)$ therefore,
 it is true.
- (B) $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A)$
 $= (A) \cup (\emptyset)$
 $= A$
- Which is true.
- (C) $A \oplus A = (A - A) \cup (A - A)$
 $= \emptyset \cup \emptyset$
 $= \emptyset$
- Which is true
- (D) Option (D) is ruled out.

Set identities:

Identity	Name
$Z \cup \emptyset = Z$ $Z \cap U = Z$	Identity laws
$Z \cup U = U$ $Z \cap \emptyset = \emptyset$	Domination laws
$Z \cup Z = Z$ $Z \cap Z = Z$	Idempotent laws

Identity	Name
$(\overline{Z}) = Z$	Double complement
$(Z \cup K) = (K \cup Z)$ $(Z \cap K) = (K \cap Z)$	Commutative laws
$Z \cup (K \cup C) = (Z \cup K) \cup C$ $Z \cap (K \cap C) = (Z \cap K) \cap C$	Associative laws
$Z \cap (K \cup C) = (Z \cap K) \cup (Z \cap C)$ $Z \cup (K \cap C) = (Z \cup K) \cap (Z \cup C)$	Distributive laws
$\overline{Z \cup K} = \overline{Z} \cap \overline{K}$ $\overline{Z \cap K} = \overline{Z} \cup \overline{K}$	De Morgan's laws
$Z \cup (Z \cap K) = Z$ $Z \cap (Z \cup K) = Z$	Absorption laws
$Z \cup \overline{Z} = U$ $Z \cap \overline{Z} = \emptyset$	Complement laws

Table 2.1 Important Laws

Previous Years' Questions

If P, Q, and R are subsets of the universal set U, then $(P \cap Q \cap R) \cup (P' \cap Q \cap R) \cup Q' \cup R'$ is:

[GATE CSE 2008]

- (A) $Q' \cup R'$
 (B) $P \cup Q' \cup R'$
 (C) $P' \cup Q' \cup R'$
 (D) U

Solution: (D)



Solved Examples

2. Use set builder method and logical equivalences to prove $A \cap B = (A \cup B)$.

Solution: $\overline{A \cap B} = \{x \mid x \notin A \cap B\}$

$$= \{x \mid x \in (\overline{A \cap B})\}$$

{By demorgan's theorem}

$$= \{x \mid x \notin A \vee x \notin B\}$$

$$= \{x \mid x \in \bar{A} \vee x \in \bar{B}\}$$

{By demorgan's theorem}

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

3. Let A , B and C be sets. Show that $A \cup (B \cap C) = (\bar{C} \cup \bar{B}) \cap \bar{A}$

Solution:

We have,

$$\Rightarrow \overline{A \cup (B \cap C)} = \bar{A} \cap (\overline{B \cap C}) \quad [\text{Using first De Morgan's law}]$$

$$\Rightarrow \bar{A} \cap (\bar{B} \cup \bar{C}) \quad [\text{Using second De Morgan's law}]$$

$$\Rightarrow (\bar{B} \cup \bar{C}) \cap \bar{A} \quad [\text{Using Commutative law of intersection}]$$

$$\Rightarrow (\bar{C} \cup \bar{B}) \cap \bar{A} \quad [\text{Using commutative law of unions}]$$

\Rightarrow Hence Proved

Generalised union and intersection:

Let's call these two sets A and B . Now, $A \cup B$ contains items that belong to at least one of the sets A or B , while $A \cap B$ contains elements that belong to both sets A and B .

Definition

The union of a collection of sets is the set that contains those elements that are the members at least one set in the collection. The intersection of a collection of sets is the set that contains those elements that are members of all the sets in the collection.

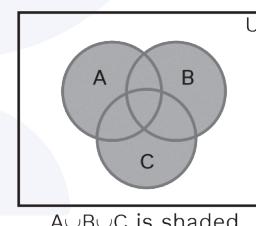
To denote the union of sets, we use the notation below.

$$A_1 \cup A_2 \cup \dots \cup A_n = \bigcup_{i=1}^n A_i$$

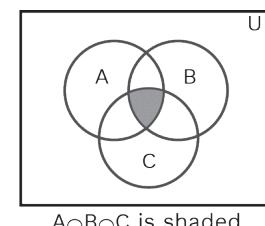
We use the following notation to represent the intersection of sets

$$A_1 \cap A_2 \cap \dots \cap A_n = \bigcap_{i=1}^n A_i$$

Below is a Venn diagram depicting the intersection and union of sets.



$A \cup B \cup C$ is shaded



$A \cap B \cap C$ is shaded

Fig. 2.5

4. Let $A = \{1, 2, 3\}$ and $B = \{1, 5, 7, 8\}$. What are $A \cup B$ and $A \cap B$?

Solution:

$$A \cup B = \{1, 2, 3, 5, 7, 8\}$$

$$A \cap B = \{1\}$$



Grey Matter Alert!

Fuzzy sets are used in artificial intelligence. Each element in the universal set U has a degree of membership, which is a real number between 0 and 1 (including 0 and 1), in a fuzzy set S . The fuzzy set S is denoted by listing the elements with their degrees of membership (elements with 0 degree of membership are not listed). For instance, we write $\{0.6 \text{ Alice}, 0.9 \text{ Brian}, 0.4 \text{ Fred}, 0.1 \text{ Oscar}, 0.5 \text{ Rita}\}$ for the set F (of famous people) to indicate that Alice has a 0.6 degree of membership in F , Brian has a 0.9 degree of membership in F , Fred has a 0.4 degree of membership in F , Oscar has a 0.1 degree of membership in F , and Rita has a 0.5 degree of membership in F (so that Brian is the most famous and Oscar is the least famous of these people). Also suppose that R is the set of rich people with $R = \{0.4 \text{ Alice}, 0.8 \text{ Brian}, 0.2 \text{ Fred}, 0.9 \text{ Oscar}, 0.7 \text{ Rita}\}$.

The complement of a fuzzy set S is the set s , with the degree of the membership of an element in S equal to 1 minus the degree of membership of this element in s .

The union of two fuzzy sets S and T is the fuzzy set $S \cup T$, where the degree of membership of an element in $S \cup T$ is the maximum of the degrees of membership of this element in S and in T .

The intersection of two fuzzy sets S and T is the fuzzy set $S \cap T$, where the degree of membership of an element in $S \cap T$ is the minimum of the degrees of membership of this element in S and in T .

Cartesian product:

Definition



The ordered n tuple (a_1, a_2, \dots, a_n) is the ordered collection that has a_1 as its first element, a_2 as its second element and a_n being the n^{th} element.

Two ordered n tuples are equal if $a_i = b_i$ for $i = 1, 2, 3 \dots n$.

Let A and B be sets. the Cartesian product of A and B , denoted by $A \times B$, is the set of all ordered pairs (a, b) , where $a \in A$ and $b \in B$. Hence,

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

The Cartesian product of the sets A_1, A_2, \dots, A_n denoted by $A_1 \times A_2 \times \dots \times A_n$, is the set of ordered n -tuples (a_1, a_2, \dots, a_n) where a_i belongs to A_i for $i = 1, 2, \dots, n$.

In other words:

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i\}$$

Solved Examples

5. What is Cartesian product of $A \times B \times C$, where $A = \{0, 1\}$, $B = \{1\}$, $C = \{1, 2\}$?

Solution:

$$A \times B \times C = \{(0, 1, 1), (0, 1, 2), (1, 1, 1), (1, 1, 2)\}$$



1. Relations:

The first thing we should understand is that relations is built on sets. For example, we have two sets A and B, a relation between A and B is written as $A R B$.

Definition

Let A and B are two non-empty sets. A relation R from set A to set B is a subset of $A \times B$. In other words, If $R \subseteq A \times B$, we call R is relation from set A to Set B.

Graph representation of relations:

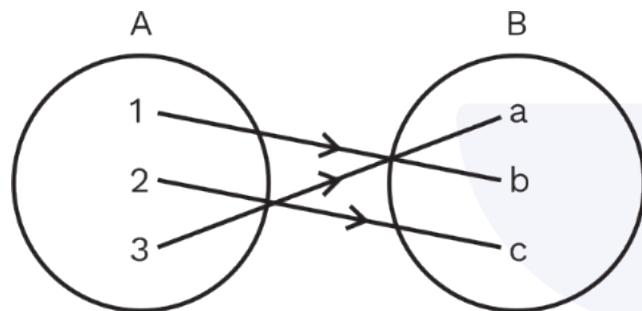


Fig. 2.6

Properties of relations:

There are many properties, some of which we will discuss here.

1. Reflexive relation:

If a relation is reflexive, then $(a, a) \in R \forall a \in A$.

It can be expressed in Quantifier as:

$$\forall a ((a, a) \in R)$$

2. Irreflexive relation:

If a relation is irreflexive, then $(a, a) \notin R \forall a \in A$.

It can be expressed in Quantifier as:

$$\forall a ((a, a) \notin R)$$

3. Symmetric:

If a relation is symmetric, then $(a, b) \in R$ then $(b, a) \in R, \forall a, b \in A$.

It can be expressed in Quantifier as:

$$\forall a \forall b ((a, b) \in R \rightarrow (b, a) \in R)$$

4. Asymmetric:

If a relation is asymmetric, then $(a, b) \in R$ then $(b, a) \notin R, \forall a, b \in A$.

It can be expressed in Quantifier as:

$$\forall a \forall b ((a, b) \in R \rightarrow (b, a) \notin R)$$

5. Antisymmetric:

If a relation is antisymmetric, then $(a, b) \in R$ and $(b, a) \in R$, then $a = b, \forall a, b \in A$.

It can be expressed in Quantifier as:

$$\forall a \forall b (((a, b) \in R \wedge (b, a) \in R) \rightarrow (a = b))$$

6. Transitive property:

If a relation is transitive, then $(z, k) \in R$ and $(k, c) \in R$ then $(z, c) \in R \forall z, k, c \in A$.

It can be expressed in Quantifier as:

$$\forall a \forall b \forall c (((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R)$$



Rack Your Brain

Consider the following relations on $\{1, 2, 3, 4\}$:

$$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$$

$$R_2 = \{(1, 1), (1, 2), (2, 1)\}$$

$$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$$

$$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$$

$$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4)\}$$

$$R_s = \{(3, 4)\}$$

Which of these relations are reflexive, irreflexive, symmetric, asymmetric, antisymmetric, and transitive?

Note:

- An empty relation is always irreflexive, symmetric, antisymmetric, asymmetric, transitive but not reflexive.
- A relation can be both symmetric as well as antisymmetric.
- Every asymmetric relation is antisymmetric.

Rack Your Brain

Which of the following is true?

1. A relation is reflexive will not be irreflexive.
2. A relation is irreflexive will not be reflexive.
3. A relation is not reflexive will be irreflexive.
4. A relation is not irreflexive will be reflexive.

Solved Examples

6. Is the "divides" relation on the set of positive integers transitive?

Solution:

Assume that a divides b and that b divides c. The positive integers k and l are then such that $b = ak$ and $c = bl$. As a result, $c = a(bl)$, and a divides c.

As a result, this relationship is transitive.

Combining relations:

Two relations can be combined in the same way, two sets are combined.



Definition



Composition of Relation/Composite Relation

Let R be a relation from a set A to set B and S a relation from B to a set C. The composite of R and S is the relation consisting of ordered pairs (a, c) , where $a \in A$, $c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. We denote the composite of R and S by $S \circ R$.

**Note:**

The relation R on a set A is transitive if $R^n \subseteq R$ for $n = 1, 2, 3, \dots$

**Rack Your Brain**

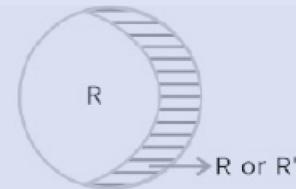
Let R be a relation $R = \{(a, b) \mid a \text{ divides } b\}$ on the set of positive integers, find R^{-1} .

Note:

Complement of a relation (R or R'):

$$R = A \rightarrow B$$

$$R \text{ or } R' : (A \times B) - R$$

**Solved Examples**

7. Find the matrix representation the relation R^2 , where the matrix representing R is

$$M_{R^2} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Solution:

The matrix for R^2 is:

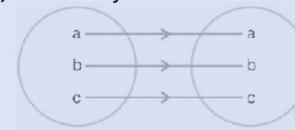
$$M_{R^2} = M_R^{[2]} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Note:

Diagonal relation

$$\Delta_A : A \rightarrow A$$

$$\Delta_A = \{(x, x) \mid x \in A\}$$

**Representation of relations:**

There are various ways to represent relations:

1. To list its ordered pairs
2. Using a table
3. Using matrices (Most appropriate one)
4. Using directed graphs

Representation using matrices:

A matrix can be used to represent a relation. Let R be a relation between A and B.

The matrix $M_R = [m_{ij}]$ can be used to describe the relation R.

$$m_{ij} = \begin{cases} 1; & \text{if } (a_i, b_j) \in R, \\ 0; & \text{if } (a_i, b_j) \notin R \end{cases}$$

Representation using digraphs:

This is another way of representing relations. Each element is represented by a point, and each ordered pair is represented using arc with its directions indicated by an arrow.

Definition

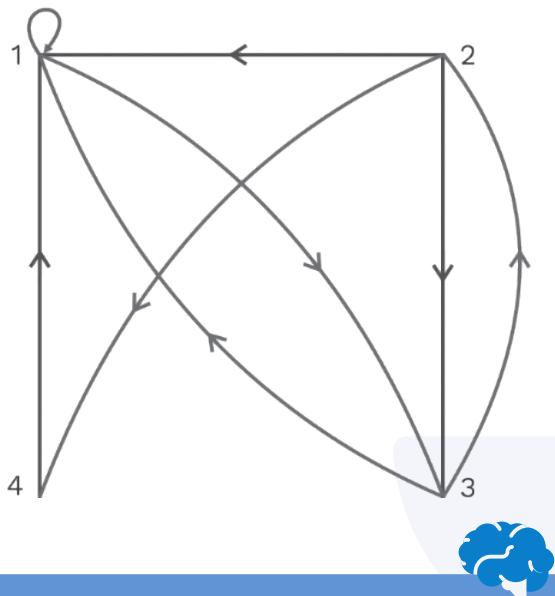
A directed graph, or digraph, consist of a set V of vertices (or nodes) together with a set E of ordered pairs of elements of V called edges (or arcs). The vertex a is called the initial vertex of the edge (a, b), and the vertex b is called the terminal vertex of this edge.



Solved Examples

8. Draw the directed graph for the given set of ordered pairs.
 $R = \{(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)\}$ on the set $\{1, 2, 3, 4\}$

Solution:

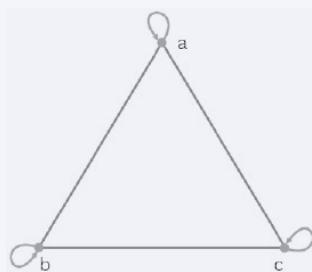


Rack Your Brain

1. List the ordered pairs in the relations on $\{1, 2, 3\}$, corresponding to this matrix

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

2. List the ordered pairs in the relation represented by the following directed graphs



Closures of relations:

Let us learn this concept with a simple family tree example. You and your mother

are directly related, but you and your maternal cousin are not directly related, you are related to your cousin through your mother. Let R be a relation containing (a, b) , if a is directly related to b . Now the question is, how to determine indirect link? Answer is right here! using “closure of relations” “concepts, we can find all pairs of relations that have a link by constructing a transitive relation S containing R , such that S is subset of every transitive relation containing R . This relation is called transitive closure of R .

General definition of closure:

Let R be a relation on set A . R may or may not have some property P but if there exists another relation S with property P containing R , such that S is subset of every relation with property P containing R , then S is called closure of R with respect to P .

Closures:

1. Reflexive closure:

Smallest reflexive relation containing relation R .

For e.g., Let relation $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$ on the set $A = \{1, 2, 3\}$. As it can be clearly seen that the relation is not reflexive, but we can make it reflexive by including $(2, 2)$ and $(3, 3)$ to R . The new relation obtained contains R . Now, every relation that contains R must also contain $(2, 2)$, $(3, 3)$ because this is reflexive relation and is contained within every reflexive relation that contains R .

Note:

Reflexive closure of $R_r = R \cup \Delta$, where $\Delta = \{(a, a) | \forall a \in A\}$.



Solved Examples

9. What is reflexive closure of the relation $R = \{(a, b) | a < b\}$ on the set of integers?

Solution:

The reflexive closure of R is

$$\begin{aligned} R \cup \Delta &= \{(a, b) | a < b\} \cup \{(a, a) | a \in z\} \\ &= \{(a, b) | a \leq b\} \end{aligned}$$

2. Symmetric closure:

Smallest symmetric relation containing relation R.

For example, relation $\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2)\}$ on $\{1, 2, 3\}$ is not symmetric, but we can make it symmetric by adding $(2, 1)$ and $(1, 3)$, then the relation obtained will be symmetric.

The symmetric closure of a relation can be constructed by taking the union of a relation with its inverse i.e., $R \cup R^{-1}$ is the symmetric closure of R, where $R^{-1} = \{(b, a) | (a, b) \in R\}$

10. What is the symmetric closure of the relation $R = \{(a, b) | a > b\}$ on the set of positive integers?

Solution:

The symmetric closure of R is the relation

$$\begin{aligned} R \cup R^{-1} &= \{(a, b) | a > b\} \cup \{(b, a) | b > a\} \\ &= \{(a, b) | a \neq b\} \end{aligned}$$

3. Transitive closure:

We all know the definition of transitivity: "A relation is said to be transitive if transitivity $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ "

To transform a non-transitive relation on a given set into a transitive closure, simply make the provided relation transitive as defined.

For e.g., relation $\{(79, 84), (84, 36), (94, 36)\}$ on given set $\{36, 79, 84, 94\}$ is not transitive. We can convert it to transitive, but it is a little on the tougher side than reflexive and symmetric.

A relation's transitive closure can be obtained by adding newer ordered pairs that must be present and continuing the

process until no more ordered pairs are required.

11. Find the zero-one matrix of the transitivity closure of the relation R where

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

Solution:

There is a theorem which states that; zero-one matrix of R^* is:

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \dots \vee M_R^{[n]}$$

Now,

$$M_R^{[2]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \text{ and } M_R^{[3]} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\therefore M_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$



Rack Your Brain

Let R be relation on the set $\{1, 2, 3, 4\}$ containing ordered pairs $\{(1, 2), (2, 2), (2, 3), (3, 1), (3, 3) \text{ and } (4, 1)\}$.

Find the

- (A) Reflexive closure of R
- (B) Symmetric closure of R
- (C) Transitive closure of R

Equivalence relations:

- If a given relation R on a given set S is: a) Reflexive b) Symmetric c) Transitive, it is called an equivalence relation.
- When a and b are equivalent elements in terms of a particular equivalence relation, the notation $a \sim b$ is frequently employed.



Solved Examples

- 12.** Is “divide” relation on the set of positive integers is an equivalence relation?

Solution:

The divide relation is reflexive and transitive, but not symmetric, on the set of all positive integers. ($2 \in z$, $4 \in z$ 2 divides 4, but 4 does not divide 2)

\therefore It is not an equivalence relation.

- 13.** Let R be a relation on the set of integers such that aRb iff $a = b$ or $a = -b$. Is this an equivalence relation.

Solution:

The given relation is:

- Reflexive
- Transitive
- Symmetric

Therefore, relation is equivalence relation.

- 14.** Let R is a relation on the set of english letters such that aRb iff $l(a) = l(b)$, where $l(x)$ is length of the string x. Is R an equivalence relation?

Solution:

Because $l(a) = l(a)$, wherever a is a string, it follows that aRa , and R is reflexive. Assume that aRb , and that $l(a) = l(b)$. Because $l(b)$

= l, the result is bRa . As a result, R is symmetric. Finally, consider aRb and bRc . As a result, $l(a) = l(c)$, resulting in aRc . As a result, R is a transitive. R is an equivalence relation since it is reflexive, symmetric, and transitive.

Equivalence classes:

Definition

Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called equivalence class of a. The equivalence class of a with respect to R is denoted by $[a]_R$. When only one relation is under consideration, we can delete the subscript R and write [a] for this equivalence class.

OR

If R is an equivalence relation on a set A, the equivalence class of the element a is $[a]_R = \{s \mid (a, s) \in R\}$.

Note:

If $b \in [a]_R$ then b is called representative of this equivalence class.

Solved Examples

- 15.** What is the equivalence class of an integer for the equivalence relation on the set of integers such that aRb if $a = b$ or $a = -b$.

Solution:

An integer is equivalent to itself, and its negative as provided.

As a result, $[a] = \{-a, a\}$ for $[0] = \{0\}$.

- 16.** What are the equivalence class of 0 and 1 for congruence modulo 4?

Solution:

All numbers a such that $a \equiv 0, 0$ are included in the equivalence class of 0. (mod 4). This class contains integers that are divisible by four. As a result, this relationship has an equivalence class of 0.

$$[0] = \{\dots -8, -4, 0, 4, 8, \dots\}$$

$$[1] = \{\dots -7, -3, 1, 5, 9, \dots\}$$



Rack Your Brain

What is the congruence class $[4]_m$ when m is:

- (A) 2
- (B) 8

Equivalence classes and partitions

We can divide R into disjoint subsets, each of which contains a certain major, if we consider R to be an equivalence. R equivalence classes make up these subsets.

Solved Examples

- 17.** What are the sets in the partition of the integers arising from congruence modulo 4.

Solution:

$$\begin{aligned}[0]_4 &= \{\dots -8, -4, 0, 4, 8, \dots\} \\ [1]_4 &= \{\dots -7, -3, 1, 5, 9, \dots\} \\ [2]_4 &= \{\dots -6, -2, 2, 6, 10, \dots\} \\ [3]_4 &= \{\dots -5, -1, 3, 7, 11, \dots\}\end{aligned}$$

These congruence classes are disjointed, and each integer belongs to one of them.

Rack Your Brain

Which of the following collection of subsets are partitions of $\{1, 2, 3, 4, 5, 6\}$

- (A) $\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}$
- (B) $\{1\}, \{2, 3, 6\}, \{4\}, \{5\}$
- (C) $\{2, 4, 6\}, \{1, 3, 5\}$
- (D) $\{1, 4, 5\}, \{2, 6\}$

An equivalence relation's equivalence class divides a set into disjoint, non-empty sets in this way. There are two theorems that show that the equivalence classes of two components of A are either identical or disjoint, and that relations and partitions are connected.

Let R be a set A equivalence relation. These are similar statements for A's elements a and b.

1. aRb
2. $[a] = [b]$
3. $[a] \cap [b] = \emptyset$

Grey Matter Alert!

If every set in P_1 is a subset of one of the sets in P_2 , the partition P_1 is called a refinement of the partition P_2 .

Partial orderings:

Definition



The relation R on set S is called a partial ordering or partial order if it is reflexive, antisymmetric and transitive. A set S together with partial ordering relation R is called a partially ordered set, or poset, and is denoted by (S, R) .

Members of S are called elements of the poset.



Solved Examples

- 18.** Show that the inclusion relation \sim is a partial ordering on the power set of a set S.

Solution:

Any set is a subset of itself, hence \subseteq is reflexive, as we all know.

- It's antisymmetric because if $A \subseteq B$ and $B \subseteq A$, then $A = B$.
- Because $A \subseteq B$ and $B \subseteq C$ imply that $A \subseteq C$, \subseteq is transitive.

As a result, $(P(S), \subseteq)$ is a poset and is a partial ordering on $P(s)$.

Solved Examples

- 19.** In the poset $(Z^+, |)$, are the integers 3 and 9 comparable?

Solution:

Integers 3 and 9 comparable, because $3|9$.

Note:

Partial word is used because pair of elements may be incomparable.

Totally ordered set:

Definition

If (S, \preceq) is a poset and every two elements of S are comparable, S is called totally ordered or linearly ordered set, and \preceq is called total order or linear order. A totally ordered set is also called a chain.

The poset (Z, \preceq) is totally ordered, because $a \preceq b$ or $b \preceq a$ whenever a and b are integers.

Comparable and incomparable posets

Definition

The elements a and b of a poset (S, \preceq) is called comparable if either $a \preceq b$ or $b \preceq a$. When a and b are elements of S such that neither $a \preceq b$ nor $b \preceq a$, a and b are called incomparable.

Well ordered set:

A set (S, \prec) is well ordered if it is a poset with \preceq is a total ordering and a least element in every non-empty subset of S.

Lexicographic order:

A lexicographic ordering \preceq on $A_1 \times A_2$ is defined as one pair being less than another if the first entry of the first pair is less than the first entry of the second pair, or if the first entries are equal, but the second entry of this pair is less than the second entry of the second pair, i.e., $(a_1, a_2) \prec (b_1, b_2)$ either if $a_1 \prec_1 b_1$ or if both $a_1 = b_1$ and $a_2 \prec_2 b_2$.



Hasse diagrams:

Hasse diagram represents partial order relations in simpler forms.

1. Omit all loops.
2. Omit all arrows that can inferred transitivity.
3. Draw arrows without heads.
4. Make sure all arrows point upwards.

The diagram is called the Hasse diagram, named after the twentieth century German mathematician Helmut Hasse.

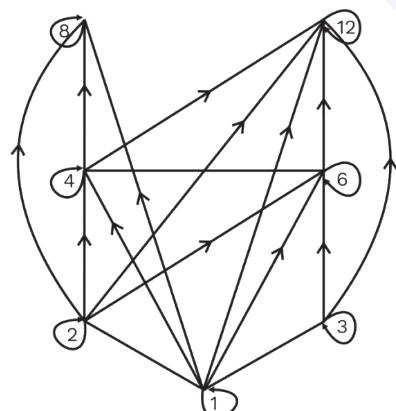


Fig. 2.7

- Diagram for this partial order.

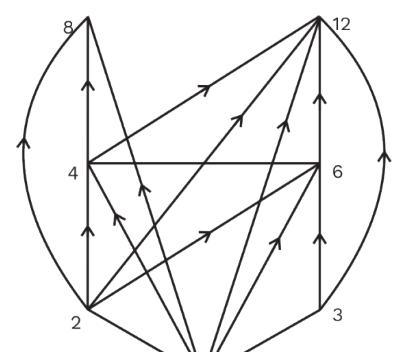


Fig. 2.8

- Remove all loops.

Solved Examples

- 20.** Determine whether $(3, 5) \prec (4, 8)$, whether $(3, 8) \prec (4, 5)$, and whether $(4, 9) \prec (4, 11)$, in the poset $(\mathbb{Z} \times \mathbb{Z}, \preceq)$, where \preceq is the lexicographic ordering constructed from the usual \leq relation on \mathbb{Z} .

Solution:

As $3 < 4$, it therefore $(3, 5) \preceq (4, 8)$ and $(3, 8) \preceq (4, 5)$. We have $(4, 9) \preceq (4, 11)$ as the first entries of $(4, 9)$ and $(4, 11)$ are the same but $9 < 11$.

Solved Examples

- 21.** Draw the Hasse diagram representing the partial ordering $\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.

Solution:

- Diagram for this partial order.

- Remove all edges implied by the transitive property and reposition all edges upwards.

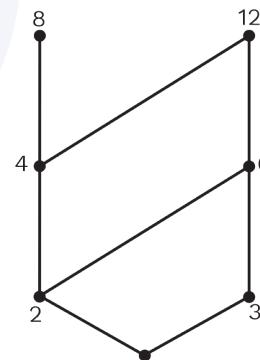


Fig. 2.9

This is the resulting Hasse diagram

- 22.** Draw the Hasse Diagram for partial ordering $\{(A, B) \mid A \subseteq B\}$ on the power set $P(S)$ where $S = \{a, b, c\}$.

Solution:

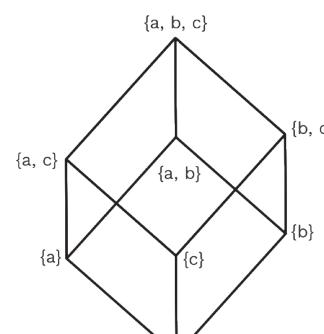


Fig. 2.10



Solved Examples

Maximal and minimal elements:

A poset element is maximal if it is not less than any other poset element, i.e., a is maximal in the poset (S, \preceq) if there is no $b \in S$ such that $a \prec b$.

Similarly, if there is no element $b \in S$ such that $b \prec a$, then a is minimum.

The “top” and “bottom” elements in the diagram are the maximal and minimal elements.

- 23.** Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, \mid)$ are maximal and which are minimal.

Solution:

The Hasse diagram will be:

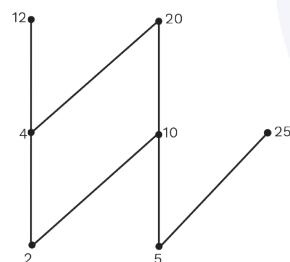


Fig. 2.11

Maximal elements = 12, 20, 25 minimal elements = 2 and 5

Upper bound and lower bound:

Let us understand this concept with the help of an example.



Rack Your Brain

Draw the Hasse diagram for the “greater than or equal to” relation on $\{0, 1, 2, 3, 4, 5\}$.

Note:

Maximal: an element is not related to any other element.

Minimal: no element is related to an element.

Greatest and least elements:

Definition



An element in a poset that is greater than every other element. such an element is called the greatest element. That is, a is the greatest element of the poset (S, \preceq) if $b \preceq a$ for all $b \in S$. The greatest element is unique when it exists. Likewise, an element is called the least element if it is less than all the other elements in the poset. That is, a is the least element of (S, \preceq) if $a \preceq b$ for all $b \in S$. The least element is unique when it exists.

Let $\langle p, \preceq \rangle$ be a poset.

An element $g \in p$ is greatest, if $x \leq g \forall x \in p$

An element $l \in p$ is least, if $l \leq y \forall y \in p$.

Example 1:

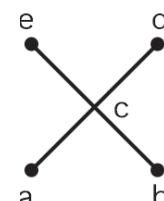


Fig. 2.12

greater → no greatest

least → no least

Example 2:

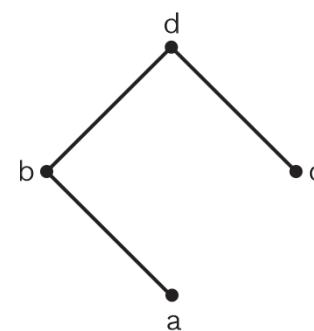


Fig. 2.13

greatest → d

least → No least



Solved Examples

- 24.** Find the greatest lower bound and the least upper bound of $\{b, d, g\}$, if they exist, in

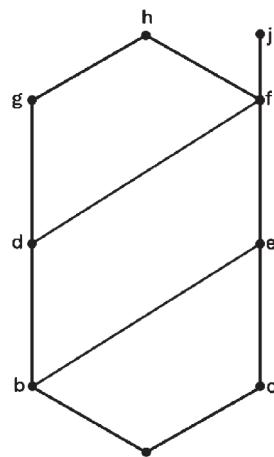


Fig. 2.14

Solution:

The upper bounds of b , d , and g are g and h , respectively. g is the least upper bound since $g \prec h$. a and b are the lower bounds of b , d ,

and g . Because $a \prec b$ is the greatest lower bound, b is the greatest upper bound.

Lattice:

"A poset 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."

Note:

	\leq	$ $	\subseteq
$a \vee b$	$\max \{a, b\}$	$\text{LCM } \{a, b\}$	$a \cup b$
$a \wedge b$	$\min \{a, b\}$	$\text{GCD } \{a, b\}$	$a \cap b$

Previous Years' Questions



Consider the following Hasse diagrams:

[GATE IT 2008]

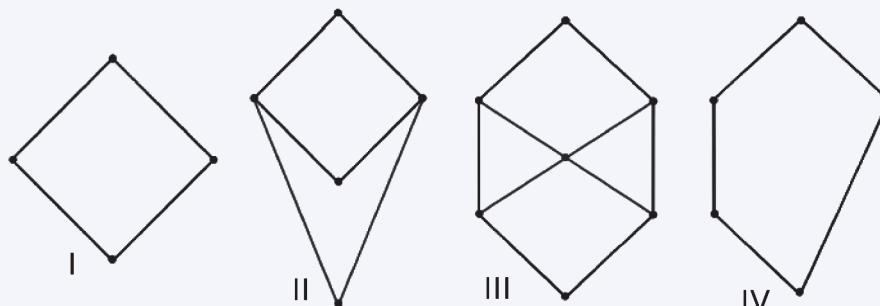


Fig. 2.15

Which of the following represent a lattice?

- (A) I and IV only
(C) III only

- (B) II and III only
(D) I, II and IV only

Solution: (A)



Previous Years' Questions



The inclusion of which of the following sets into

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

is necessary and sufficient to make S a complete lattice under the partial order defined by set containment?

[GATE CSE 2004]

- (A) $\{1\}$
- (B) $\{1\}, \{2, 3\}$
- (C) $\{1\}, \{1, 3\}$
- (D) $\{1\}, \{1, 3\}, \{1, 2, 3, 4\}, \{1, 2, 3, 5\}$

Solution: (A)

Note:

Join - The join of two elements is their least upper bound. It is denoted by \vee , not to be confused with disjunction.

Meet - The meet of two elements is their greatest lower bound. It is denoted by \wedge , not to be confused with conjunction.

Properties of lattice:

Let $< L, \preceq >$ be a lattice, then the following properties holds.

1. Idempotent:

$$\begin{aligned} a \vee a &= a \\ a \wedge a &= a \end{aligned}$$

2. Commutative:

$$\begin{aligned} a \vee b &= b \vee a \\ a \wedge b &= b \wedge a \end{aligned}$$

3. Associative:

$$\begin{aligned} a \vee (b \vee c) &= (a \vee b) \vee c \\ a \wedge (b \wedge c) &= (a \wedge b) \wedge c \end{aligned}$$

4. Absorption:

$$\begin{aligned} a \vee (a \wedge b) &= a \\ a \wedge (a \vee b) &= a \end{aligned}$$

Distributive lattice:

Distributive lattice holds following laws:

1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Non distributive lattice: There are two famous non distributive lattice:

1. Kite or Diamond lattice
2. Pentagon lattice

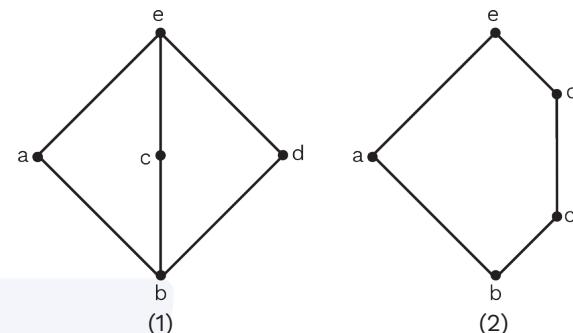


Fig. 2.16

Bounded lattice:

If a lattice L has the greatest element 1 and the least element 0, it is said to be bounded.

Example:

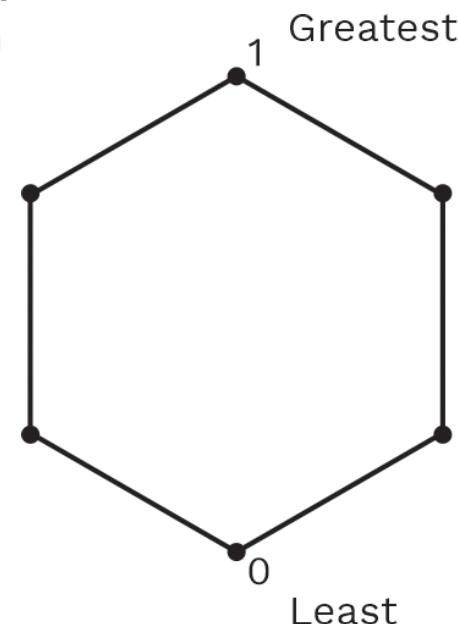


Fig. 2.17

Greatest element $\rightarrow 1$

Least element $\rightarrow 0$



Note:

Every finite lattice is always bounded.

Complement of an element in a lattice:

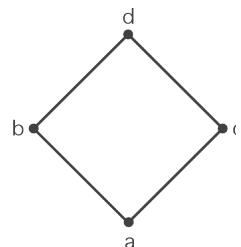
Let $\langle L, \preceq \rangle$ be a bounded lattice. An element $b \in L$ is complement of $a \in L$ when $a \vee b = 1$ (greatest element) $a \wedge b = 0$ (Least element) b is the complement of a ; then a is the complement of b .

Note:

- $1 \vee 0 = 1$
- $1 \wedge 0 = 0$

greatest and least element are complement of each other.

Example:



Element	Complement
a	d
d	a
b	c
c	b

Note:

Complement, if exist need not to be unique.

Complemented lattice:

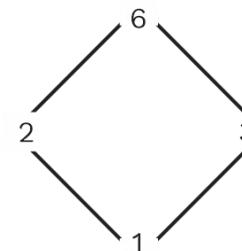
A bounded lattice in which complement of every element exist is called complemented lattice.

Note:

In a distributive lattice complement if exist are unique.

Example:

$D_6 \{1, 2, 3, 6\}$ is complemented lattice because it is bounded and every element of this lattice has a complement.



Boolean algebra:

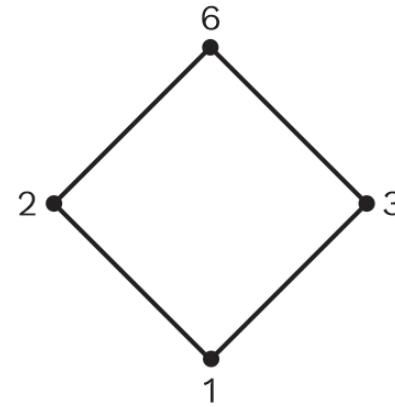
A bounded distributive and complemented lattice is called Boolean Algebra.

Example 1:

$\langle P(A), \subseteq \rangle$ is Boolean Algebra.

$n = p_1, p_2 \dots p_k$, where $p_1, p_2 \dots p_k$ are distinct prime numbers then. D_n is Boolean Algebra.

$$D_6 = 6 = 2 \times 3$$



Example 2:

$p^2 | n$, p is prime. Then D_n is not Boolean algebra

D_4 where 2 is prime

$2^2 | 4$ it is not Boolean algebra.



Not Boolean algebra



Some points to remember:

In any lattice, the semidistributive laws

$$a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

Topological sorting:

Assume a project consists of 20 separate tasks. Some tasks can only be done after the completion of others. What is the best way to find an order for these tasks? To describe this problem, we create a partial order on the

set of tasks such that $a \prec b$ means, b cannot be started if a is not completed. To create a project schedule, we must first create an order for all 20 jobs that is compatible with this partial order. We'll demonstrate how to do it.

"A total ordering \preceq is said to be compatible with the partial ordering R if $a \preceq b$ whenever aRb . Constructing a compatible total ordering from a partial ordering is called topological sorting."

Solved Examples

- 25.** Find a compatible total ordering for the poset $(\{1, 2, 4, 5, 12, 20\}, |)$.

Solution:

Step 1: Choose minimal element, i.e., 1.

Step 2: Select minimal element from $(\{2, 4, 5, 12, 20\}, |)$, i.e., 2 and 5 (let's choose 5).

Step 3: Choose minimal element from the remaining elements, i.e., 4.

Step 4: Again choose minimal out of the remaining elements, i.e., 12.

$$1 \prec 5 \prec 2 \prec 4 \prec 20 \prec 12$$



Rack Your Brain

Answer these questions for the poset $(\{2, 4, 6, 9, 12, 18, 27, 36, 48, 60, 72\}, |)$.

1. Find the maximal elements.
2. Find the minimal elements.
3. Is there a greatest element?
4. Is there a least element?
5. Find all upper bounds of {2, 9}.
6. Find the least upper bound of {2, 9}, if it exists.
7. Find all lower bounds of {60, 72}.
8. Find the greatest lower bound of {60, 72}, if it exists.



Rack Your Brain

Which of these pairs of elements are comparable in the poset $(Z^*, |)$?

- (A) 5, 15 (B) 6, 9
 (C) 8, 16 (D) 7, 7

Functions

Consider the following illustration:

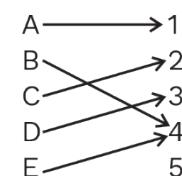


Fig. 2.18



Definition

Let A and B be two non-empty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f: A \rightarrow B$

Note:

Functions are sometimes also called mappings/transformation.

Definition

While defining a function we have to specify its domain, co-domain and mapping of elements of the domain to elements in the co-domain. Two functions are equal when they have same domain, co-domain and map elements of their common domain to the same elements in their common co-domain.

Note:

If we change either the domain or co-domain of a function, then we obtain a different function. If we change mapping of elements, then we also obtain a different f.

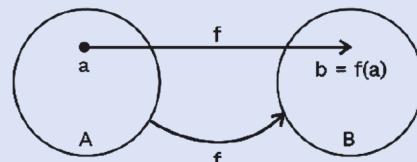


Fig. 2.19 The Function of Maps A and B



Rack Your Brain

Find the domain and range of the function

$$f(x) = \frac{\sqrt{x+2}}{x^2 - 9}$$

Definition

- If f is a function from A to B, we say that A is the domain off and B is the co-domain off. If $f(a) = b$, we say that b is the image of a and a is pre-image of b. The range of the f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f maps A to B.
- Let f_1 and f_2 be functions from A to R. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from A to R.

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$

$$(f_1 f_2)(x) = f_1(x) f_2(x)$$

- Let f be a function from set A to set B and let S be a subset of A. The image of S under the function f is the subset of B that consist of the images of the elements of S. We denote the image of S by $f(S)$, so

$$f(S) = \{t \mid \exists s \in S (t = f(s))\}$$

We can also use the shorthand $\{f(s) \mid s \in S\}$ to denote this set.



Solved Examples

- 26.** Let f_1 and f_2 be two functions from \mathbb{R} to \mathbb{R} such that $f_1(x) = x^2$ and $f_2(x) = x - x^2$. What are the functions $f_1 + f_2$ and $f_1 f_2$?

Solution:

From the definition of the sum and products of functions, it follows that

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

and

$$(f_1 f_2)(x) = x^2(x - x^2) = x^3 - x^4$$

Note:

When f is a function from a set A to set B , the image of a subset of A can also be defined.

Example:

Let $Z = \{p, m, k, f, t\}$ and $B = \{1, 2, 3, 4\}$ with $f(p) = 2$, $f(m) = 1$, $f(k) = 4$, $f(f) = 1$ and $f(t) = 1$.

Solution:

The image of the subset $S = \{m, k, f\}$ is the set $f(S) = \{1, 4\}$

Rack Your Brain



Let $S = \{-1, 0, 2, 4, 7\}$. Find $f(s)$ if
 $f(x) = 2x+1$
 $f(x) = [x/5]$



Previous Years' Question

Suppose that $f: \mathbb{R} \rightarrow \mathbb{R}$ is a continuous function on the interval $[-3, 3]$ and a differentiable function in the interval $(-3, 3)$ such that for every x in the interval, $f'(x) \leq 2$. If $f(-3) = 7$, then $f(3)$ is at most _____.

Solution: 19



Definition

A function is said to be one-to-one when it does not assign same value to two different domain elements.

Note:

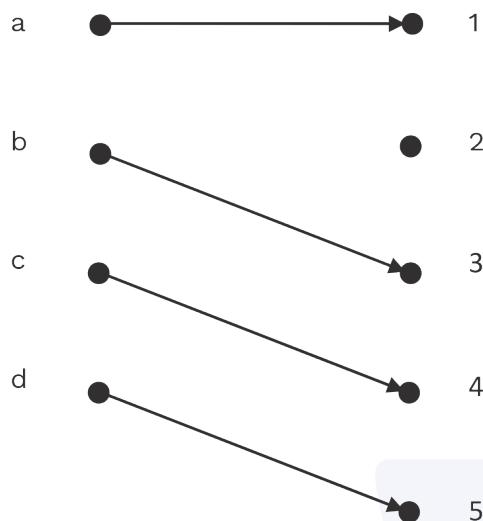
Function f is one-to-one if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain off. A function is said to be an injection if it is one-to-one.



Solved Examples

- 27.** Determine whether the function f from $\{a, b, c, d\} \rightarrow \{1, 2, 3, 4, 5\}$ with $f(a) = 1, f(b) = 3, f(c) = 4, f(d) = 5$ is one-to-one.

Solution:



The given function is one-to-one because f is taking different values for all four elements of its domain.

Definition

A function f from A to B is called onto, or surjective, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function f is called a surjection if it is onto.

Definition

A function f whose domain and co-domain are subset of the set of real numbers is called increasing if $f(x) \leq f(y)$, and strictly increasing if $f(x) < f(y)$, whenever $x < y$ and x and y are in domain off. similarly, f is called decreasing if $f(x) > f(y)$, and strictly decreasing iff $f(x) \neq f(y)$ whenever $x < y$ and x and y are in domain off. (The word strictly in this definition indicates a strict inequality.)

Now, we can see that some of the functions are strictly increasing and some of them are strictly decreasing and one-to-one. However, some function which are increasing but not strictly increasing and decreasing but not strictly decreasing need not necessarily one-to-one.

Now there are some functions whose range and co-domain are equal i.e every member of co-domain is the image of some element of the domain. Functions with this property are called onto functions.

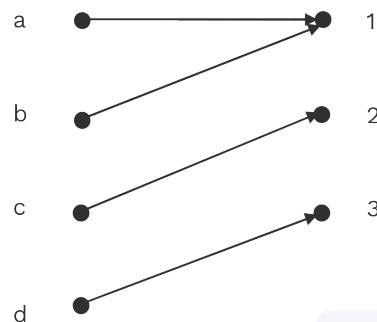


Solved Examples

- 28.** Let f be a function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 1, f(b) = 1, f(c) = 2, f(d) = 3$. Is f an onto function?

Solution:

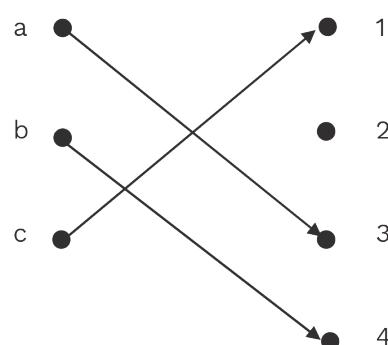
We can argue that f is onto since all of the components of the co-domain are images of items in the domain.



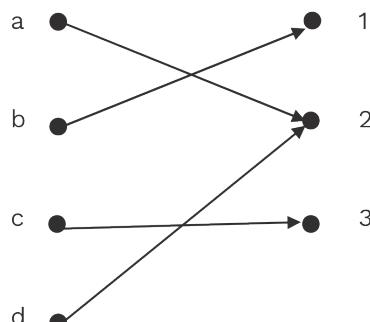
Note:

A function is said to be one-to-one correspondence, or a bijection if it is both one-to-one and onto.

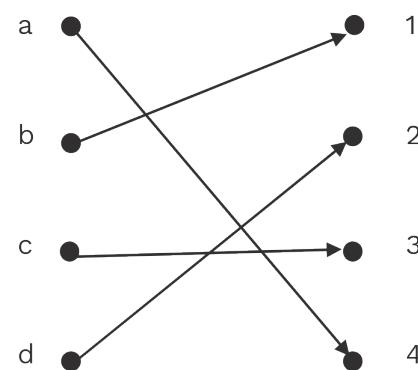
- 1. One-to-one, not onto**



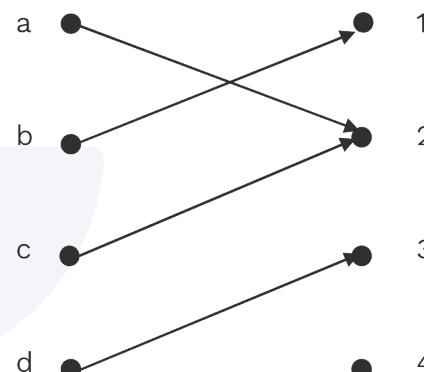
- 2. Onto, not one-to-one**



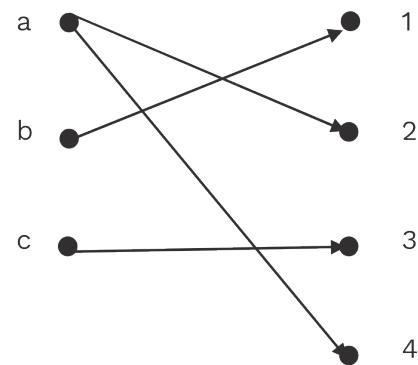
- 3. One-to-one and onto**



- 4. Neither one-to-one nor onto**



- 5. Not a function**



Examples of different type of correspondences:

Different types of functions can be seen in the diagram above. i) is one-to-one but not onto, ii) is onto but not one-to-one, iii) is both one-to-one and onto, iv) is neither one-to-one nor onto, and v) is neither one-to-one nor onto, and v) is not even a function because it sends an element to two different elements.



Let's pretend f is a function from A to A . (itself). When A is finite, f is one-to-one only if and only if it is onto. If A is infinite, this isn't always the case.

Definition

Let one-to-one correspondence from set to the set B . The inverse function off is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

The increase function off is deviated by f^{-1} . Hence $f^{-1}(b) = a$ when $f(a) = b$

Note:

Do not confuse with f^{-1} and $1/f$.

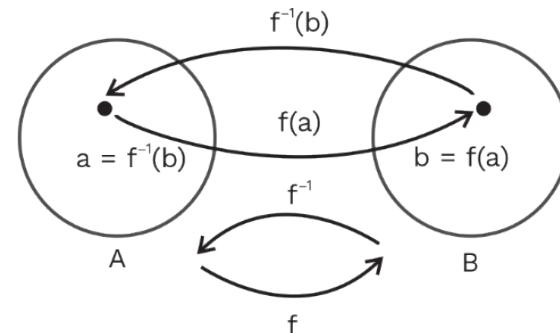


Fig. 2.20 Inverse of a Function

We can not determine the inversion of any function if that function is not a bijective function. If function is not bijection, then there are two possibilities, one is either function is not one-to-one and second is, function is not onto.

We can define inverse of a bijective function. Therefore, it is called invertible. A function is not invertible if it is not one-to-one correspondence.

Solved Examples

- 29.** Let f is the function from $\{G,A,T,E\}$ to $\{2,0,4,3\}$ such that $f(G) = 2$, $f(A) = 4$, $f(T) = 3$, $f(E) = 0$, is f invertible? If it is, what is its inverse?

Solution:

As the given function is one-to-one correspondence therefore, it is invertible.

Now,

$$f^{-1}(2) = G$$

$$f^{-1}(0) = E$$

$$f^{-1}(4) = A$$

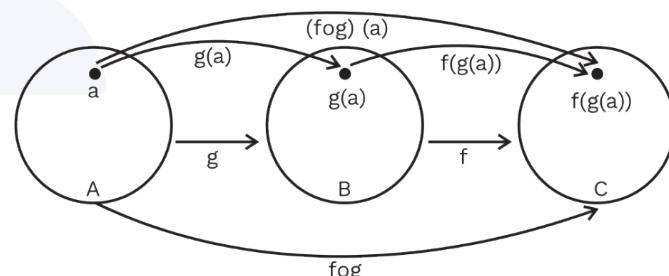
$$f^{-1}(3) = T$$

- 30.** Consider a function R to R with $f(x) = x^2$. Is f invertible?

Solution:

As $f(-4) = f(4) = 16$, f is one-to-one. If an inverse of function is defined, it will assign two values to 16. Hence, f is not invertible.

Composite of functions:



Definition

Let g be a function from the set A to the set B and let f be a function from set B to the set C . The composition of the functions f and g , denoted by $f \circ g$, is defined by $(f \circ g)(a) = f(g(a))$.



Note:

- Commutative law does not hold for composite functions, i.e., $f \circ g \neq g \circ f$.
- The composition of a function and its inverse gives identity function.

Solved Examples

- 31.** Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition off and g ?

Solution:

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) = f(3x + 2) \\ &= 2(3x + 2) + 3 \\ &= 6x + 7\end{aligned}$$

The graph of functions:

The set of pairs in $A \times B$ to each function from A to B .

This set of pair is called graph of a function.

Definition

If f be a function from a set A to set B . The graph of the function f is the set of ordered pairs.

$$\{(a, b) | a \in A \text{ and } f(a) = b\}$$

Note:

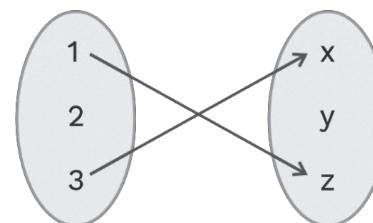
- Floor function
It is denoted by $\lfloor x \rfloor$
It means value less than or equal to x .
- Ceiling function
It is denoted by $\lceil x \rceil$
It means value greater than equal to x .

Rack Your Brain

1. Determine whether the function $f: Z \times Z \rightarrow Z$ is onto if:
 - $f(m, n) = |n|$
 - $f(m, n) = m-n$
2. Find $f \circ g$ and $g \circ f$, where $f(x) = x^2 + 1$ and $g(x) = x + 2$, are functions from R to R .

Partial functions:

When there is one element in the domain which is not defined, then that function is called partial function.



Previous Years' Questions



If $g(x) = 1 - x$ and $h(x) = \frac{x}{x-1}$ then $\frac{g(h(x))}{h(g(x))}$ is:

$$(A) \frac{h(x)}{h(x)} \quad (B) \frac{-1}{x} \quad (C) \frac{g(x)}{h(x)} \quad (D) \frac{x}{(1-x)^2}$$

Solution: (A)



Previous Years' Questions



The number of functions from an m element set to an n element set is:

[GATE CSE 1998]

- (A) $m + n$
- (B) m^n
- (C) n^m
- (D) $m * n$

Solution: (C)

Previous Years' Questions



Let N be the set of natural numbers.
Consider the following sets,
P: Set of Rational numbers (positive and negative)
Q: Set of functions from $\{0,1\}$ to N
R: Set of functions from N to $\{0,1\}$
S: Set of finite subsets of N
Which of the above sets are countable?

[GATE CSE 2018]

- (A) Q and S only
- (B) P and S only
- (C) P and R only
- (D) P, Q, and S only

Solution: (D)

Chapter Summary



- A set is a collection of objects and is represented in roster form or set builder form.

Roster Notation: $V = \{a, e, i, o, u\}$

Set Builder Notation

Here V is a set of all vowels in the english alphabet.

$: O = \{x \in \mathbb{Z}^+ \mid x \text{ is odd and } x < 10\}$
or

$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$

Both represent O is a set of odd positive integers less than 0.

Empty set (\emptyset) : Set with no elements, also known as null set

Singleton set : Set with only one element

○ Subset: The set A is a subset of B if and only if every element of A is also one element.

○ Proper Subset: $A \subset B$

Subset : $A \subseteq B$

Power Set : The power set of a set S is the set of all subsets of the set S .

It is denoted by $P(S)$

○ If a set has n -elements, then its power set has 2^n elements.

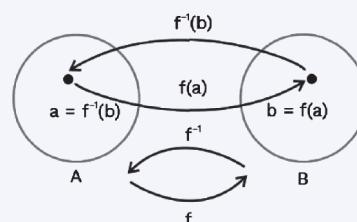
Set identities:

Identity	Name
$A \cup \emptyset = A$ $A \cap U = A$	Identity laws
$A \cap U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$(\bar{A}) = A$	Complementation laws
$(A \cup B) = (B \cup A)$ $(A \cap B) = (B \cap A)$	Commutative laws



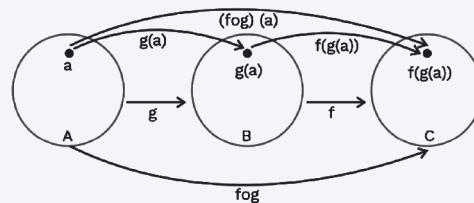
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cap (B \cup C) = (A \cap B)$ $\cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B)$ $\cap (A \cup C)$	Distributive laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

- Functions are sometimes called as mappings or transformations.
- One-to-one or injection: A function is said to be one to one if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain f .
- Onto function or surjection: A function f from A to B is called onto if and only if for every element $b \in B$. There is an element $a \in A$ with $f(a) = b$.
- Functions: Functions are also called mappings/transformations.
- A function can be one-to-one or onto.
- Inverse of a function:



Inverse of a Function

- Composite of function:





- Graph of a function: The set of pair in $A \times B$ to each function from A to B. This set of pair is called graph of a function.
- A relation is subset of cartesian product.
- A relation can be:
 - Symmetric
 - Antisymmetric
 - Asymmetric
 - Reflexive
 - Irreflexive
 - Transitive
- A relation can be represented using:
 - Diagraphs
 - Matrices
- A relation is said to be equivalence if it is:
 - Reflexive
 - Symmetric
 - Transitive
- Lattice:
 - Dual lattice is a lattice
 - Product of two lattice is a lattice
 - Every chain is a lattice
- POSET: An non-empty set P, forms a poset if it is:
 - Reflexive
 - Anti-symmetric
 - Transitive
- Hasse diagram: To obtain Hasse diagram follow these three simple steps:
 - Draw diagraph for given POSET
 - Remove all loops
 - Delete all edges implied by transitive property and arrange all edges pointing upwards

3

Graph Theory



Graph Theory

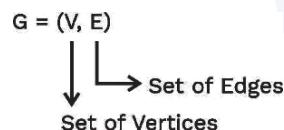
Graph theory helps in solving real time problems. In graphs theory, we will study mainly about undirected graphs.

Undirected graph and graph models:

Definition

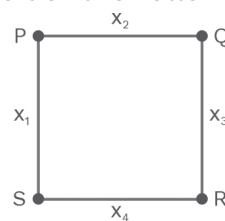
A graph $G = (V, E)$ consists of V , a non-empty set of vertices (or nodes) and E , a set of edges and every edge is associated with unordered pair of vertices.

Each edge is connected to one or two vertices, which are referred to as its endpoints.



In an undirected graph, an edge from vertex v to vertex u will be same as an edge from vertex u to vertex v .

Example: Consider the following graph:



$$V = \{P, Q, R, S\}$$

$$E = \{x_1, x_2, x_3, x_4\}$$

Terminologies:

There are some terminologies in graph theory:

Adjacent vertices:

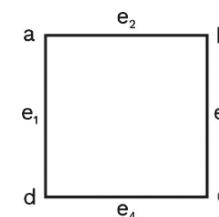
Two vertices v and u , belonging to vertex set V of an undirected graph $G(V, E)$, are adjacent if there exists an edge e , such that e belongs to set E and connects the vertices u and v .



In given figure, p and q are adjacent vertices, and x_1 is the common edge.

Adjacent edges:

Adjacent edges are those edges which are fain to the common vertex.



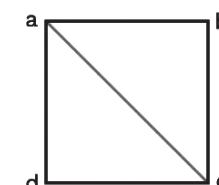
In the above shown figure, e_1 is adjacent to both e_2 (having common vertex a) and e_4 (having common vertex d).

Order of a graph:

Order of a graph G , is the total number of vertices present in the graph.
It is denoted by $O(G)$.

Size of graph:

Size of a graph G , is the total number of edges present in the graph.



$$O(G) = 4$$

$$\text{Size}(G) = 5$$

Self loop:

It is an edge in the graph which has same end points, i.e., it connects a vertex to itself.



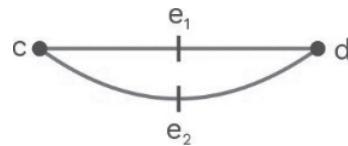
Parallel edges (multiple edges):

If in a graph between two vertices, if more than one edge is there, then those edges are known as parallel edges.

The graph, which contains parallel edges is known as multigraph.

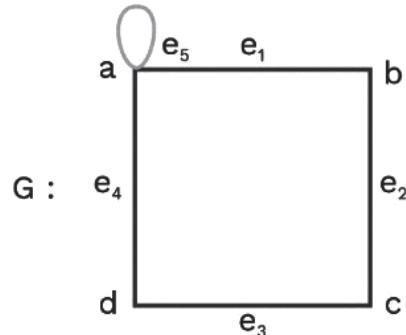


Multiple edges from c to d are shown by e_1 and e_2 in the diagram.



Edge-labelled graphs:

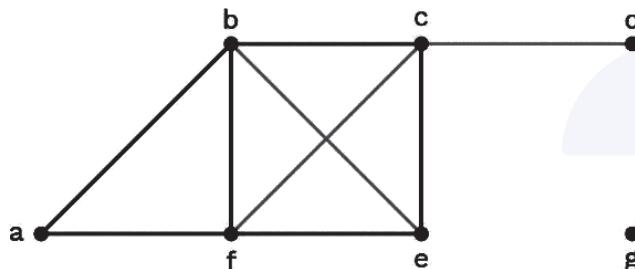
A graph with labelled edges is called edge labelled graph.



Isolated vertex:

An isolated vertex does not have any vertex adjacent to it, i.e., it is a vertex with degree zero.

Example: Consider the following figure:

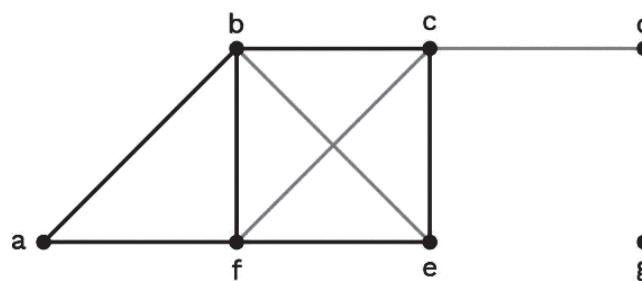


In the above figure, the isolated vertex is 'g'

Pendant vertex:

In a graph, if any vertex has degree one, then that vertex is known as pendant vertex.

Example:



In the given figure, the pendant vertex is 'd'.

Simple graph:

Simple graph can be defined as an undirected, unweighted graph having no self loops and multiple/parallel edges.

Note:

- A simple graph can be either connected or disconnected.
- For directed graph: $E \sim V \times V$

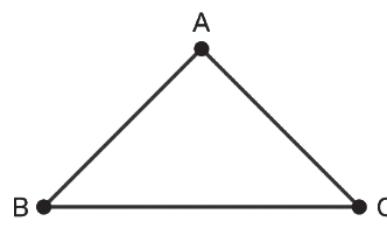


Fig. 3.1 A simple Graph

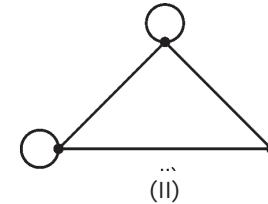
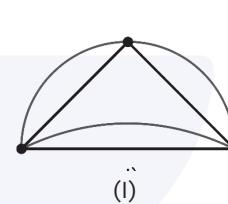


Fig. 3.2 Non-Simple Graphs (I) with Multiple Edges
(II) with Self Loops

Properties of simple graph:

- For a simple complete graph consisting of 'n' number of vertices, the maximum possible edges are:
$$= \frac{n(n - 1)}{2}$$
- Number of simple graph possible with n vertices = $2^{n(n-1)/2}$
- With 'n' vertices and 'm' edges, the number of simple graphs that are possible:

$$= C\left(\frac{n(n - 1)}{2}, m\right)$$

Example: Find the maximum number of simple graphs possible with five vertices and two edges.

Solution:

Maximum edges possible = $C(5, 2) = 10$

$$\left\{ \therefore \frac{n(n - 1)}{2} = \frac{5 \times 4}{2} = 10 \right\}$$

Maximum number of graphs = $C(10, 2) = 45$

Multigraph:

Graphs that may have multiple/parallel edges and no self loops are called multigraphs.

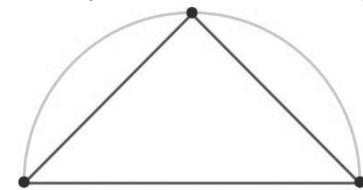


Fig. 3.3 Example of Multigraph

Pseudograph:

A graph G consisting of self loops and parallel/multiple edges can be defined as pseudograph.

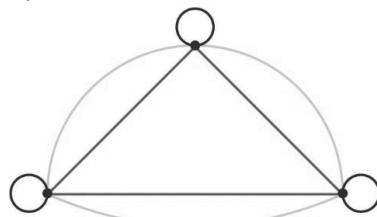
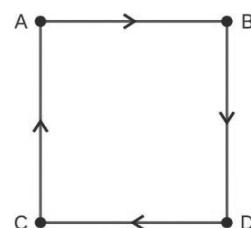


Fig. 3.4 Pseudograph

Directed graph:

If in a graph all the edges are ordered edges, i.e., edges with direction then the graph is known as directed graph, i.e., edge from vertex v to u is not same as edge from vertex u to v .



Here, $V = \{A, B, C, D\}$
 $E = \{(A, B), (B, A), (C, D), (D, C)\}$

Simple directed graph:

Definition



"A directed graph or (digraph) $G = (V, E)$ consists of a non-empty set of vertices V and a set of directed edges E associated with the ordered pair (u, v) is said to start at u and end at v . When a directed graph has no loops and has no multiple directed edges, it is called a simple directed graph."

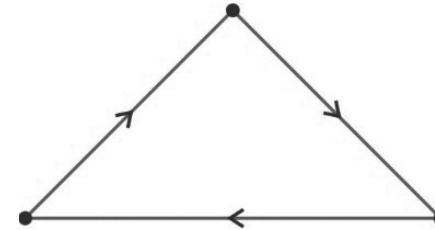


Fig. 3.5 Simple Directed Graph

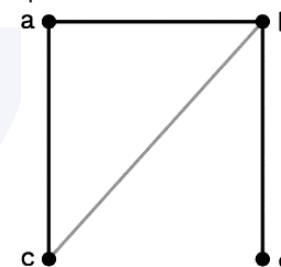
Directed Multigraph:

A directed graph having more than one edge between two vertices, is known as directed multigraph.

Note:

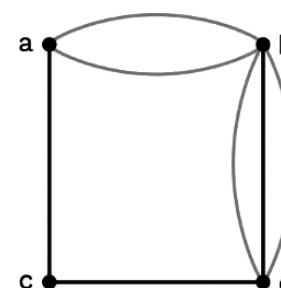
A graph with both directed and undirected edges is called mixed graph.

1. Simple graph



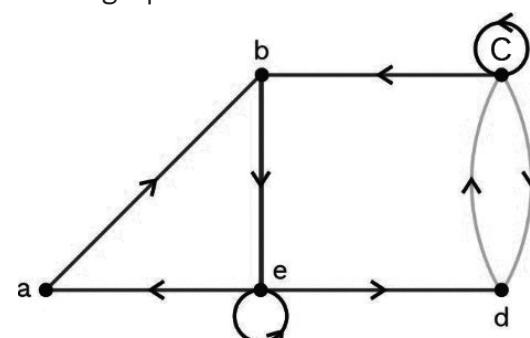
⇒ It has undirected edges, no multiple edges, no self loops.

2. Multigraph



⇒ It has undirected edges, multiple edges between a and b and no self loops.

3. Pseudograph





- a) It has directed edges.
- b) No multiple edges, first is from c to d and second is from d to c.
- c) It has 2 self loops (on c and e).



Rack Your Brain

What kind of graph can be used to model a highway system between major cities where:

1. There is an edge between the vertices, representing cities, if there is an interstate highway between them?
2. There is an edge between the vertices, representing cities, for each interstate highway between them.



Rack Your Brain

Describe a graph model that can be used to represent all forms of electronic communication between two people in a single graph. What kind of graph is needed?

Degree of vertex:

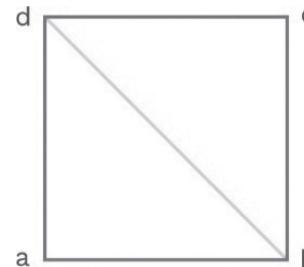
The number of edges that are incident onto a vertex is termed as the degree of that vertex.

For each self loop the degree is counted as 2.

Min-degree: Least among the degrees of all given vertices, represented by δ .

Max-degree: Maximum among the degrees of all the vertices in G. It is represented by Δ .

Example:



Solution:

	$\deg(v)$
a	2
b	3
c	2
d	3

$$\delta(G) = 2 \text{ and } \Delta(G) = 3.$$

Note:

Let G be a simple undirected graph with v -vertices and e -edges.

$$\frac{x}{(1-x)^2}$$

Solved Examples

1. What are the degree of vertices in the graphs G and H displayed in given figure:



Solution:

In G:

$$\begin{aligned}\deg(a) &= 2 \\ \deg(b) &= \deg(c) = \deg(f) = 4\end{aligned}$$

$$\deg(d) = 1$$

$$\deg(e) = 3$$

$$\deg(g) = 0$$

In H:

$$\deg(a) = 4$$

$$\deg(b) = 6$$

$$\deg(e) = 6$$

$$\deg(c) = 1$$

$$\deg(d) = 5$$



In and out degree of a vertex in directed graph:

In degree:

In-degree of a vertex V in a directed graph $G(V, E)$ is the total number of incoming edges to the vertex.

Out degree:

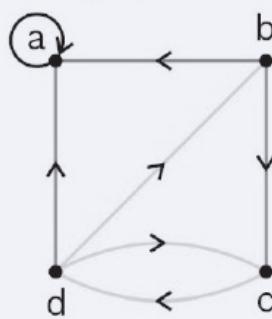
Out-degree of a vertex V in a directed graph $G(V, E)$ is the total number of outgoing edges from a vertex.

Note:

- A loop at a vertex contributes one to both the in-degree and the out degree of this vertex.
- As each edge has an initial vertex and a terminal vertex, the sum of the in-degree and the sum of the out-degree of all vertices in a graph with directed edges are the same. Both of these sums are the number of edges in the graph.

Rack Your Brain

Determine number of vertices and edges and find the in-degree and out-degree of each vertex for given directed multigraph.



Handshaking theorem: Further consequent theorems

Handshaking theorem states that the total number of edges contained in a graph is half the degree sum of all the vertices.

$$\sum_{u \in V} \deg(u) = 2|E|$$

Note:

This theorem is applicable even if multiple edges and self loops are present (pseudograph) in the graph.

Corollary 1: Let $G = (V, E)$ be a directed graph with $V = \{V_1, V_2, \dots, V_n\}$ then

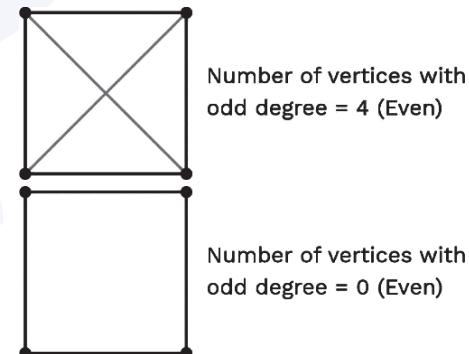
$$\sum_{i=1}^n \deg^+(V_i) = \sum_{i=1}^n \deg^-(V_i) = |E|$$

i.e., for a directed graph sum of all the out degrees of vertices is equal to sum of all in degrees of the vertices, which is equal to number of edges in the graph because in directed graph every edge will be counted as in degree for some vertex and out degree for some other vertex.

where $e = \text{number of edges in the graph}$.

$$\deg(V) = \text{in-degree}(V) + \text{out-degree}(V)$$

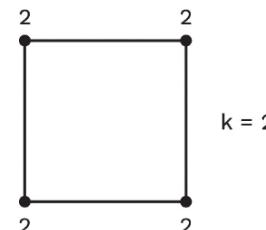
Corollary 2: In an undirected graph, the number of odd degree vertices are even.



Corollary 3: If G is an undirected graph with degree of each vertex k , then $k \times |V| = 2|E|$.

Corollary 4: If G is an undirected graph with degree of each vertex atleast k ($\geq k$) then $k \times |V| \leq 2|E|$.

Example:



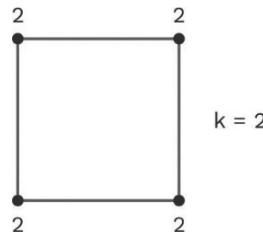
$$2 \times 4 \leq 2 \times 4$$

$$8 \leq 8$$



Corollary 5: If G is an undirected graph with degree of each vertex atmost k ($\leq k$) then $k|v| \geq 2|E|$.

Example:



$$2 \times 4 \geq 2 \times 4$$

Degree sequence:

- Arrangement of degree of all the vertices either in ascending or descending order, the sequence then obtained is called degree sequence.
- In any undirected graph, if degree of each vertex is distinct, then simple graph does not exist.

Havell-Hakimi theorem:

The purpose of this theorem is to check if a given degree sequence is a degree sequence of a simple graph or not.

Consider the degree sequences S_1 and S_2 , and assume that S_1 is in descending order.

$$S_1: \{S, t_1, t_2, \dots, t_s, d_1, d_2, \dots, d_n\}$$

$$S_2: \{t_1 - 1, t_2 - 1, \dots, t_s - 1, d_1, d_2, \dots, d_n\}$$

S_1 is graphic & S_2 is graphic.

Steps involved in this theorem:

- Sort given degree sequence in descending order.
- Pick the largest element and remove it from the list.
- Construct a new list.
- Take number of elements = largest element chosen.
- Subtract 1 from all the taken elements.
- Check if obtained degree sequence is valid or not (say this S_2).
- S_1 is a valid graphical degree sequence if S_2 is a valid graphical sequence.
- Repeat steps 1-7.

Points to remember:

- If we get atleast one negative term in degree sequence, then simple graph does not exist for the given degree sequence.
- When there are not enough degree present in the degree sequence, then also simple graph does not exist.

Solved Examples

2. $<6, 6, 6, 6, 3, 3, 2, 2>$, determine whether the given degree sequence represents a simple undirected graph.

Solution:

$$<6, 6, 6, 6, 3, 3, 2, 2>$$

$$<5 5 5 2 2 1 2>$$

$$<5 5 5 2 2 2 1>$$

$$<4 4 1 1 1 1>$$

$$<3 0 0 0 1>$$

$$<3 1 0 0 0>$$

$<0 -1 -1 0>$ As, it is visible that there are two negative integers present in degree sequence. Therefore it can not represent a simple undirected graph.

3. $<7, 6, 6, 4, 4, 3, 2, 2>$, determine whether the given degree sequence represents a simple undirected graph.

Solution:

$$<7, 6, 6, 4, 4, 3, 2, 2>$$

$$<5 5 3 3 2 1 1>$$

$$<4 2 2 1 0 1>$$

$$<4 2 2 1 1 0>$$

$$<1 1 0 0 0>$$

$<0 0 0 0>$ - All zeros present, therefore, it represents a simple undirected graph.



4. $<8, 7, 7, 6, 4, 2, 1, 1>$, determine whether the given degree sequence represents a simple undirected graph.

Solution:

In the above given degree sequence, after choosing 8 we need to subtract 1 from 8 elements out of remaining elements but there are only 7 elements left. Therefore, given degree sequence is not valid sequence for simple undirected graph.

OR

If we have 8 vertex maximum degree is 7, not 8. So simple graph does not exist.

5. How many edges are there in a graph with 10 vertices each of degree six?

Solution:

$2e = 60$ (Using handshaking theorem).
Therefore $e = 30$.

Note:

The undirected graph that results from ignoring directions of edges is called the underlying undirected graph.

Previous Years' Question



The degree sequence of a simple graph is the sequence of the degrees of the nodes in the graph in decreasing order. Which of the following sequences can not be the degree sequence of any graph? [GATE CSE 2010]

- I. 7, 6, 5, 4, 4, 3, 2, 1
 - II. 6, 6, 6, 6, 3, 3, 2, 2
 - III. 7, 6, 6, 4, 4, 3, 2, 2
 - IV. 8, 7, 7, 6, 4, 2, 1, 1
- (A) I and II (B) III and IV
 (C) IV only (D) II and IV

Solution: (D)

Some special simple graphs:

Null graph:

A graph having 'V' vertices and zero edges is known as null graph.

Trivial graph:

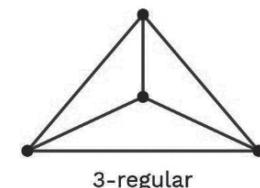
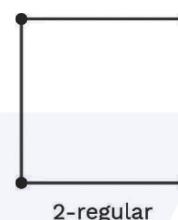
Trivial graph consists of one vertex and zero edges.

Regular graph:

A graph in which all the vertices have same degree is known as regular graph.

Note:

Every polygon is a 2-regular graph.

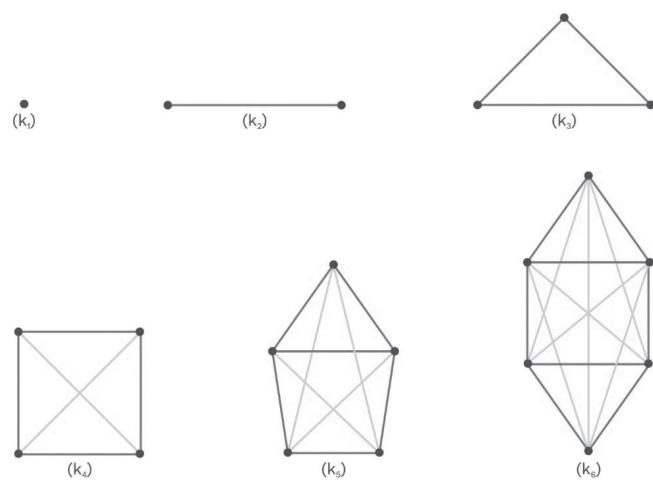


Note:

In a simple graph with n vertices at least two vertices should have same degree.

Complete graph:

A simple graph with V vertices where every vertex has an edge with all the other vertices is known as complete graph. The graph k_n , for $n = 1, 2, 3, 4, 5, 6$ as shown in the given figure.





Note:

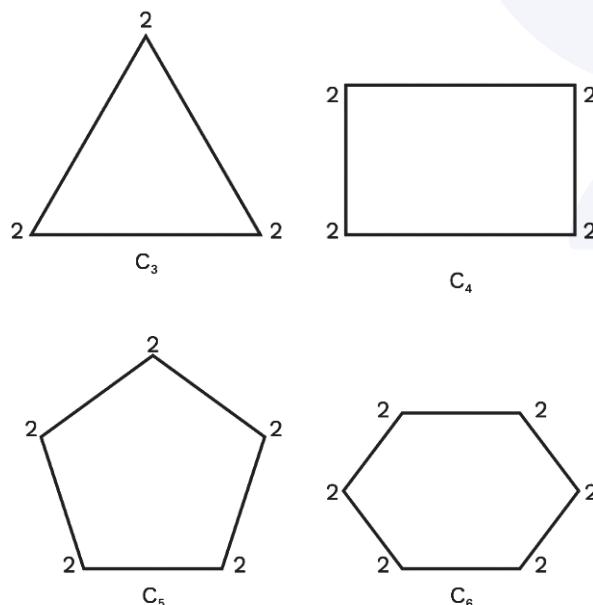
- A complete graph is a simple graph with maximum number of edges.
- A complete graph is a simple graph with every vertex having maximum degree.

Properties of complete graph:

- Every complete graph is a regular graph, but every regular graph need not be complete.
- A complete graph is a simple graph with maximum number of edges.
- Number of edges in $K_n = \frac{n(n - 1)}{2}$
- Degree of each vertex = $(n - 1)$

Cycle graph:

The cycle graph C_n , for $n \geq 3$, is a simple connected graph with degree of every vertex as 2.

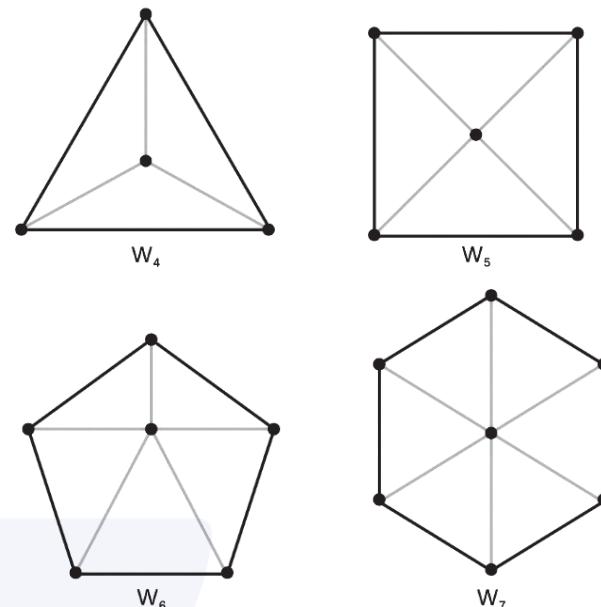


Note:

If a graph is a cycle graph then number of vertices is equal to number of edges but not vice versa.

Wheel graph:

Wheel graph represented by W_n , where n is greater than or equal to four, can be obtained by adding a vertex to the cycle graph such that the new vertex is adjacent to all vertices.

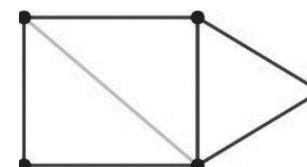


Note:

Number of edges in $W_n = 2(n - 1)$

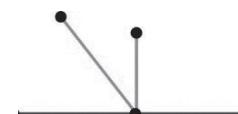
Cyclic graph:

A cyclic graph is a simple graph which contains atleast one cycle.



Acyclic graph:

Simple graph having no cycle is known as acyclic graph.



Bipartite graph:

Definition

"A simple graph G is called a bipartite graph if its vertex set V can be partitioned into two disjoint sets V_1 & V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2). When this condition holds, we call the pair (V_1, V_2) a bipartition of the vertex set V of G ."

Example:

Consider the following cyclic graph C_6 . The vertex set of C_6 can be partitioned into two sets $V_1 = \{1, 3, 5\}$ and $V_2 = \{2, 4, 6\}$, such that there is no edge between vertices of same set: therefore C_6 is a bipartite graph.

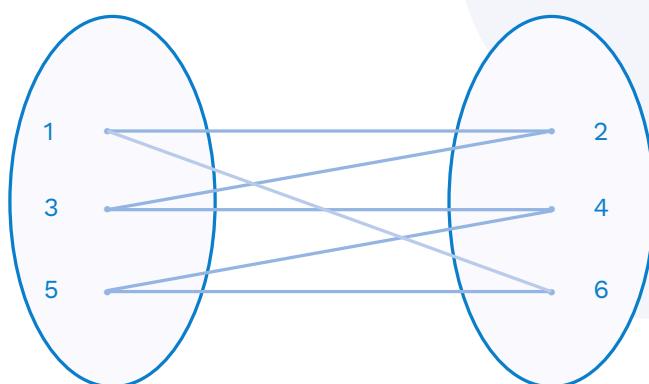
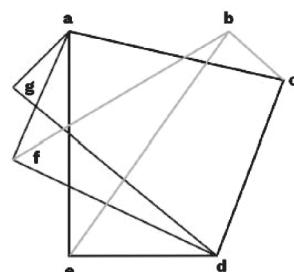


Fig. 3.6 C_6 is Bipartite

6. Determine if given graph is bipartite?



Solution:

The vertex set of the following graph can be partitioned into two sets, $V_1 = \{a, b, d\}$ and $V_2 = \{c, e, f, g\}$.

Since, there is no edge between the vertices of same set, so the given graph is bipartite graph.

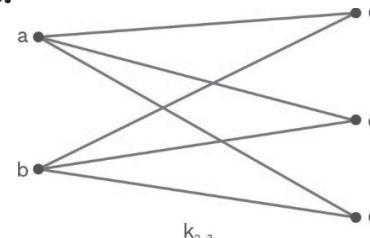
Note:

- A simple graph is bipartite if and only if it is possible to assign one of two different colours to each vertex of the graph so that no two adjacent vertices are assigned the same colour.
- A graph is bipartite iff it has no odd length cycle.

Complete bipartite graph:

The complete bipartite graph $K_{m,n}$ is a graph in which vertex set V is divided into two subsets, P having m vertices and Q having n vertices respectively, such that every vertex from set P is connected to every other vertex in set Q and there is no edge between the vertices from same subset.

Example:



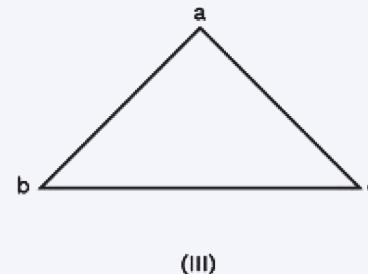
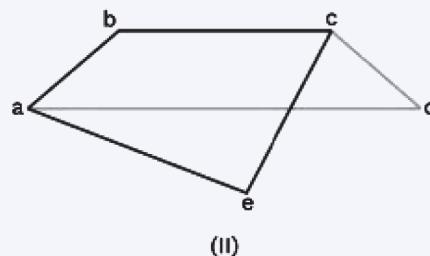
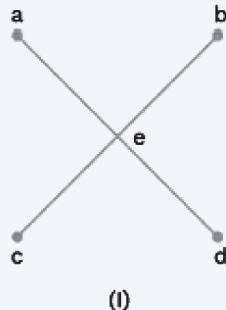
Note:

$K_{m,n}$ has $(m + n)$ vertices and $m*n$ edges.



Rack Your Brain

Determine whether the graph is bipartite or not.



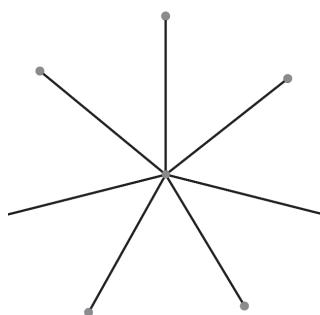
Star graph:

Star graph is a special type of graph in which a single vertex is connected to all the other vertices.

For a graph having n vertices, $n - 1$ vertices will have degree 1 and one vertex will have degree $n - 1$.

It is represented as: $k(1, n - 1)$.

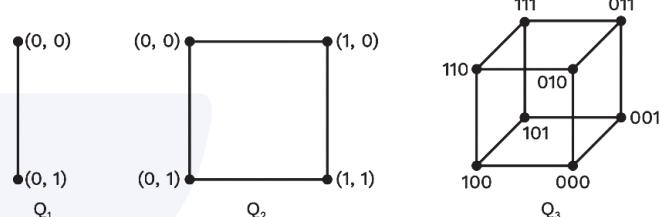
- Used in client server architecture.



Hypercube graph/n dimensional cube:

In hypercube graph, there is an edge between two vertices only if the vertices differ by single bit position.

- The hypercube graph is represented by Q_n .
- Order of hypercube graph $O(Q_n) = \text{number of vertices} = 2^n$
- Q_n is a n degree regular graph.
- Number of edges in $Q_n = n \times 2^{n-1}$ (using handshaking lemma i.e., in every finite undirected graph, the number of vertices that touch an odd number of edges is even).



Connected graph:

- A graph having V vertices and E edges, is said to be connected if there is a path between all the pairs of vertices in the graph.
- Maximally connected subgraph of a graph is a component.
- Every connected graph has exactly one component.
- If G is a simple graph with n vertices, e edges, and k components.

$$n - k \leq e \leq \frac{(n - k)(n - k + 1)}{2}$$

Examples of connected graph:

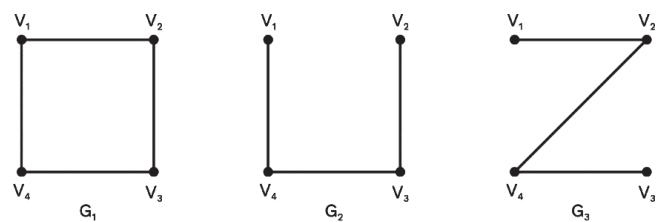


Fig. 3.6 Connected Graphs



Disconnected graph:

For a disconnected graph ($k > 1$ or $k \geq 2$), the path is not available between atleast one pair of vertices.

Examples of disconnected graph:

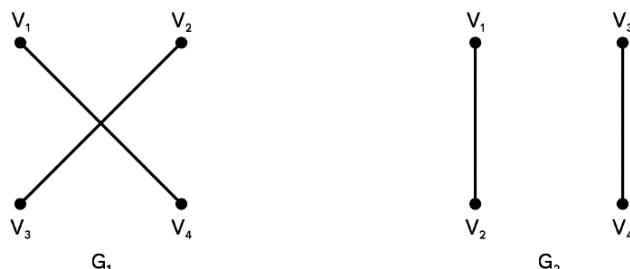


Fig. 3.7 Disconnected Graphs

Note:

- If G is a simple graph with n -vertices and $|E|$ edges, $|E| > \frac{(n-1)(n-2)}{2}$, then G is connected (sufficient condition)
- In simple connected graph with n vertices, $n-1 \leq e \leq \frac{n(n-1)}{2}$



Rack Your Brain

Which of the following graph is always connected?

- G with 5 vertex and 5 edges
- G with 5 vertex and 12 edges
- G with 5 vertex and 10 edges
- G with 10 vertex and 18 edges

Complement of a graph:

The complement of an undirected graph having v vertices is denoted by \bar{G} , which have the same number of vertices as that of G and an edge $\{u, v\} \in \bar{G}$ iff $\{u, v\} \notin G$.

Note:

- $G \cup \bar{G} = kn$, where $n =$ number of vertices.
- $|E(G)| + |E(\bar{G})| = |E(kn)|$, where $n = |V(G)|$

Example: Consider a simple graph G having 8 vertices and 15 edges. Calculate the number of edges in \bar{G} ($|E(\bar{G})|$).

Solution:

We have

$$|E(G)| + |E(\bar{G})| = |E(k_8)|$$

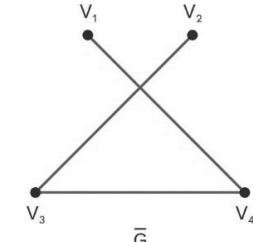
$$15 + |E(\bar{G})| = \frac{8(8-1)}{2} = \frac{8 \times 7}{2} = 28$$

$$|E(\bar{G})| = 28 - 15$$

$$|E(\bar{G})| = 13$$

Self complementary:

When a graph is isomorphic to its complement is called self complementary graph.



$$G \cong \bar{G}$$

Note:

- The number of edges in a self complementary graph is $= \frac{n(n-1)}{2}$
- The number of vertices in a self complementary graph is of the form $4k$ or $4k+1$, k is an any positive integer.

New graph from old graph:

Sometimes only a part of the graph is needed to solve a problem. In this case, we can remove some vertices, and all edges incident on that vertex are removed. This will help in obtaining a smaller graph, called as a subgraph of the original graph.

Definition

A subgraph of a graph $G(V, E)$ is a graph $H(W, F)$ where, $W \subseteq V$ and $F \subseteq E$.

A subgraph H of G is a proper subgraph of G if $H \neq G$.



The following graph is subgraph of K_5 .

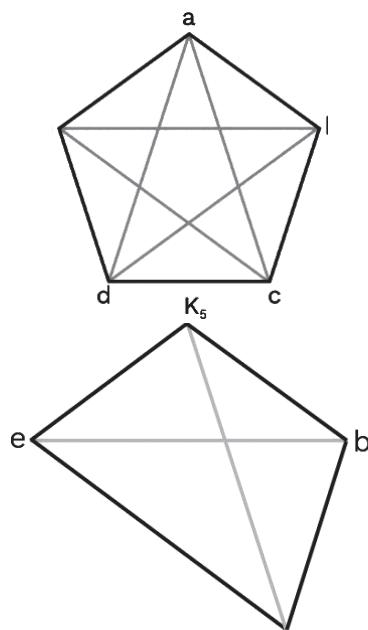


Fig. 3.8 Subgraph of K_5

Union of graphs:

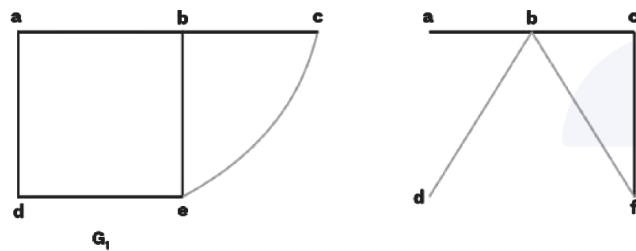
Two or more graphs can be combined in various ways; the new obtained graph after combining all the vertices and edges is called the union of graph(s).

Definition

The union of two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is a simple graph with vertex set $V = V_1 \cup V_2$ and edge set $E = E_1 \cup E_2$. The union of G_1 and G_2 is denoted by $G_1 \cup G_2$.

Solved Examples

7. Determine the union of the following graphs?



Solution:

The vertex set of $G_1 \cup G_2$ is the union of the two vertex sets, namely, $\{a, b, c, d, e, f\}$. The edge set of $G_1 \cup G_2$ is the union of the two edge sets.

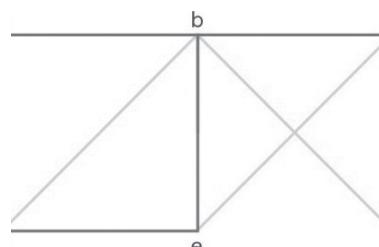


Fig. 3.9 $G_1 \cup G_2$

Representing graphs:

A graph can be represented in many ways:

- One way to represent a graph without multiple edges is to list all the edges of the given graph. Another way is to use an adjacency list.

Example:

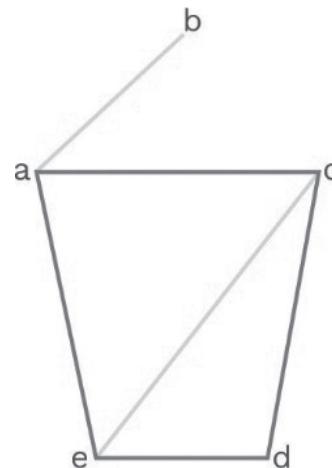


Fig. 3.10 A Simple Graph

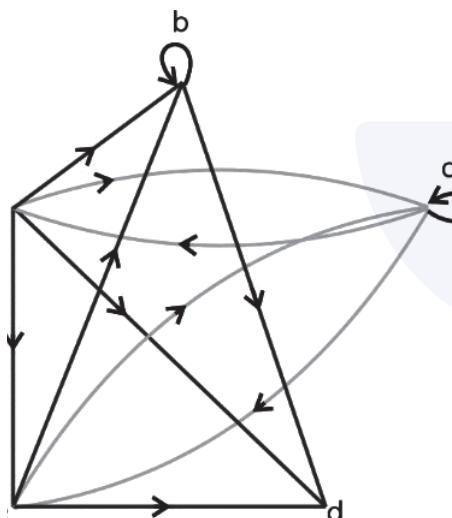
The adjacency list for the following simple graph will be.



Initial Vertex	Terminal Vertices
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

Fig. 3.11 An Adjacency List

Example: Consider the following graph. What will be its adjacency list representation?



Solution:

For the given directed graph, the adjacency list representation will be as follows:

Initial Vertex	Terminal Vertices
a	b, c, d, e
b	c, d
c	a, c, e
d	
e	b, c, d

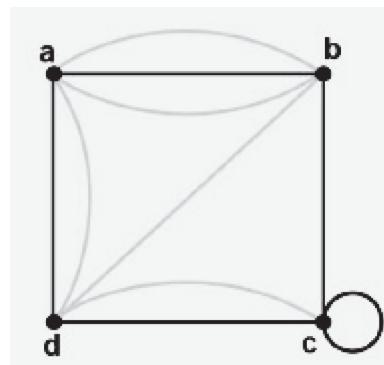
- Another method used for representing graphs is the adjacency matrix.

For a simple graph whose vertices are listed as 1, 2, ..., n. The adjacency matrix A with respect to the listing of vertices is nxn zero-one matrix.

$$a_{ij} = \begin{cases} 1 & \text{if } \{i, j\} \text{ is an edge of } G \\ 0 & \text{otherwise} \end{cases}$$

Solved Examples

8. Consider the following pseudo graph. What will be the adjacency matrix representation of the following graph?



Solution:

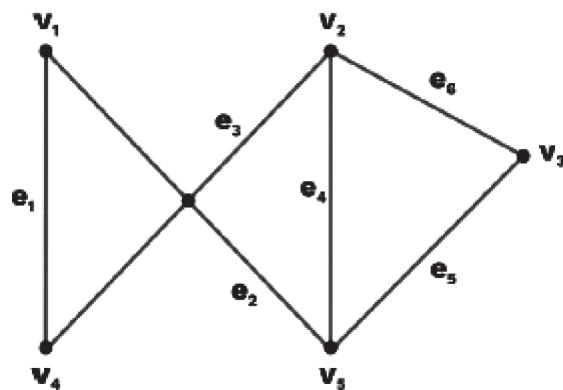
The adjacency matrix for the following graph will be:

$$\begin{array}{l} a \ b \ c \ d \\ a \left[\begin{array}{cccc} 0 & 3 & 0 & 2 \end{array} \right] \\ b \left[\begin{array}{cccc} 3 & 0 & 1 & 1 \end{array} \right] \\ c \left[\begin{array}{cccc} 0 & 1 & 1 & 2 \end{array} \right] \\ d \left[\begin{array}{cccc} 2 & 1 & 2 & 0 \end{array} \right] \end{array}$$

When a graph contains relatively fewer edges, i.e., when it is sparse, it is preferable to use an adjacency list rather than an adjacency matrix to represent a graph.



9. Represent the following graph with an incidence matrix.



Solution:

The incidence matrix for above graph is:

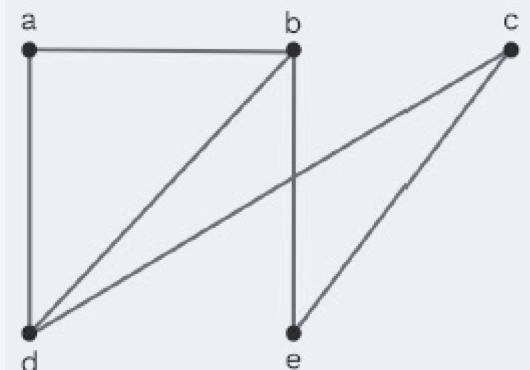
	e_1	e_2	e_3	e_4	e_5	e_6
1	1	1	0	0	0	0
2	0	0	1	1	0	1
3	0	0	0	0	1	1
4	1	0	1	0	0	0
5	0	1	0	1	1	0

Note:

Incidence matrix can also be used to represent multiple edges and self loops. Multiple edges are represented in the incidence matrix using columns with identical entries. Loops are represented using a column with exactly one entry = 1, corresponding to the vertex that is incident with this loop.

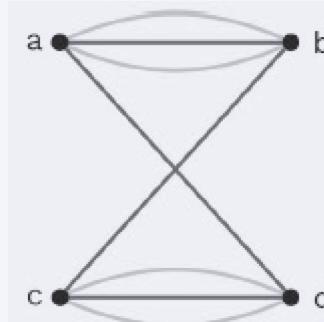
Rack Your Brain

What will be the adjacency list representation of the following graph?



Rack Your Brain

What will be the adjacency matrix representation of the following graph?



Walk, trail, circuit, path, and cycle:

Walk:

A walk is an alternative sequence of vertices and edges, which begins and end with a vertex. Both edges and vertices can be repeated in a walk.

Trail:

A walk is said to be a trail when there is no repetition of edges, but vertex can be repeated.

Closed trail:

A trail starting and ending at the same vertex is known as a closed trail.

A closed trail is called a circuit.

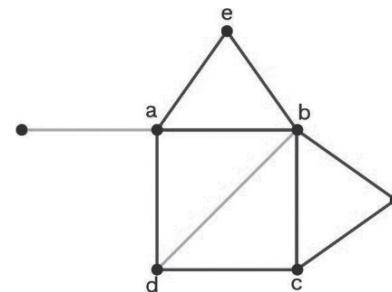
Path:

It is a walk in which repetition of vertices and edges is not allowed.

Closed path:

A path that starts at a vertex and ends in the same vertex is called a closed path.

It is also called cycles.



Walk $(u, v) = u - a - b - d - a - b - v$

Trail $(u, v) = u - a - b - d - c - b - v$

Circuit $(a, a) = a - b - v - c - b - d - a$

Path $(u, v) = u - a - b - v$

Closed path $(d, d) = d - a - e - b - d$

Graph	Repetition of Edge	Repetition of Vertex
Walk	Allowed	Allowed
Trail	Not allowed	Allowed
Path	Not allowed	Not allowed

Note:

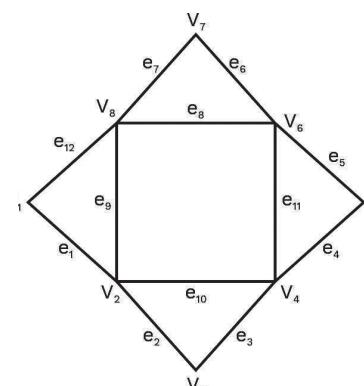
A cycle is a part of circuit but a circuit can't always be a cycle.

Euler graph:

If a graph contains Euler circuit, then it is known as an Euler graph.

Or

A graph is an Euler graph if it has a closed trail containing all edges.

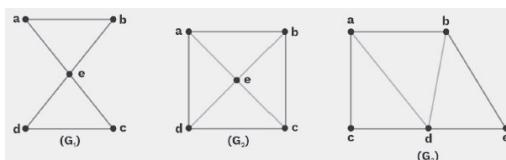


The above graph has Euler circuit $V_1 - e_1 - V_2 - e_9 - V_8 - e_8 - V_6 - e_{11} - V_4 - e_{10} - V_2 - e_2 - V_3 - e_3 - V_4 - e_4 - V_5 - e_5 - V_6 - e_6 - V_7 - e_7 - V_8 - e_{12} - V_1$



Solved Examples

10. Which of the following are Euler graph?



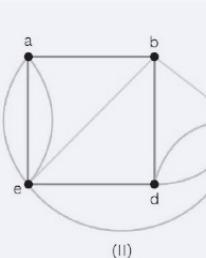
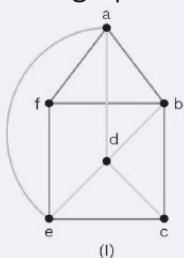
Solution:

Graph G_1 has an Euler circuit ($a - e - d - c - e - b - a$), i.e., there is a closed trail that covers all the edges. Therefore, it is an Euler graph. But G_2 and G_3 do not contain Euler circuit. So G_2 and G_3 are not Euler graph.

Rack Your Brain



Determine whether the given graph is Euler graph?

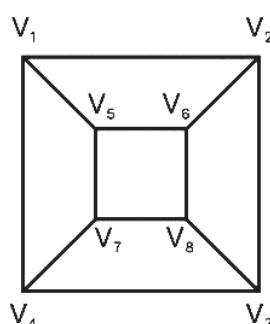


Hamiltonian graph:

A graph is said to be a Hamiltonian graph, if it contains a Hamiltonian cycle.

Hamiltonian cycle, in a connected graph, is a cycle that covers all the vertices.

If any edge is removed from the Hamiltonian cycle, then it gets converted into Hamiltonian path.

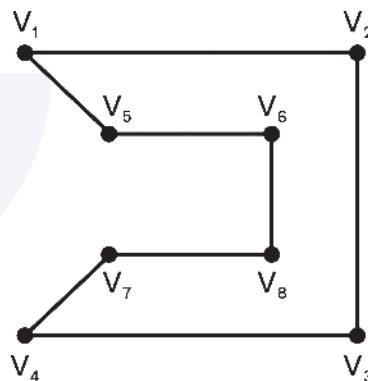


Note:

- Euler circuits are also applicable to the graph with loops (unless it is a loop in a component with one vertex).
- Euler circuits are also applicable to the Multigraph.

Result:

A graph is an Euler graph if and only if it is connected and $\forall V \in G$, degree (V) is even.



The given graph is a Hamiltonian graph because of Hamiltonian cycle

$$V_1 - V_5 - V_6 - V_8 - V_7 - V_4 - V_3 - V_2 - V_1.$$

Sufficient condition for hamiltonian graph:

DIRAC's theorem:

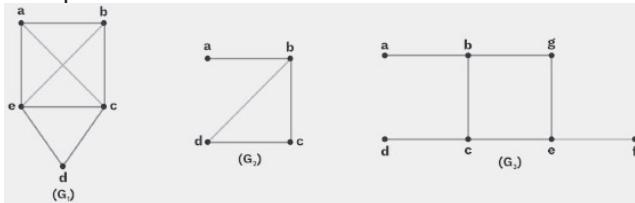
A simple connected graph G having ' v ' vertices ($v \geq 3$), is said to have a Hamiltonian cycle if the minimum degree of every vertex in the graph is $n/2$.

ORE's theorem:

If G is a simple connected graph with n vertices ($n \geq 3$), such that $\deg(u) + \deg(v) \geq n$ for every pair of non-adjacent vertices u and v in G , then G has a Hamiltonian cycle.

Solved Examples

11. Which of the following simple graphs have a Hamiltonian cycle or Hamiltonian path?

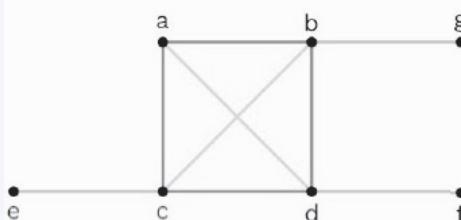


Solution:

G_1 has a Hamiltonian cycle (a – b – c – d – e – a). There is no Hamiltonian cycle in G_2 but G_2 has a Hamiltonian path (a – b – c – d). G_3 , neither has a Hamiltonian cycle nor a Hamiltonian path because edges {a – b}, {e – f}, and {e – d} are covered more than one time.

Rack Your Brain

Determine whether the following graph is Hamiltonian graph?



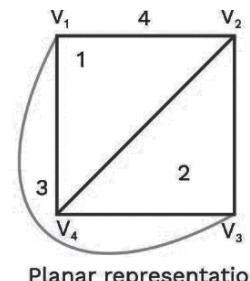
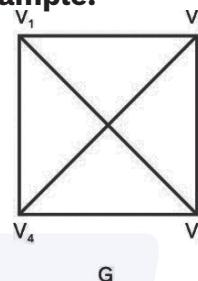
Planar graph:

- A graph having a planar representation is called a planar graph.
- Planar representation means drawing a graph on a plane without crossing the edges.
- The planar representation of a planar graph divides the entire plane into regions or faces.

Definition

"A graph is called planar, if it can be drawn on the plane without any edges crossing (where a crossing of edges is the intersection of the Lines or arcs representing them at a point other than their common end point). Such a drawing is called planar representation of a graph."

Example:



Planar representation

The given graph G is a planar graph because in planar representation, no edges intersect each other.

Euler's formula:

As we have already seen, a planar graph splits the plane into regions, including an unbounded region. According to Euler, for any simple connected graph having ' V ' vertices and ' e ' edges, the number of regions ' r ' in the planar representation of graph is given by:

$$V - e + r = 2$$

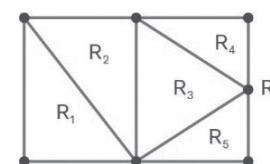


Fig. 3.12 The Regions of Planar Representation of Graph

Results for planar graph:

Minimum degree for region k

- $V - e + r = 2$
- $kr \leq 2e$
- $e \leq \frac{k(V-2)}{k-2}$



Polyhedral graph:

A planar graph in which every interior region is polygon is called polyhedral graph.

- In a polyhedral graph degree of every vertex, i.e., $\deg(V) \geq 3 \forall V \in G$
- For a polyhedral graph, the following inequality must hold:
 - $V - e + r = 2$
 - $3r \leq 2e$
 - $e \leq 3V - 6$

Previous Years' Question



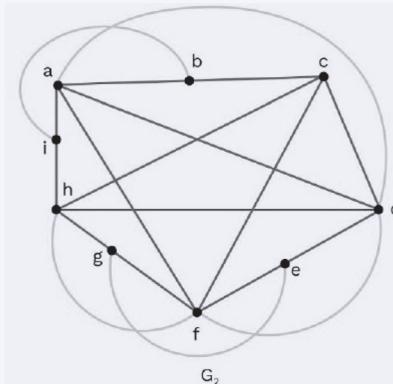
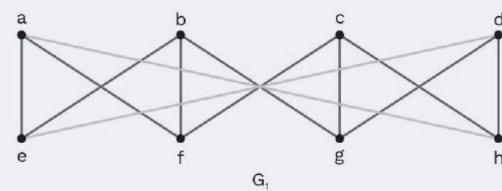
Let G be a connected planar graph with 10 vertices. If the number of edges on each face is three, then the number of edges in G is
[2015 Set 1]

Solution: 24

Rack Your Brain



Determine which of the following graphs are planar?

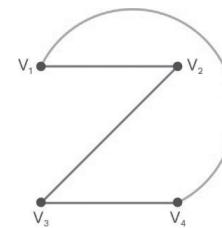
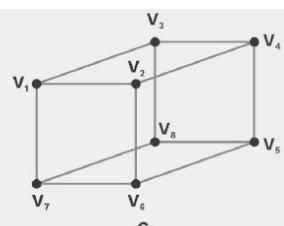
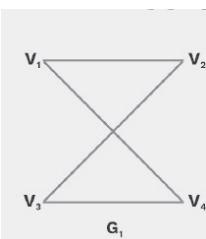


Note:

- K_5 is a non planar graph with minimum number of vertices.
- $K_{3,3}$ is non planar graph with minimum number of edges.

Solved Examples

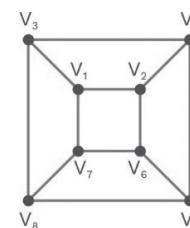
12. Which of the following graphs are planar?



G_2 is also planar because it can also be drawn without any edge crossings.

Solution:

G_1 is planar because it can be represented without edge crossings.





- 13.** Suppose that a connected planar simple graph has 10 vertices, each of degree 3. Into how many regions does a representation of this planar graph split the plane?

Solution:

Using Handshaking theorem, $\Sigma \text{ degree}(V) = 2 \times \text{number of edges}$

$$3 * 10 = 2 * e$$

$$e = 15$$

From Euler's formula the number of region is

$$r = e - v + 2$$

$$r = 15 - 10 + 2$$

$$r = 7$$

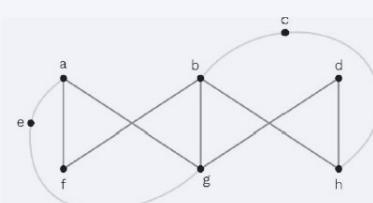
Kuratowski's theorem:

"If a graph is planar, so will be any graph obtained by removing an edge $\{u, v\}$ and adding a new vertex w together with edges $\{u, w\}$ and $\{w, v\}$. Such an operation is called an elementary subdivision. The graphs $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ are called homeomorphic if they can be obtained from the same graph by a sequence of elementary subdivision."

A graph is planar if it does not contain any graph homeomorphic to K_5 or $K_{3,3}$.

Rack Your Brain

Determine whether the given graph is homeomorphic to $K_{3,3}$.



Trees:

Basically, this is the topic of data structure and algorithms but here, we will study this topic in terms of Discrete Mathematics.

Tree can be defined as a minimally connected acyclic graph.

For every (u, v) , there exists exactly one path between u and v or it is a 1-connected graph.

Every tree is bi-chromatic and bipartite.

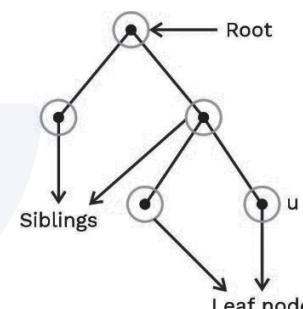
Fundamental cycle:

A cycle obtained by adding a single edge is called a fundamental cycle.

Now, number of fundamental cycles = ${}^n C_2$ when n = number of vertices.

Rooted tree:

A tree with a specific vertex is chosen as a root.



Root, siblings (having a common parent), leaf node can be only defined for a rooted tree.

depth (u) = distance (u , root), where u is node

height (T) = Maximum of depth (u), where u is node and T is a tree

level (u) = $1 + \text{depth } (u)$

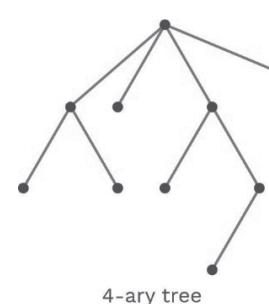
OR

level (T) = $1 + \text{height } (T)$, where u is node and T is a tree

K-ary tree:

It is a rooted tree.

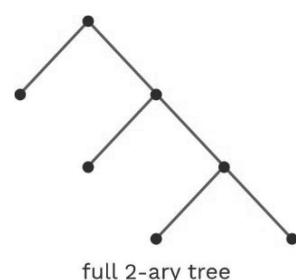
$0 \leq \text{number of children } (u) \leq k$





Full k-ary tree:

- It is a rooted tree.
- Number of children (u) = 0 or k

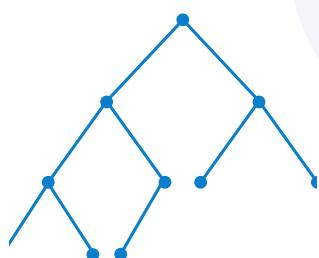


Complete k-ary tree:

- It is a rooted tree.
- All levels except the last one are completely filled.
- Last level is left adjusted.

Left adjusted:

When we start filling from left to right, then it is called left adjusted.



Note:

Complete k-ary tree does not implies a full k-ary tree and vice versa.

Properties of k-ary tree:

Considering, l = number of leaves

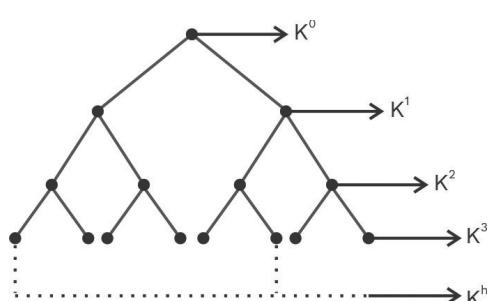
n = Number of nodes

h = Height of tree

i = Number of internal nodes

For maximum number:

$$1. l \leq k^h$$



$$2. n \leq \frac{k^{h+1} - 1}{k - 1}$$

$$3. i \leq \frac{k^h - 1}{k - 1}$$

For minimum number:

1. $n \geq h + 1$
2. $i \geq h$
3. $\log_k l \leq h$

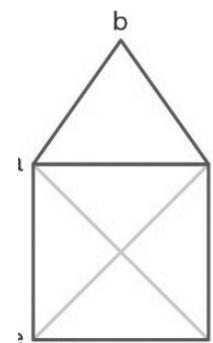
Spanning tree:

A spanning tree of G is a subgraph of G which includes every vertex of G .

Note:

Every connected graph has a spanning tree.

Example:



Solution:

Possible spanning trees:



A subgraph H of G is called a spanning tree of G , if

H is a tree

H contains all vertices of G

Circuit rank: The circuit rank of any given graph can be defined as the number of edges that are required to remove in order to obtain a spanning tree that is equal to $[m - (n-1)]$, where m is the number of edges, and n equals to the number of vertices.

Example:

$$\text{Circuit rank (G)} = m - (n - 1) = 4$$

Example: For the given graph, calculate the total number of spanning trees possible.

- (A) 6
(B) 12
(C) 8
(D) 16

Solution:

$$A = \begin{matrix} & a & b & c & d \\ a & \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{matrix}$$

$$M = \begin{bmatrix} 2 & 0 & -1 & -1 \\ 0 & 2 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{bmatrix}$$

$$\text{Cofactor of } M_{11} = (-1)^{1+1} \begin{vmatrix} 2 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{vmatrix}$$

$$= 2(9 - 1) + 1(-3 - 1) - 1(1 + 3)$$

$$= 16 - 4 - 4 = 8$$

Graph colouring:

Vertex colouring: In vertex colouring, every vertex of the graph is given a colour such that the vertices adjacent to each other must have different colours.

Chromatic number: Chromatic number is a number that tell minimum how many colours

Number of spanning trees in a complete graph

$$= n^{n-2} \text{ (Cayley's formula)}$$

$$= 16$$

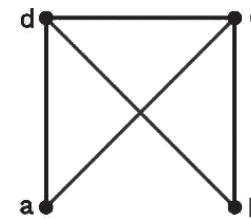
Kirchoff's theorem:

For a connected graph G, let A be its adjacency matrix representation.

Consider a matrix M obtained by replacing all 1's in matrix A with -1 and all 0's in principle diagonal of matrix A with the degree of the corresponding vertex.

Cofactor of any element of M is equal to the number of spanning trees in G.

Example: Consider the following matrix representation of a graph. Calculate the number of possible spanning trees for the graph.



will be needed to colours all the vertices of the graph such that no two vertices have the same colour. It is denoted as $\lambda(G)$

- $\lambda(G) = 1$ if G is a null graph
- If G is not a null graph, then $\lambda(G) \geq 2$
- A graph G is said to be n-colourable, if there exists a vertex colouring that uses atmost n colours, i.e., $\lambda(G) \leq n$

Four colour theorem:

Every planar graph G is 4-colourable, i.e., $\lambda(G) \leq 4$.

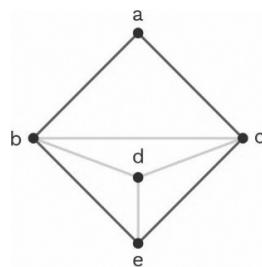


Welsh-Powell algorithm:

Welsh-Powell Algorithm

- 1. Find the degree of each vertex.
- 2. Arrange vertices of G in the descending order of their degrees.
- 3. Color the first vertex with color C_1 in sequential order, assign C_1 to each vertex which is not adjacent to previous vertex which was assigned C_1 .
- 4. Repeat step (3) with a second color C_2 and the sequence of non-colored vertices.
- 5. Repeat step (4) with a third color C_3 , then a fourth color C_4 and so on until all vertices are colored.
- 6. Exit.

Example: Consider the following graph, what will be its chromatic number?



- (A) 2
- (B) 3
- (C) 4
- (D) 5

Answer: (C)

Solution:

Vertex	a	b	c	d	e
Color	C_1	C_2	C_3	C_1	C_4

As the graph is planar, we will apply four-colour theorem chromatic number

$$\lambda(G) \leq 4 \quad \dots \text{(i)}$$

Further, we have 4 mutually adjacent vertices $\{b, c, d, e\}$
 $\therefore \lambda(G) = 4$... (ii)
 From (i) and (ii)
 $\lambda(G) = 4$

Connectivity:

Vertex connectivity:

In a connected graph G , the minimum number of vertices whose deletion makes graph disconnected or reduces G into a trivial graph is called vertex connectivity of a connected graph G . It is denoted by $k(G)$

- If G has a cut vertex, then $k(G) = 1$

Edge connectivity:

- In a connected graph G , the minimum number of edges whose deletion makes the graph disconnected is called edge connectivity of G .

It is denoted by $\lambda(G)$.

- If G has a cut edge, then edge connectivity $\lambda(G) = 1$ (also known as bridge).

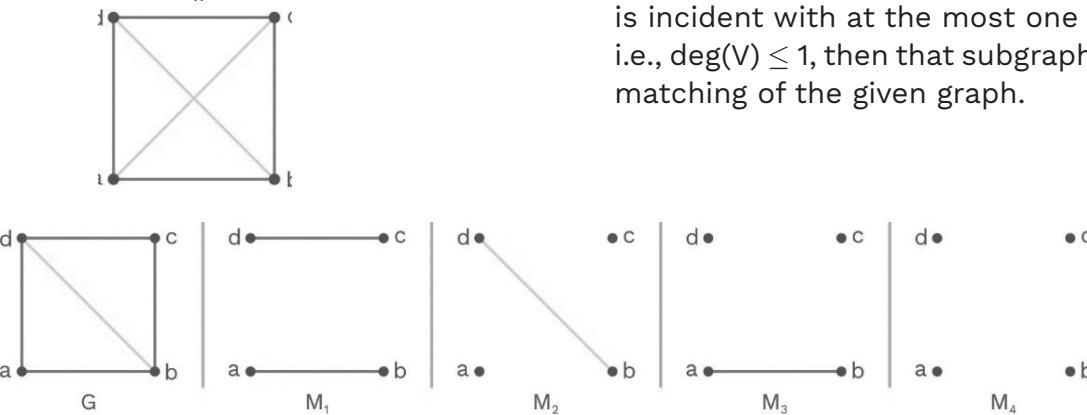


- The number of edges in the smallest cut set of G is said to be edge connectivity of G .

Example: For complete graph K_n

Vertex connectivity of $K_n = n - 1$

Edge connectivity of $K_n = n - 1$



In a matching, no two edges are adjacent, so $\deg(V) \leq 1$

- Maximal matching:** If in any matching M of graph G , further no more edges can be included then M is said to be maximal matching.

M_1 and M_2 are the maximal matching of G in the above example.

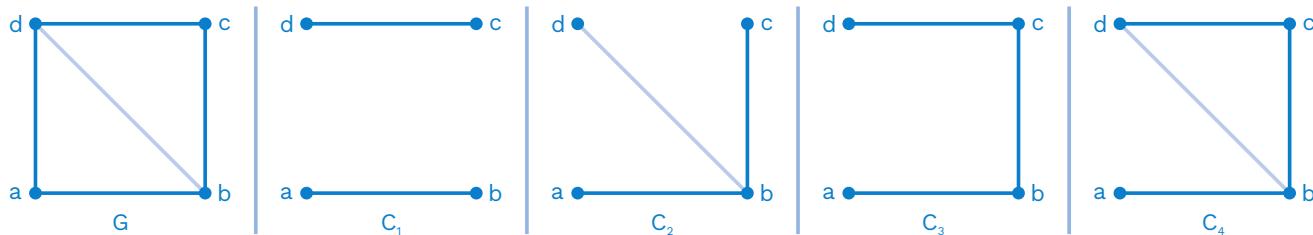
- Maximum matching:** For any matching M of Graph G , if M consists of the maximum number of edges.
- Matching number:** It is the number of edges included in a maximum matching of G .
Matching number of $M_1 = 2$
- Perfect matching:** A matching of a graph in which every vertex is matched is called perfect matching.

Example: What is the matching number of star graph with n vertices ($n \geq 2$) is:



Star graph is
 $K_{1,n-1}$
Bipartite graph

Solution: 1



Cut set:

It is the minimum set of edges whose removal will disconnect the graph.

Matching and covering:

- Matching:** If every vertex of given graph G is incident with at the most one vertex, i.e., $\deg(V) \leq 1$, then that subgraph is called matching of the given graph.

Previous Years' Questions



How many perfect matching are there in a complete graph of 6 vertices?

[GATE CSE 2003]

(A) 15

(B) 24

(C) 30

(D) 60

Solution: (A)

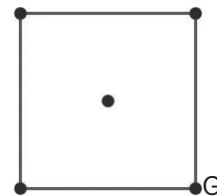
Covering:

Line covering:

A subset $S(E)$, of graph $G(V, E)$, will be a line covering of G if all the vertices of G will incident with a minimum one edge in S , i.e., degree of each vertex will be atleast 1.



If, in any case, graph G has an isolated vertex, line covering will not exist.



Minimal line covering: Line covering is minimal if the deletion of any edge from the line cover is not possible.

Minimum line covering:

- The number of edges present in minimum line covering is called the line covering number of a graph $G = \alpha_1$

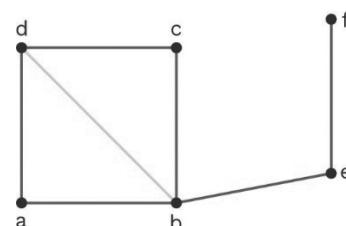
The graph above example has $\alpha_1 = 2$.
(C, graph is minimum line covering).

- Line covering of graph with n vertices contains atleast $\left\lceil \frac{n}{2} \right\rceil$ edges.

- No minimal line covering contains a cycle.
- In a line covering, if there is no path of length 3 or more, then C is minimal.
- In the line covering, if there are no paths of length 3 or more, then all components of C are star graphs. Then from those star graphs, no edge can be deleted.

Independent line set:

Let, $G = (V, E)$ be a graph, then a subset L of E is called an independent line set if no two edges in L are adjacent.



$$L_1 = \{b, d\}$$

$$L_2 = \{(b, d), (e, f)\}$$

$$L_3 = \{(a, d), (b, c), (e, f)\}$$

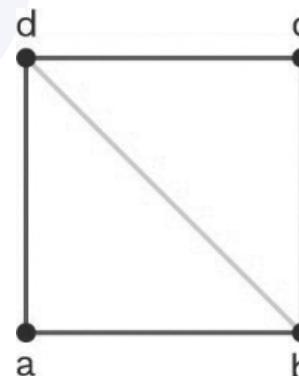
$$L_4 = \{(a, b), (e, f)\}$$

Maximal independent line set: For a graph G having an independent line set L , if no more edges of G can be included in L , then L is said to be a maximal independent line set.

Maximum independent line set: The largest maximal independent line set L of graph G which contains a maximum number of edges, is known as the maximum independent line set.

- Number of edges present in the maximum independent line set of a graph is known as the line independent number of G . It is denoted by β_1 .
 - Line independent number = matching number of G_1
- For the graph in above example L_3 is a maximum independent line set and $\beta_1 = 3$.
- For any graph $G_1 \alpha_1 + \beta_1 = |V|$ where α_1 is the line covering number.

Vertex covering: Let $G = (V, E)$ be graph then a subset k of V is called a vertex covering of G , if every edge of G is incident with a vertex in k .



$$k_1 = \{b, d\}$$

$$k_2 = \{a, b, c\}$$

$$k_3 = \{b, c, d\}$$

Minimal vertex covering: The vertex covering k is said to be minimal vertex covering if no vertex can be eliminated from it.

k_1 and k_2 are minimal vertex covering.

Minimum vertex covering: The minimum number of vertices in the vertex covering of a graph is called minimum vertex covering.

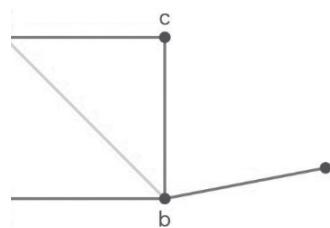
- The vertex covering a number of graph G is denoted by α_2 , which is defined as the total number of vertices present in minimum vertex covering.

In the above graph G for k , $\alpha_2 = 2$



Independent vertex set:

Let $G = (V, E)$ be a graph, then the subset S of V is called an independent set if no two vertices in S are adjacent.



$$S_1 = \{b\}$$

$$S_2 = \{d, e\}$$

$$S_3 = \{a, c\}$$

Maximal independent vertex set: An independent vertex set is said to be maximal, if no other vertex of G can be added to the set.

Example: $S_1 = \{b\}$

$$S_2 = \{d, e\}$$

$$S_3 = \{a, c\}$$

Maximum independent vertex set:

- Vertex independent number tells total how many vertices are there in the maximal independent vertex set. Vertex independent number of G denoted by β_2 .

Example: $S_3 = \{a, c, e\}$

$$\therefore \beta_2 = 3$$

- For any graph $\alpha_2 + \beta_2 = |V|$
- For any graph if S is independent set of G then $V - S$ = A vertex covering of G .

Example: For the star graph with n vertices ($n \geq 2$).

$$\text{Solution: } \alpha_2 = 1$$

$$\beta_2 = n - 1$$

$$\alpha_2 + \beta_2 = n$$

Example: For the cycle graph C_n ($n \geq 3$)

$$\text{Solution: } \alpha_2 = \lceil n/2 \rceil$$

$$\beta_2 = \lfloor n/2 \rfloor$$

Example: Wheel graph W_n ($n \geq G$).

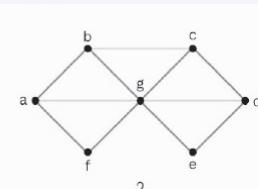
$$\text{Solution: } \alpha_2 = \left\lceil \frac{n+1}{2} \right\rceil$$

$$\beta_2 = \left\lfloor \frac{n-1}{2} \right\rfloor$$



Rack Your Brain

Find the chromatic number of the given graph.



Shortest path algorithms:

In order to find the shortest path between any two vertices in a graph, Dijkstra algorithm is used.

Dijkstra Algorithm

Dijkstra's algorithm finds the length of a shortest path between two vertices in a connected simple undirected weighted graph. (without negative weight cycle).

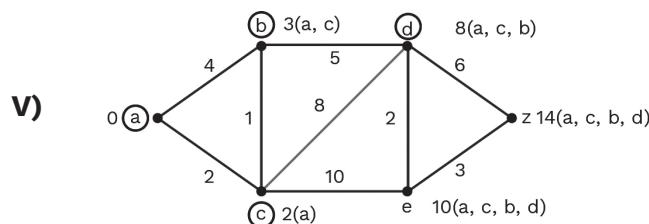
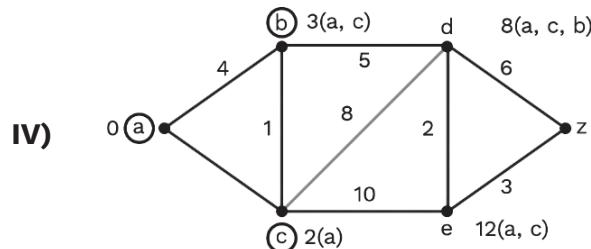
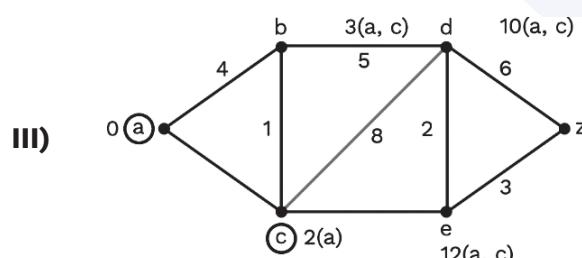
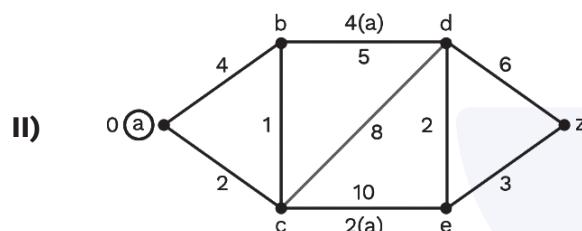
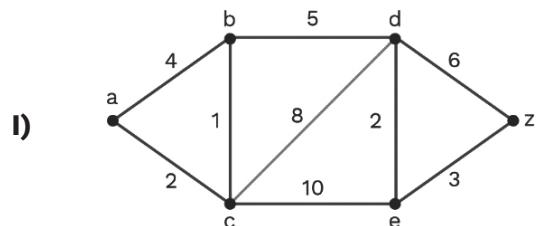
Dijkstra's algorithm uses $O(n^2)$ operations (additions and comparisons) to find the length of a shortest path between two vertices in a connected simple undirected weighted graph (without negative edge weight cycle) with n vertices.



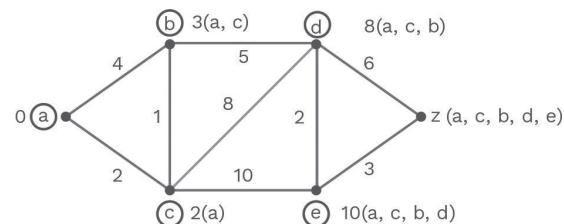
Solved Examples

- 14.** Use Dijkstra's algorithm to find the length of the shortest path between the vertices a and z in a weighted graph given below:

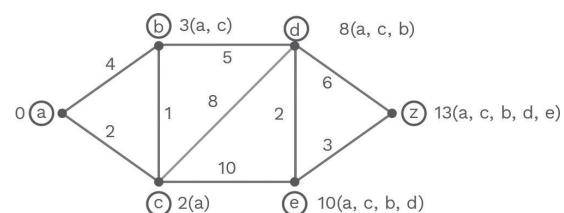
Solution:



VI)



VII)



The algorithm terminates at step (VII) when z is circled.

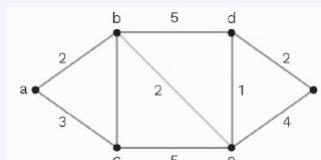
Therefore, the shortest path from a to z is a, c, b, d, e, z with length 13.

- The travelling salesman problem requires a circuit in a weighted, complete, undirected graph that visits each vertex exactly once and returns to its starting place with the least total weight. Because each vertex is visited exactly once in the circuit, this is equal to requesting a Hamiltonian circuit with the lowest total weight in the whole graph.



Rack Your Brain

Find the shortest path between a and z in the given weighted graph.





Grey Matter Alert!

Floyd Warshell's Algorithm

This algorithm can also be used to find the length of the shortest path between all pairs of vertices in a weighted connected simple graph. However, this algorithm cannot be used to construct shortest paths.



Previous Years' Questions

Let $G = (V, E)$ be a weighted undirected graph and Let T be a Minimum Spanning Tree (MST) of G maintained using adjacency Lists. Suppose a new weighed edge $(u, v) \in V \times V$ is added to G . The worst case time complexity of determining if T is still an MST of the resultant graph is:

[GATE CSE 2020]

- (A) $\Theta(|E| + |V|)$
- (B) $\Theta(|E| \cdot |V|)$
- (C) $\Theta(|E| \log |V|)$
- (D) $\Theta(|V|)$

Solution: (D)

Previous Years' Questions



Let G be a finite group on 84 elements. The size of a largest possible proper subgroup of G is _____. **[GATE CSE 2018]**

Solution: 42

Previous Years' Questions



Let G be an undirected complete graph on n vertices, where $n > 2$. Then, the number of different Hamiltonian cycles in G is equal to: **[GATE CSE 2019]**

- (A) $n!$
- (B) 1
- (C) $(n - 1)!$
- (D) $\frac{(n - 1)!}{2}$

Solution: (D)



Chapter Summary



- An undirected graph $G = (V, E)$ consists of V , a non-empty set of vertices (or nodes) and E , a set of edges, and every edge is associated with unordered pair of vertices.
- Types of graphs.

Types of Graphs	<ul style="list-style-type: none">→ Null→ Trivial→ Non-directed→ Directed→ Connected→ Disconnected→ Regular→ Complete cycle→ Cyclic→ Acyclic→ Finite→ Infinite→ Bipartite→ Planar→ Simple→ Multi→ Pseudo→ Euler→ Hamiltonian
-----------------	--

- Adjacent vertices: If two vertices have an edge in between.
- Adjacent Edges: If two edges have common vertices in between.
- A vertex with 0 edges is called the isolated vertex.
- A vertex with one edge is called a pendant vertex.
- A complete graph is a simple graph with a maximum number of edges possible.

$$|E| \text{ in } K_n = \frac{n(n-1)}{2}$$

Graph	Multiple Edges	Loops
Simple	✗	✗
Multigraph	✓	✗
Pseudo graph	✓	✓



- If G is a simple graph $G \cup \bar{G} = K_n$
- Isomorphic graphs must have:
 - Same number of vertices.
 - Same number of edges.
 - Same degrees of corresponding vertices.
- If closed trail, every edge is coverable

↓

Euler circuit

↓

Euler graph

- If closed path, every vertex is coverable

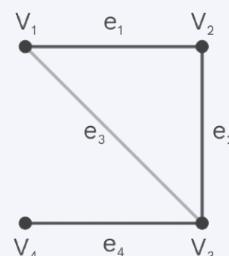
↓

Hamiltonian cycle

↓

Hamiltonian Graph

- K_5 and $K_{3,3}$ are known as Kuratowski's two graphs. These two graphs are special since, K_5 is a non-planar graph with minimum number of vertices and $K_{3,3}$ is the non-planar graph with minimum number of edges.
- Every tree with 2 or more vertices is 2-chromatic.
- Every bipartite graph is 2 colourable and vice versa.



- Cut vertex: V_3
- Bridge: e_4
- Vertex Cut Set: $\{V_3\}, \{V_3, V_1\}, \{V_3, V_2\}$
- Edge Cut Set: $\{e_1, e_3\}, \{e_1, e_2\}, \{e_4\}, \{e_1, e_2, e_3, e_4\}$

4

Counting



Sum and Product Rule

Rule of sum:

If there are m choice for one event and n choices for another event, both can not occur at the same time, then their $m + n$ choices for one event.

If a sequence of tasks $T_1, T_2 \dots T_n$ can be done in W_1, W_2, \dots, W_n ways respectively (no tasks

can be performed simultaneously), then the number of ways to do one of these tasks is $W_1 + W_2 + \dots + W_n$

Note:

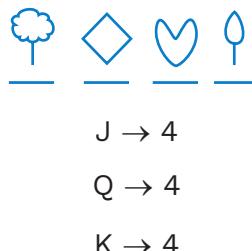
In the rule of addition, jobs are performed independently. In this case, we use the word 'or' between various jobs, and the meaning of 'or' is addition.

Solved Examples

1. In how many ways can we draw a face card from a deck?

Solution:

In a deck of 52 cards, there are 4 suits.



We want to draw a one-face card between all these no of choice = $4 + 4 + 4 = 12$

2. A pencil box contains 2 red and 3 black pens. Total number of ways for selecting 1 red pen and 1 black pen or 2 red pens.

Solution:

2 ways for selecting red pens because 2 pens are there.

3 ways for selecting black pens because 3 pens are there.

$$\therefore \text{Total ways for selecting 1 red and 1 black} \\ = 3 \times 2 = 6$$

$$\therefore \text{Number of ways of selecting 2 red pens} = 1$$

Total ways for selecting 1 red and 2 black or 2 red is $6 + 1$, i.e., 7 ways.

Rule of product:

If there are m choices for one event and n choices for another event, then there are $m \times n$ choices for both these events to occur.

If a sequence of tasks $T_1, T_2 \dots T_n$ can be done in W_1, W_2, \dots, W_n ways respectively (every task arrives after the occurrence of the previous task) then the number of ways to perform all the tasks is $W_1 \times W_2 \times \dots \times W_n$.

Note:

In the rule of multiplication, different jobs/operations are mutually inclusive, it implies that all jobs are being done in succession. In this case, we use word 'and' to complete all stages of operation, and the meaning of 'and' is multiplication.

3. Let us consider the following. Rahul has 3 pants and 2 shirts. How many different pairs of pants and a shirt, can he dress up with?

Solution:

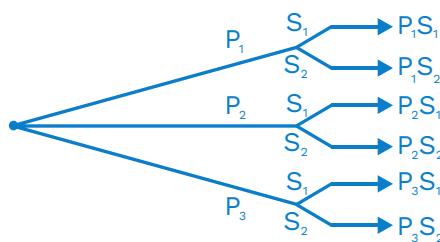
There are 3 ways in which a pant can be chosen (because 3, pants available) says P_1, P_2, P_3



Similarly, a shirt can be chosen in 2 ways. (Because 2 shirts available, say S_1, S_2).

For every choice of a pant, there are 2 choices of a shirt.

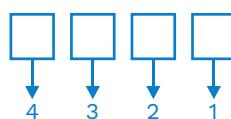
Therefore, there are $3 \times 2 = 6$ pairs of pants and shirts.



4. Find the number of 4 letter words with or without meaning possible, using the given set of 4 letters, here repetition of letters is not allowed.

Solution:

There are as many words as there are the way of filling in 4 vacant places by the 4 letters (repetition is not allowed).



First place can be filled in 4 different ways by any one of the four letters. Second place can be filled by anyone of the remaining 3 letters in 3 different ways, following third place can be 2 different ways.

Following 4 places can be filled in one way.

Thus, the no of ways in which the 4 places can be filled by the multiplication principle is $4 \times 3 \times 2 \times 1 = 24$

Note:

If the repetition of the letters was allowed in the above problem, one could easily understand that each of 4 vacant places can be filled in succession in 4 different ways. Hence the required number of words $= 4 \times 4 \times 4 \times 4 = 256$

5. If a die is cast and then a coin is tossed, find the number of all possible outcomes

Solution:

A die can fall in 6 different ways, i.e., 1, 2, 3, 4, 5, 6, and a coin can fall in 2 different ways, i.e., head or tail.

Number of possible outcomes from a die and a coin $= 6 \times 2 = 12$ ways.

6. There are 7 trains running between Delhi and Lucknow. In how many ways can a man go from Delhi to Lucknow and return by a different train?

Solution:

A man can go from Delhi to Lucknow in 7 ways (by anyone the 7 trains available).

He can return from Lucknow to Delhi in 6 ways by the remaining 6 trains (since, he cannot return by the same train by which he goes from to Lucknow to Delhi).

$$\begin{aligned} \text{Required number of ways} &= 7 \times 6 \\ &= 42 \end{aligned}$$

7. How many 3 digit numbers can be formed, whose unit digit is always zero and repetition of the digit is not allowed?

Solution:

Hundreds	Tens	Unit
↓	↓	↓
9	8	1

Since, zero is fixed for the unit digit place. So, only 9 digits are available for the hundreds place, and only 8 digits are available for the tens place out of 10 digits, i.e., 0, 1, 2, 3, ..., 9.

Therefore, required possible numbers $= 9 \times 8 \times 1 = 72$

Factorial:

Factorial of 'n' gives the product of all number the numbers between 1 to n.

$$n! = n(n - 1)(n - 2) \dots 3.2.1$$



Rack Your Brain

A GATE test paper consists of 65 questions and each question has 5 choices. If each question is necessarily attempted, then find the number of ways of answering the GATE test paper.

Permutation:

- The word permutation comes from the Latin words per + mutare that together mean “by change” or “through change”.
 - An arrangement of a set of objects is called a permutation.
 - In permutation orders matter.
 - Factorial plays an important part in determining the total permutation of a given set without repetitions.

$$n! = n(n - 1)(n - 2)\dots3.2.1$$

$n!$ represents the number of permutations of n different objects.

- The number of permutation, (arrangements) of n different things taking r at a time is considered as a partial permutation. It is written as n_{P_r} (“ n permute r ”)

$$^n P_r = p(n, r) = \frac{n!}{(n-r)!}$$

- Number of ways of arranging 'n' things in which q things are identical of one type and p things are identical of another type

$$= \frac{n!}{p!q!}$$
 - Total permutations of n distinct things round a close curve = $(n-1)!$ (if clock wise and anticlockwise arrangements are considered different)

$$= \frac{1}{2}(n-1)! \text{ (If clock wise and anticlockwise arrangement are considered identical)}$$

- Permutation of n different things taken all at a time = ${}^n p_n = n!$

- Permutation of n different things taken r at a time when a particular thing always occurs = $r^{*(n-1)}P_{(r-1)}$
 - Permutation of n different things taken r at a time when a particular thing never occurs = ${}^{(n-1)}P_r$

Permutation of n things not all different:

- Number of permutations of n things, taken all at a time, of which p are alike of one kind, q and alike of the second kind, r is alike of the third kind and rest are different = $\frac{n!}{p!q!r!}$
 - Number of permutations of n things of which P_1 are alike of one kind, P_2 are alike of second kind, P_3 are alike of third kind ... P_r are alike of r^{th} kind such that

$$P_1 + P_2 + P_3 \dots + P_r = n \text{ is } \frac{n!}{P_1! P_2! P_3! \dots P_r!}$$

- 8.** How many 4-digit even numbers are there (repetition is allowed)?

Solution:

↓ ↓ ↓ ↓

First place, one can fill in 9 ways (1 to 9) any value (Because zero cannot come at first position)

Second place, one can fill in 10 ways (0 to 9)
any value

Third place, one can fill in 10 ways (0 to 9)
any value

Fourth place, one can fill in 5 ways (0, 2, 4, 6, 8) any value

Using product rule = $9 \times 10 \times 10 \times 5 = 4500$

Previous Years' Questions

How many 4 digit even numbers have all 4 digits distinct?

Solution: (B)

[GATE 2001]



Combination:

- An unordered selection of objects is called a combination.
 - In combination arrangement of things doesn't matter until the specific thing is to be included.
 - The combination of three alphabets {a, b, c} taken two at a time are {a, b}, {a, c}, {b, c}, here {a, b} and {b, a} are not considered separately.
 - The word combination and selection are synonymous.



Rack Your Brain

How many ways 65 True/False questions can be answered if you can skip any of the questions?

- (A) ${}^{65}\text{P}_3$ (B) ${}^{65}\text{C}_3$
(C) 3^{65} (D) 65^3

The number of combinations of n distinct objects taken r at a time without repetition denoted by ${}^n\text{C}_r$ (read as n choose r).

$${}^nC_r = \frac{n(n-1)(n-2)\dots(n-(r-1))}{r(r-1)(r-2)\dots2\cdot1}$$

- $C(n, r) = {}^n C_r = \frac{n!}{r!(n-r)!}$

$$\bullet \quad {}^nC_r = \frac{{}^nP_r}{r!} = \frac{n!}{(n-r)!r!} = \frac{n!}{(n-r)!r!}$$

- Selecting r objects out of n is the same as selecting $(n-r)$ object out of n
{k-selection equal to k rejection}
 - Total selections that can be made from ' n '

distinct items are given $\sum_{k=0}^n {}^nC_k = 2^n$

$$\bullet \quad {}^nC_r = {}^{n-1}C_r + {}^{n-1}C_{r-1}$$

- Total ways of selecting one or more objects from n distinct objects

$$= 2^n - 1 = (^nC_1 + ^nC_2 + ^nC_3 + \dots + ^nC_n)$$

- $(x + y)^n = n_{C_0}x^{n-0}y^0 + n_{C_1}x^{n-1}y^1 + \dots + n_{C_n}x^{n-n}y^n$
 - $2^n = n_{C_0} + n_{C_1} + n_{C_2} + \dots + n_{C_n}$
 {Put $x = 1$ and $y = 1$ in above equation}
 - $(1 + x)^n = n_{C_0} + n_{C_1}x + n_{C_2}x^2 + \dots + n_{C_n}x^n$
 - $n \cdot 2^{n-1} = 1 \cdot n_{C_1} + 2 \cdot n_{C_2} + \dots + n \cdot n_{C_n}$
 {By differentiate above and put $x = 1$ }
 - $n_{C_0} + n_{C_1} + n_{C_2} + \dots + n_{C_3} + n_{C_4} + \dots = n_{C_1} + n_{C_2} + n_{C_3} + n_{C_4}$
 $+ \dots = \frac{2^n}{2} = 2^{n-1}$

Combination with repetition:

- The number of combinations of n objects taken r at a time with repetition.
 - The number of ways r identical objects can be distributed among n distinct boxes.
 - The number of non-negative Integral solution of the equation $x_1 + x_2 + x_3 + \dots + x_n = r$ where $x_1 \geq 0, x_2 \geq 0 \dots x_n \geq 0$
 - The solution of all the above statement is $\binom{n+r-1}{r}$

Properties of nC_r for simplification:

- ${}^nC_0 = 1, {}^nC_n = 1$
 - ${}^nC_r = {}^nC_{n-r}$
 - ${}^nC_r + {}^nC_{r-1} = {}^{n+1}C_r$
 - ${}^nC_r = {}^nC_k \Rightarrow r = k \quad \text{or} \quad r + k = n$
 - $r \cdot {}^nC_r = n \cdot {}^{n-1}C_{r-1}$
 - $\frac{1}{r+1} \cdot {}^nC_r = \frac{1}{n+1} \cdot {}^{n+1}C_{r+1}$

9. In how many ways can you distribute 10 similar balls into 3 distinct boxes.

(A) ${}^{12}C_{10}$
(B) ${}^{13}C_{10}$
(C) ${}^{12}C_2$
(D) ${}^{13}C_2$



Solution: (A), (C)

x_1	x_2	x_3
-------	-------	-------

Let x_1, x_2, x_3 are number of balls in box 1, box 2, box 3 respectively.

$$\text{So, } x_1 + x_2 + x_3 = 10 \quad [n = 3, r = 10]$$

$$\text{Using } n - 1 + {}^r C_r = 3 - 1 + {}^{10} C_{10} = {}^{12} C_{10} = {}^{12} C_2$$

Rack Your Brain

In how many ways of placing 20 similar balls into 4 boxes where each box is non empty?

Solved Examples

10. In how many ways you can place atmost 7 similar balls into 4 distinct boxes.

Solution:

Let x_1, x_2, x_3, x_4 are the number of balls in box 1, 2, 3, 4 respectively.

x_1	x_2	x_3	x_4
-------	-------	-------	-------

So, $x_1 + x_2 + x_3 + x_4 \leq 7$. $\forall x_i \geq 0$ here r value can be any of between 0 to 7.

$$\text{So, } = \sum_{r=0}^7 n - 1 + {}^r C_r \quad \{n = 4\}$$

$$\begin{aligned} &= \sum_{r=0}^7 3 + {}^r C_r \\ &= {}^3 C_0 + {}^4 C_1 + {}^5 C_2 + {}^6 C_3 + {}^7 C_4 + {}^8 C_5 + {}^9 C_6 + {}^{10} C_7 \\ &= 1 + 4 + 10 + 20 + 35 + 56 + 84 + 120 \\ &= 330 \end{aligned}$$

Note:

The above problem can also solve using taken $n = 5$ (one more box as dustbin) and r is 7 in formula ${}^{n-1+r} C_r$.

Dividing given into groups:

- The number of ways of dividing $(p + q)$ items, into two groups of p and q items, respectively is $\frac{(p+q)!}{p!q!}$
- The number of ways of dividing $2p$ items into two equal groups of p each is $\frac{(2p)!}{(p!)^2}$ where two groups have distinct identities.

- The number of ways of dividing $2p$ items into two equal groups of p each is $\frac{(2p)!}{2!(p!)^2}$, where the two groups do not have a distinct identities.
- The number of ways in which $(p + q + r)$ things can be divided into three groups containing p , q , and r things, respectively, is $\frac{(p+q+r)!}{p!q!r!}$

Difference between permutation and combination:

Permutation	Combination
Order is important	Order is not important
Arrangement	Selection
Keywords: password, number, word	Keywords: Sets, subset, team, committee

Derangement:

- Derangement is a permutational arrangement with no fixed points.
- Arrangement of elements in such a way that no is in its correct position. If n distinct items are arranged, the number of ways they can be arranged so that they do not occupy their intended spot is:

$$D_n = n! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots \frac{(-1)^n}{n!} \right)$$

$$D_n = \sum_{r=2}^n (-1)^r \frac{n!}{r!}$$



Properties of binomial coefficient:

- ${}^n C_r = {}^n C_{n-r}$ (symmetry)
- ${}^n C_r = {}^{n-1} C_r + {}^{n-1} C_{r-1}$ (Pascal identity)
- ${}^n C_r \times {}^r C_k = {}^n C_k \times {}^{n-k} C_{r-k}$ (Newton's identity)
- $\sum_{r=0}^n {}^n C_r = {}^n C_0 + {}^n C_1 + {}^n C_2 + \dots + {}^n C_n = 2^n$
(Row summation)
- $\sum_{r=0}^n (-1)^r {}^r C_r = {}^n C_0 - {}^n C_1 + {}^n C_2 - {}^n C_3 \dots = 0$
(Alternating sign row summation)
- ${}^r C_r + {}^{r+1} C_{r+1} + {}^{r+2} C_{r+2} + \dots + {}^n C_r = {}^{n+1} C_{r+1}$
(Column summation)
- $\sum_{K=0}^r {}^n C_K \cdot {}^m C_{r-K} = {}^n C_0 \cdot {}^m C_r + {}^n C_1 \cdot {}^m C_r$
 $-_1 + {}^n C_2 \cdot {}^m C_{r-2} + \dots + {}^n C_r \cdot {}^m C_0 = {}^{n+m} C_r$
(Vandemonde's identity)

Solved Examples

14. The coefficient of $a^4 b^5$ in the expansion of $(a + b)^9$ is _____.

Solution:

Coefficient of $a^4 b^5$ is

$$= \frac{9!}{4!5!} = \frac{9 \times 8 \times 7 \times 6 \times 5!}{4 \times 3 \times 2 \times 5!} = 126$$

15. The coefficient of $a^4 b^5$ in the expansion of $(2a - 3b)^9$ is _____.

Solution:

Coefficient of $a^4 b^5$ is

$$\begin{aligned} &= \frac{9!}{4!5!} (2)^4 \cdot (-3)^5 \\ &= 126 \times 16 \times (-243) \\ &= -489,888 \end{aligned}$$

Rack Your Brain

The coefficient of $\alpha^3 \beta^2 \gamma^1 \delta^4$ in the expansion of $(\alpha + 3\beta + 2\gamma - 7\delta)^{10}$ is _____.

Multinomial theorem:

The multinomial theorem describes how to expand the power of a sum in terms of the power of the terms in that sum. It is the generalisation of the binomial theorem from binomials to multinomials.

$$(x_1 + x_2 + \dots + x_t)^n = \sum_{n_1+n_2+\dots+n_t=n} \binom{n}{n_1, n_2, \dots, n_t} \cdot \prod_{m=1}^t x_m^{n_m}$$

where $\binom{n}{n_1, n_2, \dots, n_t} = \frac{n!}{n_1! n_2! \dots n_t!}$

Note:

The coefficient of $x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}$ in the expansion of $(x_1 + x_2 + \dots + x_t)^n$ where $n = n_1 + n_2 + \dots + n_t$ is $\frac{n!}{n_1! n_2! \dots n_t!}$.

Catalan numbers:

The n^{th} Catalan number is given directly in terms of binomial coefficients by

$$\frac{2n}{n+1} C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{2n!}{(n+1)! n!} = \prod_{k=2}^n \frac{n+k}{k} \quad \forall n \geq 0$$

The first Catalan number for $n = 0, 1, 2, 3, \dots$ are 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900 ...

Note:

The total number of the path without crossing the diagonal from $(0, 0)$ to (n, n) is:

$$C_n = \binom{2n}{n} - \binom{2n}{n+1}$$

$$C_n = \frac{1}{n+1} 2n C_n$$



Solved Examples

- 16.** In how many ways can we start from (0, 0) and go to (5, 5) without crossing the diagonal? (Assuming that you can move up or right).

Solution:

$$C_n = \frac{1}{n+1} {}^{2n}C_n$$

$$= \frac{1}{5+1} 2 \times 5 C_5$$

$$= \frac{1}{6} 10 C_5$$

$$= \frac{10!}{6 \cdot 5! 5!}$$

$$= 42$$

Application of catalan numbers:

There are number of applications which can be solved using Catalan numbers.

- Balanced parenthesis (form a valid group of parenthesis).

- Polygon triangulation (A convex polygon with $n + 2$ sides can be triangulated in C_n ways).
- If $2n$ people are seated around a circular table, the number of ways can all of them be simultaneously shaking hands with another person at the table in such a way that none of the arms crosses each other is C_n .
- Number of full binary trees with $n + 1$ leaves is C_n .

Generating function:

A generating function is a way of encoding an infinite sequence of numbers (a_n) by treating them as the coefficients of a formal power series. This series is called the generating function of the sequence.

Consider a sequence $(a_0, a_1, a_2, \dots, a_n, \dots)$ of real numbers then a function $f(x)$ is defined as $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$ is called generating function of the sequence.

$$f(x) = \sum_{r=0}^{\infty} a_r x^r$$

Solved Examples

- 17.** Find generating function for finite sequence:

$$a_0, a_1, a_2, a_3, a_4$$

Solution:

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$$

- 18.** Find generating function for the infinite sequence:

$$1, 1, 1, 1, \dots$$

Solution:

Generating function of 1, 1, 1, ...

$$= 1 + x + x^2 + x^3 + x^4 + \dots \underset{\infty}{\infty} = \frac{1}{1-x} \text{ (sum of infinite GP series } \frac{a}{1-x})$$

- 19.** Find the generating function for 1, 2, 3, 4

Solution:

$$f(x) = 1 + 2x + 3x^2 + 4x^3 + \dots$$

We know that,

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 \dots$$

Differentiate both side by $\frac{d}{dx}$

$$\frac{d}{dx} \left(\frac{1}{1-x} \right) = \frac{d}{dx} (1 + x + x^2 + x^3 + x^4 + \dots)$$

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



Rack Your Brain

Generating function for $1^2, 2^2, 3^2, 4^2 \dots$

Identities of generating functions:

$$1. (1+x)^n = 1 + {}^nC_1 x + {}^nC_2 x^2 + \dots {}^nC_n x^n = \sum_{r=0}^n {}^nC_r x^r$$

$$2. 1+x+x^2+\dots+x^{n-1} = \frac{1-x^n}{1-x}$$

$$3. 1+x+x^2+x^3+\dots = \sum_{r=0}^{\infty} x^r = \frac{1}{1-x}$$

$$4. \frac{1}{(1-x)^n} = \left(\frac{1}{1-x}\right)^n = \left(\sum_{r=0}^{\infty} x^r\right)^n = \sum_{r=0}^{\infty} n - 1 + {}^rC_r x^r$$

$$5. \frac{1}{(1-x)^2} = \sum_{r=0}^{\infty} {}^{(r+1)}C_r x^r = \sum_{r=0}^{\infty} (r+1)x^r$$

$$6. \frac{1}{(1-x)^3} = \sum_{r=0}^{\infty} \frac{(r+1)(r+2)}{2} x^r$$

$$7. \frac{1}{1+x} = \sum_{r=0}^{\infty} (-1)^r x^r$$

$$8. \frac{1}{1-ax} = \sum_{r=0}^{\infty} a^r x^r$$

$$9. \frac{x}{(1-x)^2} = \sum_{r=0}^{\infty} {}^{(r+1)}C_r x^{r+1} = \\ \therefore \sum_{r=0}^{\infty} (r+1)x^{r+1} = \sum_{k=1}^{\infty} Kx^K \text{ (if } r+1 = k)$$

$$10. \frac{x^2}{(1-x)^2} = \sum_{k=0}^{\infty} K \cdot x^{k+1}$$

20. Find coefficient of x^{12} in the expansion of $(x^2 + x^3 + x^4 + \dots)^2$

Solution:

To simplify the expansion. We extract x^2 coefficient of x^{12} in

\Rightarrow coefficient of x^{12} in $(x^2)^2 (1+x+x^2+\dots)^2$

$$\text{coefficient of } x^{12} \text{ in } x^4 \left(\frac{1}{1-x}\right)^2$$

$$\left\{ 1+x+x^2+x^3+\dots = \frac{1}{1-x} \right\}$$

coefficient of x^8 in the expansion of $\frac{1}{(1-x)^2}$

coefficient of x^8 in $\sum_{r=0}^{\infty} (r+1)x^r$ (put $r = 8$)

so coefficient of x^{12} in the $(x^2 + x^3 + x^4 + \dots)^2$ is $8 + 1 = 9$



Previous Years' Questions

Let $G(x) = \frac{1}{(1-x)^2} = \sum_{i=0}^{\infty} g(i)x^i$, where $|x| < 1$

what is $g(i)$.

- (A) i (B) $i + 1$
 (C) $2i$ (D) 2^i

Solution: (A)

[GATE 2005]



Rack Your Brain

Find coefficient of x^{12} in the expansion of $(x^3 + x^4 + x^5 + \dots)^2$ is _____.

The pigeonhole principle:

Principle 1:

If k is a positive integer and $k+1$ or more objects are placed into k boxes, then there is atleast one box containing two or more of the objects.



Previous Years' Questions



If the ordinary generating function of a sequence $\{a_n\}_{n=0}^{\infty}$ is $\frac{1+z}{(1-z)^3}$, then $a_3 - a_0$ is equal to _____.

Solution: 15

[GATE 2017]

Proof:

We use proof by contraposition. Suppose none of the boxes has more than one object. Then the total number of objects would be atmost K. This contradicts statements that we have K+1 objects.

Generalised pigeonhole principle:

If N objects are placed into k boxes. Then, there is atleast one box containing $\lceil \frac{N}{K} \rceil$ objects.

Theorem:

A function f from a set with K+1 elements to a set with K elements is not one-to-one.

Solved Examples

21. Owner of a house boys '3' distinct colours wall paints. He wants that in his house atleast 10 walls should be the same colour. For his desire to be full filled minimum, how many walls should be there in his house?

Solution:

By using pigeon-hole principle:

$$10 \geq \frac{n-1}{m} + 1 \quad | n = \text{no. of walls} \quad \begin{matrix} \text{ü} \\ \text{y} \\ \text{p} \end{matrix}$$

$$\hat{e} \quad \hat{u} \quad \hat{m} \quad \hat{u} \quad \hat{m} = \text{no. of distinct colours}$$

$$10 \geq \frac{n-1}{3} + 1$$

$$\hat{e} \quad \hat{u} \quad \hat{u}$$

$$N \geq 28$$

∴ Atleast 28 walls should be there for the desire of the landlord to be fulfilled.

Previous Years' Questions



Which one of the following is a closed form expression for the generating function of the sequence $\{a_n\}$, where $a_n = 2n + 3$ for all $n = 0, 1, 2, \dots$?

(A) $\frac{3}{(1-x)^2}$

(B) $\frac{3x}{(1-x)^2}$

(C) $\frac{2-x}{(1-x)^2}$

(D) $\frac{3-x}{(1-x)^2}$

Solution: (D)

[GATE 2018]

Proofs:

Use the pigeonhole principle

- Create a box for each element Y in the co-domain of f.
- Put in the box for Y all of the elements x in the domain such that $f(x) = Y$.
- Because there are K+1 elements and only K boxes, atleast one box has 2 or more elements.

Hence, f can not be one-to-one.

Application of pigeonhole principle:

- Number theory
- Economics
- Probability
- Finance
- Algorithms
- Computer science
- Mathematical analysis
- Computer programming
- Arithmetic
- Geometry



Rack Your Brain

If 100 cars are painted with 7 colours. Atleast how many cars painted with same colour?



Recurrence relation:

- Many counting problems cannot be solved easily; one such problem can be easily solved by a recurrence relation.
- A recurrence relation is a formula which relates a_n with one or more preceding terms (previous term) $a_{n-1}, a_{n-2} \dots$. Where a_0, a_1, a_2 be a sequence of real numbers.

Examples:

- For the arithmetic progression $\{a, a + d, a + 2d, \dots\}$, and d is a common difference.

The recurrence relation is

$$a_n = a_{n-1} + d \quad n \geq 1, a_0 = a$$

- For the geometric progression $\{a, ar, ar^2, ar^3 \dots\}$. The recurrence relation is

$$a_n = (a_{n-1}) \cdot r \quad n \geq 1, a_0 = a$$

- For the Fibonacci series $\{1, 1, 2, 3, 5, 8, 13, \dots\}$ The recurrence relations is

$$a_n = a_{n-1} + a_{n-2} \quad n \geq 2, a_0 = 1, a_1 = 1$$

Solved Examples

- 22.** The number of bacteria in a colony doubles every hour. If a colony begins with five bacteria, how many will be present in n hours?

Solution:

Let a_n be the number of bacteria at the end of n hours.

and a_{n-1} be the number of bacteria after $n - 1$ hours.

Since the number of bacteria doubles every hour.

Then the recurrence relation is:

$$a_n = 2a_{n-1} \quad \text{where } a_0 = 5.$$

Solution:

$$a_n = n \times a_{n-1}$$

Using substitution method

$$a_1 = 1 \cdot a_0 = 1(1) = 1! \quad \text{Put } (n = 1)$$

$$a_2 = 2 \cdot a_1 = 2(1!) = 2! \quad \text{Put } (n = 2)$$

$$a_3 = 3 \cdot a_2 = 3(2!) = 3! \quad \text{Put } (n = 3)$$

⋮

$$a_n = n!$$

Linear homogenous recurrence relation:

A linear recurrence relation of degree (order) k with constant coefficients is a recurrence relation of the form.

$$C_0 a_n + C_1 a_{n-1} + \dots + C_k a_{n-k} = f(n)$$

When $f(n) = 0$ then it homogenous linear recurrence relation and if $f(n) \neq 0$ then non homogenous linear recurrence relation.

Rack Your Brain



Write the recurrence relation of the binary string of length n which does not contain two consecutive zeros.

Types of recurrence relation:

There are two types of recurrence relation:

- Linear homogenous recurrence relation
- Non-linear homogenous recurrence relation

- 23.** What is the solution of the recurrence relation $a_n = n \times a_{n-1}$ where $a_0 = 1$?

Rack Your Brain



What is the solution of the recurrence relation $a_n = a_{n-1} + 3^{n-1}$ where $a_0 = 1$?



Characteristic equation for homogenous recurrence relation:

- If the roots are real and distinct

$$C_1 t_1^n + C_2 t_2^n + \dots + C_k t_k^n$$

- If the roots are real and equal (two roots are equal)

$$(C_1 + C_2 n) t_1^n + C_3 t_3^n + \dots + C_k t_k^n$$

- If all the roots are real and equal

$$(C_1 + C_2 n + C_3 n^2 + \dots + C_k n^k) t_1^n$$

- If roots are complex ($\alpha \pm i\beta$)

$$\gamma^n (C_1 \cos n\theta + C_2 \sin n\theta) \text{ where } \gamma = \sqrt{\alpha^2 + \beta^2} \\ \text{and } \theta = \tan^{-1}\left(\frac{\beta}{\alpha}\right)$$

- 23.** Solve the following linear homogenous recurrence relation by using characteristic root method.

$$a_n - 3a_{n-1} + 2a_{n-2} = 0$$

Solution:

Characteristic equation

$$C(t) = t^2 - 3t^1 + 2t^0 = 0$$

$$t^2 - 3t + 2 = 0$$

$$(t - 2)(t - 1) = 0$$

$$t = 2, 1$$

Since the roots are real and distinct.

$$\text{So, } a_n = C_1(2)^n + C_2(1)^n.$$



Rack Your Brain

Write the recurrence relation of binary string of length n . Which do not contain two consecutive zero.

Characteristic equation for non-homogenous linear recurrence relation ($f(n) \neq 0$):

- If $f(n) = C(b)^n$ and b is not root of $C(t)$

$$a_n = a_n H + a_n P \quad \text{where } a_n H \text{ is solution of homogenous linear recurrence relation and } a_n P \text{ is particular solution (depends on the form of } f(n)).$$

- $f(n) = C(b)^n$ and b is not root of $C(t)$

$$a_n P = D(b)^n$$

- $f(n) = C(b)^n$ and b is root of $C(t)$ of multiplicity m .

$$a_n P = Dn^m(b)^n$$

- 24.** Solve the following non-linear homogenous recurrence relation using characteristic method.

$$a_n - 3a_{n-1} = 7(2)^n$$

Solution:

$$a_n = a_n H + a_n P$$

$$a_n(H) = a_n - 3a_{n-1} = 0$$

$$C(t) = t - 3 = 0$$

$$t = 3$$

$$a_n(H) = C_1(3)^n$$

$$a_n(P) = f(n) = 7(2)^n \text{ and } 2 \text{ is not root of } C(t)$$

$$a_n(P) = D(2)^n$$

$$\text{Put this in } a_n - 3a_{n-1} = 7(2)^n$$

$$D(2)^n - 3D(2)^{n-1} = 7(2)^n$$

$$2^{n-1} [2D - 3D] = 7(2)^n$$

$$-D = 7 \times 2$$

$$D = -14$$

$$a_n(P) = -14(2)^n$$

$$a_n = a_n H + a_n P$$

$$a_n = C_1(3)^n - 14(2)^n$$



Chapter Summary



	With no Repetition	With Unlimited Repetition	With Limited Repetition
Permutation	n_{P_r}	n^r	$\frac{n!}{n_1! \cdot n_2! \dots}$
Combination	${}^n C_r$	${}^{n-1+r} C_r$	Generating function

- The number of combinations (selections) of n different things taking r at a time is considered as a combination. It is written as ${}^n C_r$ (n choose r)

$$C(n, r) = {}^n C_r = \frac{n!}{r!(n-r)!}$$

- Selecting r objects out of n is the same as selecting $(n-r)$ object out of n

$${}^n C_r = {}^n C_{c-r}$$

{k-selection equal to k rejection}

- Total selections that can be made from ' n ' distinct items is given $\sum_{k=0}^n {}^n C_k = 2^n$
- ${}^n C_r = {}^{n-1} C_r + {}^{n-1} C_{r-1}$
- The total number of selections of one or more objects from n different objects
 $= 2^n - 1 = ({}^n C_1 + {}^n C_2 + {}^n C_3 + \dots + {}^n C_n)$
- Total ways to select any number of items from n identical items
 $= n + 1$ (when selection of 0 things is allowed)
 $= n$ (when at least one thing is to be selected)
- The total number of selections from p like things, q like things of another type, and r distinct things
 $= (p+1)(q+1)2^r - 1$ (if at least one thing is to be selected)
 $= (p+1)(q+1)2^r - 2$ (if none or all cannot be selected)
- The total number of selections of r things from n different things when each thing can be repeated an unlimited number of times $= {}^{n-1+r} C_r$.
- Derangement is an arrangement such that no item should be there in its correct position

$$D_n = \sum_{r=2}^n (-1)^r \frac{n!}{r!}$$

- The coefficient of $x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}$ in the expansion of $(x_1 + x_2 + \dots + x_t)^n$

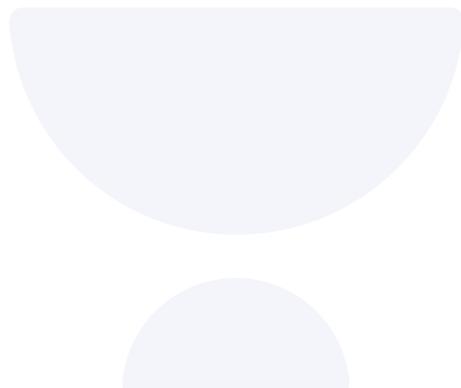
where $n = n_1 + n_2 + \dots + n_t$ is $\frac{n!}{n_1! n_2! \dots n_t!}$

- The number of shortest paths from point (i, j) to a point (p, q) is $(p+q-i-j) {}_{C_{p-i}}$



Inclusion-exclusion principle:

- $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
- $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$
- $n(A \oplus B) = n(A) - n(A \cap B)$
- $n(A - B) = n(A) - n(A \cap B)$
- $n(B - A) = n(B) - n(A \cap B)$
- $n(\bar{A} \cap \bar{B}) = n(\cup) - n(A \cup B)$
- $n(\bar{A} \cup \bar{B}) = n(\cup) - n(A \cap B)$



5

Group Theory



Closure

A non-empty set G with operation $*$ is said to be closed if $\forall a, b \in G, a * b \in G$

Example:

1. $(N, +)$, Natural number is closed with respect to addition since
 $\forall a, b \in N, a + b \in N$
2. (N, \times) Natural number is closed with respect to multiplication since
 $\forall a, b \in N, a \times b \in N$
3. $(N, -)$ Natural number is not closed with respect to subtraction since
 $\forall a, b \in N, a - b \notin N$ for e.g. $3 \in N$, and $4 \in N$ but $3 - 4 = -1 \notin N$.
4. Set of integers z is closed with respect to $(+, \times, -)$.



Rack Your Brain

Is set of non-zero rational number Q_0 is closed with respect to $\{+, -\}$.

1. Which of the following satisfies closure property.
(A) $a * b = a * b - 2020 \quad \forall a, b \in z$
(B) $a * b = a + b - 2020 \quad \forall a, b \in N$
(C) $a * b = a + b + 2021 \quad \forall a, b \in N$
(D) $a * b = a^b \quad \forall a, b \in N$

Solution: (A), (C), (D)

- $\forall a, b \in z, a * b - 2020 \in z$ so closed.
- $\forall a, b \in N, a + b - 2020 \notin N$ so not closed.
E.g. $a = 1 \in N, b = 2 \in N$. So, $1 + 2 - 2020 = -2017 \notin N$.
- $\forall a, b \in N, a + b + 2021 \in N$ so closed.
- $\forall a, b \in N, a^b \in N$ so closed.

Rack Your Brain



Check whether the following operations are closed or not.

1. $a * b = a^b \forall a, b \in Q$
2. $a * b = a^b \forall a, b \in z$

Note:

1. Set of vectors V is closed with respect to vector addition and cross product, but not with respect to the dot product.
2. Power set of a set A , i.e., $P(A)$, is closed with respect to union, intersection and symmetric difference.

Binary operation:

- An operation $*$ is said to be a binary operation on set G if $a * b \in G, \forall a, b \in G$.
- A function $f: G \times G \rightarrow G$ is said to be a binary operation, where $G \times G = \{a, b | a \in G \text{ and } b \in G\}$.

Algebraic structure:

- A non-empty set G along with one or more binary operations is called algebraic structure or algebraic system.
- If $*$ is a binary operation, then $(G, *)$ is said to be an algebraic structure.

Examples:

1. Set of natural numbers (N) with respect to addition is an algebraic structure $(N, +)$.
2. $(N, +, \times)$ is also an algebraic structure.
3. $(Z, +, -, \times)$ is also an algebraic structure, where Z is a set of integers.

**Note:**

A non-empty set G is called an algebraic structure with respect to operation $*$ if $(a * b) \in G \forall a, b \in G$ is satisfied closure property.

Groupoid or quasi group:

A non-empty set $(G, *)$ is said to be groupoid if it satisfies the closure property.

Example: $(N, +)$ is a groupoid.

Note:

An algebraic structure is also a groupoid.

Associative: A non-empty set G is associative with respect to $*$ if.

$$a * (b * c) = (a * b) * c \quad \forall a, b, c \in G.$$

Example: $(N, +)$ satisfies associative property.

Semigroup: A non-empty set G is said to be semigroup with respect to $*$ if it satisfies.

1. Closure property
2. Associative property

Rack Your Brain

Is $(N, -)$ is a semigroup?

Example: $(N, +)$ is semigroup because

1. $\forall a, b \in N, a + b \in N$ so closure
2. $\forall a, b, c \in N, a + (b + c) = (a + b) + c$

Note:

- An algebraic structure $(G, *)$ is a semigroup if it satisfies the associative property.
- Every semigroup is a groupoid, but the converse need not be true.

Identity element : A non-empty set G with $*$ is a binary operation. If for every $a \in G$, there exist an element $e \in G$ such that -

$a * e = e * a = a$, then e is called the identity element in $(G, *)$.

- If $a * e = a$, then e is called the right identity.
- If $e * a = a$, then e is called left identity.
- ' e ' is called an identity element if both left and right identity exists.

2. Find identity element in $a * b = \frac{ab}{10} \quad \forall a, b \in R_0$, where R_0 is a non-zero real number.

Solution:

Since $\forall a, b \in R, a * b = \frac{ab}{10} \in R$, So closure or $*$, is a binary operation.

Let e be the identity element.

$$a * e = e * a = a$$

Take right identity

$$a * e = a$$

$$\frac{ae}{10} = a$$

$$e = 10 \in R$$

Take left identity

$$e * a = a$$

$$\frac{ea}{10} = a$$

$$e = 10 \in R$$

Both left and right identity exists, and belong to the given domain (i.e., non-zero real number), so identity is 10.

**Rack Your Brain**

Find identity element in $a * b = a^b \quad \forall a, b \in N$, where N is natural number.

Hint: (Only the right identity exists).

Monoid: A non-empty set G with operation $*$, is said to be monoid if it satisfies.

1. Closure
2. Associative
3. Identity

**Rack Your Brain**

Is $(N, +)$ is a monoid?

Example: $(z, +)$ is a monoid, where z is set of integers since,



1. $\forall a, b \in z, a + b \in z$ so closure.
2. $\forall a, b, c \in z, a + (b + c) = (a + b) + c$ so associative.
3. $\exists e \in G, \forall a \in G, a * e = e * a = a$
 $a + 0 = 0 + a = a$. So $0 \in z$ is an identity.
So, $(z, +)$ is a monoid.

Note:

- An algebraic structure $(G, *)$ is a monoid if it satisfied associative and identity properties.
- An semigroup $(G, *)$ is a monoid if it satisfies identity properties.
- G is a non-empty set, and $*$ is an operation is called a loop if it satisfies closure and identity properties.
- Every monoid is a loop, but the converse need not be true.

Inverse property:

A non-empty set G with binary operation $*$, $\forall a \in G \exists b \in G$. Such that $a * b = b * a = e$, where e is an identity element in G , then b is the inverse of a .

- If $a * b = e$, then b is called the right inverse of a .
- If $b * a = e$, then b is called the left inverse of a .

3. Find inverse in $a * b = \frac{ab}{10} \forall a, b \in R_0$ (R_0 is a non-zero Real number).

Solution:

Since, identity $e = 10$ (calculated in identity example)

Let b is the inverse of a , i.e.

Let right inverse $a * b = b * a = e$

$$\begin{array}{l|l} a * b = e & b * a = e \text{ (left inverse)} \\ \hline \frac{ab}{10} = 10 & \frac{ba}{10} = 10 \\ ab = 100 & ba = 100 \\ b = \frac{100}{a} \in R_0 & b = \frac{100}{a} \in R_0 \\ b = \frac{100}{a} \text{ is inverse of } a. & \end{array}$$

Verification of inverse in the above problem:

$$\begin{aligned} a * b &= e \\ a * \frac{100}{a} &= 10 \\ a \cdot \frac{100}{a} &= 10 \\ 10 &= 10 \end{aligned}$$

**Rack Your Brain**

Find inverse in $a * b = a + b - ab \forall a, b \in Q - \{-1\}$. Where Q is a rational number?

Group: A non-empty set G with operation $*$, is said to be group if it satisfies.

- (A) Closure (B) Associative
(C) Identity (D) Inverse

Example: $(z, +)$ is not only monoid, but also a group. Since $\forall a \in G \exists b \in G$ such that

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

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

**Rack Your Brain**

Is (Z, x) is a group?

So the inverse of a is $(-a)$; therefore, $(z, +)$ is a group.

Note:

- A monoid $(G, *)$ is a group if it satisfies the inverse property.
- Every group is a monoid, semigroup, and groupoid, but the converse need not be true.

Commutative property: A non-empty set G with respect to the operation $*$ is said to be commutative.

$$\text{If } \forall a, b \in G \quad a * b = b * a$$



Example: $(\mathbb{N}, +)$ is commutative.



Rack Your Brain

Is (\mathbb{Z}, \times) an abelian group?

Abelian group: A group $(G, *)$ is said to be the Abelian group if it satisfies the commutative property.

Example: $(\mathbb{Z}, +)$ is not only a group, but also an abelian group since $\forall a, b \in \mathbb{Z} a + b = b + a$.

So it is commutative; hence $(\mathbb{Z}, +)$ is abelian.

Previous Years' Questions



Consider the set Σ^* of all strings over the alphabet $\Sigma = \{0, 1\}$. Σ^* with the concatenation operator for strings

[GATE CS 2003]

- (A) Does not form a group
- (B) Forms a non-commutative group
- (C) Does not have a right identity element
- (D) Forms a group if the empty string is removed from Σ^*

Solution: (A)

Previous Years' Questions



Let A be the set of all non-singular matrices over the real number, and let $*$ be the matrix multiplication operation. Then

- (A) A is closed under $*$, but $(A, *)$ is not a semigroup
- (B) $(A, *)$ is a semigroup but not a monoid
- (C) $(A, *)$ is a monoid but not a group
- (D) $(A, *)$ is a group but not an abelian group

Solution: (D)

Previous Years' Questions



Some group (G, o) is known to be abelian. Then, which one of the following is true for G ?

- (A) $g = g^{-1}$ for every $g \in G$
- (B) $g = g^2$ for every $g \in G$
- (C) $(goh)^2 = g^2oh^2$ for every $g, h \in G$
- (D) G is of finite order

Solution: (C)

Types of groups:

Group can be divided into two types.

1. Finite group
2. Infinite group

Finite and infinite group:

In a group G , if the number of elements is finite, the group is called finite; otherwise infinite group.

Order of group:

- The number of elements in a finite group is called the order of the group. It is represented by $|G|$ or $O(G)$.

Example: $G = \{1, -1\}$ is a group with respect to multiplication and $O(G) = 2$.

- An infinite group has infinite order.

Example: $(\mathbb{Z}, +)$ is an infinite group and $O(\mathbb{Z}) = \infty$.

Properties of a Group:

Let $(G, *)$ is a group, then

1. In a group, the identity element is unique.
2. The inverse of every element in a group is unique.
3. In a group, the Identity element has its own inverse.
4. In a group, $\forall a \in G (a^{-1})^{-1} = a$ (i.e., The inverse of an element is equal to the element).
5. The inverse of the product of two elements of a group G is the product of the inverse in reverse order, $\forall a, b \in G (ab)^{-1} = b^{-1} a^{-1}$.



6. In a group, if every element has its own inverse, then it is an abelian group, but the converse need not be true.
7. In a group G with multiplicative operation $\forall a \in G, a^2 = e$ where e is the identity in G , then G is called an abelian group.
8. In an abelian group of odd order with respect to multiplication, the product of all elements in a group must be an identity element.
9. In an abelian group of odd order with respect to addition, the sum of all elements in a group G is an identity element.
10. Every group of prime order is always abelian.

Solved Examples

1. Consider the set $G = \{0, 1, 2\}$ under addition modulo 3. Is G an abelian group?

Solution:

$$G = \{0, 1, 2\}_{+3}$$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(Composition table)

- Since all the elements of the composition table belong to a given set, therefore closed.
- $(0 +_3 1) +_3 2 = 0 +_3 (1 +_3 2)$, so associative.
- In the composition table, the first-row element appearing against 0 is called the identity element.
- $(0)^{-1} = 0 \quad (1)^{-1} = 2 \quad (2)^{-1} = 1$, every element has a unique inverse.

So, G is a group.

Since in the composition table, the corresponding row, and corresponding column (1st row, 1st column, 2nd row, 2nd column, 3rd row, 3rd column) are the same, then it is abelian.

Note:

$\mathbb{Z}_m = G = \{0, 1, 2, 3, \dots, (m-1)\}_{+m}$ is a finite abelian group of order m .

11. Every group of the order less than 6 is always abelian (The smallest non-abelian group is of order 6).

Addition Modulo m:

Let $a, b \in \mathbb{Z}$, and m is a fixed positive integer, r is a non-negative remainder then addition module m of (a, b) is denoted by $a +_m b$, and it can be defined as $a +_m b = r$, where $0 \leq r < m$, r is a remainder obtained by dividing $a + b$ with m .

Example: $3 +_2 4 = 1$

$$3 +_2 (-4) = 1$$



Rack Your Brain

Find the inverse of 2007 in the following group $\{0, 1, 2, \dots, 2021\}$ with respect to addition modulo 2022.

Multiplication modulo:

Let $a, b \in \mathbb{Z}$, and m is a fixed positive integer, r is a non-negative remainder then multiplication module m of (a, b) is denoted by $a \times_m b$, and it can be defined as $a \times_m b = r$, where $0 \leq r < m$, r is a remainder obtained by dividing $a \times b$ with m .

Example: $2 \times_3 4 = 2$

2. Consider the set $G = \{1, 2, 3, 4\}$ under multiplication modulo 5. Is G is an abelian group?

Solution:

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(Composition table)



- Since all the elements of the composition table belong to a given set, therefore closed.
- $(1 \times_5 2) \times_5 3 = 1 \times_5 (2 \times_5 3)$, so associative.
- In the composition table, the first-row element appearing against 1, is called the identity element.
- Every element has a unique inverse.
 $(1)^{-1} = 1, (2)^{-1} = 3, (3)^{-1} = 2, (4)^{-1} = 4$

So, G is a group.

Since in the composition table, corresponding row and column are the same, so it is an abelian group.

Note:

$\mathbb{Z}_p = G = \{1, 2, 3 \dots (p-1)_{x_p}\}$ is an abelian group of order $(p-1)$, where p is a prime number.

Previous Years' Questions



The set $\{1, 2, 4, 7, 8, 11, 13, 14\}$ is a group under multiplication modulo 15. The inverses of 4 and 7 are respectively

[GATE CS 2005]

- (A) 3 and 13
(B) 2 and 11
(C) 4 and 13
(D) 8 and 14

Solution: (C)

Cayley table:

- Let $(G, *)$ is a group, and the Cayley table of G is a table with rows and columns label led by the elements of the group.
- The binary operation table for a finite group is called the Cayley table.

Example: $G = \{1, -1\}$ is form a group with respect to multiplication.

\times	1	-1
1	1	-1
-1	-1	1

Properties of Cayley table:

1. All the entries of the Cayley table should belong to the given set otherwise the operation is not closed.

2. There should be one row in which the column label appears in order, indicating the presence of an identity element. (The column of this element should reflect the row labels); otherwise, there is no identity.
3. The identity element of the group should not only appear in every row and column (exactly once), but it should be distributed symmetrically about the main diagonal. Otherwise, one or more elements in the table do not have an inverse.
4. Every row and column of the table should contain each element exactly once.
5. If the Cayley table is symmetric along its diagonal, then the group is abelian group.

Examples of group's:

1. $G = \{0\}$ is a group with respect to '+', '-' and 'x'.

$+$	0
0	0

$-$	0
0	0

\times	0
0	0

It is also an abelian group with 0 as identity, and each element has its own inverse.

2. $G = \{1, -1\}$ is a group with respect to 'x' and ' \div '.

\times	1	-1
1	1	-1
-1	-1	+1

\div	1	-1
1	1	-1
-1	-1	1

$(G, X), (G, \div)$ is an abelian group with 1 as the identity, and each element has its own inverse.

3. $G = \{1, \omega, \omega^2\}$ is a group with respect to multiplication where $\omega^3 = 1$ (3^{rd} root of unity)

\times	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(G, \times) is an abelian group with 1 is the identity and $(1)^{-1} = 1, (\omega)^{-1} = \omega^2, (\omega^2)^{-1} = \omega$



Note:

If w represents the n^{th} root of unity, i.e., $\omega^n = 1$, then the inverse of any element can be calculated $(\omega^r)^{-1} = \omega^{n-r}$.

4. $G = \{1, -1, i, -i\}$ is a group with respect to multiplication where $i^2 = -1$

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(G, \times) is an abelian group with 1 as the identity and $(1)^{-1} = 1$, $(-1)^{-1} = -1$, $(i)^{-1} = -i$, $(-i)^{-1} = i$

Infinite order group:

1. $(z, +)$, $(2z, +)$, $(3z, +)$... $(nz, +)$ are an infinite abelian groups, where 0 is the identity.
2. $(Q, +)$, (Q_0, \times) , (Q^+, \times) are an infinite abelian group.
3. $(R, +)$, (R_0, \times) , (R^+, \times) are an infinite abelian group.
4. $(C, +)$, (C_0, \times) are an infinite abelian group.
5. The set of all matrices of order $n \times n$ whose elements are rational (or) real or complex forms an infinite abelian group with respect to matrix addition.
6. The set of all non-singular matrices whose elements are rational, real, or complex. Forms an infinite non-abelian with respect to matrix multiplication.
7. $G = \left\{ A_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \mid (\alpha \in z) \right\}$ is an infinite abelian group with respect to the matrix multiplication.
8. $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \text{ and } ad - bc = 1 \right\}$ forms an infinite non abelian group.
9. $G = \{ \cos \theta + i \sin \theta \mid \theta \in z \text{ or } \theta \in R, \text{ or } \theta \in Q \}$ forms an infinite abelian group with respect to multiplication.
10. Let 's' be a non-empty set, then $G = \{f \mid f : s \rightarrow s \text{ is a bijection}\}$ forms a group with respect to the composition mapping.

Order of an element in a group:

Let G is a group. The order of an element $a \in G$ defined as the least positive integer 'n' such that $a^n = e$, where e is the identity element.

Here a^n means n times operation on a (if the operation is addition, it means adding a , n times).

Example: Find the order of every element in the group $G = \{1, \omega, \omega^2\}$ with respect to multiplication where $\omega^3 = 1$.

Solution: In a group $(1, \omega, \omega^2)$, the identity element is 1.

$$O(1) = (1)^1 = 1$$

$$O(\omega) = (\omega)^3 = 1$$

$$O(\omega^2) = (\omega^2)^3 = 3$$



Rack Your Brain

Find the order of every element in the group G

$$G = \{0, 1, 2, 3, 4\}_{+5}$$

Properties of order of an element in a group:

- Every element of a finite group has a finite order that is less than or equal to the group's order.
- An element of a group has the same order as its inverse.
- The order of identity elements in a group is always 1.
- In a group, if the order of every element is '2' except the identity element, then the group is abelian.



Rack Your Brain

If a is an element in a group G such that $O(a) = 6$, then find the value of a^{2022} .



Cyclic Group's:

- A group $(G, *)$ is called a cyclic group if, there exists an element $g \in G$ such that every element of G , can be written as g^n for some integer n (so, g is a generator of group G .)
- An element $g \in G$ such that $O(g) = O(G)$, then g is called the generator of the group and it is represented by $\langle g \rangle$.
- A group having atleast one generator is called a cyclic group.

Example: $G = (\{1, -1, i, -i\}, \times)$ is a cyclic group generated by $\langle i \rangle$.

$$(i)^1 = i \quad (-i)^1 = -i$$

$$(i)^2 = -1 \quad (-i)^2 = -1$$

$$(i)^3 = i^2 \times i = -1 \times i = -i \quad (-i)^3 = i$$

$$(i)^4 = i^2 \times i^2 = -1 \times -1 = 1 \quad (-i)^4 = 1$$

Solution:

Here, $i, -i$ can generate all the elements of the given group, so $\langle i \rangle, \langle -i \rangle$ are generators.



Rack Your Brain

In the above problem $O(i) = O(-i) = O(G) = 4$ so you can also say $\langle i \rangle, \langle -i \rangle$ are generators and as the group has at least one generator so, it is called cyclic group.



Rack Your Brain

Whether the given group $G = \{0, 1, 2, 3\}_{+4}$ is a cyclic group or not?

Properties of cyclic group

1. Every cyclic group is also an abelian group.
2. If a is a generator of cyclic group G , then a^{-1} is also a generator of G .
3. The order of a cyclic group, as well as its generator, should be the same.

4. Every group of prime order is always cyclic.
5. If a group is cyclic, then every subgroup of that group is also cyclic.
6. If G is a cyclic group with an order n and generator g . If $m < n$, then the order of the element g^m is described by $|g^m| = \frac{n}{\gcd(m, n)}$.

Finding number of generators in cyclic group:

Let $(G, *)$ be a cyclic group of order n with generator 'a' then

- The number of generators in $G = \phi(n)$ (Euler totient function where $\phi(n)$ is the cardinality of numbers from 1 to n , which are relatively prime to n .)

Example: If n is 7 then $\phi(n) = 6$, because relative prime numbers are $\{1, 2, 3, 4, 5, 6\}$, it means if the given number is prime, let's say p , then it's a relative prime number is always $p-1$.

- a^m is also a generator of G if $\gcd(m, n) = 1$.

Example: Find the number of generators of a cyclic group of order 77.

Solution: The number of numbers from 1 to n , which are relatively prime to

$$77 = \phi(77) = \phi(7) \times \phi(11) = 6 \times 10 = 60$$

So the number of generators of a cyclic group is exactly 60.

Note:

If $\phi(n)$, if n is written into its prime factors as $n = p_1^{n_1} \cdot p_2^{n_2} \dots$ where p_1, p_2 are prime numbers, then

$$\phi(p^n) = p^n - p^{n-1}$$

For example,

$$\phi(7^1) = 7^1 - 7^{1-1} = 7 - 7^0 = 7 - 1 = 6$$

$$\phi(5^2) = 5^2 - 5^{2-1} = 25 - 5 = 20$$

Subgroup:

Let $(G, *)$ is a group, A non-empty subset H of G is said to be a subgroup if:

1. $a \in H, b \in H \Rightarrow a * b \in H$ (satisfies closure)
2. $a * (b * c) = a * (b * c) \forall a, b, c \in H$. (Associative)
3. $\exists e \in H \text{ } a * e = e * a = a \forall a \in H$ (Existence of identity)



4. $\forall a \in H \exists b \in H a * b = b * a = e$, b is the inverse of a .

In other words, $(H, *)$ is a subgroup of $(G, *)$ if $H \subseteq G$ and $(H, *)$ is itself a group.

Example: Let $G = \{1, -1, i, -i\}$ is a group with multiplication, which of the following is a subgroup with respect to the given group.

1. $\{1, i\}$
2. $\{1, -i\}$
3. $\{1, -1\}$
4. $\{1\}$

Solution:

$(H, *)$ is a subgroup of $(G, *)$ if

1. $H \subseteq G$
2. H itself is a group

Option:

1. $H = \{1, i\}$, $H \subseteq G$, but H is not a group with respect to ' $*$ ' because it is not closed ($-1 \notin H$). So not a subgroup.
2. $H = \{1, -i\}$, $H \subseteq G$, but H is not a group with respect to ' $*$ ', because it is not closed ($-1 \notin H$), so not a subgroup.
3. $H = \{1, -1\}$, $H \subseteq G$ and H is also a group with respect to ' $*$ ' so subgroup.
4. $H = \{1\}$, $H \subseteq G$ and H is also a group with respect to ' $*$ '.

Note:

For any group $(G, *)$, the identity element $(\{e\}, *)$ and the group itself are called trivial subgroups, and other subgroups (if any) are called proper subgroups. In above example the group itself i.e. $G = (\{1, -1, i, -i\}, *)$ and the identity element $(\{1\}, *)$ are trivial subgroups and $(\{1, -1\}, *)$ is a proper subgroup.

- If G is a group of prime order, then G has only two subgroups, and those are trivial subgroups.
- The identity of the subgroup is the same as that of the group.

Lagrange's theorem:

The order of each subgroup of a finite group is the divisor of the group. ($O(H)$ divides $O(G)$).

Note:

Converse of Lagrange's theorem need not be true.

Example: Find all subgroups of group $G = \{0, 1, 2, 3, \dots, 11\}_{+12}$

$$\begin{aligned}H_1 &= \{0\}_{+12} \\H_2 &= \{0, 2, 4, 6, 8, 10\}_{+12} \\H_3 &= \{0, 3, 6, 9\}_{+12} \\H_4 &= \{0, 4, 8\}_{+12} \\H_5 &= \{0, 6\}_{+12} \\H_6 &= G\end{aligned}$$

Since the order of each subgroup divides the order of the group. So it satisfies Lagrange's theorem. But if we take one set $H = \{0, 3\}_{+12}$ of the given group $G = \{0, 1, 2, 3, \dots, 11\}_{+12}$, here also $O(H)$ i.e. 2 divides $O(G)$ i.e. 12, but $H = \{0, 3\}$ is not a subgroup (since it is not closed). So the converse of Lagrange's theorem need not be true.

Previous Years' Questions

Let G be a group of 35 elements. Then the largest possible size of a subgroup of G other than G itself is _____.

Note: This question was numerical type.

- | | |
|-------|--------|
| (A) 1 | (B) 5 |
| (C) 7 | (D) 35 |

Solution: (C) [GATE CS 2020]

Previous Years' Questions

Let G be a group of order 6, and H be a subgroup of G such that 1

- (A) Both G and H are always cyclic
- (B) G may not be cyclic, but H is always cyclic
- (C) G is always cyclic, but H may not be cyclic
- (D) Both G and H may not be cyclic

Solution: (B) [GATE CS 2021]



Properties of subgroup:

1. A non-empty subset 'H' of a group (G, \circ) is a subgroup of G if and only if
 - a) $a, b \in H, \forall a \in H, b \in H$
 - b) $a^{-1} \in H, \forall a \in H$
 2. A non-empty subset (H) of a group $(G, +)$ is said to be subgroup if and only if
 - a) $a + b \in H, \forall a \in H, b \in H$
 - b) $-a \in H, \forall a \in H$
 3. A non-empty subset H of a group (G, \circ) is a subgroup if and only if $ab^{-1} \in H \forall a \in H, b \in H$
 4. If H is a subgroup of G, then $H^{-1} = H$, but the converse need not be true i.e. if $H = H^{-1}$, H may not be a subgroup.
5. If H is any subgroup of G, then $H \cdot H = H$, but the converse need not be true.
 6. If H and K are two subgroups of G, then $H(K)$ is a subgroup of G if $HK = KH$.
 7. The intersection (\cap) of any two subgroups of a group G is a subgroup.
 8. The union (\cup) of two subgroups of a group G need not be a subgroup.
 9. Union of two subgroup, H, K is again a subgroup if and only if one contains the other, i.e., $H \subseteq K$ or $K \subseteq H$.

Chapter Summary



- An non-empty set G with operation * satisfies:
Closure $\rightarrow (G, *)$ is an algebraic structure
Closure + Associative $\rightarrow (G, *)$ is a semigroup
Closure + Associative + Identity $\rightarrow (G, *)$ is monoid
Closure + Associative + Identity + Inverse $\rightarrow (G, *)$ is group
Closure + Associative + Identity + Inverse + Commutative $\rightarrow (G, *)$ is abelian group
- Existence of identity $\exists e \in G \forall a \in G a * e = e * a = a$
- Existence of inverse $\forall a \in G \exists b \in G a * b = b * a = e$
- Modulo m operation $a +_m b =$ the remainder when m divides $a + b$
 $a \times_m b =$ the remainder when m divides $a \times b$
- Set $G = \{0, 1, 2 \dots (m - 1)\}_{+m}$ is an abelian group with identity 0 and the inverse of a is $(m - a) \text{ mod } m$.
- Set $G = \{1, 2, 3 \dots (p - 1)\}_{xp}$ is an abelian group of prime order (p).
- An element $g \in G$ such that $O(g) = O(G)$, then g is called the generator of the group and it is represented by $\langle g \rangle$.
- A group having at least one generator is called a cyclic group.
- $(H, *)$ is a subgroup of $(G, *)$ if $H \subseteq G$ and $(H, *)$ is itself a group.
- If H is a subgroup of a finite group G, then $O(H)$ divides $O(G)$.