INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal, Hyderabad -500 043
Computer Science and Engineering

PPT
ON
DISCRETE MATHEMATICAL STRUCTURES

Prepared By

Ms. K Mayuri, Assistant professor
Ms. N M Deepika, Assistant professor
Ms. G Nishwitha, Assistant professor
Mr. N V Krishna Rao, Assistant professor
Ms. B.Dhana Laxmi, Assistant professor
Ms. B Pravallika, Assistant professor

COURSE OBJECTIVES (COs):

I: Describe the logical and mathematical foundations, and study abstract models of computation.

II: Illustrate the limitations of predicate logic.

III: Define modern algebra for constructing and writing mathematical proofs

IV: Solve the practical examples of sets, functions, relations and recurrence relations

V: Recognize the patterns that arise in graph problems and use this knowledge for Constructing the trees and spanning trees.

COURSE OUTCOMES (COs):

- I: To understand the concepts associated with Mathematical Logic and Predicate calculus
- II: Ability to learn the basic concepts about relations, functions and to draw different diagrams like Lattice, Hasse diagrams.
- III: To understand the concepts of Algebraic Structures And Combinatorics .
- IV: To describe various types of recurrence relations and the methods to find out their solutions .
- V: To understand the basic concepts associated with Graphs and Trees.

COURSE LEARNING OUTCOMES

- **CLO 1**: Understand logical connectives and compound prepositions for building compound statements.
- **CLO 2:** Learn the formal symbols and use the preposition logic and predicate logic to solve problems on logical equivalences and implications.
- **CLO 3**: Memorize different scientific notations to simplify the logical statements.
- **CLO 4**: Prepare valid arguments from the given propositional statements by using rules of inference.
- **CLO 5**:Identify ordered pairs to form a binary relation from the given sets.

- **CLO 6**: Construct directed graph and a matrix representation using a binary relation on finite order pairs.

- **CLO 7**: Identify the properties of relations to check for equivalence relation and partial order relation and compute relations using operations on relations.

- **CLO 8**:Construct a hasse diagram to recognize the relevant partial ordered sets from the given binary relation.

- **CLO 9**:Describe the types of functions (one to one,on-to, bijective, Identity and constant function).

- **CLO 10**:Implement the concept of the inverse and recursive functions to get an optimized solution for an appropriate problem.

- **CLO 11**: Use the concept of lattices (Greatest Lower Bound (GLB) and Least Upper Bound (LUB) to represent a defined finite set in multi-dimension applications.
- **CLO 12**: Explain about the properties and types of lattices (bounded and distributive lattice).
- **CLO 13**: Construct different algebraic structures by using concepts of groups, sub groups, monoids and rings.
- **CLO 14**: Understand binomial and multinomial theorems to compute the coefficients for the given expansions.
- **CLO15**:Understand the concept of homomorphism and isomorphism of semi-groups.

- **CLO 16**: Analyze the given sets by using inclusion and exclusion principle.
- **CLO 17**: Identify the different counting techniques (permutations) related to mathematics and computer science.
- **CLO 18**:Solve discrete probability and set problems by using permutations and combinatorics.
- **CLO 19**: Identify the series of expansion to represent the sequence by using generating functions.
- **CLO 20**:Identify the general solution for first-order and second-order linear homogeneous recurrence relations.
- **CLO 21:**Identify the roots of second and higher order linear non-homogeneous recurrence relations.

- **CLO 22**:Understand the use of graphs and trees as representation tools in a variety of context.

- **CLO 23**: Identify Euler's and Hamilton rule for a simple connected graph in NP-complete problems.

- **CLO 24**:Construct a spanning tree by using search techniques (Depth First Search and Breadth First Search).

- **CLO 25**:Construct a minimal spanning tree by using Kruskal's and Prim's algorithm in order to obtain a solution for a real time problem.

- **CLO 26**:Possess the knowledge and skills for employability and to succeed in national and international level competitive exams.

Running outcomes

CLO 1: Understand logical connectives and compound prepositions for building compound statements.

CLO 2: Learn the formal symbols and use the preposition logic and predicate logic to solve problems on logical equivalences and implications.

CLO 3: Memorize different scientific notations to simplify the logical statements.

CLO 4: Prepare valid arguments from the given propositional statements by using rules of inference.

What is Discrete Mathematics ?

Mathematics can be broadly classified into two categories:

- Continuous Mathematics
- Discrete Mathematics

What is Discrete Mathematics ?

- It is the study of discrete objects.
- An object is discrete if it is not continuous.
- In other words, discrete object is something that is countable.
- Example of discrete objects: Integers, Finite set
- Example of non discrete objects: The Real plane(R),

  A Continuous Function

Discrete Mathematics

Part of Discrete Mathematics (DM) that you have studied are:

- Integers and Natural numbers.
- Arithmetic and Geometric Progressions.
- Permutations and Combinations

Why to study Discrete Mathematics ?

- It is the foundation course for Mathematics and Computer Science
- To know the set of common tools for handling Discrete objects.
- The concepts of this subjects are used in CN, TOC, CD etc.

STANDARD TEXTBOOKS

Book 1:
Title: Mathematical Foundations of Computer Science.
Author : Dr.D.S.Chandrashekaraiah.
Publication: Prism Books Pvt Ltd.

Book 2:
Title: Discrete Mathematical Structures with Applications to Computer Science.
Authors : J.P.Tremblay , R.Manohar.
Publication: TATA McGraw Hill Edition.

Book 3:
Title: Elements of Discrete Mathematics.
Author : C.L.Liu , D.P.Mohapatra.
Publication: TATA McGraw Hill Edition.

Course Structure

Module I : Mathematical Logic and Predicates

Module II : Relations, Functions and Lattices

Module III : Algebraic Structures and Combinatorics

Module IV : Recurrence Relation

Module V : Graphs And Trees

MODULE-1

Mathematical logic: Statements and notations, connectives, well-formed formulas, truth tables, tautology, equivalence implication; Normal forms: Disjunctive normal forms, conjunctive normal forms, principle disjunctive normal forms, principle conjunctive normal forms.

Predicate calculus: Predicative logic, statement functions, variables and quantifiers, free and bound variables, rules of inference, consistency, proof of contradiction, automatic theorem proving.

Mathematical Logic

- A **statement**, or a **proposition**, is a declarative sentence that is either true or false, but not both
- Uppercase letters denote propositions
  - Examples:
    - P: 2 is an even number (true)
    - Q: 7 is an even number (false)
    - R: A is a vowel (true)
  - The following are not propositions:
    - P: My cat is beautiful
    - Q: My house is big

Mathematical Logic

- Definition: Methods of reasoning, provides rules and techniques to determine whether an argument is valid
- Theorem: a statement that can be shown to be true (under certain conditions)
  - Example: If *x* is an even integer, then *x* + 1 is an odd integer
    - This statement is true under the condition that *x* is an integer is true

Mathematical Logic

Truth value

- One of the values "*truth*" *(T)* or "*falsity*" *(F)* assigned to a statement

Negation

The **negation** of *P*, written $\neg P$, is the statement obtained by negating statement *P*

Example:

- *P*: A is a consonant
- $\neg P$: it is the case that A is not a consonant

- Truth Table

P	$\neg P$
T	*F*
F	*T*

Mathematical Logic

- Conjunction
  - Let *P* and *Q* be statements.The **conjunction** of *P* and *Q*, written *P* ^ *Q* , is the statement formed by joining statements *P* and *Q* using the word “and”
  - The statement *P* ^ *Q* is true if both p and q are true; otherwise *P* ^ *Q* is false
  - Truth Table for Conjunction:

P	Q	P ∧ Q
F	F	F
F	T	F
T	F	F
T	T	T

Mathematical Logic

- Disjunction
  - Let *P* and *Q* be statements. The **disjunction** of *P* and *Q*, written *P* v *Q* , is the statement formed by joining statements *P* and *Q* using the word "or"
  - The statement *P* v *Q* is true if at least one of the statements *P* and *Q* is true; otherwise *P* v *Q* is false
  - The symbol v is read "or"
  - Truth Table for Disjunction:

P	Q	P v Q
F	F	F
F	T	T
T	F	T
T	T	T

Mathematical Logic

- Implication
  - Let P and Q be statements.The statement "if P then Q" is called an **implication or condition**.
  - The implication "if P then Q" is written $P \rightarrow Q$
  - P is called the hypothesis, Q is called the conclusion
- Truth Table for Implication:

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

Mathematical Logic

- Implication
  - Let P: Today is Sunday and Q: I will wash the car.
  - $P \rightarrow Q$:

    If today is Sunday, then I will wash the car
  - The **converse** of this implication is written $Q \rightarrow P$

    If I wash the car, then today is Sunday
  - The **inverse** of this implication is $\neg P \rightarrow \neg Q$

    If today is not Sunday, then I will not wash the car
  - The **contrapositive** of this implication is $\neg Q \rightarrow \neg P$

    If I do not wash the car, then today is not Sunday

Mathematical Logic

Biimplication

- Let *P* and *Q* be statements. The statement "*P* if and only if *Q*" is called the **biimplication or biconditional** of *P* and *Q*
- The biconditional "*P* if and only if *Q*" is written $P \leftrightarrow Q$
- "*P* if and only if *Q*"
- Truth Table for the Biconditional:

P	Q	$P \leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Mathematical Logic

- Precedence of logical connectives is:
  - $\neg$ highest
  - $\wedge$ second highest
  - $\vee$ third highest
  - $\rightarrow$ fourth highest
  - $\leftrightarrow$ fifth highest

Connectives

- More complex propositional statements can be build from elementary statements using **logical connectives.**

- **Logical connectives:**

  - Negation
  - Conjunction
  - Disjunction
  - Exclusive or
  - Implication
  - Biconditional

Connectives

Negation

Definition: Let p be a proposition. The statement "It is not the case that p." is another proposition, called the **negation of p**. The negation of p is denoted by ¬ p and read as "not p."

Example:

- Pitt is located in the Oakland section of Pittsburgh.

- It is not the case that Pitt is located in the Oakland section of Pittsburgh.

Other examples:

- $5 + 2 \neq 8$.
- 10 is not a prime number.
- It is not the case that buses stop running at 9:00pm.

Connectives

Negation

- **Negate the following propositions:**
  - It is raining today.
    - It is not raining today.
  - 2 is a prime number.
    - 2 is not a prime number
  - There are other life forms on other planets in the universe.
    - It is not the case that there are other life forms on other planets in the universe.

Connectives

Conjunction

- **Definition**: Let p and q be propositions. The proposition "**p and q**" denoted by $p \wedge q$, is true when both p and q are true and is false otherwise. The proposition $p \wedge q$ is called the **conjunction** of p and q.

- **Examples:**

  - Pitt is located in the Oakland section of Pittsburgh and 5 + 2 = 8
  - It is raining today and 2 is a prime number.
  - 2 is a prime number and $5 + 2 \neq 8$.
  - 13 is a perfect square and 9 is a prime.

Connectives

Disjunction

- **Definition**: Let p and q be propositions. The proposition "**p or q**" denoted by $p \vee q$, is false when both p and q are false and is true otherwise. The proposition $p \vee q$ is called the **disjunction** of p and q.

- **Examples:**
  - Pitt is located in the Oakland section of Pittsburgh or 5 + 2=8
  - It is raining today or 2 is a prime number.
  - 2 is a prime number or $5 + 2 \neq 8$.
  - 13 is a perfect square or 9 is a prime.

Connectives

Truth tables

Conjunction and disjunction

- Four different combinations of values for p and q

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

- NB: $p \vee q$ (the or is used inclusively, i.e., $p \vee q$ is true when either p or q or both are true).

Connectives

Exclusive or

- **Definition:** Let p and q be propositions. The proposition "p exclusive or q" denoted by $p \oplus q$, is true when exactly one of p and q is true and it is false otherwise.

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

Connectives

Implication

- **Definition**: Let p and q be propositions. The proposition "**p implies q**" denoted by $p \rightarrow q$ is called **implication**. It is false when p is true and q is false and is true otherwise.

- In $p \rightarrow q$, p is called the **hypothesis** and q is called the **conclusion**.

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

Biconditional

- **Definition**: Let p and q be propositions. The biconditional p $\leftrightarrow$ q (**read p if and only if q**), is true when p and q have the same truth values and is false otherwise.

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

- **Note:** two truth values always agree.

Well formed formula

Definition:

- In mathematical logic, propositional logic and predicate logic, a **well-formed formula**, abbreviated WFF or wff, often simply **formula**, is a finite sequence of symbols from a given alphabet that is part of a formal language. A formal language can be identified with the set of **formulas** in the language.

Well formed formula

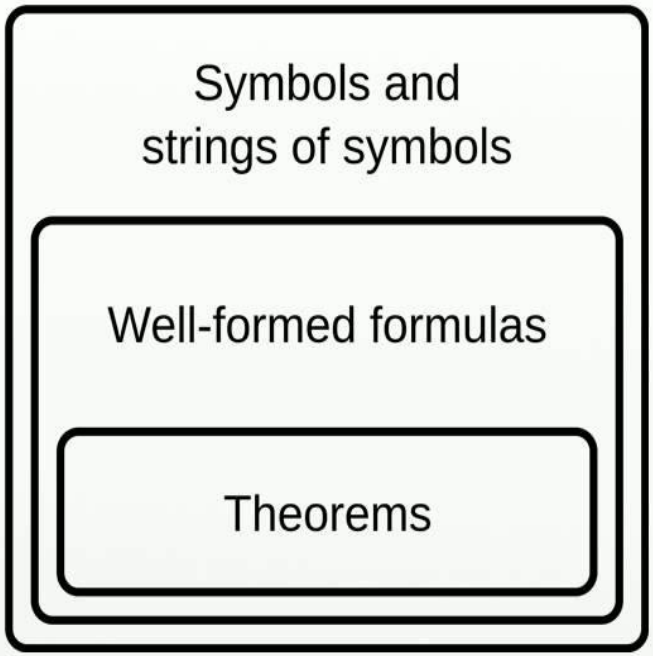
Atomic Formula

Definition:

In mathematical logic, an **atomic formula** (also known simply as an **atom**) is a **formula** with no deeper propositional structure, that is, a **formula** that contains no logical connectives or equivalently a **formula** that has no strict subformulas.

Well formed formula

Well-formed formula



https://en.wikipedia.org/wiki/File:Formal_languages.svg

Well formed formula

Rules for constructing Wffs

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

1. *An atomic formula is a well formed formula*
2. *If a is a well formed formula then ~A is a well formed formula*
3. *If A and B are well formed formulas then* $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$, *and (A B) are also well formed formulas.*
4. *If A is well formed formula and x is any variable, then (x) A and* $(\exists x)A$ *are well formed formulas.*
5. *Only those formulas obtained by using rules (1) to (4) are well formed formulas.*

Well formed formula

- One way to check whether or not an Expression is an wff is to try to state it in English.

- If you can translate it to an correct English sentence, then it is a wff.

Well formed formula

Example:

- To express the fact that Tom is taller than John, we can use the atomic formula *taller(*Tom, John), which is a well formed formula.

- This wff can also be part of some compound statement such as *taller*(Tom,John)$\wedge\sim$*taller*(John, Tom), which is also a wff.

Well formed formula

Example of well-formed formula

- By definition of WFF
  - WFF: $\neg(P \wedge Q)$, $(P \rightarrow (P \vee Q))$, $(\neg P \wedge Q)$, $((P \rightarrow Q) \wedge (Q \rightarrow R)) \leftrightarrow (P \rightarrow R))$, etc.
  - not WFF:

1. $(P \rightarrow Q) \rightarrow (\wedge Q)$: $(\wedge Q)$ is not a WFF.
2. $(P \rightarrow Q$: but $(P \rightarrow Q)$ is a WFF. etc..

Well formed formula

Predicate Well Formed Formulas (WFF)

- Predicate WFFs built by combining predicates with quantifiers, grouping symbols, and the logical connectives seen before
- Example: $(\forall x)[(\exists y)(P(x) \wedge Q(y)) \rightarrow R(x)]$
- Scope of a quantifier
- Interpretation for an expression with predicates has:
  1. Domain of interpretation
  2. Assignment of property of objects to each predicate
  3. Assignment of particular object to each constant symbol

4

Truth tables

Truth table

- The truth value of a statement is the classification as true or false which denoted by T or F.
- ▶ A truth table is a listing of all possible combinations of the individual statements as true or false, along with the resulting truth value of the compound statements.
- ▶ Truth tables are an aide in distinguishing valid and invalid arguments

Truth tables

- Conjunction
- Disjunction
- Negation
- Logical equivalence

Truth tables

Conjunction

- Joining two statements with AND forms a compound statement called a conjunction.
- p Λ q Read as “p and q”
- The truth value is determined by the possible values of ITS sub statements.
- To determine the truth value of a compound statement we create a truth table

p	*q*	*p*∧*q*
0	0	0
0	1	0
1	0	0
1	1	1

Truth tables

Disjunction

- Joining two statements with OR forms a compound statement called a conjunction.
- p V q Read as “p or q”
- The truth value is determined by the possible values of ITS sub statements.
- To determine the truth value of a compound statement we create a truth table

p	*q*	*pVq*
0	0	0
0	1	1
1	0	1
1	1	1

Truth tables

Negation

- Recall that the negation of a statement is the denial of the statement.
- If the statement p is true, the negation of p, i.e. ~p is false.
- If the statement p is false, then ¬p is true.
- Note that since the statement p could be true or false, we have 2 rows in the truth table.

P	$\neg P$
T	F
F	T

Truth tables

- Implication
  - Let *P* and *Q* be statements.The statement “if *P* then *Q*” is called an **implication or condition**.
  - The implication “if *P* then *Q*” is written *P* ? *Q*
  - *P* is called the hypothesis, *Q* is called the conclusion
- Truth Table for Implication:

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

Truth tables

Biimplication

- Let *P* and *Q* be statements. The statement "*P* if and only if *Q*" is called the **biimplication or biconditional** of *P* and *Q*
- The biconditional "*P* if and only if *Q*" is written *P* ⇔ *Q*
- "*P* if and only if *Q*"
- Truth Table for the Biconditional:

P	Q	$P \leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Truth tables

Constructing Truth tables

- Construct the truth table for the following compound proposition

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

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

Truth tables

Applications

- Truth tables are used to show/define the relationships between the truth values of
  - the individual propositions and
  - the compound propositions based on them

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

Tautology

Definitions:

- Tautology – a logical expression that is true for all variable assignments.
- Contradiction – a logical expression that is false for all variable assignments.
- Contingent – a logical expression that is neither a tautology nor a contradiction.

Tautology

Tautologies

P	¬P	P ∨ ¬P	¬(P ∨ ¬P)
T	F	T	F
F	T	T	F

Since P ∨ ¬P is true for all variable assignments, it is a tautology.

P	Q	P ∧ Q	¬(P ∧ Q)	¬(P ∧ Q) ∨ Q
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T

Tautological Derivation by Substitution

Using schemas that are tautologies, we can get other tautologies by substituting expressions for schema variables.

- Since $A \vee \neg A$ is a tautology,

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

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

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$A \wedge (A \Rightarrow B) \Rightarrow B$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T

Sound Reasoning

- A logical argument has the form:

  $$A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B$$

  and is sound if when $A_i = T$ for all i, $B = T$. (i.e. If the premises are all true, then the conclusion is also true.)
- This happens when $A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B$ is a tautology.

Intuitive Basis for Sound Reasoning

If $(A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B)$ is a tautology, and A_i = T for all *i* then B must necessarily be true!

A	B	$A \Rightarrow B$
T	?	T

B = T is the only possibility for the conclusion!

Tautology

Modus Ponens

$A \Rightarrow B$
A
B

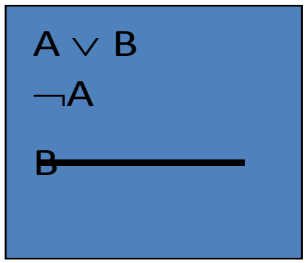
A	B	$A \Rightarrow B$
T	?	T

A	B	$(A \Rightarrow B)$	$(A \Rightarrow B) \wedge A$	$(A \Rightarrow B) \wedge A \Rightarrow B$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Hence, modus ponens is sound.

Tautology

Disjunctive Syllogism



A	B	A ∨ B	¬A	(A ∨ B) ∧ ¬A	(A ∨ B) ∧ ¬A ⇒ B
T	T	T	F	F	T
T	F	T	F	F	T
F	T	T	T	T	T
F	F	F	T	F	T

Hence, disjunctive syllogism is sound.

Equivalence implication

Equivalence implication

Implication

If p and q are propositions, then $p \rightarrow q$ is a conditional statement or implication which is read as "if p, then q" and has this truth table:

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

In $p \rightarrow q$, p is the hypothesis (antecedent or premise) and q is the conclusion (or consequence).

Implication can be expressed by disjunction and negation:

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

Equivalence implication

Understanding Implication

- In $p \rightarrow q$ there does not need to be any connection between the antecedent or the consequent. The meaning depends only on the truth values of p and q.
- This implication is perfectly fine, but would not be used in ordinary English. “If the moon is made of green cheese, then I have more money than Bill Gates.”
- One way to view the logical conditional is to think of an obligation or contract. “If I am elected, then I will lower taxes.”

Equivalence implication

Different Ways of Expressing $p \rightarrow q$

if p, then q
if p, q
q unless $\neg p$
q if p
p is sufficient for q q is necessary for p
a sufficient condition for q is p

p implies q p only if q q when p
q whenever p
q follows from p
a necessary condition for p is q

Equivalence implication

Converse, Contrapositive, and Inverse

$q \rightarrow p$ is the **converse** of $p \rightarrow q$

$\neg q \rightarrow \neg p$ is the **contrapositive** of $p \rightarrow q$

$\neg p \rightarrow \neg q$ is the **inverse** of $p \rightarrow q$

Example: Find the converse, inverse, and contrapositive of "It is raining is a sufficient condition for my not going to town."
Solution:
converse: If I do not go to town, then it is raining. inverse: If it is not raining, then I will go to town. contrapositive: If I go to town, then it is not raining.

Equivalence implication

List of Logical Equivalences

$p \wedge T \Leftrightarrow p$; $p \vee F \Leftrightarrow p$	**Identity Laws**
$p \vee T \Leftrightarrow T$; $p \wedge F \Leftrightarrow F$	**Domination Laws**
$p \vee p \Leftrightarrow p$; $p \wedge p \Leftrightarrow p$	**Idempotent Laws**
$\neg(\neg p) \Leftrightarrow p$	**Double Negation Law**
$p \vee q \Leftrightarrow q \vee p$; $p \wedge q \Leftrightarrow q \wedge p$	**Commutative Laws**
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$; $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	**Associative Laws**

Equivalence implication

List of Equivalences

$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	**Distribution Laws**
$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$	**De Morgan's Laws**
	Miscellaneous
$p \vee \neg p \Leftrightarrow \mathbf{T}$	**Or Tautology**
$p \wedge \neg p \Leftrightarrow \mathbf{F}$	**And Contradiction**
$(p \rightarrow q) \Leftrightarrow (\neg p \vee q)$	**Implication Equivalence**
$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$	**Biconditional Equivalence**

Equivalence implication

More Logical Equivalences

TABLE 7 Logical Equivalences Involving Conditional Statements.

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

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

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

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

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

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

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

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

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

TABLE 8 Logical Equivalences Involving Biconditional Statements.

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

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

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

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

Disjunctive Normal form

Disjunctive Normal form

Logical Operators

$\vee$ - Disjunction

$\wedge$ - Conjunction

$\neg$ - Negation

$\rightarrow$ - Implication $p \rightarrow q \Leftrightarrow \neg p \vee q$

$\oplus$ - Exclusive or $(p \wedge \neg q) \vee (\neg p \wedge q)$

$\leftrightarrow$ - Biconditional $p \leftrightarrow q \Leftrightarrow$

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

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

Do we need all these?

Disjunctive Normal form

Functionally Complete

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

Disjunctive Normal form

Are $\neg(p \vee (\neg p \wedge q))$
and $(\neg p \wedge \neg q)$ equivalent?

$\neg(p \vee (\neg p \wedge q))$	
$\Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$	DeMorgan
$\Leftrightarrow \neg p \wedge (\neg\neg p \vee \neg q)$	DeMorgan
$\Leftrightarrow \neg p \wedge (p \vee \neg q)$	Double Negation
$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q)$	Distribution
$\Leftrightarrow (p \wedge \neg p) \vee (\neg p \wedge \neg q)$	Commutative
$\Leftrightarrow F \vee (\neg p \wedge \neg q)$	And Contradiction
$\Leftrightarrow (\neg p \wedge \neg q) \vee F$	Commutative
$\Leftrightarrow (\neg p \wedge \neg q)$	Identity

Disjunctive Normal form

Are $\neg(p \vee (\neg p \wedge q))$
and $(\neg p \wedge \neg q)$ equivalent?

- Even though both are expressed with only $\wedge$, $\vee$, and $\neg$, it is still hard to tell without doing a proof.
- What we need is a unique representation of a compound proposition that uses $\wedge$, $\vee$, and $\neg$.
- This unique representation is called the Disjunctive Normal Form.

Disjunctive Normal form

Disjunctive Normal Form

- A disjunction of conjunctions where every variable or its negation is represented once in each conjunction (a *minterm)*
  - each minterm appears only once

Example: DNF of $p \oplus q$ is

$(p \wedge \neg q) \vee (\neg p \wedge q)$.

Disjunctive Normal form

Truth Table

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

Disjunctive Normal form

Method to construct DNF

- Construct a truth table for the proposition.
- Use the rows of the truth table where the proposition is True to construct minterms
  - If the variable is true, use the propositional variable in the minterm
  - If a variable is false, use the negation of the variable in the minterm
- Connect the minterms with $\vee$'s.

Disjunctive Normal form

How to find the DNF of $(p \vee q) \rightarrow \neg r$

p	q	r	$(p \vee q)$	$\neg r$	$(p \vee q) \rightarrow \neg r$
T	T	T	T	F	F
T	*T*	*F*	*T*	*T*	*T*
T	F	T	T	F	F
T	*F*	*F*	*T*	*T*	*T*
F	T	T	T	F	F
F	*T*	*F*	*T*	*T*	*T*
F	*F*	*T*	*F*	*F*	*T*
F	*F*	*F*	*F*	*T*	*T*

There are five sets of input that make the statement true.
Therefore there are five minterms.

Disjunctive Normal form

p	q	r	(p ∨ q)	¬r	(p ∨ q)→¬r
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	T	T
F	T	T	T	F	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	F	T	T

From the truth table we can set up the DNF

(p ∨ q)→¬r ⇔ (p∧q∧¬r) ∨ (p∧¬q∧¬r) ∨ (¬p∧q∧¬r) ∨ (¬p∧¬q∧r) ∨ (¬p∧¬q∧¬r)

Disjunctive Normal form

Can we show that just $\neg$ and $\wedge$ form a set of functionally complete operands?

It is sufficient to show that $p \vee q$ can be written in terms of $\neg$ and $\wedge$. Then using DNF, we can write every compound proposition in terms of $\neg$ and $\wedge$.

$(p \vee q)$

$\Leftrightarrow (\neg\neg p \vee \neg\neg q)$ Double negation (2)

$\Leftrightarrow \neg(\neg p \wedge \neg q)$ DeMorgan

Disjunctive Normal form

Find an expression equivalent to $p \rightarrow q$ that uses only conjunctions and negations.

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

How many minterms in the DNF?

The DNF of $p \rightarrow q$ is $(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$.

Then, applying DeMorgan's Law, we get that this is equivalent to

$\neg[\neg(p \wedge q) \wedge \neg(\neg p \wedge q) \wedge \neg(\neg p \wedge \neg q)]$.

Disjunctive Normal form

Now can we write an equivalent statement to $p \rightarrow q$ that uses only disjunctions and negations?

$p \rightarrow q$

$\Leftrightarrow \neg[\neg(p \wedge q) \wedge \neg(\neg p \wedge q) \wedge \neg(\neg p \wedge \neg q)]$ From Before

$\Leftrightarrow \neg[(\neg p \vee \neg q) \wedge (\neg\neg p \vee \neg q) \wedge (\neg\neg p \vee \neg\neg q)]$ DeMorgan

$\Leftrightarrow \neg[(\neg p \vee \neg q) \wedge (p \vee \neg q) \wedge (p \vee q)]$ Doub. Neg.

$\Leftrightarrow [\neg(\neg p \vee \neg q) \vee \neg(p \vee \neg q) \vee \neg(p \vee q)]$ DeMorgan

Conjunctive Normal form

Normal Forms

- Normal forms are standard forms, sometimes called canonical or accepted forms.
- A logical expression is said to be in *disjunctive normal form (DNF)* if it is written as a disjunction, in which all *terms* are conjunctions of *literals*.
- Similarly, a logical expression is said to be in *conjunctive normal form (CNF)* if it is written as a conjunction of disjunctions of literals.

Conjunctive Normal form

Conjunctive Normal Form (CNF)

A formula is in *conjunctive normal form* if it is a conjunction of one or more clauses.

Examples:

- $\neg p$
- $p \vee \neg q$
- $(\neg p \vee q) \wedge (r \vee \neg t \vee \neg p)$
- $(\neg p \vee q) \wedge (r \vee \neg t \vee \neg p) \wedge p$

Conjunctive Normal form

Testing validity of a formula in CNF is particularly simple:

Theorem:

- A clause $l_1 \vee l_2 \vee \ldots \vee l_n$ is valid iff there exist i, j such that $l_i = \neg l_j$.
- A CNF formula $c_1 \wedge c_2 \wedge \ldots \wedge c_n$ is valid if each of its clauses c_i is valid.

Examples:

- $\neg p \vee q \vee p \vee r$ is valid
- $(\neg p \vee q \vee p) \wedge (r \vee \neg r)$ is valid
- $(\neg p \vee q \vee p) \wedge (r \vee s)$ is not valid

Conjunctive Normal form

Step 1: Eliminate $\dashrightarrow$

Using the rule

$$A \dashrightarrow B \equiv \neg A \vee B$$

we may eliminate all occurrences of $\dashrightarrow$. Example:

$$p \dashrightarrow ((q \dashrightarrow r) \vee \neg s) \equiv p \dashrightarrow ((\neg q \vee r) \vee \neg s)$$

$$\equiv \neg p \vee ((\neg q \vee r) \vee \neg s)$$

Conjunctive Normal form

Step 2: Push negations down

Using De Morgan's Laws and the double negation rule

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

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

$$\neg\neg A \equiv A$$

we push negations down towards the atoms until we obtain a formula that is formed from literals using only $\wedge$ and $\vee$.

Conjunctive Normal form

Example:

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

$$\equiv \neg\neg p \vee \neg(q \vee \neg(r \wedge s)))$$

$$\equiv p \vee (\neg q \vee \neg\neg(r \wedge s))$$

$$\equiv p \vee (\neg q \vee (r \wedge s))$$

Conjunctive Normal form

Step 3: Use distribution to convert to CNF

Using the distribution rules

$$A \vee (B_1 \wedge \ldots \wedge B_n) \equiv (A \vee B_1) \wedge \ldots \wedge (A \vee B_n)$$

$(B_1 \wedge \ldots \wedge B_n) \vee A \equiv (B_1 \vee A) \wedge \ldots \wedge (B_n \vee A)$ we obtain a CNF formula.

Example:

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

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

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

Conjunctive Normal form

Note: we use distribution from the "tips" of the parse tree, up to the root. Each tip is a literal, which is a CNF formula.

If α and β are already in CNF then

- $\alpha \wedge \beta$ is also in CNF
- $\alpha \vee \beta$ is converted to CNF as follows:
  1. If α and β are literals then $\alpha \vee \beta$ is already in CNF
  2. If $\alpha = \alpha_1 \wedge \ldots \wedge \alpha_1$ then

$$\alpha \vee \beta = (\alpha_1 \vee \beta) \wedge \ldots \wedge (\alpha_1 \vee \beta)$$

If β is a literal the RHS is in CNF, otherwise $\beta = \beta_1 \wedge \ldots \wedge \beta_k$ and we take one more distribution step to convert each $\alpha_i \wedge \beta_i$ to CNF.

Conjunctive Normal form

A more complicated example:

$$((p \wedge q) \vee (r \wedge s)) \vee (\neg q \wedge (p \vee t))$$

$$\equiv (((p \wedge q) \vee r) \wedge ((p \wedge q) \vee s)) \vee (\neg q \wedge (p \vee t))$$

$$\equiv ((p \vee r) \wedge (q \vee r) \wedge (p \vee s) \wedge (q \vee s)) \vee (\neg q \wedge (p \vee t))$$

$$\equiv ((p \vee r) \vee (\neg q \wedge (p \vee t)) \wedge$$
$$((q \vee r) \vee (\neg q \wedge (p \vee t)) \wedge$$
$$((p \vee s) \vee (\neg q \wedge (p \vee t)) \wedge$$
$$((q \vee s) \vee (\neg q \wedge (p \vee t))$$

$$\equiv (p \vee r \vee \neg q) \wedge (p \vee r \vee p \vee t) \wedge (q \vee r \vee \neg q) \wedge (q \vee r \vee p \vee t) \wedge (p \vee s) \vee \neg q) \wedge (p \vee s \vee p \vee t) \wedge (q \vee s \vee \neg q) \wedge (q \vee s \vee p \vee t)$$

Principle Disjunctive Normal form

Principle Disjunctive Normal form

- Let us assume A and B be two statement variables.
- All possible formulas by using conjunction are given as follows. The total number of formulas for two variables A and B are 2^2 formulas. They are A ^ B, A ^~ B, ~A ^B and ~A ^ ~ B.
- These are called minterms or Boolean conjunctions of A and B. The minterms (2^n terms) are denoted by M_0, M_1, … ,M_{2^n-1}.
- ***A formula equivalent to a given formula consisting of the disjunction of minterms only is called Principal disjunctive normal form (PDNF) of the given formula.***

Principle Disjunctive Noraml form

Example 1:

Find the Principal disjunctive normal form of $\neg p \vee q$.

Solution:

$\neg p \vee q$

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

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

$(\neg p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge q)$ *which is the required Principal disjunctive normal form.*

Principle Disjunctive Normal form

Example 2:

Obtain the principal disjunctive normal form of

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

Solution:

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

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

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

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

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

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

Which is the required principal disjunctive normal form.

Principle Disjunctive Normal form

Example 3:

Obtain PDNF for $P \rightarrow ((P \rightarrow Q \wedge \sim(\sim Q \vee \sim P)))$.

Solution:

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

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

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

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

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

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

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

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

Principle Disjunctive Normal form

Ex. Obtain principal disjunctive normal form for $p \vee \neg q$.

Sol.

$$
\begin{aligned}
& p \vee \neg q \\
& \equiv [p \wedge (q \vee \neg q)] \vee [\neg q \wedge (p \vee \neg p)] \\
& \equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg q \wedge p) \vee (\neg q \wedge \neg p) \\
& \equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)
\end{aligned}
$$

Principle Conjunctive Normal form

Principle Conjunctive Normal form

- A statement formula which consists of a conjunction of maxterms only is called the principal conjunctive normal form.
- The duals of minterms are called maxterms. For a given number of variables the maxterm consists of disjunctions in which each variable or its negation, but not both, appears only once.
- Therefore for a given formula, an equivalent formula consisting of conjunctions of maxterms only is known as ***its principal conjunctive normal form***. This is also called *the* ***product of sums canonical form***.

Principle Conjunctive Normal form

Principal Conjunctive Normal Form

maxterm as a dual to minterm.

For a given number of variables, the maxterm consists of disjunctions in which each variable or its negation, but not both, appears only once.

A formula consisting of conjunction of maxterms only is known as principal conjunctive normal form.

Also called the product of sums canonical form.

Principle Conjunctive Normal form

Ex. Find principal conjunctive normal form for $(p \leftrightarrow q)$

Sol. $p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p)$

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

Ex. Find principal conjunctive normal form for

$[(p \vee q) \wedge \neg p \rightarrow \neg q]$

Sol. $[(p \vee q) \wedge \neg p \rightarrow \neg q]$

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

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

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

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

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

$\equiv \neg q \vee p$

$\equiv p \vee \neg q$

Principle Conjunctive Normal form

Example 1:

Obtain PCNF for A : $(\neg P \rightarrow R) \wedge ((Q \rightarrow P) \wedge (P \rightarrow Q))$.

Solution:

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

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

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

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

$\Leftrightarrow \pi(0,2,3,4,5)$.

Principle Conjunctive Normal form

Example 2:

Obtain the product of sums canonical form of the formula A which is given by

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

Solution:

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

$\Leftrightarrow \pi(0,3,7)$.

$\neg(\neg A) \Leftrightarrow$ consisting of missing maxterms

$\Leftrightarrow \pi(1,2,4,5,6)$

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

Principle Conjunctive Normal form

Example 3:

Obtain the product-of-sums canonical form of the formula A, which is given by

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

Solution:

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

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

$\Leftrightarrow \pi(5, 6, 9, 10, 12)$.

$\neg(\neg A) \Leftrightarrow$ consisting of missing maxterms

$\Leftrightarrow \pi(0,1,2,3,4,7,8,11,13,14,15)$

$\Leftrightarrow M_0 \wedge M_1 \wedge M_2 \wedge M_3 \wedge M_4 \wedge M_7 \wedge M_8 \wedge M_{11} \wedge M_{13} \wedge M_{14} \wedge M_{15}$

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

Principle Conjunctive Normal form

Example 4:

Obtain the product of sums canonical form of $(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$.

Solution:

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

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

$\Leftrightarrow \pi(1,2,3)$.

$\neg(\neg A) \Leftrightarrow$ consisting of missing maxterms

$\Leftrightarrow \pi(0)$

$\Leftrightarrow M_0$

$\Leftrightarrow P \vee Q$.

Predicate Calculus

Predicate Logic

- *Predicate logic* is an extension of propositional logic that permits concisely reasoning about whole *classes* of entities.

  E.g., "$x>1$", "$x+y=10$"

- Such statements are neither true or false when the values of the variables are not specified.

Applications of Predicate Logic

- It is *the* formal notation for writing perfectly clear, concise, and unambiguous mathematical *definitions*, *axioms*, and *theorems* for *any* branch of mathematics.
- Supported by some of the more sophisticated *database query engines.*
- Basis for *automatic theorem provers* and many other Artificial Intelligence systems.

Subjects and Predicates

- The proposition

  "The dog is sleeping"

  has two parts:

  - "the dog" denotes the *subject* - the *object* or *entity* that the sentence is about.
  - "is sleeping" denotes the *predicate*- a property that the subject can have.

Propositional Functions

- A *predicate* is modeled as a *function* $P(\cdot)$ from objects to propositions.
  - $P(x)$ = "x is sleeping" (where x is any object).
- The *result of applying* a predicate P to an object $x=a$ is the *proposition* $P(a)$.
  - *e.g.* if $P(x)$ = "$x > 1$",
    then $P(3)$ is the *proposition* "3 is greater than 1."
- Note: The predicate P **itself** (*e.g.* P="is sleeping") is **not** a proposition (not a complete sentence).

Propositional Functions

- Predicate logic includes propositional functions of **any** number of arguments.

  e.g. let $P(x,y,z)$ = "x gave y the grade z",

  x="Mike", y="Mary", z="A",

  $P(x,y,z)$ = "Mike gave Mary the grade A."

Universe of Discourse

- The collection of values that a variable *x* can take is called *x*'s *universe of discourse*.

  e.g., let $P(x)$="$x+1>x$".

  we could define the course of universe as the set of integers.

Variables and quantifiers, Free and bound variables

Variables and Quantifiers

Quantifier Expressions

- *Quantifiers* allow us to *quantify* (count) *how many* objects in the universe of discourse satisfy a given predicate:

  - "∀" is the FOR∀LL or *universal* quantifier.
    ∀*x* *P*(*x*) means *for all* x in the u.d., *P* holds.

  - "∃" is the ∃XISTS or *existential* quantifier.
    ∃*x* *P*(*x*) means there *exists* an x in the u.d. (that is, one or more) such that *P*(*x*) is true.

Universal Quantifier ∀: Example

- Let $P(x)$ be the *predicate* "x is full."
- Let the u.d. of x be parking spaces at UNR.
- The *universal quantification of* $P(x)$,

  $\forall x\, P(x)$, is the *proposition:*
  - "All parking spaces at UNR are full." or
  - "Every parking space at UNR is full." or
  - "For each parking space at UNR, that space is full."

Variables and Quantifiers

The Universal Quantifier ∀

- To prove that a statement of the form

  $\forall x\, P(x)$ is false, it suffices to find a **counterexample** (i.e., one value of x in the universe of discourse such that $P(x)$ is false)

  – e.g., $P(x)$ is the predicate "x>0"

Variables and Quantifiers

Existential Quantifier ∃ Example

- Let $P(x)$ be the *predicate* "x is full."
- Let the u.d. of x be parking spaces at UNR.
- The *universal quantification of* $P(x)$,

  $\exists x\, P(x)$, is the *proposition*:
  - "Some parking space at UNR is full." or
  - "There is a parking space at UNR that is full." or
  - "At least one parking space at UNR is full."

Quantifier Equivalence Laws

- Definitions of quantifiers: If u.d.=a,b,c,…
  $\forall x\, P(x) \Leftrightarrow P(\text{a}) \wedge P(\text{b}) \wedge P(\text{c}) \wedge \ldots$
  $\exists x\, P(x) \Leftrightarrow P(\text{a}) \vee P(\text{b}) \vee P(\text{c}) \vee \ldots$
- We can prove the following laws:
  $\forall x\, P(x) \Leftrightarrow \neg\exists x\, \neg P(x)$
  $\exists x\, P(x) \Leftrightarrow \neg\forall x\, \neg P(x)$
- Which *propositional* equivalence laws can be used to prove this?

DeMorgan's

More Equivalence Laws

- $\neg\exists x\, P(x) \Leftrightarrow \forall x \neg P(x)$
  $\neg\forall x\, P(x) \Leftrightarrow \exists x \neg P(x)$

- $\forall x\, \forall y\, P(x,y) \Leftrightarrow \forall y\, \forall x\, P(x,y)$
  $\exists x\, \exists y\, P(x,y) \Leftrightarrow \exists y\, \exists x\, P(x,y)$

- $\forall x\, (P(x) \wedge Q(x)) \Leftrightarrow (\forall x\, P(x)) \wedge (\forall x\, Q(x))$
  $\exists x\, (P(x) \vee Q(x)) \Leftrightarrow (\exists x\, P(x)) \vee (\exists x\, Q(x))$

Scope of Quantifiers

- The part of a logical expression to which a quantifier is applied is called the scope of this quantifier.

e.g., $(\forall x\, P(x)) \wedge (\exists y\, Q(y))$

e.g., $(\forall x\, P(x)) \wedge (\exists x\, Q(x))$

Free and Bound Variables

- An expression like $P(x)$ is said to have a *free variable* x (meaning x is undefined).
- A quantifier (either $\forall$ or $\exists$) *operates* on an expression having one or more free variables, and *binds* one or more of those variables, to produce an expression having one or more *bound variables*.

Examples of Binding

- $P(x,y)$ has 2 free variables, x and y.
- $\forall x\, P(x,y)$ has 1 free variable, and one bound variable. [which is which?]
- "$P(x)$, where x=3" is another way to bind x.
- An expression with zero free variables is an actual proposition.
- An expression with one or more free variables is still only a predicate: $\forall x\, P(x,y)$

Variables and Quantifiers

More to Know About Binding

- $\forall x\ \exists x\ P(x)$ - x is not a free variable in $\exists x\ P(x)$, therefore the $\forall x$ binding isn't used.
- $(\forall x\ P(x)) \wedge Q(x)$ - The variable x is outside of the *scope* of the $\forall x$ quantifier, and is therefore free. Not a proposition.
- $(\forall x\ P(x)) \wedge (\exists x\ Q(x))$ - Legal because there are 2 <u>different</u> x's!
- Quantifiers bind as loosely as needed: parenthesize $\forall x \quad P(x) \wedge Q(x)$

Nested Quantifiers

Exist within the scope of other quantifiers

- Let the u.d. of x & y be people.
- Let $P(x,y)$="x likes y" (a predicate with 2 f.v.'s)
- Then $\exists y\, P(x,y)$ = "There is someone whom x likes." (a predicate with 1 free variable, x)
- Then $\forall x\, (\exists y\, P(x,y))$ = "Everyone has someone whom they like."
  (A _____ with ___ free variables.)

Proposition 0

Variables and Quantifiers

Order of Quantifiers Is Important!!

If $P(x,y)$="x relies upon y," express the following in unambiguous English:

$\forall x(\exists y\ P(x,y))=$ Everyone has *someone* to rely on.

$\exists y(\forall x\ P(x,y))=$ There's a poor overworked soul whom *everyone* relies upon (including himself)!

$\exists x(\forall y\ P(x,y))=$ There's some needy person who relies upon *everybody* (including himself).

$\forall y(\exists x\ P(x,y))=$ Everyone has *someone* who relies upon them.

$\forall x(\forall y\ P(x,y))=$ *Everyone* relies upon *everybody*, (including themselves)!

Variables and Quantifiers

Natural language is ambiguous!

- "Everybody likes somebody."
  - For everybody, there is somebody they like,
    - $\forall x \exists y$ *Likes*(x,y)
  - or, there is somebody (a popular person) whom everyone likes?
    - $\exists y \forall x$ *Likes*(x,y)

Variables and Quantifiers

Notational Conventions

- Consecutive quantifiers of the same type can be combined: $\forall x\ \forall y\ \forall z\ P(x,y,z) \Leftrightarrow \forall x,y,z\ P(x,y,z)$ or even $\forall xyz\ P(x,y,z)$
- Sometimes the universe of discourse is restricted within the quantification, *e.g.*,
  - $\forall x>0\ P(x)$ is shorthand for "For all x that are greater than zero, $P(x)$."
  - $\exists x>0\ P(x)$ is shorthand for "There is an x greater than zero such that $P(x)$."

Defining New Quantifiers

As per their name, quantifiers can be used to express that a predicate is true of any given *quantity* (number) of objects.

Define $\exists!x\, P(x)$ to mean "$P(x)$ is true of *exactly one* x in the universe of discourse."

$\exists!x\, P(x) \Leftrightarrow \exists x \left(P(x) \wedge \neg\exists y \left(P(y) \wedge y \neq x\right)\right)$

"There is an x such that $P(x)$, where there is no y such that P(y) and y is other than x."

Some Number Theory Examples

- Let u.d. = the *natural numbers* 0, 1, 2, …
- "A number x is *even*, $E(x)$, if and only if it is equal to 2 times some other number."
  $\forall x\,(E(x) \leftrightarrow (\exists y\; x{=}2y))$
- "A number is *prime*, $P(x)$, iff it isn't the product of two non-unity numbers."
  $\forall x\,(P(x) \leftrightarrow (\neg\exists y,z\; x{=}yz \wedge y{\neq}1 \wedge z{\neq}1))$

Variables and Quantifiers

Calculus Example

- Precisely defining the concept of a limit using quantifiers:

$$\left(\lim_{x \to a} f(x) = L\right) \Leftrightarrow$$

$$\left(\begin{array}{l} \forall \varepsilon > 0 : \exists \delta > 0 : \forall x : \\ \left(|\, x - a \,| < \delta\right) \rightarrow \left(|\, f(x) - L \,| < \varepsilon\right) \end{array}\right)$$

Rules of Inference

- Means to draw conclusions from other assertions
- Rules of inference provide justification of steps used to show that a conclusion follows from a set of hypotheses
- The next several slides illustrate specific rules of inference

Rules of inference

Addition

A true hypothesis implies that the disjunction of that hypothesis and another are true

$$\frac{p}{\therefore\ p \vee q}$$

or $p \rightarrow (p \vee q)$

Rules of inference

Simplification

If the conjunction of 2 propositions is true, then each proposition is true

$$\frac{p \wedge q}{\therefore\ p}$$

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

Rules of inference

Conjunction

If p is true and q is true, then $p \wedge q$ is true

p

q

$\therefore p \wedge q$

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

Rules of inference

Modus Ponens

If a hypothesis and implication are both true, then the conclusion is true

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore\ q \end{array} \qquad \text{or} \quad (p \wedge (p \rightarrow q)) \rightarrow q$$

Rules of inference

Modus Tollens

If a conclusion is false and its implication is true, then the hypothesis must be false

$\neg q$

$p \rightarrow q$

$\therefore \neg p$

or $[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$

Rules of inference

Hypothetical Syllogism

If an implication is true, and the implication formed using its conclusion as the hypothesis is also true, then the implication formed using the original hypothesis and the new conclusion is also true

$p \rightarrow q \quad q \rightarrow r$

$\therefore\ p \rightarrow r$ or $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$

Rules of inference

Disjunctive Syllogism

If a proposition is false, and the disjunction of it and another proposition is true, the second proposition is true

$$p \vee q$$
$$\neg p$$
$$\therefore q$$

or $[(p \vee q) \wedge \neg p] \rightarrow q$

Rules of inference

Using rules of inference

- We can use the rules of inference to form the basis for arguments
- A valid argument is an implication in which, when all hypotheses are true, the conclusion is true: $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$
- When several premises are involved, several rules of inference my be needed to show that an argument is valid

Rules of inference

Example

Let p = “It is Monday” and

$p \rightarrow q$ = “If it is Monday, I have Discrete Math today”

Since these statements are both true, then by Modus Ponens:

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

we can conclude “I have Discrete Math today” (q)

Rules of inference

Another Example

Let $\neg q$ = "I don't have Discrete Math today" and
$p \rightarrow q$ = "If it is Monday, I have Discrete Math today"
If both of the above are true, then by Modus Tollens:

$$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$$

we can conclude "It is not Monday" $(\neg p)$

Rules of inference

Fallacies

A fallacy is an argument based on contingencies rather than tautologies; some examples:

- Fallacy of affirming the conclusion: $[(p \rightarrow q) \wedge q] \rightarrow p$

This is not a tautology because it's false when p is false and q is true

- Fallacy of denying the hypothesis: $[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$

Like the previous fallacy, this is not a tautology because it is false when p is false and q is true

Rules of inference

Rules of Inference for Quantified Statements

- Universal instantiation:

  $\forall x P(x)$

  $\therefore$ P(c) if c $\in$ U

- Universal generalization:

  P(c) for arbitrary c $\in$ U

  $\therefore$ $\forall x P(x)$ Note: c must be arbitrary

Rules of inference

Rules of Inference for Quantified Statements

- Existential instantiation:

$\exists x P(x)$

$\therefore$ P(c) for some c ? U

Note that value of c is not known; we only know it exists

- Existential generalization:

P(c) for some c $\in$ U

$\therefore \exists x P(x)$

Rules of inference

Example

Let P(x) = "A man is mortal"; then
$\forall x P(x)$ = "All men are mortal"

Assuming p = "Socrates is a man" is true, show that
q ="Socrates is mortal" is implied

This is an example of universal instantiation:
P(Socrates) = "Socrates is mortal";
Since $\forall x P(x)$

$\therefore P(c)$

Also, by modus ponens: $(p \wedge (p \rightarrow q)) \rightarrow q$

Proof Techniques: Learning Objectives

- Learn various proof techniques
  - Direct
  - Indirect
  - Contradiction
  - Induction
- Practice writing proofs
- CS: Why study proof techniques?

Proof Techniques

- Statement that can be shown to be true (under certain conditions)
  - Typically Stated in one of three ways
    - As Facts
    - As Implications
    - As Biimplications

Proof by contradiction

Validity of Arguments

- **Proof:** an argument or a proof of a theorem consists of a finite sequence of statements ending in a conclusion
- **Argument:** a finite sequence $A_1, A_2, A_3, \ldots, A_{n-1}, A_n$ of statements.
- The final statement, A_n, is the conclusion, and the statements $A_1, A_2, A_3, \ldots, A_{n-1}$ are the premises of the argument.
- An argument is logically valid if the statement formula $A_1, A_2, A_3, \ldots, A_{n-1} \rightarrow A_n$ is a tautology.

Proof by contradiction

Proof

❖A *mathematical proof* of the statement S is a sequence of logically valid statements that connect axioms, definitions, and other already validated statements into a demonstration of the correctness of S. The rules of logic and the axioms are agreed upon ahead of time.

❖At a minimum, the axioms should be independent and consistent. The amount of detail presented should be appropriate for the intended audience.

Proof by contradiction

Proof Techniques

- Direct Proof or Proof by Direct Method
  - Proof of those theorems that can be expressed in the form $\forall x\,(P(x) \rightarrow Q(x))$, D is the domain of discourse
  - Select a particular, but arbitrarily chosen, member a of the domain D
  - Show that the statement $P(a) \rightarrow Q(a)$ is true. (Assume that P(a) is true
  - Show that Q(a) is true
  - By the rule of Choose Method (Universal Generalization), $\forall x\,(P(x) \rightarrow Q(x))$ is true

Proof by contradiction

Proof Techniques

- Indirect Proof
  - The implication P → Q is equivalent to the implication (¬ Q → ¬P)
  - Therefore, in order to show that P → Q is true, one can also show that the implication (¬ Q → ¬ P) is true
  - To show that (¬ Q → ¬ P) is true, assume that the negation of Q is true and prove that the negation of P is true

Proof by contradiction

Proof Techniques

- Proof by Contradiction
  - Assume that the conclusion is not true and then arrive at a contradiction
  - Example: Prove that there are infinitely many prime numbers
  - Proof:
    - Assume there are not infinitely many prime numbers, therefore they are listable, i.e. $p_1, p_2, \ldots, p_n$
    - Consider the number $q = p_1 p_2 \ldots p_n + 1$. q is not divisible by any of the listed primes
    - Therefore, q is a prime. However, it was not listed.
    - Contradiction! Therefore, there are infinitely many primes.

Proof by Contradiction

A – We want to prove p.

We show that:

(1) $\neg p \rightarrow \mathbf{F}$ (i.e., a **False** statement , say $r \wedge \neg r$)

(2) We conclude that ¬p is false since (1) is **True** and therefore p is **True**.

B – We want to show $p \rightarrow q$

(1) Assume the negation of the conclusion, i.e., ¬q

(2) Use show that $(p \wedge \neg q) \rightarrow \mathbf{F}$

(3) Since $((p \wedge \neg q) \rightarrow \mathbf{F}) \Leftrightarrow (p \rightarrow q)$ (why?) we are done

150

Proof by contradiction

Example 1: Proof by Contradiction

Example:

Rainy days make gardens grow.
Gardens don't grow if it is not hot.
When it is cold outside, it rains.

Prove that it's hot.

Hmm. We will assume "not Hot" ≡ "Cold"

Let
R – Rainy day
G – Garden grows
H – It is hot

Given: $R \rightarrow G$
$\neg H \rightarrow \neg G$
$\neg H \rightarrow R$
Show: H

$$((R \rightarrow G) \wedge (\neg H \rightarrow \neg G) \wedge (\neg H \rightarrow R)) \rightarrow H$$
?

Proof by contradiction

Example1:Proof by contradiction

Given: $R \rightarrow G$
$\neg H \rightarrow \neg G$
$\neg H \rightarrow R$
Show: H

Aside: we assume it's either Hot or it is not Hot. Called the "law of excluded middle". In certain complex arguments, it's not so clearly valid. (hmm…) This led to "constructive mathematics" and "intuitionistic mathematics".

1. $R \rightarrow G$	Given
2. $\neg H \rightarrow \neg G$	Given
3. $\neg H \rightarrow R$	Given
4. $\neg H$	assume to the contrary
5. R	MP (3,4)
6. G	MP (1,5)
7. $\neg G$	MP (2,4)
8. $G \wedge \neg G$	contradiction

$\therefore H$

Automatic Theorem proving

String of Formulas: A string of formulas is defined as follows.

A) Any formula is a string of formulas

B) If α and β are strings of formulas, then

α , β and β, α are strings of formulas.

C) Only those strings which are obtained by steps (A) and (B) are strings of formulas, with the exception of empty string which is also a string of formulas.

Sequents : If α and β are strings of formulas, then $\alpha \overset{s}{\rightarrow} \beta$ is called a sequent in which α is called antecedent and β is called consequent.

Sequents (Contd.,)

- A sequent $\alpha \xrightarrow{S} \beta$ is true <u>if and only if</u> either at least one of the formulas of the antecedent is false or at least one of the formulas of the consequent is true.
- Thus

  $A, B, C \xrightarrow{S} D, E, F$ is true iff $(A \wedge B \wedge C) \rightarrow (D \vee E \vee F)$ is true .
- $\alpha \overset{S}{\Rightarrow} \beta$ means that $\alpha \xrightarrow{S} \beta$ is true.

Axioms –theorems -Rules

- Ex: $A,B,C \rightarrow P,B,R$ is an axiom.

  If $\alpha \xrightarrow{S} \beta$ is an axiom, then $\alpha \overset{S}{\Rightarrow} \beta$.

- Theorem: The following sequents are theorems of our system.

  a) Every axiom is a theorem .

  b) If a sequent α is a theorem and a sequent β results from α through the use of one of the 10 rules of the system which are given below, then β is a theorem.

  c) Sequents obtained by (a) and (b) are the only theorems.

- Rules: The following rules are used to combine formulas withinstrings by introducing connectives.Corresponding to each of the connectives there are two rules, one for introducing the connective in the antecedent and the other for its introduction in the consequent.

Rules for Automatic Theorem proving

- Antecedent rules:
- Rule $\sim \Rightarrow$: If $\alpha, \beta \overset{s}{\Rightarrow} X, \gamma$ then $\alpha, \sim X, \beta \overset{s}{\Rightarrow} \gamma$
- Rule $\wedge \Rightarrow$: If $X, Y, \alpha, \beta \overset{s}{\Rightarrow} \gamma$ then $\alpha, X \wedge Y, \beta \overset{s}{\Rightarrow} \gamma$
- Rule $\vee \Rightarrow$: If $X, \alpha, \beta \overset{s}{\Rightarrow} \gamma$ and $Y, \alpha, \beta \overset{s}{\Rightarrow} \gamma$,
  then $\alpha, X \vee Y, \beta \overset{s}{\Rightarrow} \gamma$
- Rule $\rightarrow \Rightarrow$: If $Y, \alpha, \beta \overset{s`}{\Rightarrow} \gamma$ and $\alpha, \beta \overset{s}{\Rightarrow} X, \gamma$
  then $\alpha, X \rightarrow Y, \beta \overset{s}{\Rightarrow} \gamma$
- Rule $\leftrightarrow \Rightarrow$: If $X, Y, \alpha, \beta \overset{s}{\Rightarrow} \gamma$ and $\alpha, \beta \Rightarrow X, Y, \gamma$
  then $\alpha, X \leftrightarrow Y, \beta \overset{s}{\Rightarrow} \gamma$

Automatic Theorem proving

Rules for Automatic Theorem proving (contd.,)

- Consequent rules:
- Rule $\Rightarrow\sim$: If $X, \alpha \overset{s}{\Rightarrow} \beta, \gamma$ then $\alpha \overset{s}{\Rightarrow} \beta, \sim X, \gamma$
- Rule $\Rightarrow\wedge$: If $\alpha \overset{s}{\Rightarrow} X, \beta, \gamma$ and $\alpha \overset{s}{\Rightarrow} Y, \beta, \gamma$ then $\alpha \overset{s}{\Rightarrow} \beta, X \wedge Y, \gamma$
- Rule $\Rightarrow\vee$: If $\alpha \overset{s}{\Rightarrow} X, Y, \beta, \gamma$ then $\alpha \overset{s}{\Rightarrow} \beta, X \vee Y, \gamma$
- Rule $\Rightarrow\rightarrow$: If $X, \alpha \overset{s}{\Rightarrow} Y, \beta, \gamma$ and $\alpha \overset{s}{\Rightarrow} \beta, X \rightarrow Y, \gamma$
- Rule $\Rightarrow\leftrightarrow$: If $X, \alpha \overset{s}{\Rightarrow} Y, \beta, \gamma$ and $Y, \alpha \overset{s}{\Rightarrow} X, \beta, \gamma$ then $\alpha \overset{s}{\Rightarrow} \beta, X \leftrightarrow Y, \gamma$

Examples

Ex: Using Automatic theorem proving, Show that $P \vee Q$ follows from P.

Solution: we need to show that

(1) $\overset{S}{\Rightarrow} P \rightarrow (P \vee Q)$

(1) if (2) $P \overset{S}{\Rightarrow} (P \vee Q)$ (By the rule, $\Rightarrow \rightarrow$)

(2) if (3) $P \overset{S}{\Rightarrow} P, Q$ (By the rule, $\Rightarrow \vee$)

Now, (3) is an axiom

Hence, the theorem (1) follows.

Automatic Theorem proving

Ex: Using Automatic theorem proving,
Show that P does not follow from $P \vee Q$.

- Solution: Assume

$(1) \quad \overset{s}{\Rightarrow} (P \vee Q) \rightarrow P$

(1) if $(2) \quad (P \overset{s}{\vee} Q) \Rightarrow P \qquad$ (By the rule, $\Rightarrow \rightarrow$)

(2) if $(3) \quad P \Rightarrow P$ and $(4) \quad Q \overset{s}{\Rightarrow} P \quad$ (By the rule, $\vee \Rightarrow$)

Note that (3)is an axiom, but (4) is not.

Hence, P does not follow from $P \vee Q$.

Automatic Theorem proving

Ex: Using Automatic theorem proving, prove the following (a)
$\{P \wedge (\sim P \wedge Q)\} \rightarrow R$
(b) $R \rightarrow \{P \vee (\sim P \vee Q)\}$

Solution: (a) To show (1) $\overset{s}{\Rightarrow} \{P \wedge (\sim P \wedge Q)\} \rightarrow R$

(1) if (2) $\{P \wedge (\sim P \wedge Q)\} \overset{s}{\Rightarrow} R$ (By using the rule, $\Rightarrow\rightarrow$, twice)

(2) if (3) $\{P, \sim P, Q)\} \overset{s}{\Rightarrow} R$ (By the rule, $\wedge \Rightarrow$)

(3) if (4) $\{P,Q)\} \overset{s}{\Rightarrow} , R\}$ {P (By the rule, $\sim \Rightarrow$) Now (4) is an axiom , therefore the result follows.

(b) To show (1) $\overset{s}{\Rightarrow} R \rightarrow \{P \vee (\sim P \vee Q)\}$

(1) if (2) $R \overset{s}{\Rightarrow} \{P \vee (\sim P \vee Q)\}$ (By the rule, $\Rightarrow\rightarrow$)

(2) if (3) $R \overset{s}{\Rightarrow} \{P, \sim P, Q)\}$ (By using the rule, $\Rightarrow \vee$, twice)

(3) if (4) $\{R,P\} \overset{s}{\Rightarrow} \{P, Q)\}$ (By using the rule, $\Rightarrow \sim$)

Now (4) is an axiom , therefore the result follows.

Automatic Theorem proving

Ex: Using Automatic theorem proving, Show that

$$\overset{s}{\Rightarrow} \{\sim Q \wedge (P \rightarrow Q)\} \rightarrow \sim P$$

- Solution: (1) $\overset{s}{\Rightarrow} \{\sim Q \wedge (P \rightarrow Q)\} \rightarrow \sim P$
- (1) if (2) $\{\sim Q \wedge (P \rightarrow Q)\} \overset{s}{\Rightarrow} \sim P$ (By the rule, $\Rightarrow\rightarrow$)
- (2) if (3) $\{\sim Q , (P \rightarrow Q)\} \overset{s}{\Rightarrow} \sim P$ (By the rule, $\wedge \Rightarrow$)
- (3) if (4) $(P \rightarrow Q) \overset{s}{\Rightarrow} \sim P, Q$ (By the rule, $\sim \Rightarrow$)
- (4) if (5) $Q \overset{s}{\Rightarrow} \sim P, Q$ and

  (6) $\overset{s}{\Rightarrow} P, \sim P, Q$ (By the rule, $\rightarrow \Rightarrow$)
- (5) if (7) $P, Q \overset{s}{\Rightarrow} Q$ (By the rule, $\rightarrow \sim$)
- (6) if (8) $P \Rightarrow P, Q$ (By the rule, $\rightarrow \sim$)
- Now (7) and (8) are axioms, hence the theorem (1) follows.

References

- D S Chandra shekaraiah, “Mathematical Foundations of Computer Science (Discrete Structures)”, Prism Books Pvt. Ltd., 2nd Reprint, 2007

MODULE 2
RELATIONS, FUNCTIONS AND LATTICES

Running outcomes

CLO 1:Identify ordered pairs to form a binary relation from the given sets.

CLO 2: Identify the properties of relations to check for equivalence relation and partial order relation and compute relations using operations on relations.

CLO 3:Construct a hasse diagram to recognize the relevant partial ordered sets from the given binary relation.

CLO 4:Describe the types of functions (one to one,on-to, bijective, Identity and constant function).

CLO 5:Implement the concept of the inverse and recursive functions to get an optimized solution for an appropriate problem.

Running outcomes

CLO 6: Use the concept of lattices (Greatest Lower Bound (GLB) and Least Upper Bound (LUB) to represent a defined finite set in multi-dimension applications.

CLO 7: Explain about the properties and types of lattices (bounded and distributive lattice).

Relation

If we want to describe a relationship between elements of two sets A and B, we can use **ordered pairs** with their first element taken from A and their second element taken from B.

Since this is a relation between **two sets**, it is called a **binary relation**.

Definition: Let A and B be sets. A binary relation from A to B is a subset of A´B.

In other words, for a binary relation R we have R Í A´B. We use the notation aRb to denote that (a, b)ÎR and aRb to denote that (a, b)ÏR.

When (a, b) belongs to R, a is said to be **related** to b by R.

Example: Let P be a set of people, C be a set of cars, and D be the relation describing which person drives which car(s).

P = {Carl, Suzanne, Peter, Carla}, C = {Mercedes, BMW, tricycle}

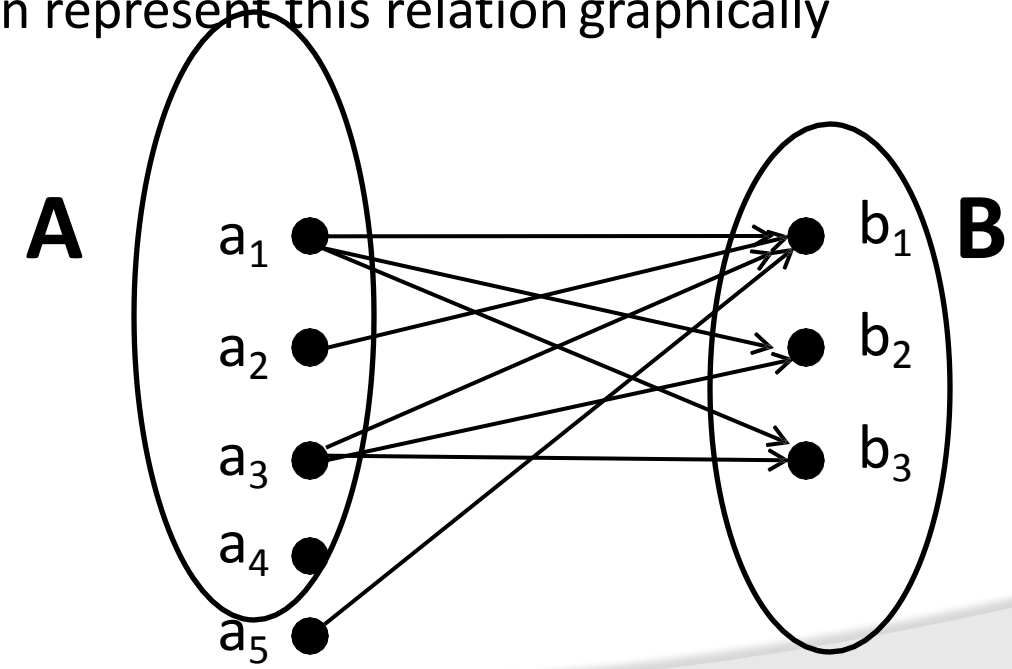
D = {(Carl, Mercedes), (Suzanne, Mercedes), (Suzanne, BMW), (Peter, tricycle)}

This means that Carl drives a Mercedes, Suzanne drives a Mercedes and a BMW, Peter drives a tricycle, and Carla does not drive any of these vehicles.

Relations: Representation

- To represent a relation, we can enumerate every element of R
- Example
  - Let A={a_1,a_2,a_3,a_4,a_5} and B={b_1,b_2,b_3}
  - Let *R* be a relation from A to B defined as follows

    R={(a_1,b_1),(a_1,b_2),(a_1,b_3),(a_3,b_1),(a_3,b_2),(a_3,b_3),(a_5,b_1)}
- We can represent this relation graphically



Properties

- We will study several properties of relations
  - Reflexive
  - Symmetric
  - Transitive
  - Antisymmetric
  - Asymmetric

Properties: Reflexivity

- In a relation on a set, if all ordered pairs (a,a) for every $a \in A$ appears in the relation, R is called reflexive
- **Definition**: A relation *R* on a set A is called reflexive iff

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

Example

- Recall the relations below, which is reflexive?

$$R_1 = \{ (a,b) \mid a \leq b \}$$

$$R_2 = \{ (a,b) \mid a,b \in N,\ a/b \in Z \}$$

$$R_3 = \{ (a,b) \mid a,b \in N,\ a-b=2 \}$$

- R_1 is reflexive since for every $a \in N$, $a \leq a$
- R_2 is reflexive since $a/a=1$ is an integer
- R_3 is not reflexive since $a-a=0$ for every $a \in N$

Properties: Symmetry

- **Definitions**:
  - A relation R on a set A is called <u>symmetric</u> if

$$\forall a,b \in A\ (\ (b,a) \in R \Leftrightarrow (a,b) \in R\ )$$

  - A relation R on a set A is called <u>antisymmetric</u> if

$$\forall a,b \in A\ [(a,b) \in R \wedge (b,a) \in R \Rightarrow a=b]$$

- In a <u>symmetric</u> relation $aRb \Leftrightarrow bRa$
- In an <u>antisymmetric</u> relation, if we have aRb and bRa hold only when $a=b$
- An antisymmetric relation is not necessarily a reflexive relation
- A relation can be
  - both symmetric and antisymmetric
  - or neither
  - or have one property but not the other
- A relation that is not symmetric is not necessarily asymmetric

Properties: Transitivity

- **Definition**: A relation R on a set A is called transitive if whenever $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$ for all $a,b,c \in A$

$$\forall a,b,c \in A\ ((aRb) \wedge (bRc)) \Rightarrow aRc$$

- Is the relation $R=\{(x,y) \in R^2 \mid x \leq y\}$ transitive?
- Yes, it is transitive because xRy and $yRz \Rightarrow x \leq y$ and $y \leq z \Rightarrow x \leq z \Rightarrow xRz$
- Is the relation $R=\{(a,b),(b,a),(a,a)\}$ transitive?

  No, it is not transitive because bRa and aRb but bRb

Equivalence

Let E be a relation on set A.

E is an *equivalence relation* if & only if it is:

- Reflexive
- Symmetric
- Transitive.

Examples

- a E b when a mod 5 = b mod 5. (Over **N**)
  - (i.e., a ≡ b mod 5)
- a E b when a is a sibling of b. (Over humans)

Equivalence Class

Let E be an equivalence relation on A.

We denote aEb as $a \sim b$. (sometimes, it is denoted $a \equiv b$)

The equivalence class of a is $\{ b \mid a \sim b \}$, denoted [a].

What are the equivalence classes of the example equivalence relations?

For these examples:

Do distinct equivalence classes have a non-empty intersection?

Does the union of all equivalence classes equal the underlying set?

Partition

A *partition of set S* is a *set of nonempty subsets*,

$S_1, S_2, \ldots, S_n$, of S such that:

1. $\forall i \, \forall j \, (i \neq j \rightarrow S_i \cap S_j = \emptyset)$.

2. $S = S_1 \cup S_2 \cup \ldots \cup S_n$.

Let E be an equivalence relation on S.

E's equivalence classes partition S.

For any partition P of S, there is an equivalence relation on S

whose equivalence classes form partition P.

Example: The relation “is equal to”, denoted “=”, is an equivalence relation on the set of real numbers since for any $x, y, z \in R$:

1. (Reflexivity) $x = x$,
2. (Symmetry) if $x = y$ then $y = x$,
3. (Transitivity) if $x = y$ and $y = z$ then $x = z$.

Transitivity

A relation R on set A is said to be transitive relation if whenever
$(a,b) \in R$ and $(b,c) \in R$ then
$(a,c) \in R$ for all $(a,b,c) \in A$. It follows that R is not transitive. if their exists
$(a,b,c) \in R$ such that $(a,b) \in R$ and $(b,c) \in R$ but $(a,c) \in R$

example:
if we consider a set A={1,2,3} the relation
R1={(1,1)(1,2)(2,3)(1,3)(3,1)(3,2)}
R2={(1,2)(2,3)(1,3)(3,1)}
here in the above example R1 is transitive and R2 is not transitive

Transitivity

A relation is transitive if, for every $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$

If $a < b$ and $b < c$, then $a < c$

Thus, < is transitive

If $a = b$ and $b = c$, then $a = c$

Thus, = is transitive

Transitivity example

- Let A={1,2,3,4} determine the nature of the following relations on A

R1={(1,1)(1,2)(2,1)(2,2)(3,3)(3,4)(4,3)(4,4)}

R2={(1,2)(1,3)(3,1)(1,1)(3,3)(3,2)(1,4)(4,2)(3,4)}

Here in the above example R1 is transitive because {(1,2)(2,1)(1,1)}

And R2 is also transitive because{(1,3)(3,1)(1,1)}

Transitivity examples

Consider isAncestorOf()

- Let Alice be Bob's parent, and Bob be Claire's parent
- Thus, Alice is an ancestor of Bob, and Bob is an ancestor of Claire
- Thus, Alice is an ancestor of Claire
- Thus, isAncestorOf() is a transitive relation

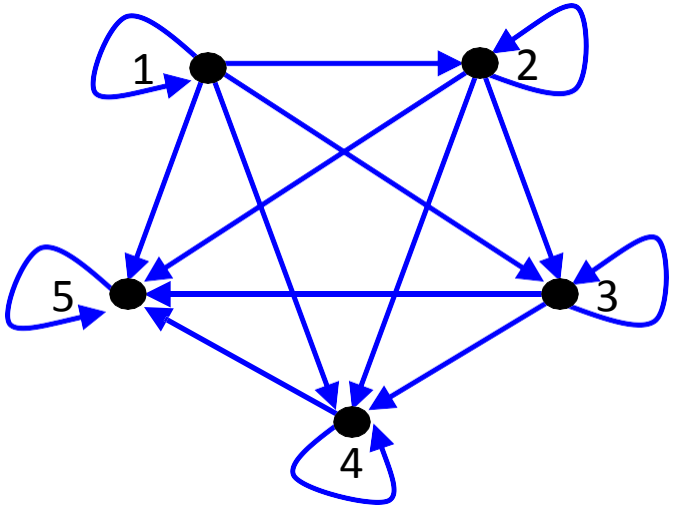
Consider isParentOf()

- Let Alice be Bob's parent, and Bob be Claire's parent
- Thus,Alice is a parent of Bob, and Bob is a parent of Claire
- However, Alice is *not* a parent of Claire
- Thus, isParentOf() is *not* a transitive relation

Consider an transitive relation: ≤

One which if *a* is related to *b* and *b* is related to *c* then *a* is related to *c* for all (*a*,*b*), (*b*,*c*) and (*a*,*c*)

Let A = { 1, 2, 3, 4, 5 }



- A digraph is transitive if, for there is a edge from *a* to *c* when there is a edge from *a* to *b* and from *b* to *c*

Partial Order

Definitions:

A relation R on a set S is called a partial order if it is

Reflexive

Antisymmetric

Transitive

A set S together with a partial ordering R is called a partially ordered set (poset, for short) and is denote (S,R)

Partial orderings are used to give an order to sets that may not have a natural one

In our renovation example, we could define an ordering such that $(a,b) \in R$ if 'a must be done before b can be done'

Partial Orderings: Notation

- We use the notation:
  - apb, when $(a,b) \in R$
  - apb, when $(a,b) \in R$ and $a \neq b$
- The notation p is not to be mistaken for "less than" (p versus $\leq$)
- The notation p is used to denote <u>any</u> partial ordering

Partial ordering examples

- Show that ≥ is a partial order on the set of integers
  - It is reflexive: $a \geq a$ for all $a \in \mathbf{Z}$
  - It is antisymmetric: if $a \geq b$ then the only way that $b \geq a$ is when $b = a$
  - It is transitive: if $a \geq b$ and $b \geq c$, then $a \geq c$

- Note that ≥ is the partial ordering on the set of integers
- ($\mathbf{Z}$, ≥) is the partially ordered set, or poset

Anti symmetric:

- A relation R on set A is said to be Anti symmetric relation if whenever (a,b)€R and (b,a)€R then a=b
- It follows that R is not anti symmetric if their exists (a,b)€A such that (a,b)€R and (b,a)€R then a≠b

Example

Let A={1,2,3}

R1={(1,1)(2,2)}

R2={(1,2)(2,1)(2,3)}

Solution:

R1 is both symmetric and anti symmetric

R2 is neither symmetric nor anti symmetric

Compatibility:

- A relation R on set A is said to be compatability relation which contains both reflecive and symmetric relation
  Reflexive: if (a,a)€R for all a€a
  Symmetric:(b,a)€R whenever (a,b)€R for all (a,b)€A

Example

R1={(1,1)(2,2)(3,3)(1,3)(3,1)}

R2={(1,1)(2,2)(1,2)(2,1)}

R3={(1,1)(2,2)(3,3)(1,2)(2,3)} are the relations on set A={1,2,3}

Solution:

R1 is compatibility relation because it is reflexive{(1,1)(2,2)(3,3) A}and symmetric

{(1,3)(3,1)€A}

R2 is not compatibility relation because R2 is symmetric but not reflexive

R3 is reflexive but not symmetric so it is not compatibility

Hasse Diagrams

Hasse diagrams are meant to present partial order relations in equivalent but somewhat simpler forms by removing certain deducible ``noncritical'' parts of the relations.. For better motivation and understanding, we'll introduce it through the following examples.

Hasse Diagrams

Definitions:

A relation *R* on a set *S* is called a partial order if it is

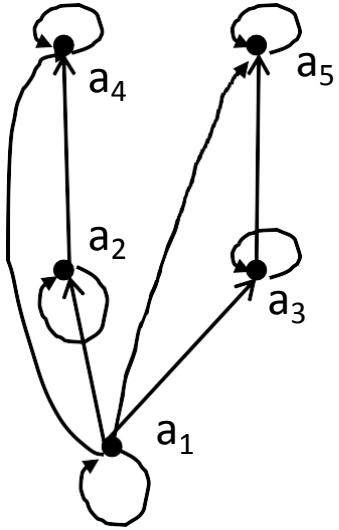
- Reflexive
- Antisymmetric
- Transitive

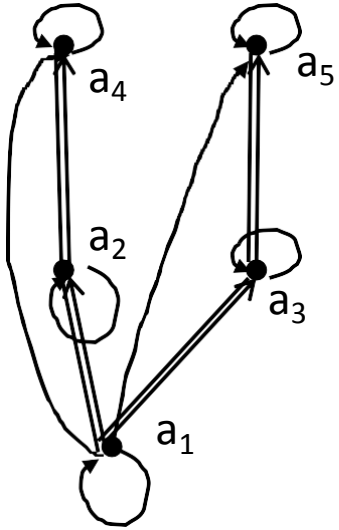
A set S together with a partial ordering R is called a partially ordered set (poset, for short) and is denote (*S*,*R*)

Partial orderings are used to give an order to sets that may not have a natural one

In our renovation example, we could define an ordering such that (a,b)$\in$*R* if ‘a must be done before b can be done’

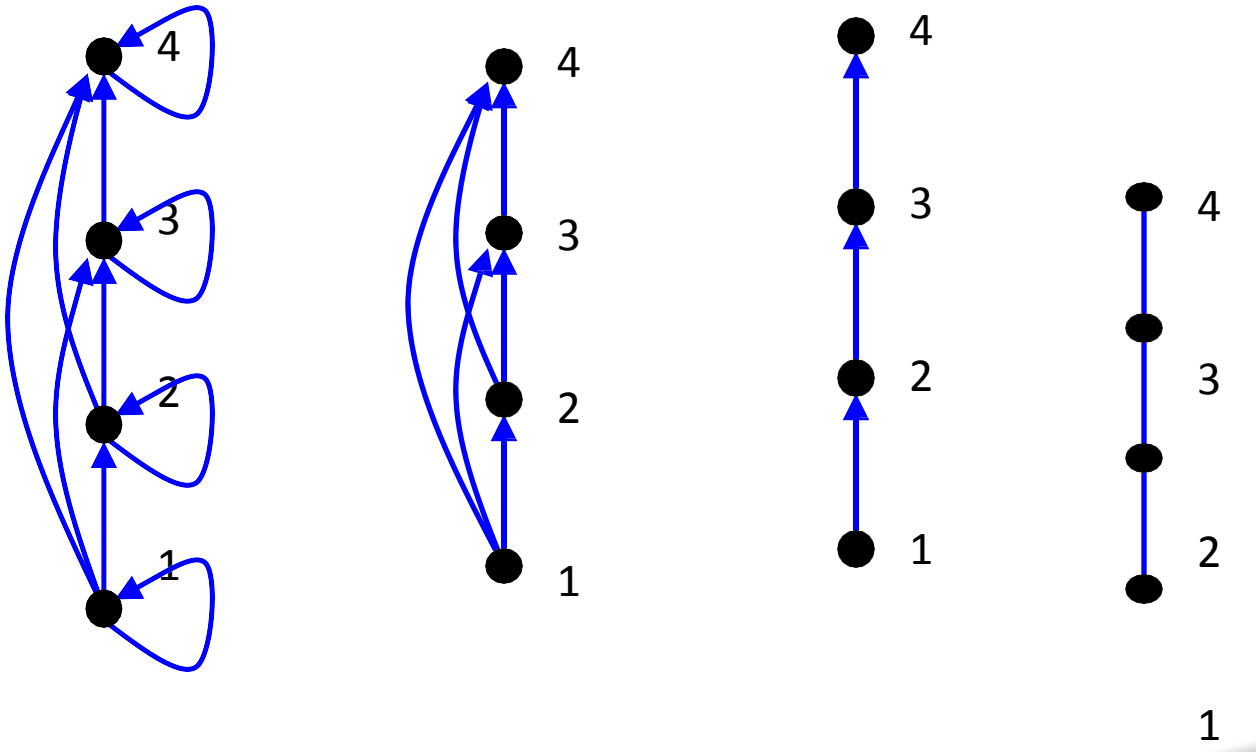
Hasse Diagram: Example





Hasse Diagrams

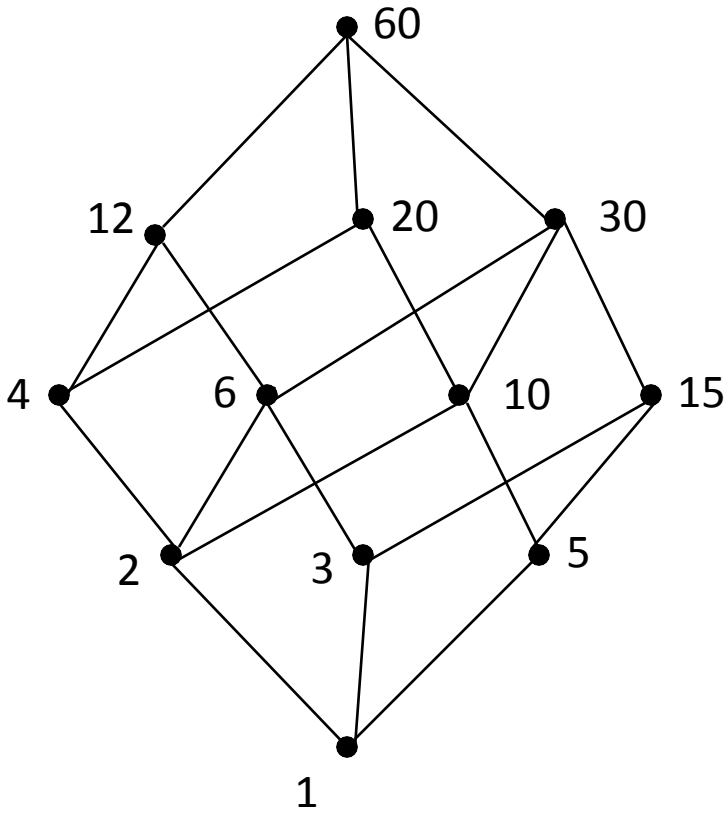
- Consider the graph for a finite poset $(\{1,2,3,4\},\leq)$
- When we KNOW it's a poset, we can simplify the graph



Called the Hasse diagram

Hasse Diagrams: Example (1)

- Of course, you need not always start with the complete relation in the partial order and then trim everything.
- Rather, you can build a Hasse Diagram directly from the partial order
- Example: Draw the Hasse Diagram
  - for the following partial ordering: {(a,b) | a|b }
  - on the set {1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60}
  - (these are the divisors of 60 which form the basis of the ancient Babylonian base-60 numeral system)

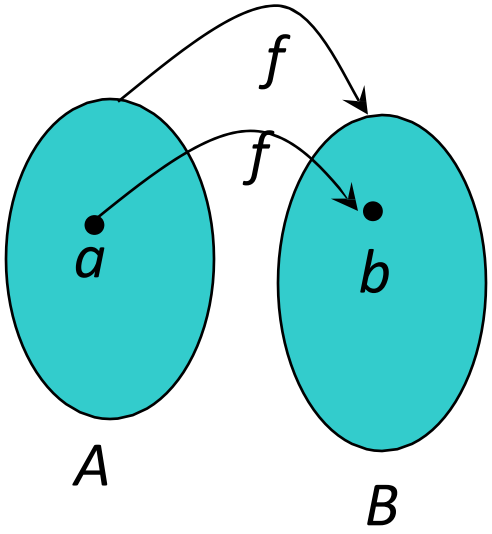

60
12
20
30
4
6
10
15
2
3
5
1

Functions

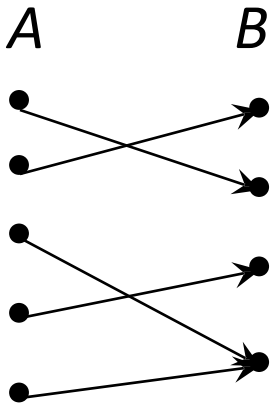
Given any sets A, B, a function f from *(or "mapping") A to B* ($f: A \rightarrow B$) is an assignment of **exactly one** element $\boldsymbol{f(x) \in B}$ to each element $\boldsymbol{x \in A}$.

Graphical Representations

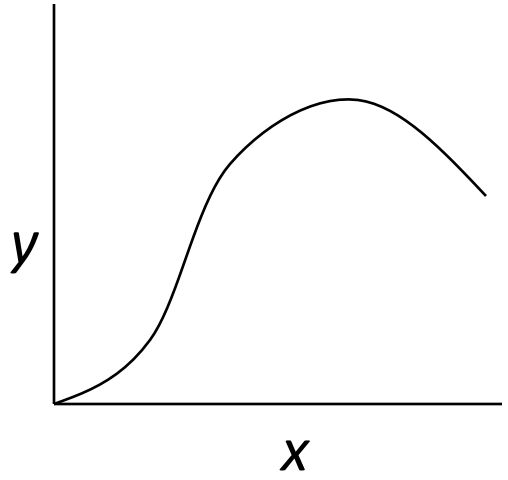
- Functions can be represented graphically in several ways:



Like Venn diagrams



Graph



Plot

Some Function Terminology

- If $f{:}A \to B$, and $f(a)=b$ (where $a \in A$ & $b \in B$), then:
  - A is the *domain* of f.
  - B is the *codomain* of f.
  - b is the *image* of a under f.
  - a is a *pre-image* of b under f.
    - In general, b may have more than one pre-image.
  - The *range* $R \subseteq B$ of f is $\{b \mid \exists a\ f(a)=b\}$.

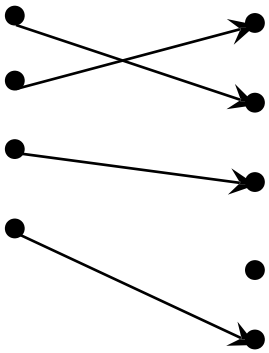
Types of functions

One-to-One Function

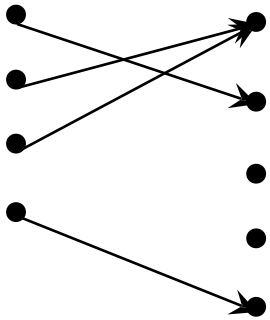
- A function is *one-to-one (1-1)*, or *injective*, or *an injection*, iff every element of its range has **only one** pre-image.
- Only one element of the domain is mapped to any given one element of the range.
  - Domain & range have same cardinality. What about codomain?

One-to-One Illustration

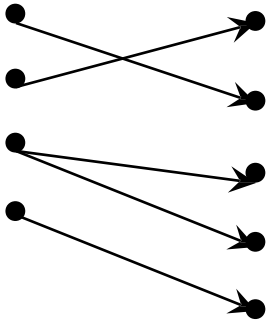
- Graph representations of functions that are (or not) one-to-one:



One-to-one



Not one-to-one



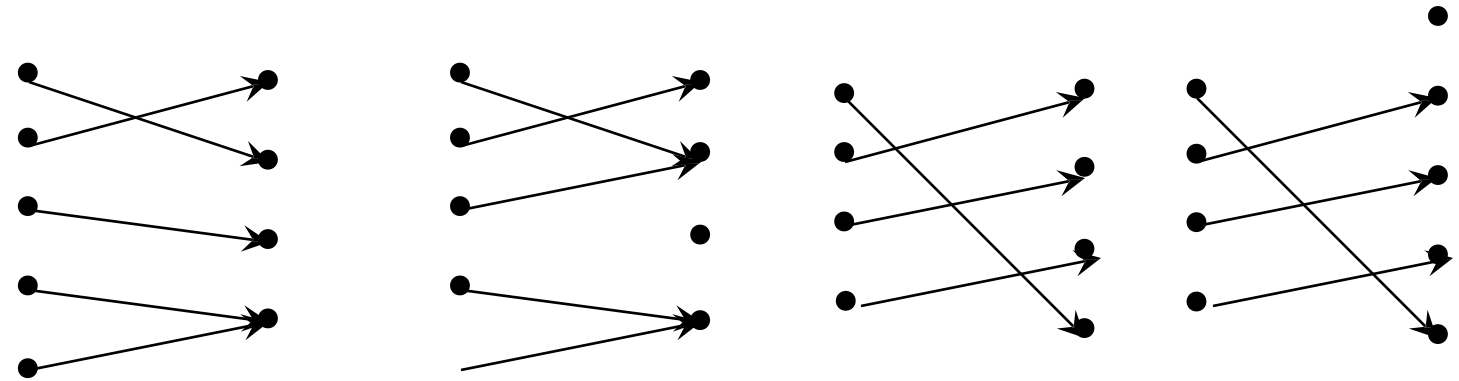
Not even a function!

Onto (Surjective) Functions

- A function $f:A \to B$ is *onto* or *surjective* or *a surjection* iff its **range is equal to its codomain** ($\forall b \in B, \exists a \in A: f(a)=b$).
- An *onto* function maps the set A onto (over, covering) the *entirety* of the set B, not just over a piece of it.
  - *e.g.*, for domain & codomain **R**, x^3 is onto, whereas x^2 isn't. (Why not?)

Illustration of Onto

- Some functions that are or are not *onto* their co domains:



Bijections

- A function *f* is *a one-to-one correspondence*, or *a bijection*, or *reversible*, or *invertible*, iff **it is both one-to-one and onto**.

Inverse of a Function

For bijections $f:A \to B$, there exists an *inverse* of f, written $f^{-1}:B \to A$, which is the unique function such that:

$$f^{-1} \circ f = I$$

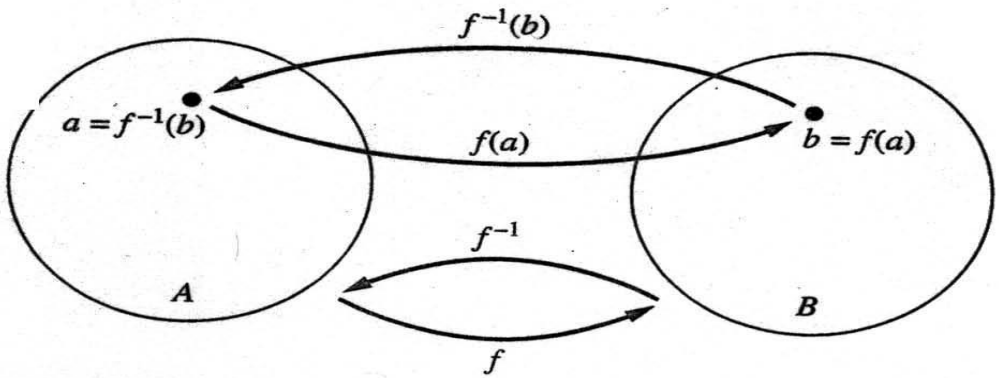


FIGURE 6 The Function f^{-1} Is the Inverse of Function f.

Inverse Function

- EXAMPLE

  {(2, 3), (5, 0), (-2, 4), (3, 3)}

  Inverse = switch the x and y, (domain and range)

  I = {(3, 2), (0, 5), (4, -2), (3, 3)}

{(4, 7), (1, 4), (9, 11), (-2, -1)}

Inverse = ?

I = {(7, 4), (4, 1), (11, 9), (-1, -2)}

- Given $f(x) = 3x - 4$, find its inverse ($f^{-1}(x)$).

  $y = 3x - 4$

  switch. $x = 3y - 4$

  solve for y. $x + 4 = 3y$

  $y = (x + 4)/3$

- Given h(x) = -3x + 9, find it's inverse.

  $y = -3x + 9$

  $x = -3y + 9$

  $x - 9 = -3y$

  $(x - 9) / -3 = y$

Composite Functions

- Composite functions are functions that are formed from two functions $f(x)$ and $g(x)$ in which the output or result of one of the functions is used as the input to the other function. Notation ally we express composite functions

$$fog(x) \text{ or } f(g(x)$$

In this case the result or output from g becomes the input to f.

Example 1

Given $f(x) = x^3$ $g(x) = x + 2$ the composite function

$$f \circ g(x) = f(g(x)) = f(x+2) = (x+2)^3 = x^3 + 6x^2 + 8x + 8$$

Replace $g(x)$ with $x+2$

Replace the variable x in the f function with $x+2$

Expand

Problem 1

For the functions $f(x)=\frac{1}{x}$ $g(x)=3x-5$ find

$$f \circ g(x)$$

$$f(g(x)) = f(3x-5) = \frac{1}{3x-5}$$

$$g \circ f(x)$$

$$g(f(x)) = g\left(\frac{1}{x}\right) = 3\left(\frac{1}{x}\right) - 5 = \frac{3}{x} - 5$$

Breaking Composite Functions Apart

There are instances when we want to take a composite function and break it into its component parts. In this case we'll be looking for an "inner" function and an "outer" function. To help you find the inner function look for expressions in parentheses, or under radical signs or in denominators.

Example 1

Break the composite function $h(x)=(5-4x)^2$ into two smaller functions $f(x)$ and $g(x)$ so that $h(x)=f(g(x))$

$h(x)=(5-4x)^2$

$g(x)=5-4x$

$f(x)=x^2$

Inner part

Outer part

Recursive function

- The term "recursive function" is often used informally to describe any function that is defined with recursion. There are several formal counterparts to this informal definition, many of which only differ in trivial respects.

- Kleene (1952) defines a "partial recursive function" of nonnegative integers to be any function that is defined by a noncontradictory system of equations whose left and right sides are composed from
- function symbols (for example, , , , etc.), (2) variables for nonnegative integers (for example, , , , etc.), (3) the constant 0, and (4) the successor function .
-

- defines to be the function that computes the product of and .
- Note that the equations might not uniquely determine the value of for every possible input, and in that sense the definition is "partial." If the system of equations determines the value of f for every input, then the definition is said to be "total." When the term "recursive function" is used alone, it is usually implicit that "total recursive function" is intended. Note that some authors use the term "general recursive function to mean partial recursive function, although others use it to mean "total recursive function."
- The set of functions that can be defined recursively in this manner is known to be equivalent to the set of functions computed by Turing machines and by the lambda calculus.

Some more examples of functions

Example:

Let f:R->R and g:R->R and h:R->R is defined as f(x)=2x+1 ∀ X€ R h(x)=2x-2 ∀ X€ R and g(x)=3x+2 then find

- fog
- gof
- fo(goh)
- fo(hog)
- go(foh)
- go(fof)
- ho(gof)

Solution

f(x)=2x+1

g(x)=3x+2

h(x)=2x-2

fog(x)=f(g(x))

=f(3x+2)

=2(3x+2)+1

= 6x+4+1

= 6x+5

- 2.gof(x)=g(f(x))

  =g(2x+1)

  =3(2x+1)+2

  =6x+3+2

  =6x+5

3.fo(goh)=f(g(h(x)))

=f(g(2x-2))

=f(3(2x-2)+2)

=f(6x-4)

=2(6x-4)+1

=12x-8+1

=12x-7

$$fo(hog)=f(h(g(x)))$$
$$=f(h(3x+2))$$
$$=f(2(3x+2)-2)$$
$$=f(6x+4-2)$$
$$=f(6x+2)$$
$$=2(6x+2)+1$$
$$=12x+4+1$$
$$=12x+5$$

$$go(foh) = g(f(h(x)))$$
$$= g(f(2x-2))$$
$$= g(2(2x-2)+1)$$
$$= g(4x-4+1)$$
$$= g(4x-3)$$
$$= 3(4x-3)+2$$
$$= 12x-9+2$$
$$= 12x-7$$

6. go(fof)=g(f(f(x))

=g(f(2x+1))

=g(2(3x+2)-2)

=g(6x+4-2)

=g(6x+2)

=2(6x+2)+1

=12x+4+1

=12x+5

7. ho(gof)=h(g(f(x)))

=h(g(2x+1))

=h(3(2x+1)+2)

=h(6x+3+2)

=h(6x+5)

=2(6x+5)-2

=12x+10-2

=12x+8

LATTICE

Lattice introduced as poset (p,≤) in which every pair has a greatest lower bound(GLB) and least upper bound(LUP) is called lattice.

GLB:-(greatest lower bound) : greatest lower bound of(a,b)=a*b(or) a.b (or) gcd of a and b (or) a∩b

Example:

GLB of (2,3)=6

Gcd of (2,3) =6

LUB:-(least upper bound): least upper bound of(a,b)=a+b=a b=lcm of a and b=aUb

EXAMPLE

1. Let p={2,3,6,12} then prove that (p,≤) this notation is lattice(or) not

Solution:

Given that p=(2,3,6,12}

Consider one pair(2,3) from set p

GLB of(2,3) =1 p means it is not GLB from set p

LUB of (2,3)=6 p then (p,≤) is not a lattice

2. if A is finite set and p(a) is power set then prove that (p(a), ≤) is lattice for

   i) A={a}

   ii) A={a,b}

Solution:

A={a}

P(a)={{∅},{a}}

GLB of (∅,{a})=∅∩{a}

=∅ p(a)

Therefore ($\varnothing$, {a}) has a GLB

P(a)={{$\varnothing$},{a}}

LUB of ($\varnothing$,{a})=$\varnothing \cap$ {a}

={a} p(a)

Therefore ($\varnothing$, {a}) has a LUB

(p(a), ≤) is a lattice

A={a,b}

P(a)={{∅},{a},{b},{a,b}}

GLB of (∅,{a})=∅∩{a}

=∅ p(a)

Therefore (∅, {a}) has a GLB

LUB of (∅,{a})=∅U{a}

={a} p(a)

Therefore (ø, {a}) has a LUB

Therefore (ø, {a}) has GLB and LUB-----→1

GLB of (ø,{b})=ø∩{b}

=ø p(a)

Therefore (⊘, {b}) has a GLB

LUB of (⊘,{b})=⊘U{b}

={b} p(a)

Therefore (⊘, {b}) has a LUB

Therefore (⊘, {b}) has GLB and LUB-----→2

GLB of (⊘,{a,b})=⊘∩{a,b}

=⊘ p(a)

Therefore (⊘, {a,b}) has a GLB

LUB of (⊘,{a,b})=⊘U{a,b}

={a,b} p(a)

Therefore (⊘, {a,b}) has a LUB

Therefore (⊘, {a,b}) has GLB and LUB-----→3

GLB of ({a},{b})={a}∩{b}

=(a,b} p(a)

Therefore ({a}{b}) has a GLB

LUB of ({a},{b})={a}U{b}

={a,b} p(a)

Therefore ({a},{b}) has a LUB

Therefore ({a},{b}) has GLB and LUB-----→4

GLB of ({b},{a,b})={b}∩{a,b}

=(b} p(a)

Therefore has ({b},{a,b}) a GLB

LUB of ({b},{a,b})={b}U{a,b}

={a,b} p(a)

Therefore ({b},{a,b})has a LUB

Therefore ({b},{a,b}) has GLB and LUB-----→5

GLB of ({b},{a,b})={a}∩{a,b}

={a} p(a)

Therefore has ({a},{a,b}) a GLB

LUB of ({a},{a,b})={a}U{a,b}

={a,b} p(a)

Therefore ({a},{a,b})has a LUB

Therefore ({a},{a,b}) has GLB and LUB-----→6

From equation 1,2,3,4,5,6 (p(a),≤) is lattice

PROPERTIES OF LATTICE

PROPERTIES OF LATTICE

We shall discuss some properties of two binary operations of meet and join denoted by $\otimes$ *and* $\oplus$ on lattice $(L, \leq)$.for all $a,b,c \in L$ WE HAVE

1. $a*a=a$	$a \oplus a=a$	(idempotent)
2. $a*b=b*a$	$a \oplus b=b \oplus a$	(commutative)
3. $(a*b)*c=a*(b*c)$	$(a \oplus b) \oplus c=a \oplus (b \oplus c)$	(associative)
4.$a*(a \oplus b)=a$	$a \oplus (a*b)=a$	(absorption law)

LATTICE AS ALGEBRAIC SYSTEM

LATTICE AS ALGEBRAIC SYSTEM:

A lattice is an algrbraic system $(L, *, \oplus)$ with two binary operations $*, \oplus$ on L which are both commutative and associative and satisfy the absorption law.

Here consider the below

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

we have replaced the second a in a*a by $a \oplus (a*a)$ and then from fourth law we obtained a in the second stepthe identity $a \oplus a=a$ can be proved in a similar manner or by the principle of duality

let us define a relation R on L such that for $a.b \in L$

$aRb \Leftrightarrow a*b=a$

we have replaced the second a in a*a by a⊕(a*a) and then from fourth law we obtained a in the second stepthe identity a⊕a=a can be proved in a similar manner or by the principle of duality

let us define a relation R on L such that for a,b ∈ L

aRb⇔a*b=a

for any a ∈ L,a*a=a, so that aRa, or the relation R is reflexive now for some a,b ∈ L. let us assume that aRb and bRa,so that a*b=a and b*a=b,but a*b=b*a,and so a=b,the assumptions aRb and bRa imply a=b,or that the relation R is antisymmetric. finally let us assume that for some a,b,c ∈ L, aRb and bRc. this requires that a*b=a, or aRc. the last step shows that the relation R is transitive,from this we can conclude that R is a partial ordering relation.

It is easy to show that a*b=a⇔a ⊕⊕b=b. hence we could have defined the same partial ordering relation R on L as

$aRb \Leftrightarrow a \oplus b = b$ for any $a, b \in L$

our next step is to show that for any two elements $a, b \in L$, the greatest lower bound and the least upper bound of $\{a, b\} \subseteq L$ with respect to the partial ordering R are $a * b$ and $a \oplus b$ respectively.

From the absorption laws $a*(a \oplus b)=a$ and $b*(a \oplus b)=b$, we have $a R(a \oplus b)$ and $bR(a \oplus b)$.

Let us now assume that there exist an element $c \in L$ such that aRc and bRc

This means that

$$a \oplus c = c \text{ and } b \oplus c = c$$

BOUNDED LATTICE

BOUNDED LATTICE:

A Lattice (L,R) is said to be bounded lattice if it has greatest element and least element

In the bounded lattice a gretest element is denoted by I and least element is denoted by O

NOTE:

$a \vee o = a$

$a \wedge o = o$

$a \vee I = I$

$a \wedge I = a$

DISTRIBUTIVE LATTICE:

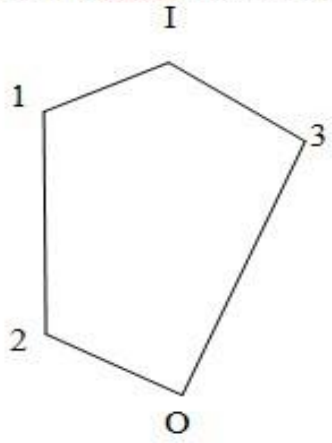
A LATTICE (L,R) is said to be distributive if for any a,b,c ∈ L,the following distributive laws hold,

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

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

EXAMPLE

Prove that the hasse diagram is distributive lattice



Assume that

A=1

B=2

C=3

By distributive law we get

By distributive law we get

$$1 \wedge (2 \vee 3) = (1 \wedge 2) \vee (1 \wedge 3)$$

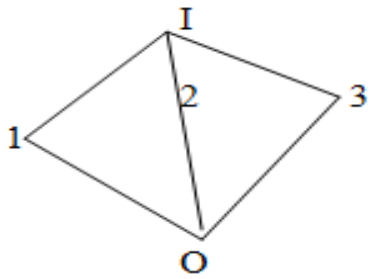
$$1 \wedge I = 2 \vee O$$

$$1 = 2$$

Therefore it is not distributive lattice

EXAMPLE

Prove that the hasse diagram is distributive lattice or not



Assume that

A=1

B=2

C=3

By distributive law we get

$1 \wedge (2 \vee 3) = (1 \wedge 2) \vee (1 \wedge 3)$

$1 \wedge I = 2 \vee O$

$1 = O$

Therefore it is not distributive lattice

BOUNDED LATTICE

A Lattice (L,R) is said to be bounded lattice if it has greatest element and least element

In the bounded lattice a greatest element is denoted by I and least element is denoted by O

$$a \vee o = a$$
$$a \wedge o = o$$
$$a \vee I = I$$
$$a \wedge I = a$$

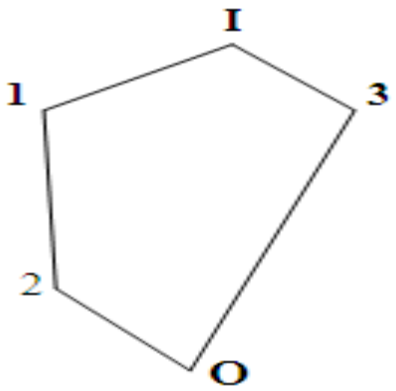
DISTRIBUTIVE LATTICE

- A LATTICE (L,R) is said to be distributive if for any a,b,c L,the following distributive laws hold,

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

EXAMPLE

prove that the hasse diagram is distributive lattice or not



Solution:

Assume that

a=1

b=2

c=3

by distributive law we get

$1 \wedge (2 \vee 3) = (1 \wedge 2) \vee (1 \wedge 3)$

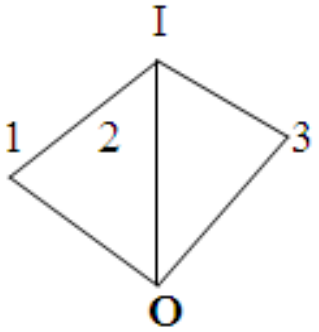
$1 \wedge I = 2 \vee O$

$1 = 2$

Therefore it is not a distributive lattice

EXAMPLE

prove that in the above Hasse diagram is distributive lattice or not



Assume that

A=1

B=2

C=3

by distributive law we get

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

$1 \wedge (2 \vee 3)=(1 \wedge 2) \vee (1 \wedge 3)$

$1 \wedge I=O \vee O$

1=0

Therefore it is not a distributive lattice

References

- D S Chandra shekaraiah, “Mathematical Foundations of Computer Science (Discrete Structures)”, Prism Books Pvt. Ltd., 2nd Reprint, 2007

MODULE 3
ALGEBRAIC STRUCTURES AND COMBINATORICS

Running outcomes

CLO 1: Construct different algebraic structures by using concepts of groups, sub groups, monoids and rings.

CLO 2: Understand binomial and multinomial theorems to compute the coefficients for the given expansions.

CLO 3:Understand the concept of homomorphism and isomorphism of semi-groups.

CLO 4: Analyze the given sets by using inclusion and exclusion principle.

CLO 5: Identify the different counting techniques (permutations) related to mathematics and computer science.

CLO 6:Solve discrete probability and set problems by using permutations and combinatorics.

.

Algebraic structures: Algebraic Systems

N = {1,2,3,4,…..∝ } = Set of all natural numbers.

Z = { 0, ±1, ±2, ±3, ±4 , ….. ∝} = Set of all integers.

Q = Set of all rational numbers.

R = Set of all real numbers.

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

Ex: (N, +), (Z, +, –), (R, +, . , –) are algebraic systems.

Algebraic Systems

Algebra is about operations on sets. You have met many operations;

For Example:

- addition and multiplication of numbers;
- modular arithmetic;
- addition and multiplication of polynomials;
- addition and multiplication of matrices;
- union and intersection of sets;
- composition of permutations.

Algebraic Systems

- Many of these operations satisfy similar familiar laws.
- In all these cases, the “associative law” holds, while most (but not all!) also satisfy the “commutative law”.

Some Laws of Algebra

- $a + 0 = a$ {+ identity}
- $(-a) + a = 0$ {+ complement}
- $a \times 1 = a$ {× identity}
- $a \times 0 = 0$ {× null}
- $a + b = b + a$ {+ commutative}
- $a + (b+c) = (a+b) + c$ {+ associative}
- $a \times (b+c) = a \times b + a \times c$ {distributive law}

Theorem $(-1) \times (-1) = 1$

$(-1) \times (-1)$	
$= ((-1) \times (-1)) + 0$	{+ id}
$= ((-1) \times (-1)) + ((-1) + 1)$	{+ comp}
$= (((-1)\times(-1)) + (-1)) + 1$	{+ assoc}
$= (((-1)\times(-1)) + (-1)\times 1) + 1$	{× id}
$= ((-1)\times((-1) + 1)) + 1$	{dist law}
$= ((-1)\times 0) + 1$	{+ comp}
$= 0 + 1$	{× null}
$= 1 + 0$	{+ comm}
$= 1$	{+ id}

Algebraic structures: Algebraic Systems

Binary Operations and General Properties

Let S- be a non-empty set and * (read as star) be an operation on S. The operation on the set is a rule, which assigns to each ordered pair of elements of the set, a unique element of S.

Closure Property

Consider a binary operation, . The operation * is said to be closed, if for all $\forall a,b \in S, a*b \in S$

The new element also belongs to S.

Examples and General Properties

Example : A set of integers Z is closed with respect to the binary operations, namely, addition, multiplication and subtraction but not with respect to division.

$$\forall a,b \in Z,\ (a \pm b) \in S, (a \bullet b) \in Z, (a / b) \notin Z$$

Example: The set of odd integers is not closed with respect to addition, since sum of two odd integers is an even, which is not the member of the set.

Examples and General Properties

Commutative Property

Commutative means that the *order* does not make any difference.

a + b = b + a

a * b = b * a

Examples

4 + 5 = 5 + 4

2 * 3 = 3 * 2

The commutative property does not work for subtraction or division.

Examples and General Properties

Associative Property

Consider a binary operation *.

For any $\forall a, b, c \in S : (a * b) * c = a * (b * c)$

- **Example** The addition (+) and multiplication (.) are Associative in the following sets .
- N = The set of natural numbers, I or Z = The set of Integers, Q = The set of Rational, R = The set of real,
- C = The set of Complex numbers

Examples and General Properties

Existence of Identity Element

Consider an element e , such that. Then the element is called the identity element of S with respect to the $e \in S$binary operation . For example , 0 and 1 are the identity elements of Z with respect to the operations of addition and multiplication respectively.

Existence of Inverse:

Consider an element . The element , is called the inverse of a under the operation *. such that

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

Examples and General Properties

Distributive Property

If '+' and '*' are two operations defined on set 'A' such that

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

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

Semi Groups

A Semi group is an algebra which consists of a set and a binary associative operation. There need not be an identity element nor inverses for all elements.

A finite or infinite set 'S' with a binary operation 'o'(Composition) is called semigroup if it holds following two conditions simultaneously.

Semi Groups

Closure Property:
For every pair $(a,b) \in S, (aob)$ has to be present in the set S.

Associative Property: For every element $a,b,c \in S, (aob)oc = ao(boc)$ must hold.

Example

The set of positive integers (excluding zero) with addition operation is a semigroup.

For example:

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

Here closure property holds as for every pair $(a,b)\in S,(a+b)$ is present in the set S.

For example:

$1+2=3\in S$

Associative property also holds for every element $a,b,c\in S,(a+b)+c=a+(b+c)$

For example:

$(1+2)+3=1+(2+3)=5$

Semi Group

Let A be a set, with a binary function $\oplus: A \times A \rightarrow A$ defined on it.

1. <A, $\oplus$> is a **semigroup** if $\oplus$ is associative:

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

2. <A, $\oplus$> is a **group** if also:

   (i) there exists some o such that for all a:

   $a = a \oplus o = o \oplus a$

   (ii) for all a, there is some -a such that:

   $o = a \oplus -a = -a \oplus a$

Semi Group

Let S- be a nonempty set and is a binary operation on S, then the algebraic system (S,*) is called a semi-group , if the operation * is associative. The algebraic system is called semigroup.

$$\forall a,b,c \in S,\ a*(b*c)=(a*b)*c$$

It is to note that since the characteristic property of a binary operation on a set S is the closure property, it is not necessary to mention it explicitly when algebraic system is defined.

Monoids

A monoid is a semigroup with an identity element. The identity element (denoted by *e* or E) of a set S is an element such that (*aoe*)=*a*, for every element *a*∈*S*.

- An identity element is also called a **unit element**.
- So, a monoid holds three properties simultaneously − **Closure, Associative, Identity element**.

Example

The set of positive integers (excluding zero) with multiplication operation is a monoid.

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

Here closure property holds as for every pair $(a,b)\in S,(a\times b)$ is present in the set S.

- [For example, $1\times 2=2\in S$and so on]

Associative property also holds for every element

$a,b,c\in S,(a\times b)\times c=a\times(b\times c)$

- [For example, $(1\times 2)\times 3=1\times(2\times 3)=6$and so on]

Identity property also holds for every element $a\in S,(a\times e)=a$

[For example, $(2\times 1)=2,(3\times 1)=3$ and so on].

Here identity element is 1.

Monoids

Monoid: If a semi- group (M,*) has an identity element with respect to the operation * , then (M,*) is called a monoid. The algebraic system is called a monoid.

$$\forall a,b,c \in M, a*(b*c) = (a*b)*c$$

$$\forall\ e\ \in\ M\ ,\ a\ *\ e\ =\ e\ *\ a\ =\ a$$

The set of positive even numbers is a semi-group with respect to the binary operation addition and multiplication.

Example

Example: The set of negative integers is not a semi-group. Hence, the operation - is closed in Z. But the operation is not associative.

Consider a = 2 , b = 5, and c = 6
(2-5) - 6 = -3 – 6 = - 9
2-(5 – 6) = 2 - (-1) = 3, which is not the element of Z

Example : The set of natural numbers N ={ 1,2,3,----} is a semi-group under the operation addition, but not a monoid, since the identity element does not exists i.e.,

$$0 \notin N$$

Monoids

A semi-group is a set X with an operation which is associative, $(xy)z=x(yz)$.

A semi-group with an identity 1 is called a monoid . The model for monoids is the composition of morphisms $\varphi : X \rightarrow X$ in any category (e.g. the functions X^X).

The ordered product of n -terms is associative (by induction), so can omit brackets $x_1 \ldots . x_n$

Groups, Sub groups

Groups: A group is a monoid with an inverse element. The inverse element (denoted by I) of a set S is an element such that $(aoI)=(Ioa)=a$, for each element $a \in S$. So, a group holds four properties simultaneously - i) Closure, ii) Associative, iii) Identity element, iv) Inverse element. The order of a group G is the number of elements in G and the order of an element in a group is the least positive integer n such that a is the identity element of that group G.

Examples

- The set of $N \times N$ non-singular matrices form a group under matrix multiplication operation.
- The product of two $N \times N$ non-singular matrices is also an $N \times N$ non-singular matrix which holds closure property.
- Matrix multiplication itself is associative. Hence, associative property holds.
- The set of $N \times N$ non-singular matrices contains the identity matrix holding the identity element property.
- As all the matrices are non-singular they all have inverse elements which are also nonsingular matrices. Hence, inverse property also holds.

Abelian Group

An abelian group G is a group for which the element pair $(a,b) \in G$ always holds commutative law. So, a group holds five properties simultaneously - i) Closure, ii) Associative, iii) Identity element, iv) Inverse element, v) Commutative.

Example

- The set of positive integers (including zero) with addition operation is an abelian group. $G=\{0,1,2,3,\ldots\}$
- Here closure property holds as for every pair $(a,b) \in S,(a+b)$ is present in the set S.
- [For example, $1+2=2 \in S$ and so on]

Example

- Associative property also holds for every element $a,b,c \in S$, $(a+b)+c=a+(b+c)$
- [For example, (1+2)+3=1+(2+3)=6 and so on]
- Identity property also holds for every element $a \in S,(a \times e)=a$
- [For example, $(2 \times 1)=2,(3 \times 1)=3$ and so on]. Here, identity element is 1.
- Commutative property also holds for every element $a \in S,(a \times b)=(b \times a)$
- [For example, $(2 \times 3)=(3 \times 2)=3$ and so on]

Cyclic Group and Subgroup

A cyclic group is a group that can be generated by a single element. Every element of a cyclic group is a power of some specific element which is called a generator. A cyclic group can be generated by a generator ‘g’, such that every other element of the group can be written as a power of the generator ‘g’.

Example

- The set of complex numbers $\{1,-1,i,-i\}$ under multiplication operation is a cyclic group.
- There are two generators $-i$ and $-i$ as $i1=i, i2=-1, i3=-i, i4=1$ and also $(-i)1=-i, (-i)2=-1, (-i)3=i, (-i)4=1$ which covers all the elements of the group. Hence, it is a cyclic group.

Subgroup

- A **subgroup** H is a subset of a group G (denoted by $H \leq G$) if it satisfies the four properties simultaneously − **Closure, Associative, Identity element**, and **Inverse**.
- A subgroup H of a group G that does not include the whole group G is called a proper subgroup (Denoted by $H < G$). A subgroup of a cyclic group is cyclic and a abelian subgroup is also abelian.
- **Note** : A **cyclic group** is always an abelian group but not every abelian group is a cyclic group. The rational numbers under addition is not cyclic but is abelian.

Examples

Let a group $G=\{1,i,-1,-i\}$

Then some subgroups are $H1=\{1\}, H2=\{1,-1\}$

This is not a subgroup − $H3=\{1,i\}$

because that $(i)-1=-i$ is not in $H3$

Homomorphism

- A homomorphism is a map between two algebric structures of the same type (that is of the same name), that preserves the operations of the structures.
- This means a map f : A → B between two sets *A*, *B* equipped with the same structure such that, if ∗ is an operation of the structure, then f (x ∗ y) = f (x) ∗ f (y) for every pair *x*, *y* of elements of *A*.
- If (G, ▪) and (H, *) are two groups, the function f :G → H is called a *group homomorphism* if f (a ▪ b) = f (a) * f (b) for all a, b ∈ G.
- We often use the notation f : (G, ▪) → (H, *) for such a homomorphism.
- Many authors use *morphism* instead of *homomorphism*.
- A *group isomorphism* is a bijective group homomorphism.

Isomorphism

Definition : Let (G,*) and (H,*) be the group and its subgroup then the function f : G H is a homomorphism and the following relation holds, A homomorphism is an isomorphism if it is bijective equivalently, if it has an inverse.

$$f(x \circ y) = f(x) * f(y) \ \forall x, y \in G$$

- If G and H are groups, G and H are isomorphic if there is an isomorphism.
- f : G → H . Isomorphic groups are the same as groups.
- Note: Let (G,∗) be an arbitrary group and H = { e } ,then the function f : G → H such that, f(x) – e for any x ∈ G is a homomorphism.

Isomorphism

- Groups G and H are not isomorphic if they have different orders, or if one satisfies the group property that the other doesn't.
- For example, two groups are not isomorphic if one is abelian and the other is not; two groups are not isomorphic if the orders of elements of one are not the same as the orders of elements of the other.

Homomorphism, Isomorphism

- In abstract algebra, an isomorphism is a bijective map f such that both f and its inverse $f\ -1$ are homomorphisms, i.e., *structure-preserving* mappings. In the more general setting of category theory, an isomorphism is a morphism f: $X \rightarrow Y$ in a category for which there exists an "inverse" $f\ -1$: $Y \rightarrow X$, with the property that both $f\ -1f$ = idX and $f\ f\ -1$ = idY.
- Informally, an isomorphism is a kind of mapping between objects, which shows a relationship between two properties or operations. If there exists an isomorphism between two structures, we call the two structures isomorphic. In a certain sense, isomorphic structures are structurally identical, if you choose to ignore finer-grained differences that may arise from how they are defined.

monoids

Semigroup homomorphism:

- Let (S, *) and (T, D) be any two semigroups. A mapping

  g: S ® T such that any two elements a, b Î S , g(a * b) = g(a) D g(b) is called a semigroup homomorphism.

Monoid homomorphism:

- Let (M, *,eM) and (T, D,eT) be any two monoids. A mapping g: M® T such that any two elements a, b Î M ,

  g(a * b) = g(a) D g(b) and g(eM) = eT is called a monoid homomorphism.

Rings

Definition: A structure $(R, +, \cdot)$ is a *ring* if R is a non-empty set and + and are binary operations: such that

$+ : R \times R \to R, \quad (a, b) \mapsto a + b$

$. : R \times R \to R, \quad (a, b) \mapsto a \cdot b$

Addition: (R, +) is an abelian group, that is,

- Associativity: For all $a, b, c \in R$ we have
  $a + (b + c) = (a + b) + c$
- Zero element: There exists $0 \in R$ such that for all $a \in R$ we have $a + 0 = 0 + a = a$
- Inverse: For any $a \in R$ there exists $-a \in R$ such that
  $a + (-a) = (-a) + a = 0$
- Commutativity: For all $a, b \in R$ we have
  $a + b = b + a$

Rings

Multiplication:

- Associativity: For all a, b, c ∈ R we have a·(b·c) = (a·b)·c

Addition and multiplication together:

- For all a, b, c ∈ R,

a · (b + c) = a · b + a · c and (a + b) · c = a · b + b · c

- We sometimes say 'R is a ring', taken it as given that the ring operations are denoted + and ·. As in ordinary arithmetic we shall frequently suppress · and write ab instead of a · b
- We do NOT demand that multiplication in a ring be commutative. As a consequence we must postulate distributivity as 2 laws, since neither follows from the other in general.

Examples of Rings

- All of Z, Q, R and C are commutative rings with identity (with the number 1 as the identity).
- N is NOT a ring for the usual addition and multiplication. These are binary operations and we do have a zero element, namely 0, so axiom holds. However (existence of additive inverses) fails: there is no $n \in N$ for which $1+n=0$, for example.
- **Note:** Polynomials, with real coefficients, form a commutative ring with identity under the usual addition and multiplication; we denote this by R[x].

Calculation rules for rings

- Assume that (R; +,) is a commutative ring. Let a, b, c R.

i. If a + b = a + c then b = c.

ii. If a + a = a then a = 0.

iii. −(−a) = a.

iv. 0a = 0.

- v. −(ab) = (−a)b = a(−b).

vi. (−1)a = −a. (Assume in addition that R has an identity 1)

vii. If a ∈ R has a multiplicative identity a^{-1} then ab

Fields

Definition:

A field F is a set together with two binary operations + and ×, satisfying the following properties:

- (F,+) is a commutative group
- (F-{0},×) is a commutative group
- The distributive law holds in F:

  $(a + b) \times c = (a \times c) + (b \times c)$

Note: A field is a commutative ring with identity where each non-zero element has a multiplicative inverse.

Principles

- Combinatorics is the study of collections of objects. Specifically, counting objects, arrangement, derangement, etc. along with their mathematical properties.
- Counting objects is important in order to analyze algorithms and compute discrete probabilities.
- Originally, combinatorics was motivated by gambling: counting configurations is essential to elementary probability.

- **A simple example:** How many arrangements are there of a deck of 52 cards?
- In addition, combinatorics can be used as a proof technique.
- A combinatorial proof is a proof method that uses counting arguments to prove a statement

Fundamental Counting Principle

- Fundamental Counting Principle can be used to determine the number of possible outcomes when there are two or more characteristics .
- Fundamental Counting Principle states that if an event has m possible outcomes and another independent event has n possible outcomes, then there are $m * n$ possible outcomes for the two events together.

Fundamental Counting Principle

- Lets start with a simple example.
- A student is to roll a die and flip a coin. How many possible outcomes will there be?

1H 2H 3H 4H 5H 6H
1T 2T 3T 4T 5T 6T

6*2 = 12 outcomes

12 outcomes

Fundamental Counting Principle

- For a college interview, Robert has to choose what to wear from the following: 4 slacks, 3 shirts, 2 shoes and 5 ties. How many possible outfits does he have to choose from?

  4*3*2*5 = 120 outfits

- **Example:** If a password is 6,7,or 8 characters long; a character is an uppercase letters or a digit, and the password is required to include at least one digit - how many passwords can there be?
- First, two most basic rules:
  1. Sum rule
  2. Product rule

Fundamental Counting Principle

- Let us consider two tasks:
  - *m* is the number of ways to do task 1
  - *n* is the number of ways to do task 2
  - Tasks are independent of each other, i.e.,
    - Performing task 1 does not accomplish task 2 and vice versa.

- *Sum rule*: the number of ways that "either task 1 or task 2 can be done, but not both", is $m + n$.

Fundamental Counting Principle

- Let us consider two tasks:
  - *m* is the number of ways to do task 1
  - *n* is the number of ways to do task 2
  - Tasks are independent of each other, i.e.,
    - Performing task 1does not accomplish task 2 and vice versa.

- *Product rule*: the number of ways that "both tasks 1 and 2 can be done" in *mn*.

Permutations

A Permutation is an arrangement of items in a particular order.

Notice, ORDER MATTERS!

To find the number of Permutations of n items, we can use the Fundamental Counting Principle or factorial notation.

Permutations

The number of ways to arrange the letters ABC:

	___	___	___
Number of choices for first blank?	3		
Number of choices for second blank?	3	2	
Number of choices for third blank?	3	2	1

3*2*1 = 6 3! = 3*2*1 = 6

ABC ACB BAC BCA CAB CBA

Permutations

To find the number of Permutations of n items chosen r at a time, you can use the formula

$$ {}_n p_r = \frac{n!}{(n-r)!} \quad \text{where } 0 \le r \le n . $$

$$ {}_5 p_3 = \frac{\mathbf{5!}}{\mathbf{(5-3)!}} = \frac{5!}{2!} = \mathbf{5 * 4 * 3 = 60} $$

Permutations

Practice:

A combination lock will open when the right choice of three numbers (from 1 to 30, inclusive) is selected. How many different lock combinations are possible assuming no number is repeated?

Answer Now

Permutations

Practice:

A combination lock will open when the right choice of three numbers (from 1 to 30, inclusive) is selected. How many different lock combinations are possible assuming no number is repeated?

$$_{30}p_3 = \frac{\mathbf{30!}}{\mathbf{(30-3)!}} = \frac{30!}{27!} = \mathbf{30*29*28} = \mathbf{24360}$$

Permutations

Practice:

From a club of 24 members, a President, Vice President, Secretary, Treasurer and Historian are to be elected. In how many ways can the offices be filled?

Answer Now

Permutations

Practice:

From a club of 24 members, a President, Vice President, Secretary, Treasurer and Historian are to be elected. In how many ways can the offices be filled?

$$_{24}p_5 = \frac{\mathbf{24!}}{\mathbf{(24-5)!}} = \frac{24!}{19!} =$$

$$\mathbf{24 * 23 * 22 * 21 * 20 = 5{,}100{,}480}$$

Disarrangements

A derangement of $\{1,2,\ldots,n\}$ is a permutation $i_1 i_2 \ldots i_n$ of $\{1,2,\ldots,n\}$ in which no integer is in its natural position: $i_1 \neq 1, i_2 \neq 2, \ldots, i_n \neq n$.

We denote by D_n the number of derangements of $\{1,2,\ldots,n\}$.

Theorem: For $n \geq 1$,

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right)$$

Disarrangements

- **Proof:** Let S={1,2,…,n} and X be the set of all permutations of S. Then |X|=n!.
- For j=1,2,…,n, let p_j be the property that in a permutation, j is in its natural position. Thus the permutation $i_1,i_2,\ldots,i_n$ of S has property p_j provided i_j=j. A permutation of S is a derangement if and only if it has none of the properties $p_1,p_2,\ldots,p_n$.
- Let A_j denote the set of permutations of S with property p_j (j=1,2,…,n).

Examples

Example:

- (1)Determine the number of permutations of {1,2,3,4,5,6,7,8,9} in which no odd integer is in its natural position and all even integers are in their natural position.
- (2) Determine the number of permutations of {1,2,3,4,5,6,7,8,9} in which four integers are in their natural position.

Examples

- Permutations with relative forbidden position
- A Permutations of {1,2,…,n} with relative forbidden position is a permutation in which none of the patterns i,i+1(i=1,2,…,n) occurs.
- We denote by Q_n the number of the permutations of {1,2,…,n} with relative forbidden position.

Examples

- **Theorem :** For $n \geq 1$,

  $Q_n = n! - C(n-1,1)(n-1)! + C(n-1,2)(n-2)! - \ldots + (-1)^{n-1} C(n-1,n-1)1!$

- **Proof:** Let $S=\{1,2,\ldots,n\}$ and X be the set of all permutations of S.

  Then $|X|=n!$.

  $j(j+1)$, p_j

  A_j: p_j

  $Q_n = D_n + D_{n-1}$

Combinations

A Combination is an arrangement of items in which order does not matter.

ORDER DOES NOT MATTER!

Since the order does not matter in combinations, there are fewer combinations than permutations. The combinations are a "subset" of the permutations.

Combinations

To find the number of Combinations of n items chosen r at a time, you can use the formula

$$ {}_nC_r = \frac{n!}{r!(n-r)!} \quad \text{where} \quad 0 \le r \le n . $$

Combinations

To find the number of Combinations of n items chosen r at a time, you can use the formula

$$ {}_nC_r = \frac{n!}{r!(n-r)!} \quad \text{where} \quad 0 \le r \le n . $$

$$ {}_5C_3 = \frac{5!}{3!(5-3)!} = \frac{5!}{3!2!} = $$

$$ \frac{5*4*3*2*1}{3*2*1*2*1} = \frac{5*4}{2*1} = \frac{20}{2} = 10 $$

Combinations

Practice:

To play a particular card game, each player is dealt five cards from a standard deck of 52 cards. How many different hands are possible?

Combinations

Practice:

To play a particular card game, each player is dealt five cards from a standard deck of 52 cards. How many different hands are possible?

$$_{52}C_5 = \frac{\mathbf{52!}}{\mathbf{5!(52-5)!}} = \frac{52!}{5!47!} =$$

$$\frac{\mathbf{52*51*50*49*48}}{\mathbf{5*4*3*2*1}} = \mathbf{2{,}598{,}960}$$

Combinations

Practice:

A student must answer 3 out of 5 essay questions on a test. In how many different ways can the student select the questions?

Combinations

Practice:

A student must answer 3 out of 5 essay questions on a test. In how many different ways can the student select the questions?

$$ {}_{5}C_{3} = \frac{\mathbf{5!}}{\mathbf{3!(5-3)!}} = \frac{5!}{3!2!} = \frac{\mathbf{5*4}}{\mathbf{2*1}} = \mathbf{10} $$

Combinations

Practice:

A basketball team consists of two centers, five forwards, and four guards. In how many ways can the coach select a starting line up of one center, two forwards, and two guards?

Answer Now

Combinations

Practice:

A basketball team consists of two centers, five forwards, and four guards. In how many ways can the coach select a starting line up of one center, two forwards, and two guards?

Center:

$$_2C_1 = \frac{2!}{1!1!} = 2$$

Forwards:

$$_5C_2 = \frac{5!}{2!3!} = \frac{5*4}{2*1} = 10$$

Guards:

$$_4C_2 = \frac{4!}{2!2!} = \frac{4*3}{2*1} = 6$$

$$_2C_1 * {}_5C_2 * {}_4C_2$$

Thus, the number of ways to select the starting line up is 2*10*6 = 120.

Permutations with Repetitions

The number of permutations of “n” objects, “r” of which are alike, “s” of which are alike, ‘t” of which are alike, and so on, is given by the expression

$$\frac{n!}{r! \times s! \times t! \ldots}$$

Permutations with Repetitions

Example 1: In how many ways can all of the letters in the word **SASKATOON** be arranged?

Solution: If all 9 letters were different, we could arrange then in 9! Ways, but because there are 2 identical S's, 2 identical A's, and 2 identical O's, we can arrange the letters in:

$$\frac{n!}{r! \times s! \times t! \ldots} = \frac{9!}{2! \times 2! \times 2!} = 45360$$

Therefore, there are 45360 different ways the letters can be arranged.

Permutations with Repetitions

Example 2: Along how many different routes can one walk a total of 9 blocks by going 4 blocks north and 5 blocks east?

Solution: If you record the letter of the direction in which you walk, then one possible path would be represented by the arrangement NNEEENENE. The question then becomes one to determine the number of arrangements of 9 letters, 4 are N's and 5 are E's.

$$\frac{9!}{5! \times 4!} = 126$$

→ Therefore, there are 126 different routes.

Circular and Ring Permutations

Circular Permutations Principle

"*n*" different objects can be arranged in circle in (n – 1)! ways.

Ring Permutations Principle

"n" different objects can arranged on a circular ring in ways.

$$\frac{(n-1)!}{2}$$

Circular and Ring Permutations

Example 1: In how many different ways can 12 football players be arranged in a circular huddle?

Solution: Using the circular permutations principle there are:

$(12 - 1)! = 11! = 39\ 916\ 800$ arrangements

If the quarterback is used as a point of reference, then the other 11 players can be arranged in 11! ways.

Circular and Ring Permutations

Example 2: In how many ways can 8 different charms be arranged on a circular bracelet?

Solution: Using the ring permutation principle there are:

$$\frac{(n-1)!}{2} = \frac{(8-1)!}{2} = \frac{7!}{2} = 2520 \ ways$$

Combinations with repetition

- A combination with repetition of objects from is a way of selecting objects from a list of . The selection rules are:
- The order of selection does not matter (the same objects selected in different orders are regarded as the same combination);
- Each object can be selected more than once.
- Thus, the difference between simple combinations and combinations with repetition is that objects can be selected only once in the former, while they can be selected more than once in the latter.

repetition

- A more rigorous definition of combination with repetition involves the concept of multiset, which is a generalization of the notion of set.
- The difference between a multiset and a set is the following: the same object is allowed to appear more than once in the list of members of a multiset, while the same object is allowed to appear only once in the list of members of an ordinary set.
- Like sets, multisets are unordered collections of objects, i.e. the order in which the elements of a multiset are listed does not matter.
- A **combination with repetition** of objects from the objects , is one of the possible ways to form a multiset containing objects taken from the set .

Binomial Theorem

$$(a+b)^4 = (a+b)(a+b)(a+b)(a+b)$$

$$= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4$$

Binomial Theorem: Let x and y be variables, and let n be any nonnegative integer. Then

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

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

What is the coefficient of a^8b^9 in the expansion of $(3a+2b)^{17}$?

What is n? 17

What is j? 9

What is x? 3a

What is y? 2b

$$\binom{17}{9}(3a)^8(2b)^9 = \binom{17}{9} 3^8 2^9 a^8 b^9$$

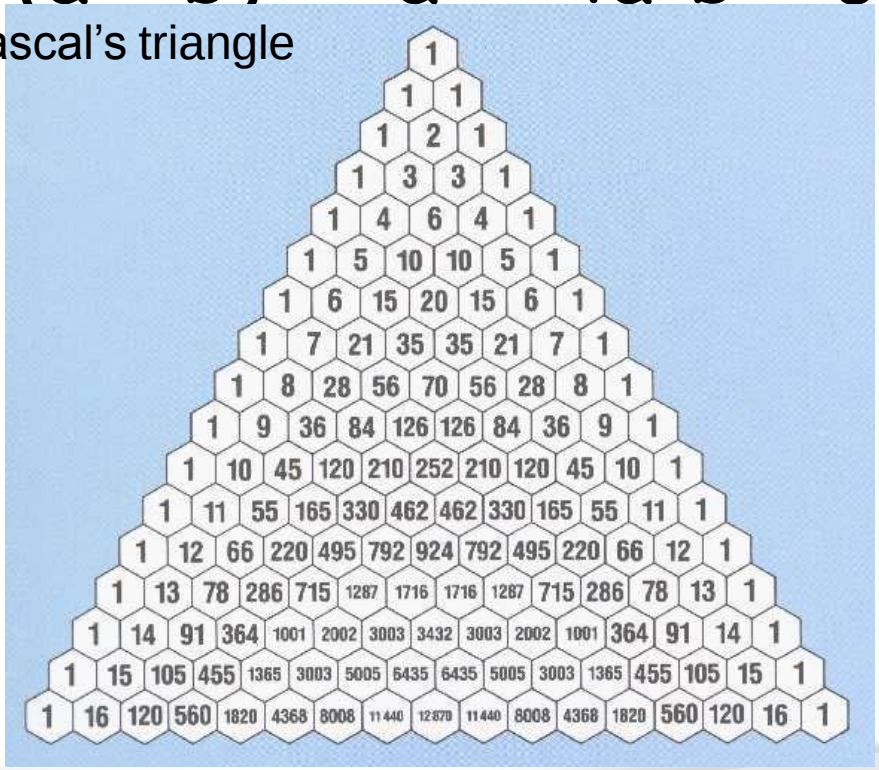
Binomial Coefficients

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 +$$

Pascal's triangle



What is coefficient of a^9b^3 in $(a + b)^{12}$?

A. 36
B. 220
C. 15
D. 6
E. No clue

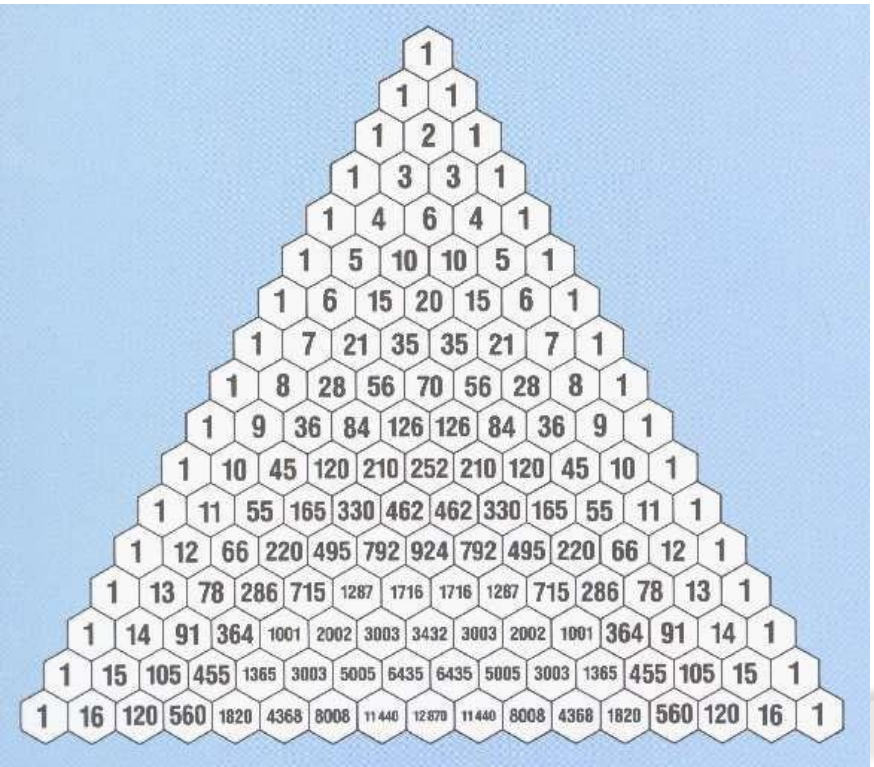
A.: 220

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

Powers of 2

Sum each row of Pascal's Triangle:

$$\sum_{j=0}^{n} \binom{n}{j} = 2^n$$



Suppose you have a set of size n. How many subsets does it have?

2^n

How many subsets of size 0 does it have?

${}_nC_0$

How many subsets of size 1 does it have?

${}_nC_1$

How many subsets of size 2 does it have?

${}_nC_2$

Add them up we have the result.

$$\sum_{j=0}^{n}\binom{n}{j} = 2^n$$

Alternative (clever) proof? Look at binomial theorem.

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

x and y are variables; can pick any numbers….

Pick x=1 and y=1 !

$$\sum_{j=0}^{n}\binom{n}{j}1^{n-j}1^j = (1+1)^n$$

$$\sum_{j=0}^{n}\binom{n}{j} = 2^n$$

Multinomial Theorem

Theorem: In the expansion of

$$(a_1 + \ldots + a_k)^n,$$

the coefficient of $a_1^{n1} a_2^{n2} \ldots a_k^{nk}$ is

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

Example: The Multinomial Theorem

- Expand $(a + b + c + d)^3$.
- The terms are
  - a^3, b^3, c^3, d^3, with coefficient $3!/3! = 1$.
  - a^2b, a^2c, a^2d, ab^2, b^2c, b^2d, ac^2, bc^2, c^2d, ad^2, bd^2, cd^2, with coefficient $3!/(1!2!) = 3$.
  - abc, abd, acd, bcd, with coefficient $3!/(1!1!1!) = 6$.

Example: The Multinomial Theorem

- Therefore,

$$(a+b+c+d)^3 = a^3 + b^3 + c^3 + d^3 + 3a^2b + 3a^2c + 3a^2d + 3ab^2 + 3b^2c + 3b^2d + 3ac^2 + 3bc^2 + 3c^2d + 3ad^2 + 3bd^2 + 3cd^2 + 6abc + 6abd + 6acd + 6bcd.$$

Trinomial and Multinomial Coefficients

- **Example:** Suppose we want to form nine-letter words comprising 4 x's, 3 y's, and 2 z's. How many such words are there (words are different if they are visually distinct). Denote the number by $\binom{9}{4,3,2}$ Suppose for a moment that we distinguish the letters by attaching subscripts to them: x_1, x_2, x_3, x_4, y_1, etc. Now there are 9! different nine-letter words using these nine symbols. We can count them in another way, however: First choose the positions for the x's, y's, and z's (without subscripts. There are $\binom{9}{4,3,2}$ ways to do this. Next there are 4! ways to assign subscripts to the x's, 3! ways to do it for the y's, and 2! ways to do it for the z's. Thus $\binom{9}{4,3,2} 4!3!2! = 9!$. Dividing yields $\binom{9}{4,3,2} = \frac{9!}{4!3!2!}$.

Trinomial and Multinomial Coefficients

- Definition: Given nonnegative integers n, n_1, n_2, n_3 with $n_1 + n_2 + n_3 = n$, we define the trinomial coefficient by

$$\binom{n}{n_1, n_2, n_3} = \frac{n!}{n_1! n_2! n_3!}$$

Trinomial and Multinomial Coefficients

- Theorem : Under these circumstances, the trinomial coefficient $\binom{n}{n_1, n_2, n_3} = \frac{n!}{n_1!n_2!n_3!}$ counts the number of words (sequences) of length n with n_1 x's, n_2 y's, and n_3 z's. Equivalently it counts the ways to distribute n labeled balls among three labeled urns such that the first gets n_1 balls, the second gets n_2 , and the third gets n_3 . (Think of the position numbers in the word corresponding to the balls and the letters x, y, and z being the labels on the urns).

- **Proof:** The above example illustrates the central idea.

Trinomial and Multinomial Coefficients

- Theorem : For nonnegative n, the sum of all trinomial coefficients of order n is 3^n . That is,

$$\sum_{\substack{n_1+n_2+n_3=n \\ n_i \in N}} \binom{n}{n_1, n_2, n_3} = 3^n$$

- Proof: Summing the trinomial coefficients counts every word of length n on x, y, and z. There are 3^n such words.

Trinomial and Multinomial Coefficients

- Theorem (The Trinomial Theorem): For nonnegative n we have

$$(x+y+z)^n = \sum_{\substack{n_1+n_2+n_3=n \\ n_i \in N}} \binom{n}{n_1, n_2, n_3} x^{n_1} y^{n_2} z^{n_3}$$

- Proof sketch: In expanding the nth power of the trinomial on the left, we get every word of length n on x, y, and z. Much as in the binomial case, the coefficient on a particular term is the number of words with the specified number of x's, y's, and z's.

Principle of Inclusion-Exclusion (PIE)

- Say there are two events, e_1 and e_2, for which there are n_1 and n_2 possible outcomes respectively.
- Now, say that only <u>one</u> event can occur, not both
- In this situation, we cannot apply the sum rule. Why?

  … because we would be over counting the number of possible outcomes.
- Instead we have to count the number of possible outcomes of e_1 and e_2 minus the number of possible outcomes in common to both; i.e., the number of ways to do both tasks
- If again we think of them as sets, we have

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Principle of Inclusion-Exclusion (PIE)

- More generally, we have the following
- **Lemma**: Let A, B, be subsets of a finite set U. Then
  1. $|A \cup B| = |A| + |B| - |A \cap B|$
  2. $|A \cap B| \leq \min\{|A|, |B|\}$
  3. $|A \backslash B| = |A| - |A \cap B| \geq |A| - |B|$
  4. $|\overline{A}| = |U| - |A|$
  5. $|A \oplus B| = |A \cup B| - |A \cap B| = |A| + |B| - 2|A \cap B| = |A \backslash B| + |B \backslash A|$
  6. $|A \times B| = |A| \times |B|$

PIE: Theorem

- **Theorem**: Let $A_1, A_2, \ldots, A_n$ be finite sets, then

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \Sigma_i |A_i|$$
$$- \Sigma_{i<j} |A_i \cap A_j|$$
$$+ \Sigma_{i<j<k} |A_i \cap A_j \cap A_k|$$
$$- \ldots$$
$$+(-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

Each summation is over

- all i,
- pairs i,j with i<j,
- triples with i<j<k, etc.

PIE Theorem: Example 1

- To illustrate, when n=3, we have

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - [|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|] + |A_1 \cap A_2 \cap A_3|$$

PIE Theorem: Example 2

- To illustrate, when n=4, we have

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1|+|A_2|+|A_3|+|A_4|$$
$$- [|A_1 \cap A_2|+|A_1 \cap A_3|+|A_1 \cap A_4|$$
$$+|A_2 \cap A_3|+|A_2 \cap A_4|+|A_3 \cap A_4|]$$
$$+ [|A_1 \cap A_2 \cap A_3|+|A_1 \cap A_2 \cap A_4|$$
$$+|A_1 \cap A_3 \cap A_4|+|A_2 \cap A_3 \cap A_4|]$$
$$- |A_1 \cap A_2 \cap A_3 \cap A_4|$$

Application of PIE: Example A (1)

- How many integers between 1 and 300 (inclusive) are
  - Divisible by at least one of 3,5,7?
  - Divisible by 3 and by 5 but not by 7?
  - Divisible by 5 but by neither 3 or 7?
- Let

$$A = \{n \in \mathbb{Z} \mid (1 \le n \le 300) \wedge (3 \mid n)\}$$

$$B = \{n \in \mathbb{Z} \mid (1 \le n \le 300) \wedge (5 \mid n)\}$$

$$C = \{n \in \mathbb{Z} \mid (1 \le n \le 300) \wedge (7 \mid n)\}$$

- How big are these sets? We use the floor function

$$|A| = \lfloor 300/3 \rfloor = 100$$

$$|B| = \lfloor 300/5 \rfloor = 60$$

$$|C| = \lfloor 300/7 \rfloor = 42$$

Application of PIE: Example A (2)

- How many integers between 1 and 300 (inclusive) are divisible by at least one of 3,5,7?

  Answer: $|A \cup B \cup C|$

- By the principle of inclusion-exclusion

$$|A \cup B \cup C| = |A| + |B| + |C| - [|A \cap B| + |A \cap C| + |B \cap C|] + |A \cap B \cap C|$$

- How big are these sets? We use the floor function

$|A| = \lfloor 300/3 \rfloor = 100$ $\quad$ $|A \cap B| = \lfloor 300/15 \rfloor = 20$

$|B| = \lfloor 300/5 \rfloor = 60$ $\quad$ $|A \cap C| = \lfloor 300/21 \rfloor = 100$

$|C| = \lfloor 300/7 \rfloor = 42$ $\quad$ $|B \cap C| = \lfloor 300/35 \rfloor = 8$

$|A \cap B \cap C| = \lfloor 300/105 \rfloor = 2$

- Therefore:

$$|A \cup B \cup C| = 100 + 60 + 42 - (20+14+8) + 2 = 162$$

Application of PIE: Example A (3)

- How many integers between 1 and 300 (inclusive) are divisible by 3 and by 5 but not by 7?

  Answer: $|(A \cap B) \backslash C|$

- By the definition of set-minus

$$|(A \cap B) \backslash C| = |A \cap B| - |A \cap B \cap C| = 20 - 2 = 18$$

- Knowing that

$|A| = \lfloor 300/3 \rfloor = 100$ $\quad$ $|A \cap B| = \lfloor 300/15 \rfloor = 20$

$|B| = \lfloor 300/5 \rfloor = 60$ $\quad$ $|A \cap C| = \lfloor 300/21 \rfloor = 100$

$|C| = \lfloor 300/7 \rfloor = 42$ $\quad$ $|B \cap C| = \lfloor 300/35 \rfloor = 8$

$|A \cap B \cap C| = \lfloor 300/105 \rfloor = 2$

References

- D S Chandra shekaraiah, “Mathematical Foundations of Computer Science (Discrete Structures)”, Prism Books Pvt. Ltd., 2nd Reprint, 2007

MODULE 4
RECURRENCE RELATION

Running outcomes

CLO 19: Identify the series of expansion to represent the sequence by using generating functions.

CLO 20:Identify the general solution for first-order and second-order linear homogeneous recurrence relations.

CLO 21: Identify the roots of second and higher order linear non-homogeneous recurrence relations.

CLO 4: Prepare valid arguments from the given propositional statements by using rules of inference.

GENERATING FUNCTIONS

- Consider a sequence of real numbers $a_0,a_1,a_2,\ldots$. Suppose there exists a function

$$f(x)=a_0+a_1x+a_2x^2+\ldots..a_{n-1}x^{n-1}+\ldots=\sum_{r=0}^{\infty}x^r a_r$$

Then f(x) is the generating function for the sequence $a_0,a_1,a_2,\ldots.a_n$

- Examples:

Since $(1-x)^{-1}=1+x+x^2+x^3\ldots..=\sum_{r=0}^{\infty}x^r$

f(x)= $(1-x)^{-1}$ is a generating function for the sequence 1,1,1,1…..

- Similarly

Since $(1+x)^{-1}=1-x+x^2-x^3\ldots..=\sum_{r=0}^{\infty}(-1)x^r$

f(x)= $(1+x)^{-1}$ is a generating function for the sequence 1,-1,1,-1….

GENERATING FUNCTIONS

Examples for finding Generating Functions:

1) 1, 2, 3, 4…

Here $a_0=1$, $a_1=2$, $a_2=3$, $a_3=4$

So, $f(x) = 1x^0+2x^1+3x^2+4x^3+\ldots..$

$= 1+2x+3x^2+4x^3+\ldots\ldots$

$= \mathbf{(1-x)^{-2}}$

is the generating function for the given sequence.

GENERATING FUNCTIONS

Examples for finding Generating Functions:

2) 1, -2, 3, -4…

Here $a_0=1$, $a_1= -2$, $a_2=3$, $a_3= -4$

$f(x) = 1x^0-2x^1+3x^2-4x^3+\ldots..$

$= 1-2x+3x^2-4x^3+\ldots...$

$= \mathbf{(1+x)^{-2}}$

is the generating function for the given sequence.

GENERATING FUNCTIONS

Examples for finding Generating Functions:

3) 0, 1, 2, 3, 4…

Here $a_0=0$, $a_1=1$, $a_2=2$, $a_3=3$

- $f(x) = 0x^0+1x^1+2x^2+3x^3+\ldots..$
- $= x+2x^2+3x^3+4x^4+\ldots\ldots$
- $= x\,(1+2x+3x^2+4x^3+\ldots\ldots)$
- $= \mathbf{x\,(1-x)^{-2}}$

- is the generating function for the given sequence.

GENERATING FUNCTIONS

Examples for finding Generating Functions:

4) 0, -1, 2, -3, 4…

Here $a_0=0$, $a_1= -1$, $a_2=2$, $a_3= -3$

- $= 0x^0-1x^1+2x^2-3x^3+\ldots..$

$f(x) = - x+2x^2-3x^3+4x^4+\ldots...$

- $= -x(1-2x+3x^2-4x^3+\ldots...)$
- $= \mathbf{-x\,(1+x)^{-2}}$

- is the generating function for the given sequence.

Calculating Co-efficient

We have formulas for Calculating Co-efficient

- $(1+x)^n = \sum_{r=0}^{\infty} nc_r\, x^r$
- $(1+x)^{-n} = \sum_{r=0}^{\infty} (-1)(n+r-1c_r)x^r$
- $(1-x)^n = \sum_{r=0}^{\infty} nc_r\, (-1)x^r$
- $(1-x)^{-n} = \sum_{r=0}^{\infty} (n+r-1c_r)\, x^r$

Calculating Co-efficient

Examples:

1) Determine the coefficient of $\mathbf{X^{12}}$ **in** $\mathbf{x^3(1-2x)^{10}}$

- $x^3(1-2x)^{10} = x^3 \sum_{r=0}^{10} \binom{10}{r} (-2x)^r$

$$= \sum_{r=0}^{10} \binom{10}{r} (-2)^r \; x^{r+3}$$

- Therefore the coefficient of X^{12} is

$C_{12} = (-2)^9 \binom{10}{9}$

$= -\mathbf{5210.}$

Calculating Co-efficient

Examples:

2) Determine the coefficient of $\mathbf{X^5}$ **in** $\mathbf{(1-2x)^{-7}}$

- $(1-2x)^{-7} = \sum_{r=0}^{\infty} \binom{7+r-1}{r} (2x)^r$

$= \sum_{r=0}^{\infty} \binom{6+r}{r} (2x)^r$

- Therefore the coefficient of X^5 is

$C_5 = (2)^5 \binom{11}{5}$

$= \mathbf{14,784.}$

Calculating Co-efficient

Examples:

3) Determine the coefficient of X^0 in $(3x^2-(\ ^2/_x))^{15}$

- We have $(3x^2-(\ ^2/_x))^{15} = (3x^2)^{15}(1 - \frac{2}{3x^3})^{15}$

$$= (3^{15}\ x^{30}) \sum_{r=0}^{15} \binom{15}{r} (-\frac{2}{3x^3})^r$$

$$= 3^{15} \sum_{r=0}^{15} \binom{15}{r} (-\frac{2}{3})^r \quad x^{30-3r}$$

- Therefore the coefficient of X^0 is

$$C_0 = (3)^{15} \binom{15}{10} (-\frac{2}{3})$$

$$= \mathbf{3^5 * 2^{10} * \binom{15}{10}}$$

Calculating Co-efficient

Examples:

4) Determine the coefficient of X^{10} **in** $(x^3-5x)/(1-x)^3$

- We have $(x^3-5x)/(1-x)^3 = (x^3-5x)(1-x)^{-3}$

$$= (x^3-5x)\sum_{r=0}^{\infty}\binom{3+r-1}{r}(x)^r$$

$$= (x^3-5x)\sum_{r=0}^{\infty}\binom{2+r}{r}(x)^r$$

- Therefore the coefficient of X^0 is

$$C_{10} = \binom{9}{7} - 5\binom{11}{9}$$

$$= \mathbf{-239}.$$

Counting Technique

Suppose we wish to determine number of integer solutions of the equation

$$\mathbf{x_1+x_2+x_3+.....+x_n = r},\qquad \text{where } n \geq r \geq 0$$

under constraints that

x_1 can take integer values $p_{11},p_{12},p_{13}.....$
x_2 can take integer values $p_{21},p_{22},p_{23}.....$
.....
.....
x_n can take integer values $p_{n1},p_{n2},p_{n3}.....$

Counting Technique

To solve this problem, we first define the functions f1(x), $f_2(x)$... $f_n(x)$ as follows

$$f_1(x) = x^{p11} + x^{p12} + x^{p13} + \ldots\ldots$$
$$f_2(x) = x^{p21} + x^{p22} + x^{p23} + \ldots\ldots$$
$$\ldots\ldots\ldots\ldots$$
$$f_n(x) = x^{pn1} + x^{pn2} + x^{pn3} + \ldots\ldots$$

We then consider

$$\mathbf{f(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \ldots\ldots f_n(x)}$$

Here **f(x) is generating function** for the problem.

Counting Technique

Examples:

Using generating function find the number of
i. Non-negative
ii. Positive
integer solutions of the equation

$$x_1+x_2+x_3+x_4=25$$

Counting Technique

i) In case of Non-negative integer solutions, x_i can take values 0, 1, 2, 3… Accordingly whose

$$f_i(x) = x^0 + x^1 + x^2 + x^3 + \ldots \quad \text{for } i=1, 2,3,4.$$

Therefore generating function is

$$f(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x)$$
$$= (x^0 + x^1 + x^2 + x^3 + \ldots)^4$$
$$= ((1-x)^{-1})^4$$
$$= (1-x)^{-4}$$
$$= \sum_{r=0}^{\infty} \binom{3+r}{r} (x)^r$$

- The **coefficient of X^{25}** in this is

$$\binom{3+25}{25} = \mathbf{3276.}$$

- Thus the given equation has 3276 Non-negative integer solutions.

Counting Technique

- In case of Positive integer solutions, x_i can take values 1, 2, 3… Accordingly whose

  $f_i(x) = x^{1+} x^2 + x^3 + \ldots\ldots$ for i=1, 2,3,4.

  Therefore generating function is

  $f(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x)$

  $= (x^{1+} x^2 + x^3 + \ldots\ldots)^4$

  $= x^4(1 + x^+ x^2 + x^3 + \ldots\ldots)4$

  $= x^4 ((1-x)^{-1})^4$

  $= x^4 (1-x)^{-4}$

  $= x^4 \sum_{r=0}^{\infty} \binom{2+r}{r} (x)^r$

- The **coefficient of X^{25}** in this is

  $\binom{3+21}{21}$ = **2024.**

- Thus the given equation has 2024 Positive integer solutions.

Counting Technique

2) Find the number of integer solutions of the equation

$$x_1+x_2+x_3+x_4+x_5=30$$

under constraints $x_i>=0$ for i=1,2,3,4,5 and further x_2 is even and x_3 is odd.

- So, We take

$$f_1(x)= (x^0+ x^1+ x^2+ x^3+.....) = (1-x)^{-1}$$

$$f_2(x)= (x^0+ x^2+ x^4+.....) = (1-x^2)^{-1}$$

$$f_3(x)= (x + x^3+ x^5+.....) = x(1-x^2)^{-1}$$

$$f_4(x)= (x^0+ x^1+ x^2+ x^3+.....) = (1-x)^{-1}$$

$$f_5(x)= (x^0+ x^1+ x^2+ x^3+.....) = (1-x)^{-1}$$

Counting Technique

- Therefore generating function is

$$f(x) = f_1(x) \cdot f_2(x) \cdot f_3(x) \cdot f_4(x) \cdot f_5(x)$$

$$= x\,(1-x^2)^{-2}\,(1-x)^{-3}$$

$$= x \sum_{r=0}^{\infty} \binom{2+r-1}{r} (x^2)^r \quad \sum_{s=0}^{\infty} \binom{3+s-1}{s} (x)^s$$

- The **coefficient of X^{25}** in this is

$$C_{30} = \binom{1}{0}\binom{31}{29} + \binom{2}{2}\binom{29}{27} + \cdots .. + \binom{15}{14}\binom{3}{1}$$

is required number.

Substitution Method

Recurrence Relation:

- A recurrence relation is an equation that defines a sequence based on a rule that gives the next term as a function of the previous term(s).
- A recurrence relation is an equation that recursively defines a sequence where the next term is a function of the previous terms (Expressing F_n as some combination of F_i with $i<n$)
- **Examples:** i) Fibonacci series $F_n=F_{n-1}+F_{n-2}$

  ii) Tower of Hanoi $F_n= 2F_{n-1}+1$

Substitution Method

Solving Recurrence Relation by Substitution Method:

In this method we solve relations by substituting values for n and from those results we can get solution for that recurrence relation.

Solving Recurrence Relation by Substitution Method Examples:

1) Solve Recurrence Relation $\mathbf{a_n=a_{n-1}+n}$, n>=1 where $a_0=2$ by Substitution Method

- Given Recurrence Relation $a_n=a_{n-1}+n$

  If n=1 then $a_1 = a_{1-1}+1$

  $= a_0+1$

  $= 2+1 = 3$

Substitution Method

- If n=2 then $a_2 = a_{2-1}+2$
  $= a_1+2$
  $= (a_0+1)+2$
  $= 3+2 = 5$
- If n=3 then $a_3 = a_{3-1}+3$
  $= a_2+3$
  $= (a_1+2)+3$
  $= (a_0+1)+2+3$
  $= 5+3 = 8$
  .....
- So $\mathbf{a_n = a_0+1+2+3+\ldots. +n.}$
- Therefore $a_n = a_0 + \frac{n(n+1)}{2}$

  $\mathbf{a_n = 2 + \frac{n(n+1)}{2}}$

Substitution Method

2) Solve Recurrence Relation $\mathbf{a_n=a_{n-1}+n^3}$, n>=1 where $a_0=5$ by Substitution Method

- Given Recurrence Relation $a_n=a_{n-1}+n^3$
- If n=1 then $a_1 = a_{1-1}+1$

  $= a_0+1$

  $= a_0+1^3$
- If n=2 then $a_2 = a_{2-1}+8$

  $= a_1+8$

  $= (a_0+1)+8$

  $= a_0+1^3+2^3$
- So $\mathbf{a_n = a_0+1^3+2^3+3^3+\ldots+n^3}$

  $\mathbf{a_n = a_0 + \sum n^3}$

Substitution Method

3) Solve Recurrence Relation $\mathbf{a_n=a_{n-1}+n^2}$, n>=1 where $a_0=4$ by Substitution Method

- Given Recurrence Relation $a_n=a_{n-1}+n^2$
- If n=1 then $a_1 = a_{1-1}+1$

  $= a_0+1$

  $= a_0+1^2$
- If n=2 then $a_2 = a_{2-1}+4$

  $= a_1+4$

  $= (a_0+1)+4$

  $= a_0+1^2+2^2$
- So $\mathbf{a_n =}$

  $\mathbf{a_0+1^2+2^2+3^2+\ldots+n^2}$ $\mathbf{a_n =}$

  $\mathbf{a_0 + \sum n^2}$

FIRST ORDER RECURRENCE RELATIONS

- We consider for solution recurrence relations of the form

$$a_n = ca_{n-1} + f(n), \quad \text{for } n \geq 1$$

- Where c is a constant and f(n) is a known function. Such a relation is called recurrence relation of first order with constant coefficient.
- The solution for this relation is

$$a_n = c^n a_0 + \sum_{k=1}^{n} c^{n-k} f(k)$$

- If f(n)=0, the relation is called homogeneous, otherwise non-homogeneous relation.
- So, the solution for homogeneous relation where f(n)=0, is $a_n = c^n a_0$
- i.e. if the recurrence relation is of the form

$$a_n = ca_{n-1}$$

- then solution for this is $a_n = c^n a_0$

FIRST ORDER RECURRENCE RELATIONS

Examples:

1)Solve the recurrence relation $\mathbf{a_{n+1} = 4a_n}$ for $n>0$ and $a_0=3$

- Given recurrence relation is $a_{n+1} = 4a_n$ which is homogeneous.

  Its solution is $\mathbf{a_n = 4^n a_0}$ for $n\geq 1$.

  It is given that $a_0=3$

  So we get

  $\mathbf{a_n = 3.4^n}$ for $n\geq 1$ is the required solution.

FIRST ORDER RECURRENCE RELATIONS

Examples:

2) Solve the recurrence relation $\mathbf{a_n = 7a_{n-1}}$ for $n \geq 1$ and $a_0 = 98$

- Given recurrence relation can be written as $a_{n+1} = 7a_n$ for $n \geq 0$ which is homogeneous.

  Its solution is $\mathbf{a_n = 7^n a_0}$ for $n \geq 1$.

  It is given that $a_0 = 98$

  So we get

  $\mathbf{a_n = 98.7^n}$ for $n \geq 1$ is the required solution.

FIRST ORDER RECURRENCE RELATIONS

Examples:

3) Solve the recurrence relation $\mathbf{a_n = na_{n-1}}$ for $n \geq 1$ and $a_0 = 1$

- From the given recurrence relation we find that

$a_1 = 1 * a_0$

$a_2 = 2 * a_1 = (2*1)\, a_0$

$a_3 = 3 * a_2 = (3*2*1)\, a_0$ and so on.

Its solution is $a_n = n! a_0$ for $n \geq 1$.

It is given that $a_0 = 1$

So we get

$\mathbf{a_n = n!}$ for $n \geq 1$ is the required solution.

FIRST ORDER RECURRENCE RELATIONS

4) If a_n is a solution of recurrence relation $\mathbf{a_{n+1} = k\, a_n}$ for $n \geq 0$ and $a_3 = 153/49$ and $a_5 = 1377/2401$, what is k?

- The solution of relation is $\mathbf{a_n = k^n a_0}$ for $n \geq 1$

  From this we get $a_3 = k^3 a_0$ and $a_5 = k^5 a_0$, so that $a_5 / a_3 = k^2$

  Using the given values we get $k^2 = 9/49$.

  Therefore $\mathbf{k = \pm 3/7}$.

References

- D S Chandra shekaraiah, “Mathematical Foundations of Computer Science (Discrete Structures)”, Prism Books Pvt. Ltd., 2nd Reprint, 2007

MODULE 5
GRAPHS AND TREES

Running outcomes

CLO 1:Understand the use of graphs and trees as representation tools in a variety of context.

CLO 2: Identify Euler's and Hamilton rule for a simple connected graph in NP-complete problems.

CLO 3:Construct a spanning tree by using search techniques (Depth First Search and Breadth First Search).

CLO 4:Construct a minimal spanning tree by using Kruskal's and Prim's algorithm in order to obtain a solution for a real time problem.

CLO 5:Possess the knowledge and skills for employability and to succeed in national and international level competitive exams.

Graphs: Basic concepts of graphs

Basic graph concepts

A graph is a mathematical object that is used to model different situations – objects and processes:

- Linked list
- Tree
- Flowchart of a program
- Structure chart of a program
- Finite state automata
- City map
- Electric circuits
- Course curriculum

- **Definition**

A graph is a collection (nonempty set) of vertices and edges

Vertices: can have names and properties

Edges: connect two vertices, can be labeled, can be directed

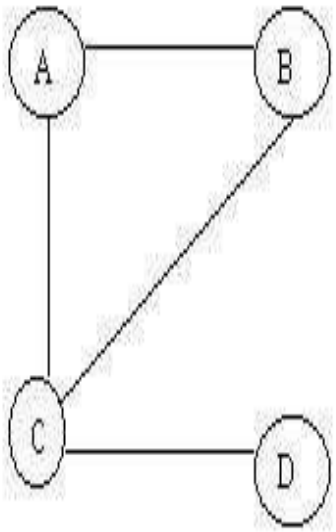
Adjacent vertices: if there is an edge between them.

Example:

Vertices: A,B,C,D

Edges: AB, AC, BC, CD

Graph1:



- **Directed graphs and undirected graphs**

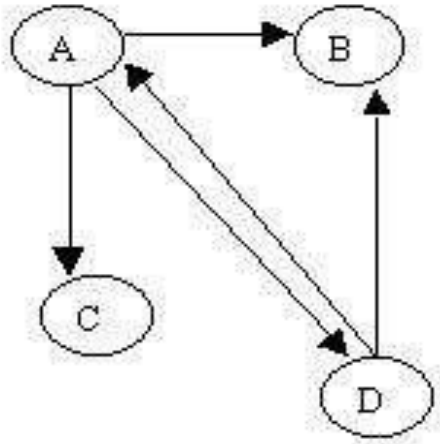
There are two basic types of graphs - *directed and undirected*.

In undirected graphs the edges are symmetrical, e.g. if A and B are vertices,
A B and B A are one and the same edge.
Graph1 above is undirected.

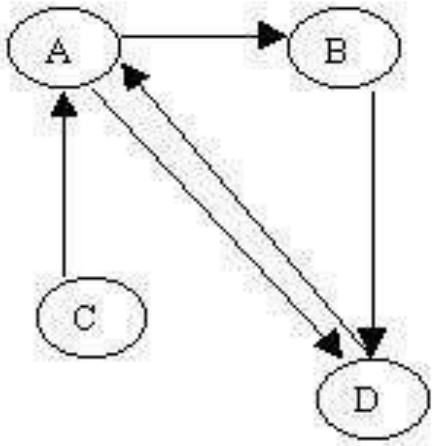
In directed graphs the edges are oriented, they have a beginning and an end.
Thus A B and B A are different edges.
Sometimes the edges of a directed graph are called **arcs**.

Examples of directed graphs

Graph2:



Graph3:



Graph2 and ***Graph3*** are different graphs

Paths

A path is a list of vertices in which successive vertices are connected by edges

Examples

Some paths in ***Graph1*** :

A B C D

A C B A C D

A B

D C B

C B A

Some paths in ***Graph2***:

D A B

A D A C

Simple path No vertex is repeated.

Examples:

In ***Graph1,*** D C B A is a simple path, while D C B A C is not a simple path

In ***Graph2,*** D A B is a simple path, while D A D B is not a simple path

Cycles

A cycle is a simple path with distinct edges, where the first vertex is equal to the last.

Examples:

Cycles in ***Graph1:*** C A B C, C B A C, A B C A, A C B A, B A C B, B C A B

A B A is not a cycle, because the edge A B is the same as B A

Cycles in ***Graph3:*** A D A, D A B D

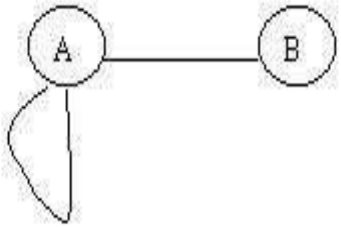
A graph without cycles is called **acyclic graph**

Loop

An edge that connects the vertex with itself

Connected graphs

Connected graph: There is a path between each two vertices



Graph1, Graph2 and ***Graph3*** are connected graphs.

Disconnected graph: There are at least two vertices not connected by a path.

Isomorphic graphs

Two graphs which contain the same number of graph vertices connected in the same way are said to be isomorphic. Formally, two graphs G and H with graph vertices Vn={1,2,…,n} are said to be isomorphic if there is a permutation p of Vn such that {u,v} is in the set of graph edges E(G) iff {p(u),p(v)} is in the set of graph edges E(H) .

Two graphs G_1 and G_2 are said to be isomorphic if −

- Their number of components (vertices and edges) are same.
- Their edge connectivity is retained.

Note – In short, out of the two isomorphic graphs, one is a tweaked version of the other. An unlabelled graph also can be thought of as an isomorphic graph.

There exists a function 'f' from vertices of G_1 to vertices of G_2

[f: $V(G_1) \Rightarrow V(G_2)$], such that

Case (i): *f* is a bijection (both one-one and onto)

Case (ii): *f* preserves adjacency of vertices, i.e., if the edge $\{U, V\} \in G_1$, then the

edge $\{f(U), f(V)\} \in G_2$, then $G_1 \equiv G_2$.

Note

If $G_1 \equiv G_2$ then –

$|V(G_1)| = |V(G_2)|$

$|E(G_1)| = |E(G_2)|$

Degree sequences of G_1 and G_2 are same.

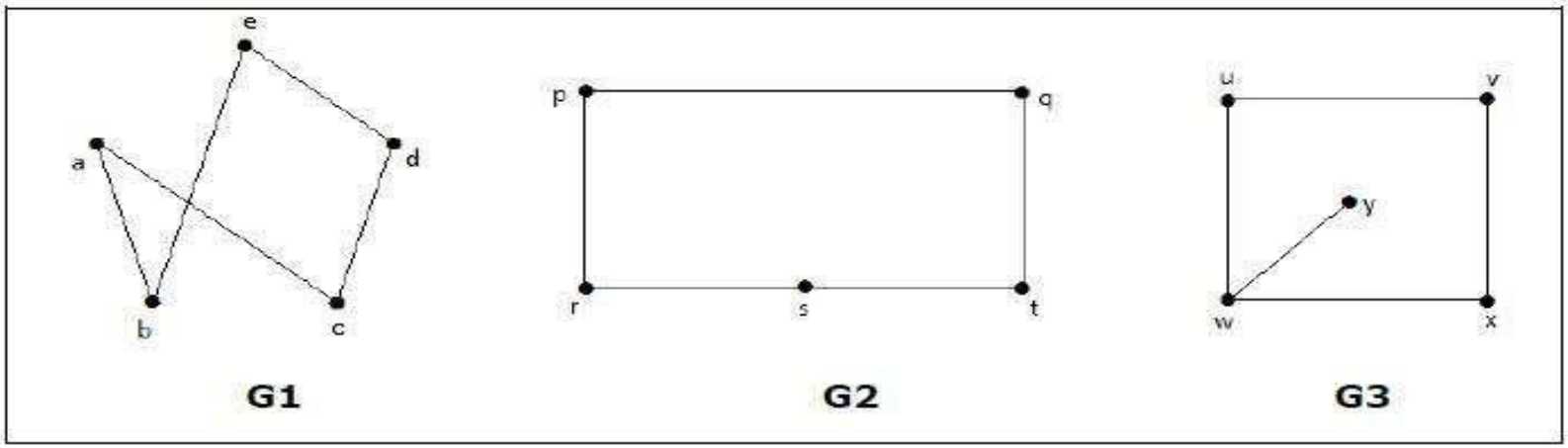
If the vertices $\{V_1, V_2, .. V_k\}$ form a cycle of length K in G_1, then the vertices $\{f(V_1), f(V_2),\ldots f(V_k)\}$ should form a cycle of length K in G_2.

All the above conditions are necessary for the graphs G_1 and G_2 to be isomorphic, but not sufficient to prove that the graphs are isomorphic.

- $(G_1 \equiv G_2)$ if and only if $(G_1- \equiv G_2-)$ where G_1 and G_2 are simple graphs.
- $(G_1 \equiv G_2)$ if the adjacency matrices of G_1 and G_2 are same.
- $(G_1 \equiv G_2)$ if and only if the corresponding subgraphs of G_1 and G_2(obtained by deleting some vertices in G_1 and their images in graph G_2) are isomorphic.

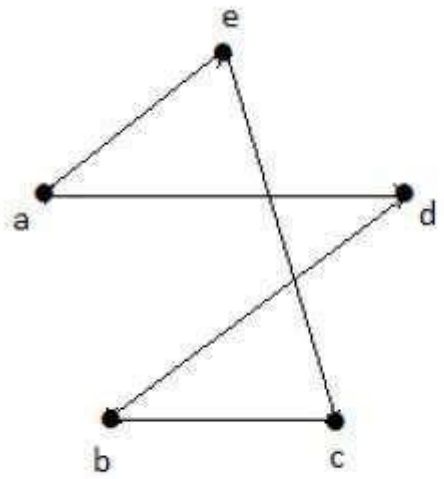
Example

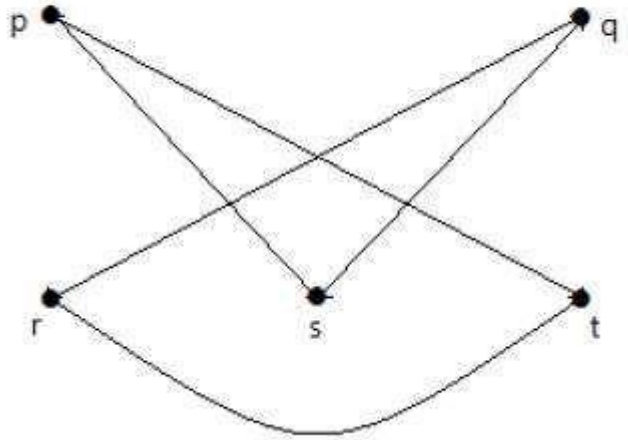
Which of the following graphs are isomorphic?



In the graph G_3, vertex 'w' has only degree 3, whereas all the other graph vertices has degree 2. Hence G_3 not isomorphic to G_1 or G_2.

Taking complements of G_1 and G_2, you have –



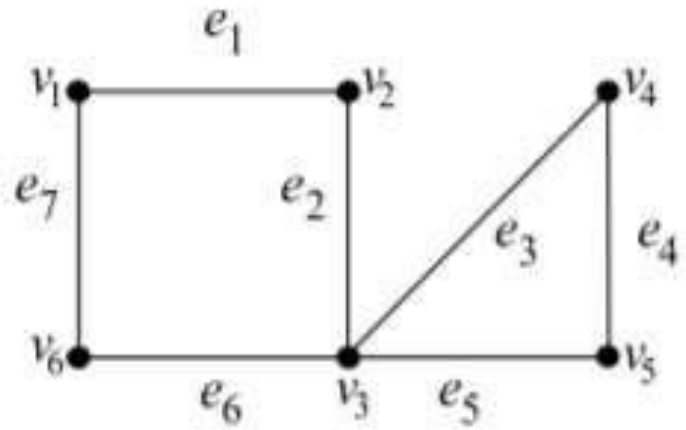


Here, (G_1– ≡ G_2–), hence ($G_1 \equiv G_2$).

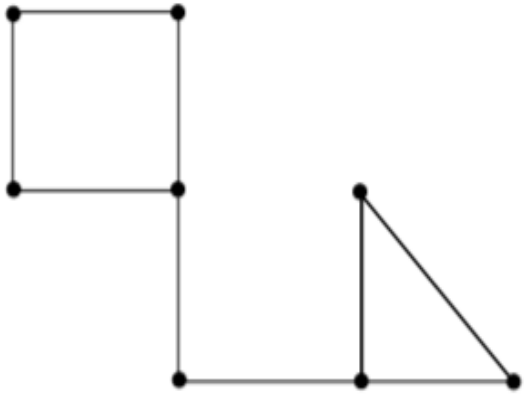
Euler graph

- A closed walk in a graph G containing all the edges of G is called an Euler line in G.
- A graph containing an Euler line is called an Euler graph. We know that a walk is always connected.
- Since the Euler line (which is a walk) contains all the edges of the graph, an Euler graph is connected except for any isolated vertices the graph may contain.
- As isolated vertices do not contribute anything to the understanding of an Euler graph, it is assumed now onwards that Euler graphs do not have any isolated vertices and are thus connected.

- Example Consider the graph shown in Figure. Clearly, v1 e1 v2 e2 v3 e3 v4 e4 v5 e5 v3 v6 e7 v1 in (a) is an Euler line, whereas the graph shown in (b) is non-Eulerian.

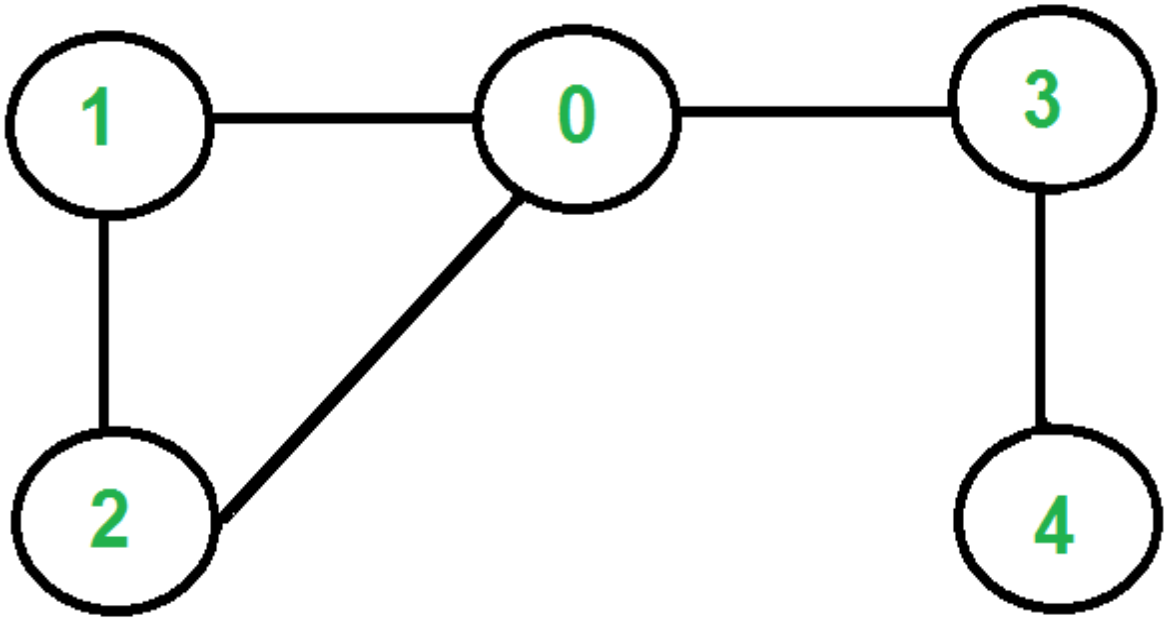


Eulerian graph

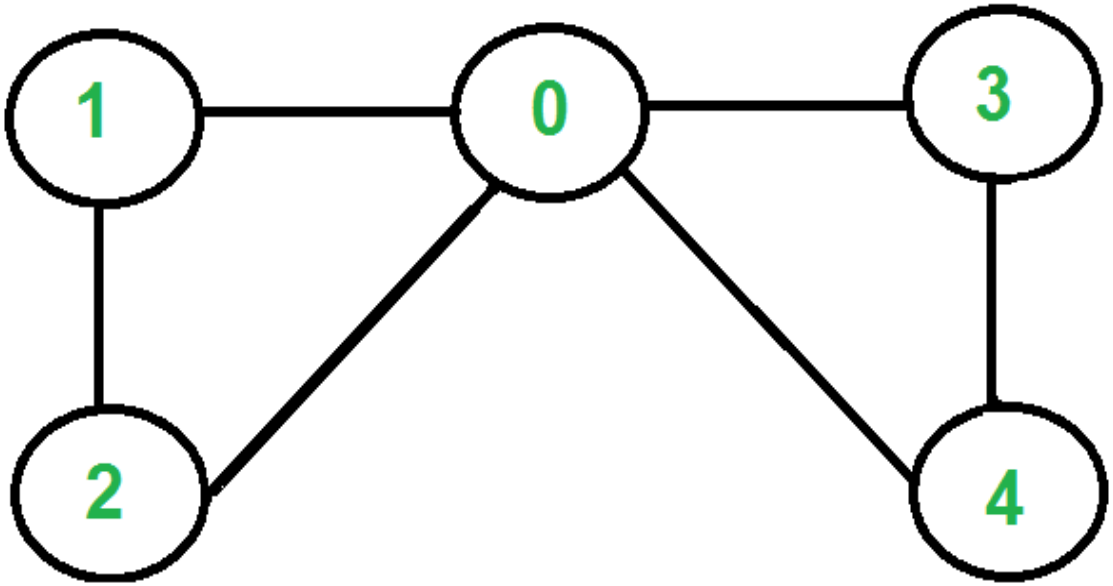


Non- Eulerian graph

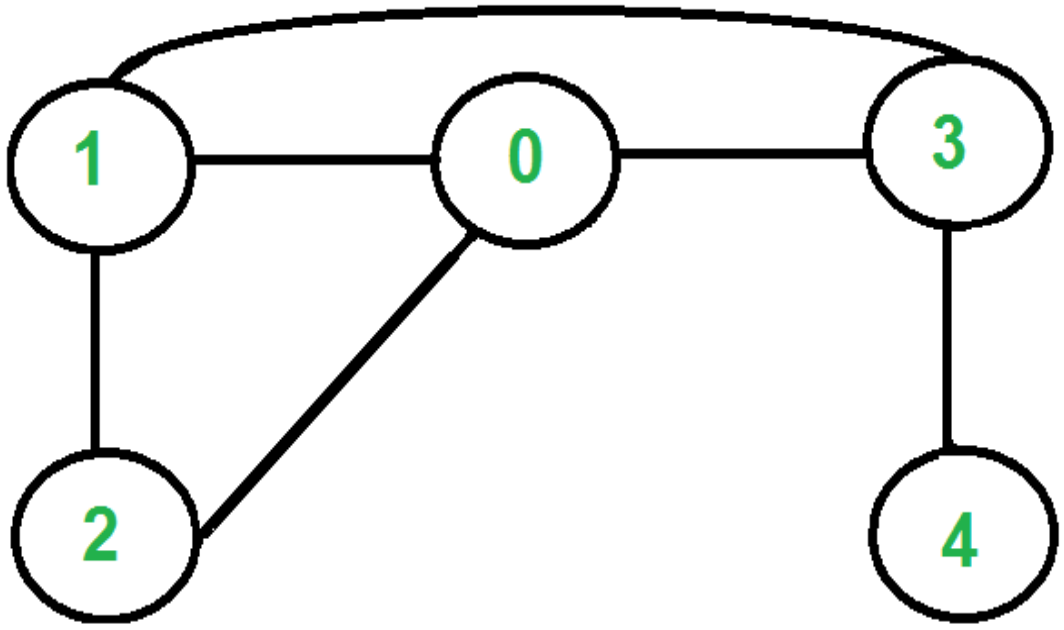
- Eulerian Path is a path in graph that visits every edge exactly once. Eulerian Circuit is an Eulerian Path which starts and ends on the same vertex.



The graph has Eulerian Paths, for example "4 3 0 1 2 0", but no Eulerian Cycle. Note that there are two vertices with odd degree (4 and 0)



The graph has Eulerian Cycles, for example "2 1 0 3 4 0 2"
Note that all vertices have even degree



The graph is not Eulerian. Note that there are four vertices with odd degree (0, 1, 3 and 4)

Eulerian Cycle

An undirected graph has Eulerian cycle if following two conditions are true.

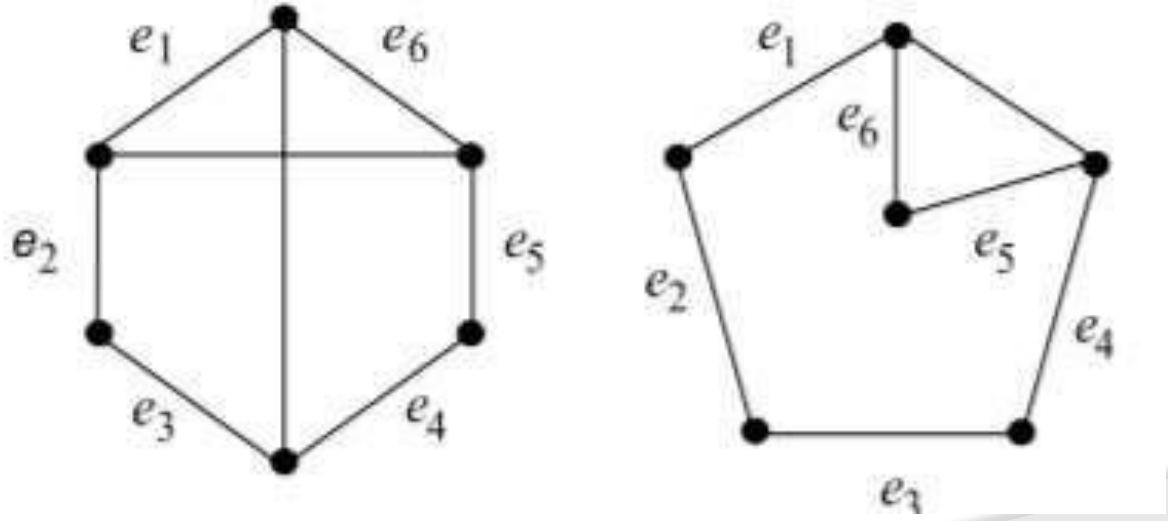
….a) All vertices with non-zero degree are connected. We don’t care about vertices with zero degree because they don’t belong to Eulerian Cycle or Path (we only consider all edges).

….b) All vertices have even degree.

- **Eulerian Path**
  An undirected graph has Eulerian Path if following two conditions are true.
  ….a) Same as condition (a) for Eulerian Cycle
  ….b) If zero or two vertices have odd degree and all other vertices have even degree. Note that only one vertex with odd degree is not possible in an undirected graph (sum of all degrees is always even in an undirected graph)
- Note that a graph with no edges is considered Eulerian because there are no edges to traverse.

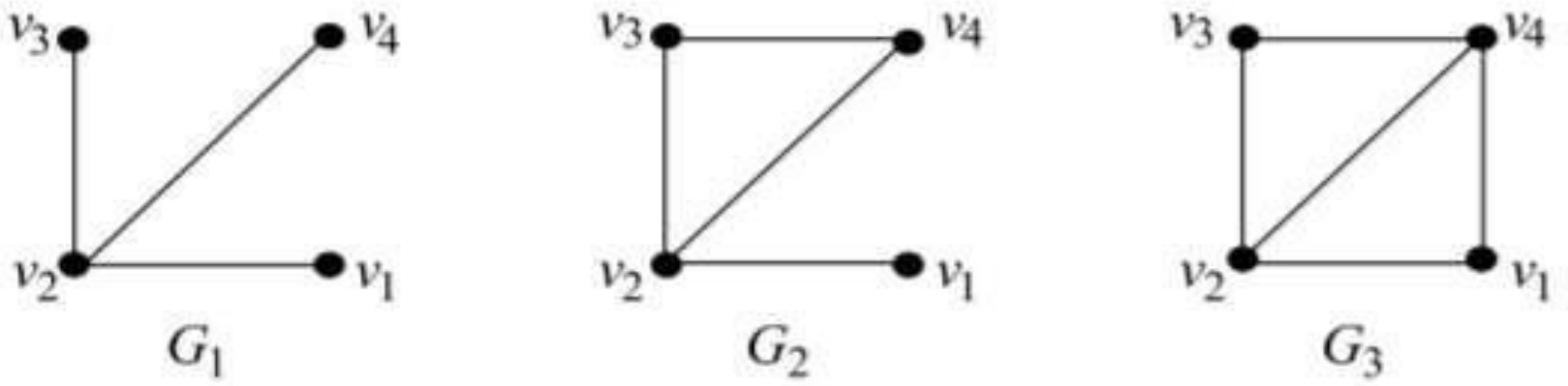
Hamiltonian graphs

A cycle passing through all the vertices of a graph is called a Hamiltonian cycle. A graph containing a Hamiltonian cycle is called a Hamiltonian graph. A path passing through all the vertices of a graph is called a Hamiltonian path and a graph containing a Hamiltonian path is said to be traceable. Examples of Hamiltonian graphs are given in Figure.



If the last edge of a Hamiltonian cycle is dropped, we get a Hamiltonian path. However, a non-Hamiltonian graph can have a Hamiltonian path, that is, Hamiltonian paths cannot always be used to form Hamiltonian cycles.

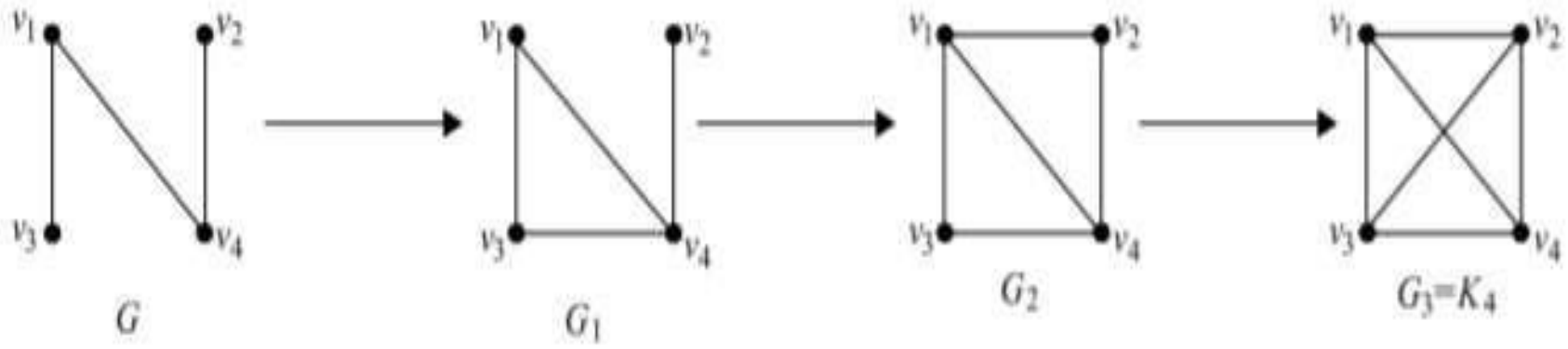
For example, in Figure, G1 has no Hamiltonian path, and so no Hamiltonian cycle; G2 has the Hamiltonian path v1v2v3v4, but has no Hamiltonian cycle, while G3 has the Hamiltonian cycle v1v2v3v4v1.



- A multigraph or general graph is Hamiltonian if and only if its underlying graph is Hamiltonian, because if G is Hamiltonian, then any Hamiltonian cycle in G remains a Hamiltonian cycle in the underlying graph of G.

- Conversely, if the underlying graph of a graph G is Hamiltonian, then G is also Hamiltonian.

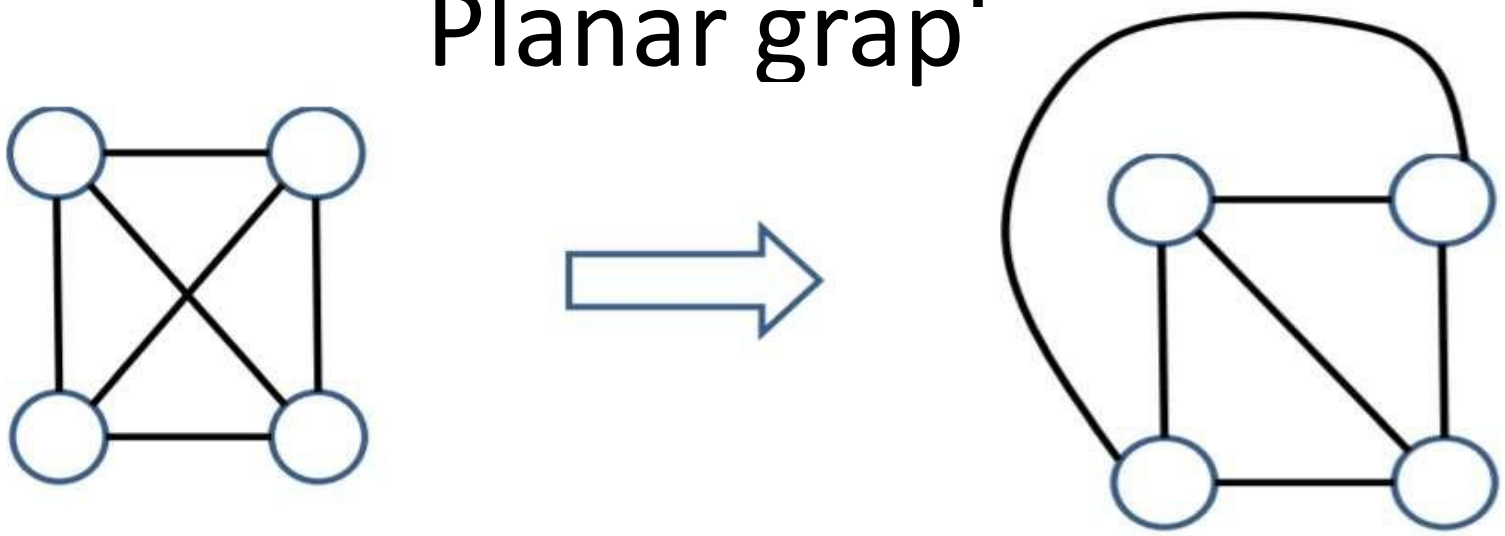
Let G be a graph with n vertices. Clearly, G is a subgraph of the complete graph Kn. From G, we construct step by step supergraphs of G to get Kn, by adding an edge at each step between two vertices that are not already adjacent.



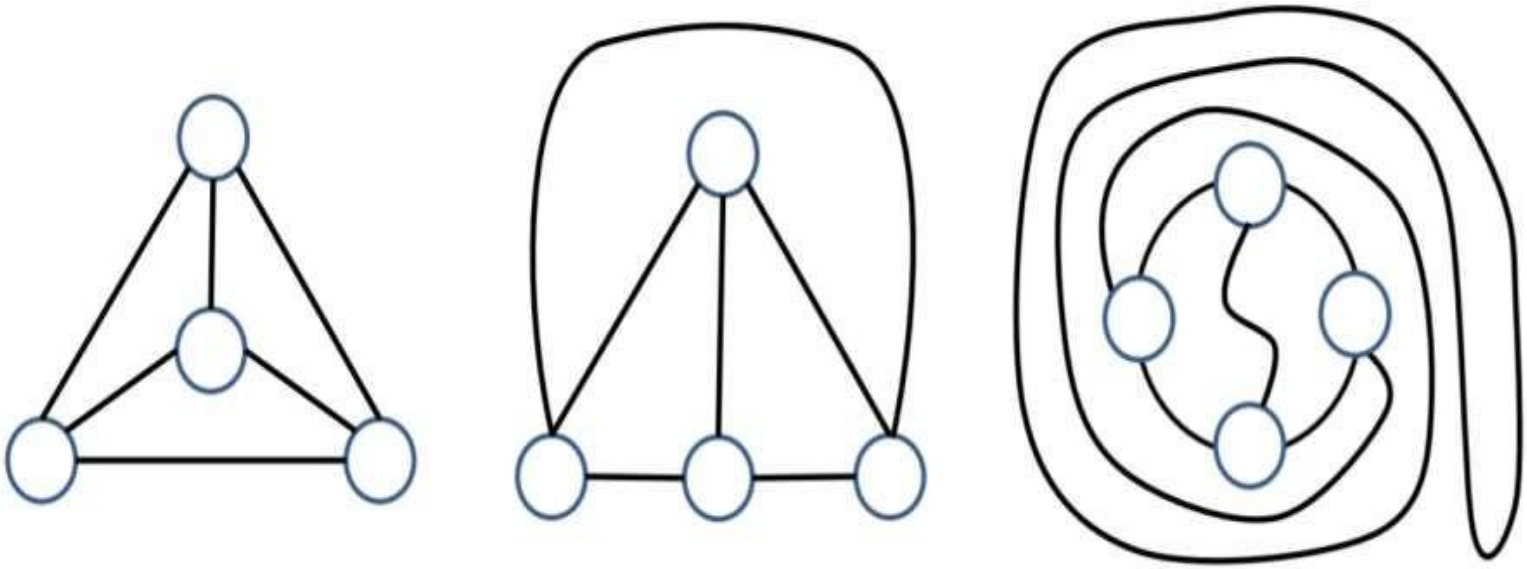
- Now, let us start with a graph G which is not Hamiltonian. Since the final outcome of the procedure is the Hamiltonian graph Kn, we change from a non-Hamiltonian graph to a Hamiltonian graph at some stage of the procedure.
- For example, the non-Hamiltonian graph G1 above is followed by the Hamiltonian graph G2. Since supergraphs of Hamiltonian graphs are Hamiltonian, once a Hamiltonian graph is reached in the procedure, all the subsequent supergraphs are Hamiltonian.

A planar graph is an undirected graph that can be drawn on a plane without any edges crossing. Such a drawing is called a planar representation of the graph in the plane. Ex : K4 is a planar graph

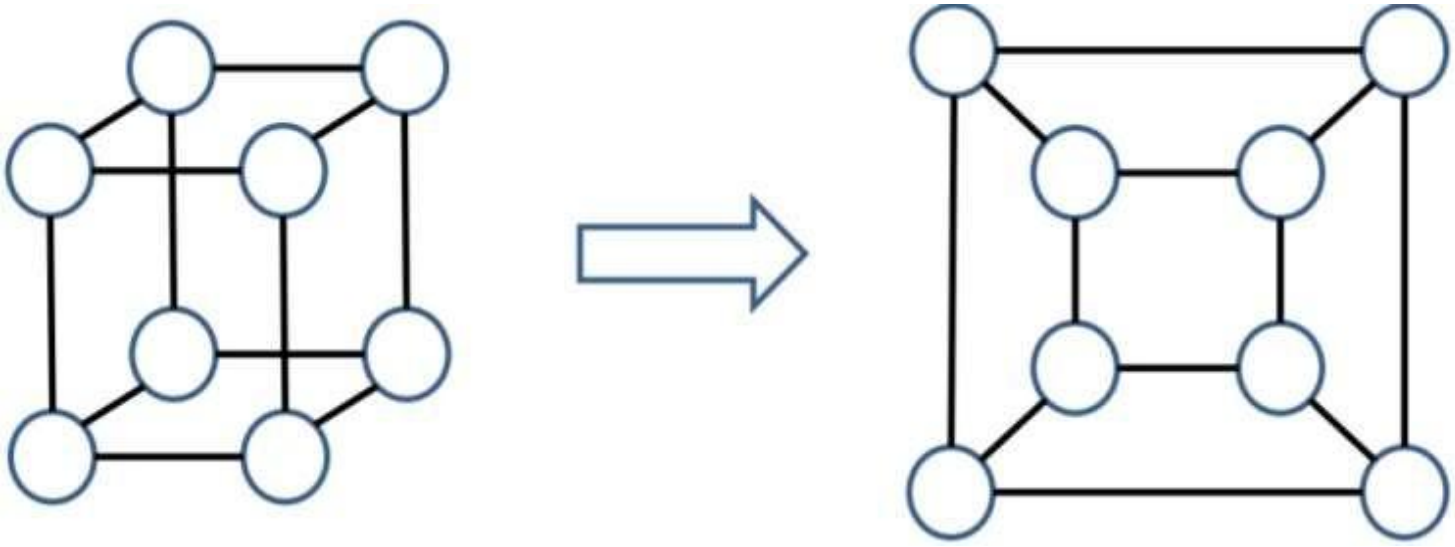
Planar grap'



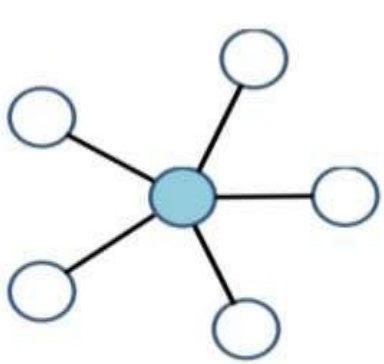
Other planar representations of K4



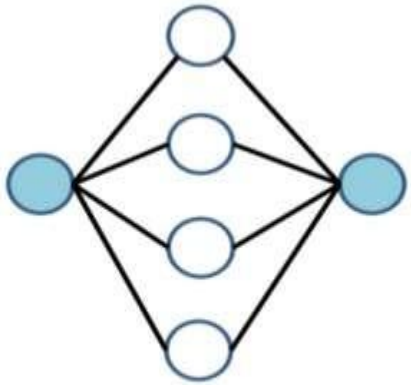
Q3 is a planar graph



K1,n and K2,n are planar graphs for all n



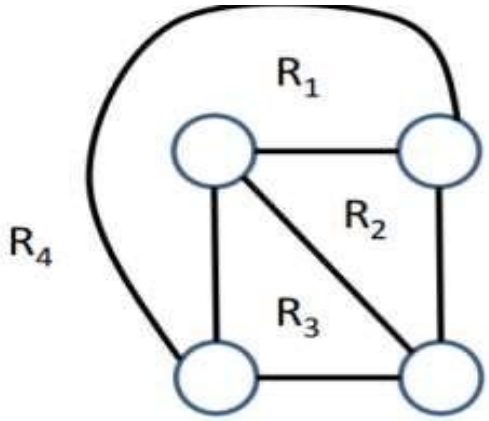
$K_{1,5}$



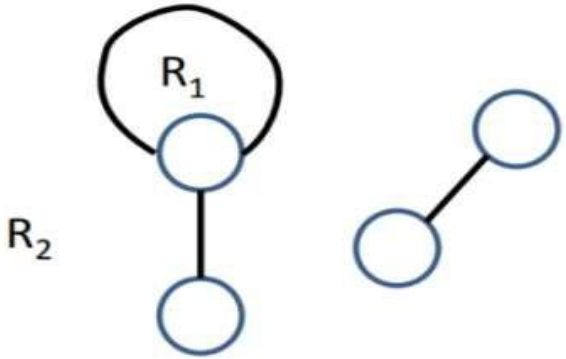
$K_{2,4}$

Euler's Planar Formula

Definition : A planar representation of a graph splits the plane into regions, where one of them has infinite area and is called the infinite region.



4 regions



2 regions

Euler's Planar Formula

Let G be a connected planar graph, and consider a planar representation of G.

Let V = # vertices, E = # edges, F = # regions.

$$V + F = E + 2.$$

Graph Coloring

- Graph coloring is the procedure of assignment of colors to each vertex of a graph G such that no adjacent vertices get same color.
- The objective is to minimize the number of colors while coloring a graph.
- The smallest number of colors required to color a graph G is called its chromatic number of that graph.
- Graph coloring problem is a NP Complete problem.

Method to Color a Graph

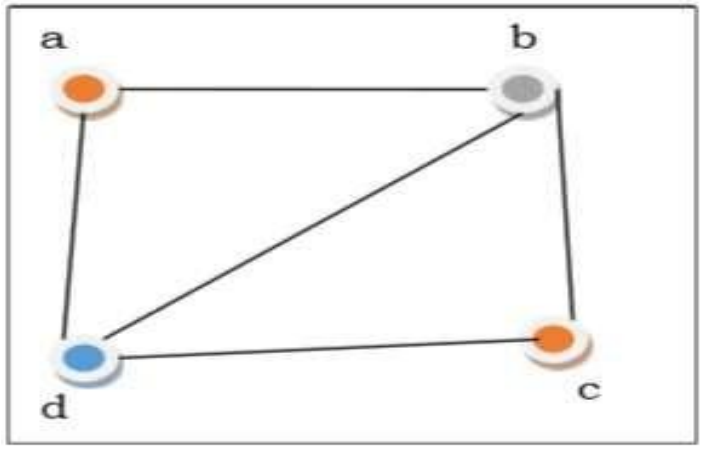
The steps required to color a graph G with n number of vertices are as follows −

Step 1 − Arrange the vertices of the graph in some order.

Step 2 − Choose the first vertex and color it with the first color.

Step 3 − Choose the next vertex and color it with the lowest numbered color that has not been colored on any vertices adjacent to it. If all the adjacent vertices are colored with this color, assign a new color to it. Repeat this step until all the vertices are colored.

Example



In the above figure, at first vertex aa is colored red.

As the adjacent vertices of vertex a are again adjacent, vertex bb and vertex dd are colored with different color, green and blue respectively.

Then vertex cc is colored as red as no adjacent vertex of cc is colored red. Hence, we could color the graph by 3 colors. Hence, the chromatic number of the graph is 3.

Applications of Graph Coloring

- Some applications of graph coloring include –
- Register Allocation
- Map Coloring
- Bipartite Graph Checking
- Mobile Radio Frequency Assignment
- Making time table, etc.

Graph Traversal

Graph traversal is the problem of visiting all the vertices of a graph in some systematic order. There are mainly two ways to traverse a graph.

- Breadth First Search
- Depth First Search

Breadth First Search

Breadth First Search (BFS) starts at starting level-0 vertex XX of the graph GG. Then we visit all the vertices that are the neighbors of XX.

After visiting, we mark the vertices as "visited," and place them into level-1. Then we start from the level-1 vertices and apply the same method on every level-1 vertex and so on.

The BFS traversal terminates when every vertex of the graph has been visited.

BFS Algorithm

- The concept is to visit all the neighbor vertices before visiting other
- neighbor vertices of neighbor vertices.
- Initialize status of all nodes as “Ready”.
- Put source vertex in a queue and change its status to “Waiting”.
- Repeat the following two steps until queue is empty −
  - Remove the first vertex from the queue and mark it as “Visited”.
  - Add to the rear of queue all neighbors of the removed vertex

Applications of BFS

- Finding the shortest path
- Minimum spanning tree for un-weighted graph
- GPS navigation system
- Detecting cycles in an undirected graph
- Finding all nodes within one connected component

Depth First Search

- Depth First Search (DFS) algorithm starts from a vertex vv, then it traverses to its adjacent vertex (say x) that has not been visited before and marks as "visited" and goes on with the adjacent vertex of xx and so on.
- If at any vertex, it encounters that all the adjacent vertices are visited, then it backtracks until it finds the first vertex having an adjacent vertex that has not been traversed before. Then, it traverses that vertex, continues with its adjacent vertices until it traverses all visited vertices and has to backtrack again. In this way, it will traverse all the vertices reachable from the initial vertex vv.

DFS Algorithm

The concept is to visit all the neighbor vertices of a neighbor vertex before visiting the other neighbor vertices.

- Initialize status of all nodes as “Ready”
- Put source vertex in a stack and change its status to “Waiting”
- Repeat the following two steps until stack is empty –
  - Pop the top vertex from the stack and mark it as “Visited”
  - Push onto the top of the stack all neighbors of the removed vertex whose status is “Ready”. Mark their status as “Waiting”.

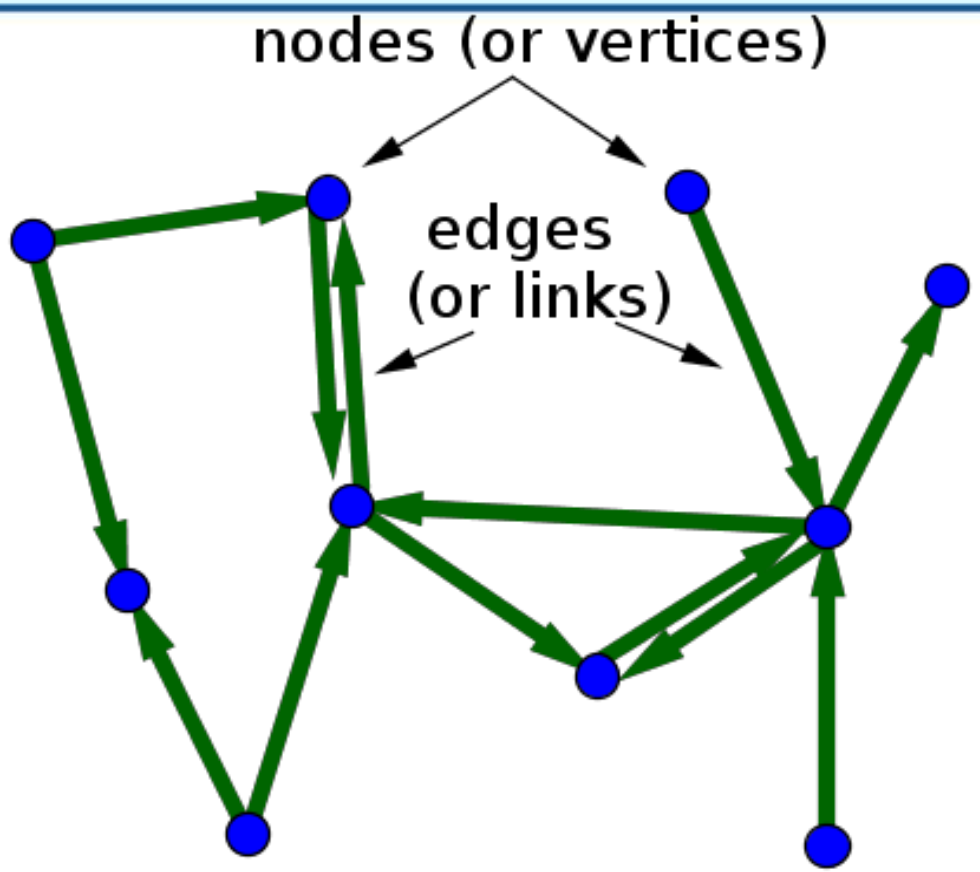
Applications

- Detecting cycle in a graph
- To find topological sorting
- To test if a graph is bipartite
- Finding connected components
- Finding the bridges of a graph
- Finding bi-connectivity in graphs
- Solving the Knight’s Tour problem
- Solving puzzles with only one solution

Digraphs

- A graph in which each graph edge is replaced by a directed graph edge, also called a digraph.
- A directed graph having no multiple edges or loops (corresponding to a binary adjacency matrix with 0s on the diagonal) is called a simple directed graph.
- A complete graph in which each edge is bidirected is called a complete directed graph. A directed graph having no symmetric pair of directed edges (i.e., no bidirected edges) is called an oriented graph.
- A complete oriented graph (i.e., a directed graph in which each pair of nodes is joined by a single edge having a unique direction) is called a tournament.

- If is an undirected connected graph, then one can always direct the circuit graph edges of and leave the separating edges undirected so that there is a directed path from any node to another. Such a graph is said to be transitive if the adjacency relation is transitive.
- When drawing a directed graph, the edges are typically drawn as arrows indicating the direction, as illustrated in the following figure.



A directed graph with 10 vertices (or nodes) and 13 edges

One can formally define a directed graph as G=(N,E)G=(N,E), consisting of the set NN of nodes and the set EE of edges, which are ordered pairs of elements of NN.

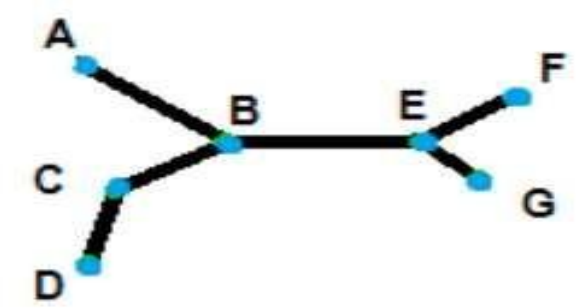
Directed acyclic graphs

- Directed acyclic graphs (DAGs) are used to model probabilities, connectivity, and causality. A “graph” in this sense means a structure made from nodes and edges.

- **Nodes** are usually denoted by circles or ovals (although technically they can be any shape of your choosing).

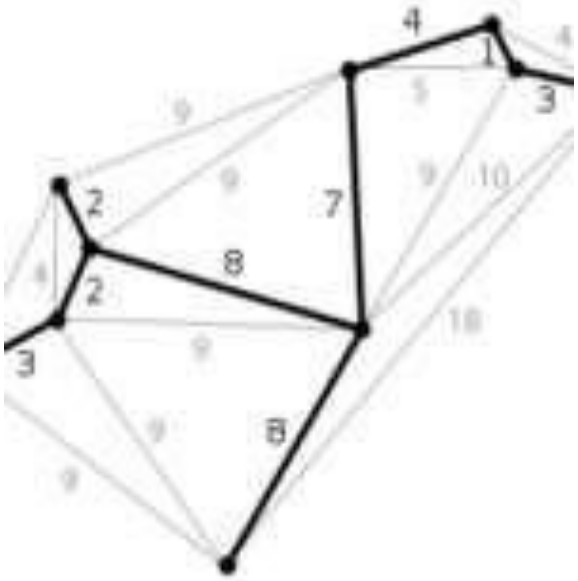
- **Edges** are the connections between the nodes. An edge connects two nodes. They are usually represented by lines, or lines with arrows.

DAGs are based on basic acyclic graphs.



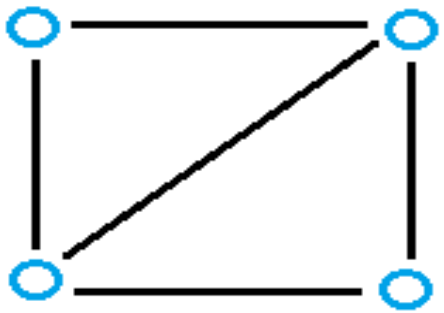
A tree with nodes A B C D E F and G.

An acyclic graph is a graph without cycles (a cycle is a complete circuit). When following the graph from node to node, you will never visit the same node twice.



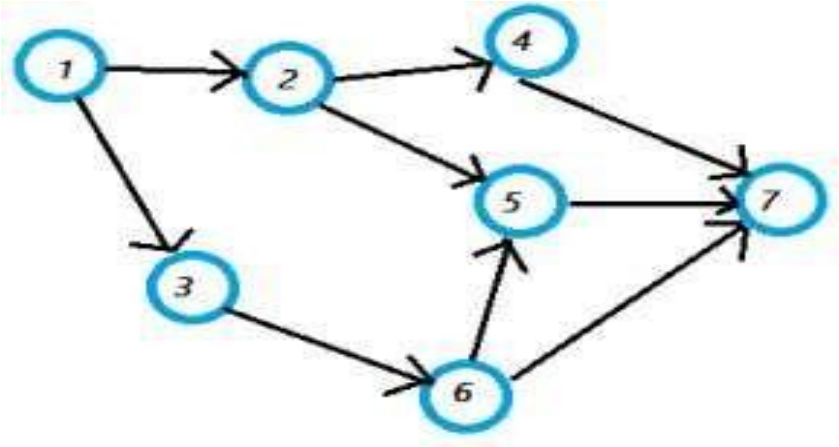
This graph (the thick black line) is acyclic, as it has no cycles (complete circuits).

A connected acyclic graph, like the one above, is called a **tree**. If one or more of the tree "branches" is disconnected, the acyclic graph is a called a **forest**.



This graph has a complete circuit and so is not acyclic.

- A directed acyclic graph is an acyclic graph that has a direction as well as a lack of cycles.



- The parts of the above graph are:

Integer = the set for the the Vertices.

Vertices set = {1,2,3,4,5,6,7}.

Edge set = {(1,2), (1,3), (2,4), (2,5), (3,6), (4,7), (5,7), (6,7)}.

- A directed acyclic graph has a **topological ordering**. This means that the nodes are ordered so that the starting node has a lower value than the ending node.

- A DAG has a unique topological ordering if it has a directed path containing all the nodes; in this case the ordering is the same as the order in which the nodes appear in the path.

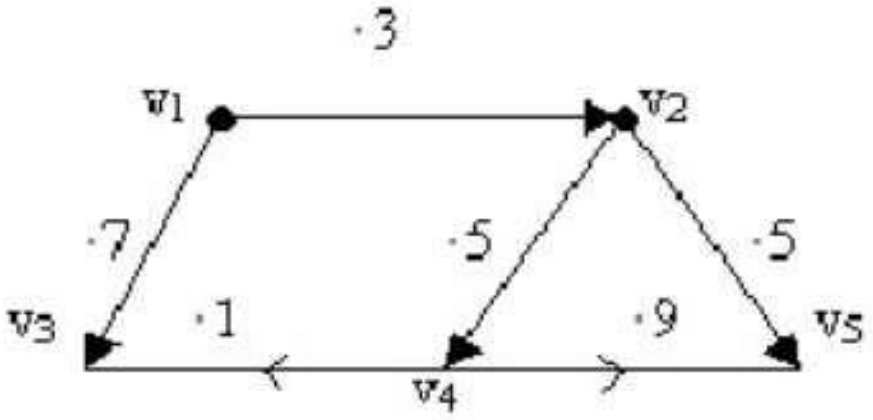
Weighted digraphs

- We can assign numbers to the edges or vertices of a graph in order to enable them to be used in physical problems. Such an assignment is called the weight of the edges or vertices.

- Weighted graphs are defined as the quadruples (V, E, f, g) or the triplets (V, E, f)or the triplets (V, E, g), where V is the set of vertices, E is the set of domains, f is the function with domain V, which assigns weights to vertices and g is the function with domain E, which assigns weights to edges

Example

Following diagram is a weighted digraph which represents the communication network among five individuals v1,v2,v3,v4,v5. The number assigned for each directed edge gives the probability of their communication.

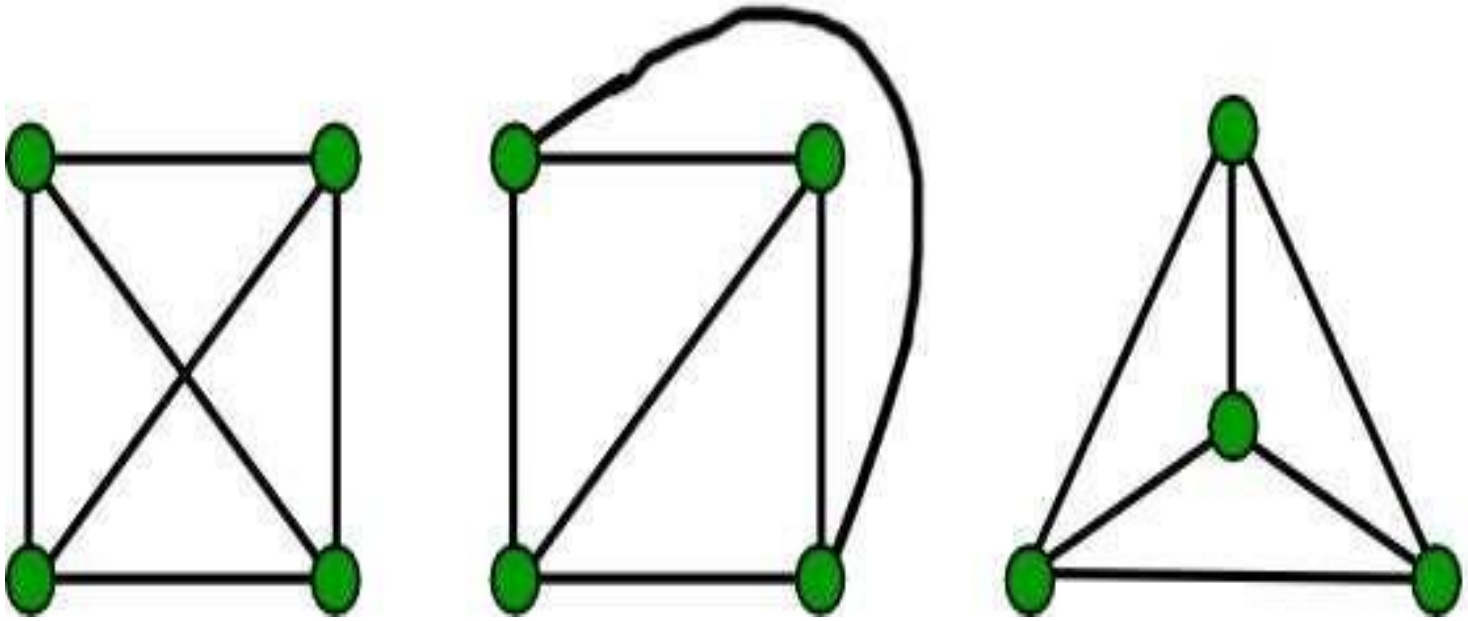


Region graph

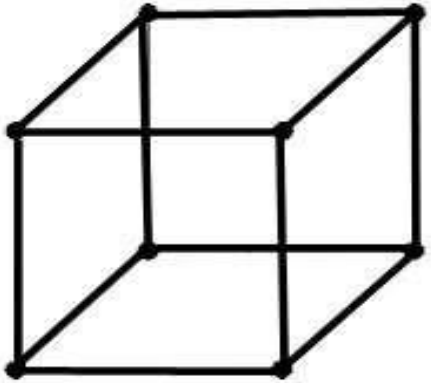
- **Planarity –** "A graph is said to be planar if it can be drawn on a plane **without any edges crossing**. Such a drawing is called a planar representation of the graph."

- **Important Note –** A graph may be planar even if it is drawn with crossings, because it may be possible to draw it in a different way without crossings.

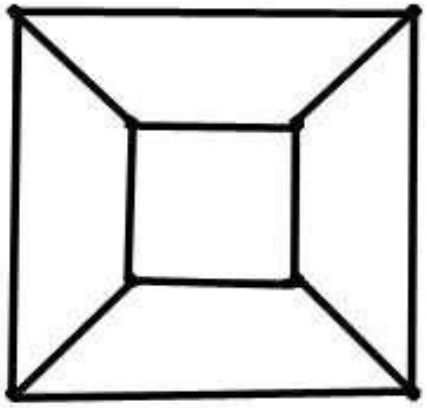
- For example consider the complete graph k4 and its two possible planar representations –



Example – Is the hypercube Q3 planar?

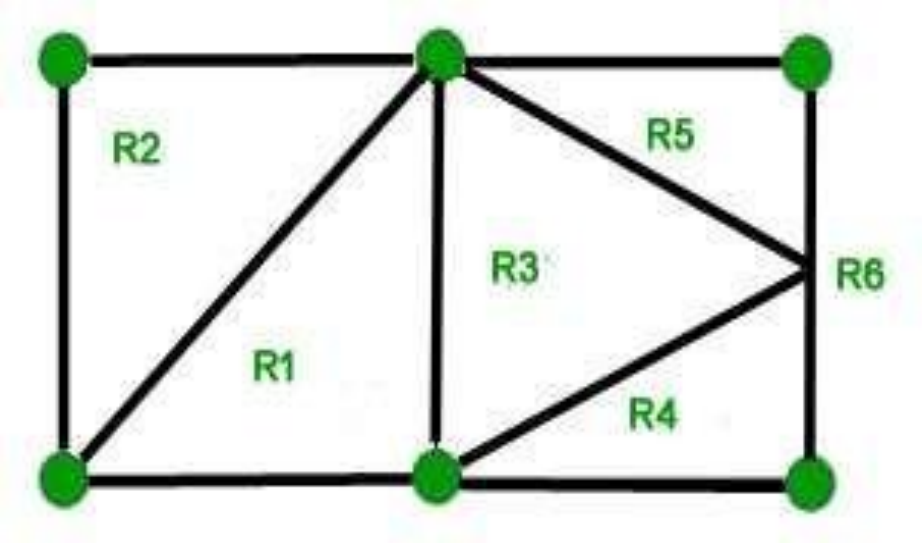


Solution – Yes, Q3 is planar. Its planar representation-



Regions in Planar Graphs

The planar representation of a graph splits the plane into **regions**. These regions are bounded by the edges except for one region that is unbounded. For example, consider the following graph



There are a total of 6 regions with 5 bounded regions and 1 bounded region R6.

- **Theorem –** "Let G be a **connected simple planar graph** with e edges and v vertices. Then the number of regions r in the graph is equal to **e-v+2**."
- **Example –** What is the number of regions in a connected planar simple graph with 20 vertices each with a degree of 3?
- **Solution –** Sum of degrees of edges = 20 * 3 = 60. By handshaking theorem, 2e=60 which gives e=30 .
  By Euler's theorem, the number of regions = e-v+2 which gives 12 regions.

An important result obtained by Euler's formula is the following inequality –

Note –"If G is a connected planar graph with e edges and v vertices, where v>=3, then **e<=ev-6**. Also G cannot have a vertex of degree exceeding 5."

Example – Is the graph K5 planar?

Solution – Number of vertices and edges in K5 is 5 and 10 respectively. Since 10 > 3*5 – 6, 10 > 9 the inequality e<=3v-6 is not satisfied. Thus the graph is not planar.