MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

LECTURE NOTES

ON

MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

II B. Tech I semester

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(R17A0503) MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

II Year B. Tech CSE - I Sem	L	T/P/D	C
	3	**1 / - / -**	**3**

Objectives:

- To explain with examples the basic terminology of functions, relations, and sets.
- To perform the operations associated with sets, functions, and relations.
- To relate practical examples to the appropriate set, function, or relation model, and interpret the associated operations and terminology in context.
- To describe the importance and limitations of predicate logic.
- To relate the ideas of mathematical induction to recursion and recursively defined structures.
- To use Graph Theory for solving problems

UNIT-I

Mathematical Logic: Statements and notations, Connectives, Well formed formulas, Truth Tables, tautology, equivalence implication, Normal forms, Quantifiers, universal quantifiers.

Predicates : Predicative logic, Free & Bound variables, Rules of inference, Consistency, proof of contradiction, Automatic Theorem Proving.

UNIT-II

Relations: Properties of Binary Relations, equivalence, transitive closure, compatibility and partial ordering relations, Lattices, Hasse diagram. Functions: Inverse Function Composition of functions, recursive Functions, Lattice and its Properties,

Algebraic structures: Algebraic systems Examples and general properties, Semigroups and monads, groups sub groups' homomorphism, Isomorphism.

UNIT-III

Elementary Combinatorics: Basis of counting, Combinations & Permutations, with repetitions, Constrained repetitions, Binomial Coefficients, Binomial Multinomial theorems, the principles of Inclusion – Exclusion. Pigeon hole principles and its application.

UNIT-IV

Recurrence Relation: Generating Functions, Function of Sequences Calculating Coefficient of generating function, Recurrence relations, Solving recurrence relation by substitution and Generating funds. Characteristics roots solution of In homogeneous Recurrence Relation.

UNIT-V

Graph Theory: Representation of Graph, DFS, BFS, Spanning Trees, planar Graphs. Graph Theory and Applications, Basic Concepts Isomorphism and Sub graphs, Multi graphs and Euler circuits, Hamiltonian graphs, Chromatic Numbers.

TEXT BOOKS:

1. Elements of DISCRETE MATHEMATICS- A computer Oriented Approach- C L Liu, D P Mohapatra. Third Edition, Tata McGraw Hill.

2. Discrete Mathematics for Computer Scientists & Mathematicians, J.L. Mott, A. Kandel, T.P. Baker, PHI.

REFERENCE BOOKS:

1.Discrete Mathematics and its Applications, Kenneth H. Rosen, Fifth Edition.TMH. 2.Discrete Mathematical structures Theory and application- Malik & Sen, Cengage. 3.Discrete Mathematics with Applications, Thomas Koshy, Elsevier.

4.Logic and Discrete Mathematics, Grass Man & Trembley, Pearson Education.

Outcomes:

- Ability to Illustrate by examples the basic terminology of functions, relations, and sets and demonstrate knowledge of their associated operations.
- Ability to Demonstrate in practical applications the use of basic counting principles of permutations, combinations, inclusion/exclusion principle and the pigeonhole methodology.
- Ability to represent and Apply Graph theory in solving computer science problems.

Unit – I
Mathematical Logic

INTRODUCTION

Proposition: A **proposition** or **statement** is a declarative sentence which is either true or false but not both. The truth or falsity of a proposition is called its **truth-value.**

These two values ‗true' and ‗false' are denoted by the symbols *T* and *F* respectively. Sometimes these are also denoted by the symbols 1 and 0 respectively.

Example 1: Consider the following sentences:

1. Delhi is the capital of India.
2. Kolkata is a country.
3. 5 is a prime number.
4. 2 + 3 = 4.

These are propositions (or statements) because they are either true of false. Next consider the following sentences:

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

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

Propositional Calculus is also known as **statement calculus.** It is the branch of mathematics that is used to describe a logical system or structure. A logical system consists of (1) a universe of propositions, (2) truth tables (as axioms) for the logical operators and (3) definitions that explain equivalence and implication of propositions.

Connectives

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

Negation

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

Table 1. Truth table for negation

p	¬p
T	F
	T
F	

Example 2: Consider the statement *p*: Kolkata is a city. Then ¬p: Kolkata is not a city.

Although the two statements ‗Kolkata is not a city' and ‗It is not the case that Kolkata is a city' are not identical, we have translated both of them by *p*. The reason is that both these statements have the same meaning.

Conjunction

The **conjunction** of two statements (or propositions) *p* and *q* is the statement *p* ∧ *q* which is read as ‗*p* and *q*'. The statement *p* ∧ *q* has the truth value *T* whenever both *p* and *q* have the truth value *T*. Otherwise it has truth value *F*.

Table 2. Truth table for conjunction

p	*q*	*p* ∧ *q*
T	*T*	*T*
T	*F*	*F*
F	*T*	*F*
F	*F*	*F*

Example 3: Consider the following statements

p : It is raining today.

q : There are 10 chairs in the room.

Then *p* ∧ *q* : It is raining today and there are 10 chairs in the room.

Note: Usually, in our everyday language the conjunction ‗and' is used between two statements which have some kind of relation. Thus a statement ‗It is raining today and 1 + 1 = 2' sounds odd, but in logic it is a perfectly acceptable statement formed from the statements ‗It is raining today' and ‗1 + 1 = 2'.

Example 4: Translate the following statement:

‗Jack and Jill went up the hill' into symbolic form using conjunction.

Solution: Let p : Jack went up the hill, q : Jill went up the hill.

Then the given statement can be written in symbolic form as p ∧ q.

Disjunction

The **disjunction** of two statements p and q is the statement p ∨ q which is read as ‗p or q'. The statement p ∨ q has the truth value F only when both p and q have the truth value F. Otherwise it has truth value T.

Table 3: Truth table for disjunction

p	*q*	*p* ∨ *q*
T	*T*	*T*
T	*F*	*T*
F	*T*	*T*
F	*F*	*F*

Example 5: Consider the following statements p : I shall go to the game.

q : I shall watch the game on television.

Then $p \vee q$: I shall go to the game or watch the game on television.

Conditional proposition

If p and q are any two statements (or propositions) then the statement $p \rightarrow q$ which is read as,

‗If p, then q' is called a **conditional statement** (or **proposition**) or **implication** and the connective is the **conditional connective.**

The conditional is defined by the following table:

Table 4. Truth table for conditional

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

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

To understand better, this connective can be looked as a conditional promise. If the promise is violated (broken), the conditional (implication) is false. Otherwise it is true. For this reason, the only circumstances under which the conditional $p \rightarrow q$ is false is when p is true and q is false.

Example 6: *Translate the following statement:*

'The crop will be destroyed if there is a flood' into symbolic form using conditional connective.

Solution: Let c : the crop will be destroyed; f : there is a flood. Let us rewrite the given statement as

‗If there is a flood, then the crop will be destroyed'. So, the symbolic form of the given statement is $f \rightarrow c$.

Example 7: Let p and q denote the statements: p : You drive over 70 km per hour.

q : You get a speeding ticket.

Write the following statements into symbolic forms.

(i) You will get a speeding ticket if you drive over 70 km per hour.

(ii) Driving over 70 km per hour is sufficient for getting a speeding ticket.

(iii) If you do not drive over 70 km per hour then you will not get a speeding ticket.
(iv) Whenever you get a speeding ticket, you drive over 70 km per hour.
Solution: (i) $p \rightarrow q$ (ii) $p \rightarrow q$ (iii) $p \rightarrow q$ (iv) $q \rightarrow p$.

Notes: 1. In ordinary language, it is customary to assume some kind of relationship between the antecedent and the consequent in using the conditional. But in logic, the antecedent and the

consequent in a conditional statement are not required to refer to the same subject matter. For example, the statement ‗If I get sufficient money then I shall purchase a high-speed computer' sounds reasonable. On the other hand, a statement such as ‗If I purchase a computer then this pen is red' does not make sense in our conventional language. But according to the definition of conditional, this proposition is perfectly acceptable and has a truth-value which depends on the truth-values of the component statements.

2. Some of the alternative terminologies used to express $p \rightarrow q$ (if p, then q) are the following: (*i*) p implies q

(ii) p only if q (‗If p, then q' formulation emphasizes the antecedent, whereas ‗p only if q' formulation emphasizes the consequent. The difference is only stylistic.)

(iii) q if p, or q when p.

(iv) q follows from p, or q whenever p.

(v) p is sufficient for q, or a sufficient condition for q is p. (*vi*) q is necessary for p, or a necessary condition for p is q. (*vii*) q is consequence of p.

Converse, Inverse and Contrapositive

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

(2). $\neg P \rightarrow \neg Q$ is called its *inverse*

(3). $\neg Q \rightarrow \neg P$ is called its *contrapositive*. Truth table for $Q \rightarrow P$ (converse of $P \rightarrow Q$)

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

Truth table for $\neg P \rightarrow \neg Q$ (inverse of $P \rightarrow Q$)

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

Truth table for $\neg Q \rightarrow \neg P$ (contrapositive of $P \rightarrow Q$)

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

Example: Consider the statement

P : It rains.

Q: The crop will grow. The implication $P \rightarrow Q$ states that

R: If it rains then the crop will grow.

The converse of the implication $P \rightarrow Q$, namely $Q \rightarrow P$ sates that *S*: If the crop will grow then there has been rain.

The inverse of the implication $P \rightarrow Q$, namely $\neg P \rightarrow \neg Q$ sates that *U*: If it does not rain then the crop will not grow.

The contraposition of the implication $P \rightarrow Q$, namely $\neg Q \rightarrow \neg P$ states that *T* : If the crop do not grow then there has been no rain.

Example 9: *Construct the truth table for* $(p \rightarrow q) \wedge (q \rightarrow p)$

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

Biconditional proposition

If *p* and *q* are any two statements (propositions), then the statement $p \leftrightarrow q$ which is read as ‗*p* if and only if *q*' and abbreviated as ‗*p* iff *q*' is called a **biconditional statement** and the connective is the **biconditional connective.**

The truth table of $p \leftrightarrow q$ is given by the following table:

Table 6. Truth table for biconditional

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

It may be noted that *p q* is true only when both *p* and *q* are true or when both *p* and *q* are false. Observe that *p q* is true when both the conditionals $p \rightarrow q$ and $q \rightarrow p$ are true, *i.e.*, the truth- values of $(p \rightarrow q) \wedge (q \rightarrow p)$, given in Ex. 9, are identical to the truth-values of *p q* defined here.

Note: The notation $p \leftrightarrow q$ is also used instead of $p \leftrightarrow q$.

TAUTOLOGY AND CONTRADICTION

Tautology: A statement formula which is true regardless of the truth values of

the statements which replace the variables in it is called a **universally valid formula** or a **logical truth** or a **tautology.**

Contradiction: A statement formula which is false regardless of the truth values of the statements which replace the variables in it is said to be a **contradiction.**

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

Substitution Instance

A formula A is called a substitution instance of another formula B if A can be obtained form B by substituting formulas for some variables of B, with the condition that the same formula is substituted for the same variable each time it occurs.

Example: Let $B : P \rightarrow (J \wedge P)$.

Substitute $R \leftrightarrow S$ for P in B, we get

(i): $(R \leftrightarrow S) \rightarrow (J \wedge (R \leftrightarrow S))$

Then A is a substitution instance of B.

Note that $(R \leftrightarrow S) \rightarrow (J \wedge P)$ is not a substitution instance of B because

the variables P in $J \wedge P$ was not replaced by $R \leftrightarrow S$.

Equivalence of Formulas

Two formulas A and B are said to equivalent to each other if and only if $A \leftrightarrow B$ is a tautology.

If $A \leftrightarrow B$ is a tautology, we write $A \Leftrightarrow B$ which is read as A is equivalent to B.

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

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

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

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

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

As $P \vee Q \quad \neg(\neg P \wedge \neg Q)$ is a tautology, then $P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$. Example: Prove $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Solution:

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

F	F	T	T	T	T

As $(P \rightarrow Q)$ $(\neg P \vee Q)$ is a tautology then $(P \rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Equivalence Formulas:

1. Idempotent laws:

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

2. Associative laws:

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

3. Commutative laws:

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

4. Distributive laws:

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

5. Identity laws:

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

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

6. Component laws:

   (a) (i) $P \vee \neg P \Leftrightarrow T$ (ii) $P \wedge \neg P \Leftrightarrow F$

   (b) (i) $\neg \neg P \Leftrightarrow P$ (ii) $\neg T \Leftrightarrow F$, $\neg F \Leftrightarrow T$

7. Absorption laws:

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

8. Demorgan‘s laws:

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

Method II. Replacement Process: Consider a formula $A : P \rightarrow (Q \rightarrow R)$. The formula $Q \rightarrow R$ is a part of the formula *A*. If we replace $Q \rightarrow R$ by an equivalent formula $\neg Q \vee R$ in *A*, we get another formula $B : P \rightarrow (\neg Q \vee R)$. One can easily verify that the formulas *A* and *B* are equivalent to each other. This process of obtaining *B* from *A* as the replacement process.

Example: Prove that $P \rightarrow (Q \rightarrow R) \Leftrightarrow P \rightarrow (\neg Q \vee R) \Leftrightarrow (P \wedge Q) \rightarrow R$.(May. 2010) Solution: $P \rightarrow (Q \rightarrow R) \Leftrightarrow P \rightarrow (\neg Q \vee R)$ $[\because Q \rightarrow R \Leftrightarrow \neg Q \vee R]$

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

$\Leftrightarrow (\neg P \vee \neg Q) \vee R$ [by Associative laws]

$\Leftrightarrow \neg(P \wedge Q) \vee R$ [by De Morgan‘s laws]

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

Example: Prove that $(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q$. Solution: $(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (\neg P \vee Q) \wedge (\neg R \vee Q)$

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

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

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

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

and

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

So, $P \rightarrow (Q \rightarrow P) \Leftrightarrow \neg P \rightarrow (P \rightarrow Q)$.

***Example: Prove that $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$. (Nov. 2009) Solution:

$$(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R)$$
$\Leftrightarrow ((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$ [Associative and Distributive laws]

$\Leftrightarrow (\neg(P \vee Q) \wedge R) \vee ((Q \vee P) \wedge R)$ [De Morgan's laws]

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

$\Leftrightarrow T \wedge R$ [$\because \neg P \vee P \Leftrightarrow T$]

$\Leftrightarrow R$

**Example: Show $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is tautology. Solution: By De Morgan's laws, we have

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

Therefore

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

Also

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

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

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

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

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

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

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

$\Leftrightarrow T$

Hence the given formula is a tautology.

Example: Show that $(P \wedge Q) \rightarrow (P \vee Q)$ is a tautology. (Nov. 2009) Solution: $(P \wedge Q) \rightarrow (P \vee Q) \Leftrightarrow \neg(P \wedge Q) \vee (P \vee Q)$ [$\because P \rightarrow Q \Leftrightarrow \neg P \vee Q$]

$\Leftrightarrow (\neg P \vee \neg Q) \vee (P \vee Q)$ [by De Morgan's laws]

$\Leftrightarrow (\neg P \vee P) \vee (\neg Q \vee Q)$ [by Associative laws and commutative laws]

$\Leftrightarrow (T \vee T)$[by negation laws]

$\Leftrightarrow T$

Hence, the result.

Example: Write the negation of the following statements.

(a). Jan will take a job in industry or go to graduate school. (b). James will bicycle or run tomorrow.

(c). If the processor is fast then the printer is slow.

Solution: (a). Let P : Jan will take a job in industry.

Q: Jan will go to graduate school.

The given statement can be written in the symbolic as $P \vee Q$. The negation of $P \vee Q$ is given by $\neg(P \vee Q)$.

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

$\neg P \wedge \neg Q$: Jan will not take a job in industry and he will not go to graduate school. (b). Let P : James will bicycle.

Q: James will run tomorrow.

The given statement can be written in the symbolic as $P \vee Q$. The negation of $P \vee Q$ is given by $\neg(P \vee Q)$.

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

$\neg P \wedge \neg Q$: James will not bicycle and he will not run tomorrow. (c). Let P : The processor is fast.

Q: The printer is slow.

The given statement can be written in the symbolic as $P \rightarrow Q$.

The negation of $P \rightarrow Q$ is given by $\neg(P \rightarrow Q)$.

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

$P \wedge \neg Q$: The processor is fast and the printer is fast.

Example: Use Demorgans laws to write the negation of each statement. (a). I want a car and worth a cycle. (b). My cat stays outside or it makes a mess. (c). I‘ve fallen and I can‘t get up.
(d). You study or you don‘t get a good grade.

Solution: (a). I don‘t want a car or not worth a cycle.
(b). My cat not stays outside and it does not make a mess.

(c). I have not fallen or I can get up.

(d). You can not study and you get a good grade. Exercises: 1. Write the negation of the following statements. (a). If it is raining, then the game is canceled.

(b). If he studies then he will pass the examination.

Are $(p \to q) \to r$ and $p \to (q \to r)$ logically equivalent? Justify your answer by using the rules of logic to simply both expressions and also by using truth tables. Solution: $(p \to q) \to r$ and $p \to (q \to r)$ are not logically equivalent because

Method I: Consider

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

and

$$p \to (q \to r) \Leftrightarrow p \to (\neg q \vee r)$$
$$\Leftrightarrow \neg p \vee (\neg q \vee r) \Leftrightarrow$$
$$\neg p \vee \neg q \vee r.$$

Method II: (Truth Table Method)

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

Here the truth values (columns) of $(p \to q) \to r$ and $p \to (q \to r)$ are not identical.

Consider the statement: ‖If you study hard, then you will excel‖. Write its converse, contra positive and logical negation in logic.

Duality Law

Two formulas A and A^* are said to be *duals* of each other if either one can be

obtained from the other by replacing $\wedge$ by $\vee$ and $\vee$ by $\wedge$. The connectives $\vee$ and $\wedge$ are called *duals* of each other. If the formula A contains the special variable T or F , then A^*, its dual is obtained by replacing T by F and F by T in addition to the above mentioned interchanges. Example: Write the dual of the following formulas:

(i). $(P \vee Q) \wedge R$ (ii). $(P \wedge Q) \vee T$ (iii). $(P \wedge Q) \vee (P \vee \neg(Q \wedge \neg S))$

Solution: The duals of the formulas may be written as

(i). $(P \wedge Q) \vee R$ (ii). $(P \vee Q) \wedge F$ (iii). $(P \vee Q) \wedge (P \wedge \neg(Q \vee \neg S))$

Result 1: The negation of the formula is equivalent to its dual in which every variable is replaced by its negation.

We can prove

$$\neg A(P_1, P_2, ..., P_n) \Leftrightarrow A^*(\neg P_1, \neg P_2, ..., \neg P_n)$$

Example: Prove that (a). $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (\neg P \vee Q)$ (b). $(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge Q)$

Solution: (a). $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (P \wedge Q) \vee (\neg P \vee (\neg P \vee Q))$ [$\because P \rightarrow Q \Leftrightarrow \neg P \vee Q$]

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

(b). From (a)

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

Writing the dual

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

Tautological Implications

A statement formula A is said to *tautologically imply* a statement B if and only if $A \rightarrow B$ is a tautology.

In this case we write $A \Rightarrow B$, which is read as 'A implies B'.

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

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

Clearly $A \Rightarrow B$ guarantees that B has a truth value T whenever A has the truth value T .

One can determine whether $A \Rightarrow B$ by constructing the truth tables of A and B in the same manner as was done in the determination of $A \Leftrightarrow B$. Example: Prove that $(P \rightarrow Q) \Rightarrow (\neg Q \rightarrow \neg P)$.

Solution:

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

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

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

In order to show any of the given implications, it is sufficient to show that an assignment of the truth value T to the antecedent of the corresponding conditional leads to the truth value T for the consequent. This procedure guarantees that the conditional becomes tautology, thereby proving the implication.

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

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

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

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

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

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

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

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

Other Connectives

We introduce the connectives NAND, NOR which have useful applications in the design of computers.

NAND: The word NAND is a combination of ‘NOT‘ and ‘AND‘ where ‘NOT‘ stands for negation and ‘AND‘ for the conjunction. It is denoted by the symbol ↑.

If P and Q are two formulas then

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

The connective $\uparrow$ has the following equivalence:

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

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

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

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

NAND is Commutative: Let P and Q be any two statement formulas.

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

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

$$(Q \uparrow P)$$

$\therefore$ NAND is commutative.

NAND is not Associative: Let P , Q and R be any three statement formulas. Consider $\uparrow (Q \uparrow R) \Leftrightarrow \neg(P \wedge (Q \uparrow R)) \Leftrightarrow$

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

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

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

$Q) \uparrow R$

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

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

Therefore the connective $\uparrow$ is not associative.

NOR: The word NOR is a combination of 'NOT' and 'OR' where 'NOT' stands for negation and

_OR' for the disjunction. It is denoted by the symbol $\downarrow$.

If P and Q are two formulas then

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

Q) The connective $\downarrow$ has the following equivalence:

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

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

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

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

NOR is Commutative: Let P and Q be any two statement formulas.

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

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

$$(Q \downarrow P)$$

$\therefore$ NOR is commutative.

NOR is not Associative: Let P , Q and R be any three statement formulas. Consider

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

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

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

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

$Q) \downarrow R$

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

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

Therefore the connective $\downarrow$ is not associative.

Evidently, $P \uparrow Q$ and $P \downarrow Q$ are duals of each other. Since

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

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

Example: Express $P \downarrow Q$ interms of $\uparrow$ only. Solution:

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

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

$$\Leftrightarrow [(P \uparrow P) \uparrow (Q \uparrow Q)] \uparrow [(P \uparrow P) \uparrow (Q \uparrow Q)]$$

Example: Express $P \uparrow Q$ interms of $\downarrow$ only.

(May-2012) Solution: $\uparrow Q \Leftrightarrow \neg(P \wedge Q)$

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

$$\Leftrightarrow [(P \downarrow P) \downarrow (Q \downarrow Q)] \downarrow [(P \downarrow P) \downarrow (Q \downarrow Q)]$$

Truth Tables

Example: Show that $(A \oplus B) \vee (A \downarrow B) \Leftrightarrow (A \uparrow B)$.

(May-2012) Solution: We prove this by constructing truth table.

A	B	$A \oplus B$	$A \downarrow B$	$(A \oplus B) \vee (A \downarrow B)$	$A \uparrow B$
T	T	F	F	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	T	T	T

As columns $(A \oplus B) \vee (A \downarrow B)$ and $(A \uparrow B)$ are identical.

$$\therefore (A \oplus B) \vee (A \downarrow B) \Leftrightarrow (A \uparrow B).$$

Normal Forms

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

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

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

The construction of truth table involves a finite number of steps, but the construc-tion may not be practical. We therefore reduce the given statement formula to normal form and find whether a given statement formula is a Tautology or Contradiction or atleast satisfiable.

It will be convenient to use the word ‖product‖ in place of ‖conjunction‖ and ‖sum‖ inplace of ‖disjunction‖ in our current discussion.

A product of the variables and their negations in a formula is called an *elementary product*. Similarly, a sum of the variables and their negations in a formula is called an *elementary sum*.

Let P and Q be any atomic variables. Then P , $\neg P \wedge Q$, $\neg Q \wedge P$ $\neg P$, P $\neg P$, and $Q \wedge \neg P$

are some examples of elementary products. On the other hand, P , $\neg P \vee Q$, $\neg Q \vee P$ $\vee \neg P$, P

$\vee \neg P$, and $Q \vee \neg P$ are some examples of elementary sums.

Any part of an elementary sum or product which is itself an elementary sum or product is called a *factor* of the original elementary sum or product. Thus $\neg Q, \wedge \neg P$, and $\neg Q \wedge P$ are some of the factors of $\neg Q \wedge P \wedge \neg P$.

Disjunctive Normal Form (DNF)

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

Example: Obtain disjunctive normal forms of

(a) $P \wedge (P \rightarrow Q)$; (b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$.

Solution: (a) We have

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

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

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

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

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

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

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

which is the required disjunctive normal form.

Note: The DNF of a given formula is not unique.

Conjunctive Normal Form (CNF)

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

The method for obtaining conjunctive normal form of a given formula is

similar to the one given for disjunctive normal form. Again, the conjunctive normal form is not unique.

Example: Obtain conjunctive normal forms of

(a) $P \wedge (P \rightarrow Q)$; (b) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$.

Solution: (a). $P \wedge (P \rightarrow Q) \Leftrightarrow P \wedge (\neg P \vee Q)$ (b). $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

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

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

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

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

Note: A given formula is tautology if every elementary sum in CNF is tautology. Example: Show that the formula $Q \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$ is a tautology.

Solution: First we obtain a CNF of the given formula.

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

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

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

Since each of the elementary sum is a tautology, hence the given formula is tautology.

Principal Disjunctive Normal Form

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

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

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

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

Minterms for three variables P , Q and R are $P \wedge Q \wedge R$, $P \wedge Q \wedge \neg R$, $P \wedge \neg Q \wedge R$,P$\wedge \neg Q \wedge \neg R$, $\neg P \wedge Q \wedge R$, $\neg P \wedge Q \wedge \neg R$, $\neg P \wedge \neg Q \wedge R$ and $\neg P \wedge \neg Q \wedge \neg R$. From the truth tables of these minterms of P and Q, it is clear that

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

F	F	F	F	F	T

(i). no two minterms are equivalent

(ii). Each minterm has the truth value *T* for exactly one combination of the truth values of the variables *P* and *Q*.

Definition: For a given formula, an equivalent formula consisting of disjunctions of minterms only is called the Principal disjunctive normal form of the formula.

The principle disjunctive normal formula is also called the sum-of-products canonical form.

Methods to obtain PDNF of a given formula

(a). By Truth table:

(i). Construct a truth table of the given formula.

(ii). For every truth value T in the truth table of the given formula, select the minterm which also has the value T for the same combination of the truth values of P and Q.

(iii). The disjunction of these minterms will then be equivalent to the given formula.

Example: Obtain the PDNF of $P \rightarrow Q$. Solution: From the truth table of $P \rightarrow Q$

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

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

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

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

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

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

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

(b). Without constructing the truth table:

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

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

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

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

Example: Obtain the principal disjunctive normal form of (*a*) $\neg P \vee Q$; (*b*) $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$.

Solution:

(a) $\neg P \vee Q \Leftrightarrow (\neg P \wedge T) \vee (Q \wedge T)$ $[\because A \wedge T \Leftrightarrow A]$

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

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

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

$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q)$ $[\because P \vee P \Leftrightarrow P]$ (*b*) $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$

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

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

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

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

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

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

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

Solution: We write the principal disjunctive normal form of each formula and com-pare these normal forms.

(*a*) $P \vee (P \wedge Q) \Leftrightarrow (P \wedge T) \vee (P \wedge Q)$ $[\because P \wedge Q \Leftrightarrow P]$

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

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

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

$\Leftrightarrow P]$ which is the required PDNF.

Now, $\Leftrightarrow P \wedge T$

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

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

$\neg Q$) which is the required PDNF.

Hence, $P \vee (P \wedge Q) \Leftrightarrow P$.

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

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

$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$ which is the required PDNF.

Now,

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

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

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

$\Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$ which is the required PDNF.

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

Example: Obtain the principal disjunctive normal form of

$P \rightarrow ((P \rightarrow Q) \wedge \neg(\neg Q \vee \neg P))$. (Nov. 2011) Solution: Using $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ and De Morgan's law, we obtain

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

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

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

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

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

$\Leftrightarrow (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q)$ Hence $(P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q)$ is the required PDNF.

Principal Conjunctive Normal Form

The dual of a minterm is called a Maxterm. For a given number of variables, the *maxterm* consists of disjunctions in which each variable or its negation, but not both,

appears only once. Each of the maxterm has the truth value *F* for exactly one combination of the truth values of the variables. Now we define the principal conjunctive normal form.

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

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

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

which is required principal conjunctive normal form.

Note: If the principal disjunctive (conjunctive) normal form of a given formula A containing n variables is known, then the principal disjunctive (conjunctive) normal form of $\neg A$ will consist of the disjunction (conjunction) of the remaining minterms (maxterms) which do not appear in the

principal disjunctive (conjunctive) normal form of A. From $A \Leftrightarrow \neg\neg A$ one can obtain the principal conjunctive (disjunctive) normal form of A by repeated applications of De Morgan‘s laws to the principal disjunctive (conjunctive) normal form of $\neg A$.

Example: Find the PDNF form PCNF of $S : P \vee (\neg P \rightarrow (Q \vee (\neg Q \rightarrow R)))$.
Solution:

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

which is the
PCNF.

Now PCNF of $\neg S$ is the conjunction of remaining maxterms, so

PCNF of $\neg S : (P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R)$
$$\wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee$$
$\neg R)$ Hence the PDNF of S is

$\neg$(PCNF of $\neg S$) : $(\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R)$

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

Theory of Inference for Statement Calculus

Definition: The main aim of logic is to provide rules of inference to infer a conclusion from certain premises. The theory associated with rules of inference is known as inference theory .

Definition: If a conclusion is derived from a set of premises by using the accepted rules of reasoning, then such a process of derivation is called a deduction or a formal proof and the argument is called a *valid argument* or conclusion is called a *valid conclusion*.

Note: Premises means set of assumptions, axioms, hypothesis.

Definition: Let A and B be two statement formulas. We say that $\|B$ *logically follows from* $A\|$ or

$\|B$ is a *valid conclusion (consequence)* of the premise $A\|$ iff $A \rightarrow B$ is a tautology,

that is $A \Rightarrow B$. *We say that from a set of premises {H1, H2,* $\cdots$ *, Hm}, a conclusion C follows logically iff*

$$H1 \wedge H2 \wedge ... \wedge Hm \Rightarrow C$$

(1)

Note: To determine whether the conclusion logically follows from the given premises, we use the following methods:

- Truth table method
- Without constructing truth table method.

Validity Using Truth Tables

Given a set of premises and a conclusion, it is possible to determine whether the conclusion logically follows from the given premises by constructing truth tables as follows.

Let $P_1, P_2, \cdots, P_n$ be all the atomic variables appearing in the premises $H_1, H_2, \cdots, H_m$ and in the conclusion C. If all possible combinations of truth values are assigned to $P_1, P_2, \cdots, P_n$ and if the truth values of $H_1, H_2, ..., H_m$ and C are entered in a table. We look for the rows in which all $H_1, H_2, \cdots, H_m$ have the value T. If, for every such row, C also has the value T, then (1) holds. That is, the conclusion follows logically.

Alternatively, we look for the rows on which C has the value F. If, in every such row, at least one of the values of $H_1, H_2, \cdots, H_m$ is F, then (1) also holds. We call such a method a _truth table technique' for the determination of the validity of a conclusion.

Example: Determine whether the conclusion C follows logically from the premises H_1 and H_2.

(a) $H_1 : P \rightarrow Q \quad H_2 : P \; C : Q$

(b) $H_1 : P \rightarrow Q \quad H_2 : \neg P \; C : Q$

(c) $H_1 : P \rightarrow Q \quad H_2 : \neg(P \wedge Q) \; C : \neg P$

(d) $H_1 : \neg P \quad H_2 : P \; Q \; C : \neg(P \wedge Q)$

(e) $H_1 : P \rightarrow Q \quad H_2 : Q \; C : P$

Solution: We first construct the appropriate truth table, as shown in table.

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

(a) We observe that the first row is the only row in which both the premises have the value *T*
. The conclusion also has the value *T* in that row. Hence it is valid.

In (b) the third and fourth rows, the conclusion Q is true only in the third row, but not in the fourth, and hence the conclusion is not valid.
Similarly, we can show that the conclusions are valid in (c) and (d) but not in (e).

Rules of Inference

The following are two important rules of inferences.

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

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

Implication Formulas

$I_1 : P \wedge Q \Rightarrow P$ (simplification)

$I_2 : P \wedge Q \Rightarrow$

Q $I_3 : P \Rightarrow P$

$\vee Q$ $I_4 : Q \Rightarrow$

$P \vee Q$

$I_5 : \neg P \Rightarrow P \rightarrow Q$

$I_6 : Q \Rightarrow P \rightarrow$

Q $I_7 : \neg(P \rightarrow$

$Q) \Rightarrow P$

$I_8 : \neg(P \rightarrow Q) \Rightarrow \neg Q$

$I_9 : P, Q \Rightarrow P \wedge Q$

$I_{10} : \neg P, P \vee Q \Rightarrow Q$ (disjunctive syllogism)

$I_{11} : P, P \rightarrow Q \Rightarrow Q$ (modus ponens)

$I_{12} : \neg Q, P \rightarrow Q \Rightarrow \neg P$ (modus tollens)

$I_{13} : P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$ (hypothetical syllogism)

$I_{14} : P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$ (dilemma)

Example: Demonstrate that *R* is a valid inference from the premises $P \rightarrow Q$, $Q \rightarrow R$, and P . Solution:

{1}	(1)	$P \rightarrow Q$	Rule P
{2}	(2)	P	Rule P,
{1, 2}	(3)	Q	Rule T, (1), (2), and $I13$
{4}	(4)	$Q \rightarrow R$	Rule P
{1, 2, 4}	(5)	R	Rule T, (3), (4), and $I13$

Hence the result.

Example: Show that $R \vee S$ follows logically from the premises $C \vee D$, $(C \vee D) \rightarrow \neg H$, $\neg H \rightarrow (A \wedge \neg B)$, and $(A \wedge \neg B) \rightarrow (R \vee S)$. Solution:

$\{1\}$	(1)	$(C \vee D) \rightarrow \neg H$	Rule P
$\{2\}$	(2)	$\neg H \rightarrow (A \wedge \neg B)$	Rule P
$\{1, 2\}$	(3)	$(C \vee D) \rightarrow (A \wedge \neg B)$	Rule T, (1), (2), and I_{13}
$\{4\}$	(4)	$(A \wedge \neg B) \rightarrow (R \vee S)$	Rule P
$\{1, 2, 4\}$	(5)	$(C \vee D) \rightarrow (R \vee S)$	Rule T, (3), (4), and I_{13}
$\{6\}$	(6)	$C \vee D$	Rule P
$\{1, 2, 4, 6\}$	(7)	$R \vee S$	Rule T, (5), (6), and I_{11}

Hence the result.

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

Solution:

$\{1\}$	(1)	$P \vee Q$	Rule P
$\{1\}$	(2)	$\neg P \rightarrow Q$	Rule T, (1) $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
$\{3\}$	(3)	$Q \rightarrow S$	Rule P
$\{1, 3\}$	(4)	$\neg P \rightarrow S$	Rule T, (2), (3), and I_{13}
$\{1, 3\}$	(5)	$\neg S \rightarrow P$	Rule T, (4), $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
$\{6\}$	(6)	$P \rightarrow R$	Rule P
$\{1, 3, 6\}$	(7)	$\neg S \rightarrow R$	Rule T, (5), (6), and I_{13}
$\{1, 3, 6\}$	(8)	$S \vee R$	Rule T, (7) and $P \rightarrow Q \Leftrightarrow \neg P \vee Q$

Hence the result.

Example: Show that $R \wedge (P \vee Q)$ is a valid conclusion from the

premises $P \vee Q$, $Q \rightarrow R$, $P \rightarrow M$, and $\neg M$.

Solution:

$\{1\}$	(1)	$P \rightarrow M$	Rule P
$\{2\}$	(2)	$\neg M$	Rule P
$\{1, 2\}$	(3)	$\neg P$	Rule T, (1), (2), and I_{12}
$\{4\}$	(4)	$P \vee Q$	Rule P

{1, 2, 4, 6}	(7)	R	Rule T, (5), (6), and I_{11}
{1, 2, 4, 6}	(8)	$R \wedge (P \vee Q)$	Rule T, (4), (7) and I_9

Hence the result.

Example: Show $I_{12} : \neg Q, P \rightarrow Q \Rightarrow \neg P$. Solution:

{1}	(1)	$P \rightarrow Q$	Rule P
{1}	(2)	$\neg Q \rightarrow \neg P$	Rule T, (1), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{3}	(3)	$\neg Q$	Rule P
{1, 3}	(4)	$\neg P$	Rule T, (2), (3), and I_{11}

Hence the result.

Example: Test the validity of the following argument:

‖If you work hard, you will pass the exam. You did not pass. Therefore, you did not work hard‖.

Example: Test the validity of the following statements:

‖If Sachin hits a century, then he gets a free car. Sachin does not get

a free car. Therefore, Sachin has not hit a century‖.

Rules of Conditional Proof or Deduction Theorem

We shall now introduce a third inference rule, known as CP or rule of conditional proof.
Rule CP: If we can derive S from R and a set of premises, then we can derive $R \rightarrow S$ from the set of premises alone.
Rule CP is not new for our purpose her because it follows from the equivalence

$$(P \wedge R) \rightarrow S \Leftrightarrow P \rightarrow (R \rightarrow S)$$

Let P denote the conjunction of the set of premises and let R be any formula. The above equivalence states that if R is included as an additional premise and S is derived from $P \wedge R$, then $R \rightarrow S$ can be derived from the premises P alone.

Rule CP is also called the *deduction theorem* and is generally used if the conclusion of the form $R \rightarrow S$. In such cases, R is taken as an additional premise and S is derived from the given premises and R.

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

(Nov. 2011)

Solution: Instead of deriving $R \rightarrow S$, we shall include R as an additional premise and show S
first.

{1}	(1)	$\neg R \vee P$	Rule P
{2}	(2)	R	Rule P (assumed premise)
{1, 2}	(3)	P	Rule T, (1), (2), and I_{10}
{4}	(4)	$P \rightarrow (Q \rightarrow S)$	Rule P
{1, 2, 4}	(5)	$Q \rightarrow S$	Rule T, (3), (4), and I_{11}
{6}	(6)	Q	Rule P
{1, 2, 4, 6}	(7)	S	Rule T, (5), (6), and I_{11}
{1, 2, 4, 6}	(8)	$R \rightarrow S$	Rule CP

Example: Show that $P \rightarrow S$ can be derived from the premises $\neg P \vee Q$, $\neg Q \vee R$, and $R \rightarrow S$. Solution: We include P as an additional premise and derive S.

{1}	(1)	$\neg P \vee Q$	Rule P
{2}	(2)	P	Rule P (assumed premise)
{1, 2}	(3)	Q	Rule T, (1), (2), and I_{10}
{4}	(4)	$\neg Q \vee R$	Rule P
{1, 2, 4}	(5)	R	Rule T, (3), (4), and I_{10}
{6}	(6)	$R \rightarrow S$	Rule P
{1, 2, 4, 6}	(7)	S	Rule T, (5), (6), and I_{11}
{1, 2, 4, 6}	(8)	$P \rightarrow S$	Rule CP

Example: If there was a ball game, then traveling was difficult. If they arrived on

time, then traveling was not difficult. They arrived on time. Therefore, there was no ball game‘. Show that these statements constitute a valid argument. Solution: Let us indicate the statements as follows:

P : There was a ball game. *Q*: Traveling was difficult. *R*: They arrived on time.

Hence, the given premises are $P \rightarrow Q$, $R \rightarrow \neg Q$, and R. The conclusion is $\neg P$.

{1}	(1) $R \rightarrow \neg Q$	Rule P
{2}	(2) R	Rule P
{1, 2}	(3) $\neg Q$	Rule T, (1), (2), and I_{11}
{4}	(4) $P \rightarrow Q$	Rule P
{4}	(5) $\neg Q \rightarrow \neg P$	Rule T, (4), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{1, 2, 4}	(6) $\neg P$	Rule T, (3), (5), and I_{11}

Example: By using the method of derivation, show that following statements constitute a valid argument: ‖If A works hard, then either B or C will enjoy. If B enjoys, then A will not work hard. If D enjoys, then C will not. Therefore, if A works hard, D will not enjoy.

Solution: Let us indicate statements as follows:

Given premises are $P \rightarrow (Q \vee R)$, $Q \rightarrow \neg P$, and $S \rightarrow \neg R$. The conclusion is $P \rightarrow \neg S$. We include P as an additional premise and derive $\neg S$.

{1}	(1) P	Rule P (additional premise)
{2}	(2) $P \rightarrow (Q \vee R)$	Rule P
{1, 2}	(3) $Q \vee R$	Rule T, (1), (2), and I_{11}
{1, 2}	(4) $\neg Q \rightarrow R$	Rule T, (3) and $P \rightarrow Q \Leftrightarrow P \vee Q$
{1, 2}	(5) $\neg R \rightarrow Q$	Rule T, (4), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{6}	(6) $Q \rightarrow \neg P$	Rule P
{1, 2, 6}	(7) $\neg R \rightarrow \neg P$	Rule T, (5), (6), and I_{13}
{1, 2, 6}	(8) $P \rightarrow R$	Rule T, (7) and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{9}	(9) $S \rightarrow \neg R$	Rule P
{9}	(10) $R \rightarrow \neg S$	Rule T, (9) and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{1, 2, 6, 9}	(11) $P \rightarrow \neg S$	Rule T, (8), (10) and I_{13}
{1, 2, 6, 9}	(12) $\neg S$	Rule T, (1), (11) and I_{11}

Example: Determine the validity of the following arguments using propositional logic:
‖Smoking is healthy. If smoking is healthy, then cigarettes are prescribed

by physi- cians. Therefore, cigarettes are prescribed by physicians‖.

(May-2012)

Solution: Let us indicate the statements as follows:

P : Smoking is healthy.

Q: Cigarettes are prescribed by physicians.

Hence, the given premises are P , $P \rightarrow Q$. The conclusion is Q.

{1}	(1) $P \rightarrow Q$	Rule P
{2}	(2) P	Rule P

{1, 2}	(3) Q	Rule T, (1), (2), and I_{11}

Hence, the given statements constitute a valid argument.

Consistency of Premises

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

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

Alternatively, a set of formulas $H_1, H_2, \cdots, H_m$ is inconsistent if their conjunction implies a contradiction, that is,

$$H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow R \wedge \neg R$$

where R is any formula.

Example: Show that the following premises are inconsistent:

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

Solution: Let us indicate the statements as follows:

E: Jack misses many classes through illness.
S: Jack fails high school.
A: Jack reads a lot of books.
H: Jack is uneducated.

The premises are $E \rightarrow S$, $S \rightarrow H$, $A \rightarrow \neg H$, and $E \wedge A$.

{1}	(1) $E \rightarrow S$	Rule P
{2}	(2) $S \rightarrow H$	Rule P
{1, 2}	(3) $E \rightarrow H$	Rule T, (1), (2), and I_{13}
{4}	(4) $A \rightarrow \neg H$	Rule P
{4}	(5) $H \rightarrow \neg A$	Rule T, (4), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{1, 2, 4}	(6) $E \rightarrow \neg A$	Rule T, (3), (5), and I_{13}
{1, 2, 4}	(7) $\neg E \vee \neg A$	Rule T, (6) and $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
{1, 2, 4}	(8) $\neg(E \wedge A)$	Rule T, (7), and $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
{9}	(9) $E \wedge A$	Rule P

{1, 2, 4, 9}	(10)	$\neg(E \wedge A) \wedge (E \wedge A)$	Rule T, (8), (9) and $I9$

Thus, the given set of premises leads to a contradiction and hence it is inconsistent.

Example: Show that the following set of premises is inconsistent: ‖If the contract is valid, then John is liable for penalty. If John is liable for penalty, he will go bankrupt. If the bank will loan him money, he will not go bankrupt. As a matter of fact, the contract is valid, and the bank will loan him money.‖

Solution: Let us indicate the statements as follows:

V : The contract is valid.

L: John is liable for

penalty. M: Bank will

loan him money. B: John

will go bankrupt.

{1}	(1) $V \rightarrow L$	Rule P
{2}	(2) $L \rightarrow B$	Rule P
{1, 2}	(3) $V \rightarrow B$	Rule T, (1), (2), and I_{13}
{4}	(4) $M \rightarrow \neg B$	Rule P
{4}	(5) $M \rightarrow \neg M$	Rule T, (4), and $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
{1, 2, 4}	(6) $V \rightarrow \neg M$	Rule T, (3), (5), and I_{13}
{1, 2, 4}	(7) $\neg V \vee \neg M$	Rule T, (6) and $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
{1, 2, 4}	(8) $\neg(V \wedge M)$	Rule T, (7), and $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
{9}	(9) $V \wedge M$	Rule P
{1, 2, 4, 9}	(10) $\neg(V \wedge M) \wedge (V \wedge M)$	Rule T, (8), (9) and I_9

Thus, the given set of premises leads to a contradiction and hence it is inconsistent.

Indirect Method of Proof

The method of using the rule of conditional proof and the notion of an inconsistent set of premises is called the *indirect method of proof* or *proof by contradiction*.

In order to show that a conclusion C follows logically from the premises $H_1, H_2, \cdots, H_m$, we assume that C is false and consider $\neg C$ as an additional premise. If the new set of premises is inconsistent, so that they imply a contradiction. Therefore, the assump-tion that $\neg C$ is true does not hold.

Hence, C is true whenever $H_1, H_2, \cdots, H_m$ are true. Thus, C follows

logically from the premises $H_1, H_2, \cdots, H_m$.

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

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

{1}	(1) $\neg\neg(P \wedge Q)$	Rule P (assumed)
{1}	(2) $P \wedge Q$	Rule T, (1), and $\neg\neg P \Leftrightarrow P$
{1}	(3) P	Rule T, (2), and I_1
{4}	(4) $\neg P \wedge \neg Q$	Rule P
{4}	(5) $\neg P$	Rule T, (4), and I_1
{1, 4}	(6) $P \wedge \neg P$	Rule T, (3), (5), and I_9

Hence, our assumption is wrong.

Thus, $\neg(P \wedge Q)$ follows from $\neg P \wedge \neg Q$.

Example: Using the indirect method of proof, show that

$$P \rightarrow Q,\ Q \rightarrow R,\ \neg(P \wedge R),\ P \vee R \Rightarrow R.$$

Solution: We include $\neg R$ as an additional premise. Then we show that this leads to a contradiction.

{1}	(1) $P \rightarrow Q$	Rule P
{2}	(2) $Q \rightarrow R$	Rule P
{1, 2}	(3) $P \rightarrow R$	Rule T, (1), (2), and I_{13}
{4}	(4) $\neg R$	Rule P (assumed)
{1, 2, 4}	(5) $\neg P$	Rule T, (4), and I_{12}
{6}	(6) $P \vee R$	Rule P
{1, 2, 4, 6}	(7) R	Rule T, (5), (6) and I_{10}
{1, 2, 4, 6}	(8) $R \wedge \neg R$	Rule T, (4), (7), and I_9

Hence, our assumption is wrong.

Example: Show that the following set of premises are inconsistent, using proof by contradiction

$$P \rightarrow (Q \vee R),\ Q \rightarrow \neg P,\ S \rightarrow \neg R,\ P \Rightarrow P \rightarrow \neg S.$$

Solution: We include $\neg(P \rightarrow \neg S)$ as an additional premise. Then we show that this leads to a contradiction.

$$\therefore \neg(P \rightarrow \neg S) \Leftrightarrow \neg(\neg P \vee \neg S) \Leftrightarrow P \wedge S.$$

{1}	(1)	$P \rightarrow (Q \vee R)$	Rule P
{2}	(2)	P	Rule P
{1, 2}	(3)	$Q \vee R$	Rule T, (1), (2), and Modus Ponens
{4}	(4)	$P \wedge S$	Rule P (assumed)
{1, 2, 4}	(5)	S	Rule T, (4), and $P \wedge Q \Rightarrow P$

{6}	(6)	$S \rightarrow \neg R$	Rule P
{1, 2, 4, 6}	(7)	$\neg R$	Rule T, (5), (6) and Modus Ponens
{1, 2, 4, 6}	(8)	Q	Rule T, (3), (7), and $P \wedge Q, \neg Q \Rightarrow P$
{9}	(9)	$Q \rightarrow \neg P$	Rule P
{1, 2, 4, 6}	(10)	$\neg P$	Rule T, (8), (9), and $P \wedge Q, \neg Q \Rightarrow P$
{1, 2, 4, 6}	(11)	$P \wedge \neg P$	Rule T, (2), (10), and $P, Q \Rightarrow P \wedge Q$
{1, 2, 4, 6}	(12)	F	Rule T, (11), and $P \wedge \neg P \Leftrightarrow F$

Hence, it is proved that the given premises are inconsistent.

The Predicate Calculus

Predicate

A part of a declarative sentence describing the properties of an object is called a predicate. The logic based upon the analysis of predicate in any statement is called predicate logic.

Consider two statements:

John is a bachelor Smith is a bachelor.

In each statement ‖is a bachelor‖ is a predicate. Both John and Smith have the same property of being a bachelor. In the statement logic, we require two diff erent symbols to express them and these symbols do not reveal the common property of these statements. In predicate calculus these statements can be replaced by a single statement ‖*x* is a bachelor‖. A predicate is symbolized by a capital letters which is followed by the list of variables. The list of variables is enclosed in parenthesis. If *P* stands for the predicate ‖is a bachelor‖, then *P* (*x*) stands for ‖*x* is a bachelor‖,where *x* is a predicate variable.

`The domain for *P* (*x*) : *x* is a bachelor, can be taken as the set of all human names. Note that *P* (*x*) is not a statement, but just an expression. Once a value is assigned to *x*, *P* (*x*) becomes a statement and has the truth value. If *x* is Ram, then *P* (*x*) is a statement and its truth value is true.

Quantifiers

Quantifiers: Quantifiers are words that are refer to quantities such as ‘some‘ or ‘all‘. Universal Quantifier: The phrase ‘forall‘ (denoted by ∀) is called the universal quantifier. For example, consider the sentence ‖All human beings are mortal‖.

Let *P* (*x*) denote ‘*x* is a mortal‘.

Then, the above sentence can be

written as $(\forall x \in S)P(x)$ or

$\forall x P(x)$

where S denote the set of all human beings.

$\forall x$ represents each of the following phrases, since they have essentially the same for all x

For every x
For each x.

Existential Quantifier: The phrase ‘there exists‘ (denoted by $\exists$) is called the exis-tential quantifier.

For example, consider the sentence

‖There exists x such that $x^2 = 5$.

This sentence can be written as

$$(\exists x \in R)P(x) \text{ or } (\exists x)P(x), \text{ where } P(x) : x^2 = 5.$$

$\exists x$ represents each of the following phrases There exists an x
There is an x
For some x
There is at least one x.

Example: Write the following statements in symbolic form: (i). Something is good
(ii). Everything is good (iii). Nothing is good
(iv). Something is not good.

Solution: Statement (i) means ‖There is atleast one x such that, x is good‖.
Statement (ii) means ‖Forall x, x is good‖. Statement (iii) means, ‖Forall x, x is not good‖.
Statement (iv) means, ‖There is atleast one x such that, x is not good.
Thus, if $G(x)$: x is good, then

statement (i) can be denoted by

$(\exists x)G(x)$ statement (ii) can be denoted

by $(\forall x)G(x)$ statement (iii) can be

denoted by $(\forall x)\neg G(x)$

statement (iv) can be denoted by $(\exists x)\neg G(x)$.

Example: Let $K(x)$: x is a man
$L(x)$: x is mortal
$M(x)$: x is an integer
$N(x)$: x either positive or negative Express the following using quantifiers:

- All men are mortal
- Any integer is either positive or negative.

Solution: (a) The given statement can be written as
for all x, if x is a man, then x is mortal and this can be expressed as $(x)(K(x) \rightarrow L(x))$.

(b) The given statement can be written as
for all x, if x is an integer, then x is either positive or negative and this can be expressed as $(x)(M(x) \rightarrow N(x))$.

Free and Bound Variables

Given a formula containing a part of the form $(x)P(x)$ or $(\exists x)P(x)$, such a part is called an x-bound part of the formula. Any occurrence of x in an x-bound part of the formula is called a bound occurrence of x, while any occurrence of x or of any variable that is not a bound occurrence is called a free occurrence. The smallest formula immediately following $(\forall x)$ or $(\exists x)$ is called the scope of the quantifier.

Consider the following formulas:

- $(x)P(x, y)$
- $(x)(P(x) \rightarrow Q(x))$
- $(x)(P(x) \rightarrow (\exists y)R(x, y))$
- $(x)(P(x) \rightarrow R(x)) \vee (x)(R(x) \rightarrow Q(x))$
- $(\exists x)(P(x) \wedge Q(x))$
- $(\exists x)P(x) \wedge Q(x)$.

In (1), $P(x, y)$ is the scope of the quantifier, and occurrence of x is bound occurrence, while the occurrence of y is free occurrence.

In (2), the scope of the universal quantifier is $P(x) \rightarrow Q(x)$, and all concrescences of x are bound.

In (3), the scope of (x) is $P(x) \rightarrow (\exists y)R(x, y)$, while the scope of $(\exists y)$ is $R(x, y)$. All occurrences of both x and y are bound occurrences.

In (4), the scope of the first quantifier is $P(x) \rightarrow R(x)$ and the scope of the second is $R(x) \rightarrow Q(x)$. All occurrences of x are bound

occurrences. In (5), the scope $(\exists x)$ is $P(x) \wedge$

$Q(x)$.

In (6), the scope of $(\exists x)$ is $P(x)$ and the last of occurrence of x in $Q(x)$ is free.

Negations of Quantified Statements

(i). $\neg(x)P(x) \Leftrightarrow (\exists x)\neg P(x)$

(ii). $\neg(\exists x)P(x) \Leftrightarrow (x)(\neg P(x))$.

Example: Let $P(x)$ denote the statement ‖x is a professional athlete‖ and let $Q(x)$ denote the statement ‖x plays soccer‖. The domain is the set of all people.

(a). Write each of the following proposition in English.

- $(x)(P(x) \rightarrow Q(x)$

- $(\exists x)(P(x) \wedge Q(x))$
- $(x)(P(x) \vee Q(x))$

(b). Write the negation of each of the above propositions, both in symbols and in words. Solution:

(a). (i). For all x, if x is an professional athlete then x plays soccer.

‖All professional athletes plays soccer‖ or ‖Every professional athlete plays soccer‖.

(ii). There exists an x such that x is a professional athlete and x plays soccer.

‖Some professional athletes paly soccer‖.

(iii). For all x, x is a professional athlete or x plays soccer.

‖Every person is either professional athlete or plays soccer‖.

(b). (i). In symbol: We know that

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

$$\Leftrightarrow (\exists x)(P(x) \wedge \neg Q(x))$$

There exists an x such that, x is a professional athlete and x does not paly soccer.

In words: ‖Some professional athlete do not play soccer‖. (ii). $\neg(\exists x)(P(x) \wedge Q(x)) \Leftrightarrow (x)(\neg P(x) \vee \neg Q(x))$

In words: ‖Every people is neither a professional athlete nor plays soccer‖ or All people either not a professional athlete or do not play soccer‖. (iii). $\neg(x)(P(x) \vee Q(x)) \Leftrightarrow (\exists x)(\neg P(x) \wedge \neg Q(x))$.

In words: ‖Some people are not professional athlete or do not paly soccer‖.

Inference Theory of the Predicate Calculus

To understand the inference theory of predicate calculus, it is important to be famil-iar with the following rules:

Rule US: Universal specification or instaniation

$$(x)A(x) \Rightarrow A(y)$$

From $(x)A(x)$, one can conclude $A(y)$.

Rule ES: Existential specification

$$(\exists x)A(x) \Rightarrow A(y)$$

From $(\exists x)A(x)$, one can conclude $A(y)$.

Rule EG: Existential generalization

$$A(x) \Rightarrow (\exists y)A(y)$$

From $A(x)$, one can conclude $(\exists y)A(y)$. Rule UG: Universal generalization

$$A(x) \Rightarrow (y)A(y)$$

From $A(x)$, one can conclude $(y)A(y)$.

Equivalence formulas:

$E31 : (\exists x)[A(x) \vee B(x)] \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$

$E32 : (x)[A(x) \wedge B(x)] \Leftrightarrow (x)A(x) \wedge (x)B(x)$

$E33 : \neg(\exists x)A(x) \Leftrightarrow (x)\neg A(x)$

$E34 : \neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$

$E35 : (x)(A \vee B(x)) \Leftrightarrow A \vee (x)B(x)$

$E36 : (\exists x)(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)B(x)$

$E37 : (x)A(x) \rightarrow B \Leftrightarrow (x)(A(x) \rightarrow B)$

$E38 : (\exists x)A(x) \rightarrow B \Leftrightarrow (x)(A(x) \rightarrow B)$

$E39 : A \rightarrow (x)B(x) \Leftrightarrow (x)(A \rightarrow B(x))$

$E40 : A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$

$E41 : (\exists x)(A(x) \rightarrow B(x)) \Leftrightarrow (x)A(x) \rightarrow (\exists x)B(x)$

$E42 : (\exists x)A(x) \rightarrow (x)B(X) \Leftrightarrow (x)(A(x) \rightarrow B(X))$.

Example: Verify the validity of the following arguments:

‖All men are mortal. Socrates is a man. Therefore, Socrates is mortal‖.

or

Show that $(x)[H(x) \rightarrow M(x)] \wedge H(s) \Rightarrow$

$M(s)$.

Solution: Let us represent the statements as follows:

$H(x)$: x is a man $M(x)$: x is a mortal s : Socrates

Thus, we have to show that $(x)[H(x) \rightarrow M(x)] \wedge H(s) \Rightarrow M(s)$.

{1}	(1)	$(x)[H(x) \rightarrow M(x)]$	Rule P
{1}	(2)	$H(s) \rightarrow M(s)$	Rule US, (1)
{3}	(3)	$H(s)$	Rule P
{1, 3}	(4)	$M(s)$	Rule T, (2), (3), and $I11$

Example: Establish the validity of the following argument:‖All integers are rational numbers. Some integers are powers of 2. Therefore, some rational numbers are powers of 2‖.

Solution: Let $P(x)$: x is an integer

$R(x)$: x is rational number

$S(x)$: x is a power

of 2 Hence, the given

statements becomes

$(x)(P(x) \rightarrow R(x)), (\exists x)(P(x) \wedge S(x)) \Rightarrow (\exists x)(R(x) \wedge S(x))$ Solution:

{1}	(1)	$(\exists x)(P(x) \wedge S(x))$	Rule P
{1}	(2)	$P(y) \wedge S(y)$	Rule ES, (1)
{1}	(3)	$P(y)$	Rule T, (2) and $P \wedge Q \Rightarrow P$
{1}	(4)	$S(y)$	Rule T, (2) and $P \wedge Q \Rightarrow Q$

{5}	(5) $(x)(P(x) \rightarrow R(x))$	Rule P
{5}	(6) $P(y) \rightarrow R(y)$	Rule US, (5)
{1, 5}	(7) $R(y)$	Rule T, (3), (6) and $P, P \rightarrow Q \Rightarrow Q$
{1, 5}	(8) $R(y) \wedge S(y)$	Rule T, (4), (7) and $P, Q \Rightarrow P \wedge Q$
{1, 5}	(9) $(\exists x)(R(x) \wedge S(x))$	Rule EG, (8)

Hence, the given statement is valid.

Example: Show that $(x)(P(x) \rightarrow Q(x)) \wedge (x)(Q(x) \rightarrow R(x)) \Rightarrow (x)(P(x) \rightarrow R(x))$. Solution:

{1}	(1) $(x)(P(x) \rightarrow Q(x))$	Rule P
{1}	(2) $P(y) \rightarrow Q(y)$	Rule US, (1)
{3}	(3) $(x)(Q(x) \rightarrow R(x))$	Rule P
{3}	(4) $Q(y) \rightarrow R(y)$	Rule US, (3)
{1, 3}	(5) $P(y) \rightarrow R(y)$	Rule T, (2), (4), and I_{13}
{1, 3}	(6) $(x)(P(x) \rightarrow R(x))$	Rule UG, (5)

Example: Show that $(\exists x)M(x)$ follows logically from the premises $(x)(H(x) \rightarrow M(x))$ and $(\exists x)H(x)$.

Solution:

{1}	(1) $(\exists x)H(x)$	Rule P
{1}	(2) $H(y)$	Rule ES, (1)
{3}	(3) $(x)(H(x) \rightarrow M(x))$	Rule P
{3}	(4) $H(y) \rightarrow M(y)$	Rule US, (3)
{1, 3}	(5) $M(y)$	Rule T, (2), (4), and I_{11}
{1, 3}	(6) $(\exists x)M(x)$	Rule EG, (5)

Hence, the result.

Example: Show that $(\exists x)[P(x) \wedge Q(x)] \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$. Solution:

{1}	(1) $(\exists x)(P(x) \wedge Q(x))$	Rule P
{1}	(2) $P(y) \wedge Q(y)$	Rule ES, (1)
{1}	(3) $P(y)$	Rule T, (2), and I_1
{1}	(4) $(\exists x)P(x)$	Rule EG, (3)
{1}	(5) $Q(y)$	Rule T, (2), and I_2
{1}	(6) $(\exists x)Q(x)$	Rule EG, (5)
{1}	(7) $(\exists x)P(x) \wedge (\exists x)Q(x)$	Rule T, (4), (5) and I_9

Hence, the result. Note: Is the converse true?

{1}	(1) $(\exists x)P(x) \wedge$	Rule

	$(\exists x)Q(x)$	P
{1}	(2) $(\exists x)P(x)$	Rule T, (1) and I_1
{1}	(3) $(\exists x)Q(x)$	Rule T, (1), and I_1
{1}	(4) $P(y)$	Rule ES, (2)
{1}	(5) $Q(s)$	Rule ES, (3)

Here in step (4), y is fixed, and it is not possible to use that variable again in step (5). Hence, the *converse is not true.*

Example: Show that from $(\exists x)[F(x) \wedge S(x)] \rightarrow (y)[M(y) \rightarrow W(y)]$ and $(\exists y)[M(y) \wedge \neg W(y)]$ the conclusion $(x)[F(x) \rightarrow \neg S(x)]$ follows.

{1}	(1)	$(\exists y)[M(y) \wedge \neg W(y)]$	Rule P
{1}	(2)	$[M(z) \wedge \neg W(z)]$	Rule ES, (1)
{1}	(3)	$\neg[M(z) \rightarrow W(z)]$	Rule T, (2), and $\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$
{1}	(4)	$(\exists y)\neg[M(y) \rightarrow W(y)]$	Rule EG, (3)
{1}	(5)	$\neg(y)[M(y) \rightarrow W(y)]$	Rule T, (4), and $\neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
{1}	(6)	$(\exists x)[F(x) \wedge S(x)] \rightarrow (y)[M(y) \rightarrow W(y)]$	Rule P
{1, 6}	(7)	$\neg(\exists x)[F(x) \wedge S(x)]$	Rule T, (5), (6) and I_{12}
{1, 6}	(8)	$(x)\neg[F(x) \wedge S(x)]$	Rule T, (7), and $\neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
{1, 6}	(9)	$\neg[F(z) \wedge S(z)]$	Rule US, (8)
{1, 6}	(10)	$\neg F(z) \vee \neg S(z)$	Rule T, (9), and De Morgan's laws
{1, 6}	(11)	$F(z) \rightarrow \neg S(z)$	Rule T, (10), and $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
{1, 6}	(12)	$(x)(F(x) \rightarrow \neg S(x))$	Rule UG, (11)

Hence, the result.

Example: Show that $(x)(P(x) \vee Q(x)) \Rightarrow (x)P(x) \vee (\exists x)Q(x)$. (May. 2012)

Solution: We shall use the indirect method of proof by assuming $\neg((x)P(x) \vee (\exists x)Q(x))$ as an additional premise.

{1}	(1)	$\neg((x)P(x) \vee (\exists x)Q(x))$	Rule P (assumed)
{1}	(2)	$\neg(x)P(x) \wedge \neg(\exists x)Q(x)$	Rule T, (1) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$
{1}	(3)	$\neg(x)P(x)$	Rule T, (2), and I_1
{1}	(4)	$(\exists x)\neg P(x)$	Rule T, (3), and $\neg(x)A(x) \Leftrightarrow (\exists x)\neg A(x)$
{1}	(5)	$\neg(\exists x)Q(x)$	Rule T, (2), and I_2
{1}	(6)	$(x)\neg Q(x)$	Rule T, (5), and $\neg(\exists x)A(x) \Leftrightarrow (x)\neg A(x)$
{1}	(7)	$\neg P(y)$	Rule ES, (5), (6) and I_{12}
{1}	(8)	$\neg Q(y)$	Rule US, (6)
{1}	(9)	$\neg P(y) \wedge \neg Q(y)$	Rule T, (7), (8)and I_9
{1}	(10	$\neg(P(y) \vee Q(y))$	Rule T, (9), and $\neg(P \vee Q) \Leftrightarrow \neg P$

	)		$\wedge \neg Q$
{11}	(11)	$(x)(P(x) \vee Q(x))$	Rule P
{11}	(12)	$(P(y) \vee Q(y))$	Rule US
{1, 11}	(13)	$\neg(P(y) \vee Q(y)) \wedge (P(y) \vee Q(y))$	Rule T, (10), (11), and $I9$
{1, 11}	(14)	F	Rule T, and (13)

which is a contradiction.Hence, the statement is valid.

Example: Using predicate logic, prove the validity of the following argument: ‖Every husband argues with his wife. *x* is a husband. Therefore, *x* argues with his wife‖.

Solution: Let $P(x)$: *x* is a husband.

$Q(x)$: *x* argues with his wife.

Thus, we have to show that $(x)[P(x) \rightarrow Q(x)] \wedge P(x) \Rightarrow Q(y)$.

{1}	(1) $(x)(P(x) \rightarrow Q(x))$	Rule P
{1}	(2) $P(y) \rightarrow Q(y)$	Rule US, (1)
{1}	(3) $P(y)$	Rule P
{1}	(4) $Q(y)$	Rule T, (2), (3), and I_{11}

Example: Prove using rules of inference
Duke is a Labrador retriever.
All Labrador retriever like to swim. Therefore Duke likes to swim.

Solution: We denote

$L(x)$: *x* is a Labrador retriever.

$S(x)$: *x* likes to swim.

d: Duke.

We need to show that $L(d) \wedge (x)(L(x) \rightarrow S(x)) \Rightarrow S(d)$.

{1}	(1)	$(x)(L(x) \rightarrow S(x))$	Rule P
{1}	(2)	$L(d) \rightarrow S(d)$	Rule US, (1)
{2}	(3)	$L(d)$	Rule P
{1, 2}	(4)	$S(d)$	Rule T, (2), (3), and I_{11}.

Previous questions

1. Test the Validity of the Following argument: ‒All dogs are barking. Some animals are dogs. Therefore, some animals are barking‖.
2. Test the Validity of the Following argument:
‒Some cats are animals. Some dogs are animals. Therefore, some cats are dogs‖.
3. Symbolizes and prove the validity of the following arguments :

(i) Himalaya is large. Therefore every thing is large.
(ii) Not every thing is edible. Therefore nothing is edible.

4 a) Find the PCNF of (~p↔r) ^(q↔p) ?
b) Explain in brief about duality Law?

c) Construct the Truth table for ~(~p^~q)?
d) Find the disjunctive Normal form of ~(p → (q^r)) ?

5 Define Well Formed Formula? Explain about Tautology with example?

6 Explain in detail about the Logical Connectives with Examples?

7. Obtain the principal conjunctive normal form of the formula (¬ P→R)Λ(Q↔P)
8. Prove that (□ x)P(x)□ Q(x) → (□ x)P(x)□ (□ x)Q(x). Does the converse hold?
9. Show that from i) (□ x)(F(x) □ S(x)) □ (y)(M(y) □W(y))
   ii) (□ y) (M(y)□ ¬ W(y)) the conclusion (x)(F(x) □ ¬ S(x)) follows.

10. Obtain the principal disjunctive and conjunctive normal forms of (P □ (Q□ R)) □ (¬ P□ (¬ Q□ ¬ R)). Is this formula a tautology?
11. Prove that the following argument is valid: No Mathematicians are fools. No one who is not a fool is an administrator. Sitha is a mathematician. Therefore Sitha is not an administrator.
12. Test the Validity of the Following argument: If you work hard, you will pass the exam. You did not pass. Therefore you did not work hard.
13. Without constructing the Truth Table prove that (p□ q)□ q=pvq?
14. Using normal forms, show that the formula Q□ (P□ ¬ Q)□ (¬ P□ ¬ Q) is a tautology.
15. Show that (x) (P(x) □ Q(x)) □ (x)P(x) □ (□ x)Q(x) 16. Show that ¬ (P□ Q) □ (¬ P□ (¬ P□ Q)) □ ¬ P□ Q) (P□ Q)□ (¬ P□ (¬ P□ Q)) □ (¬ P□ Q) 17. Prove that (□ x) (P(x) □ Q(x)) □ (□ x)P(x) □(□ x)Q(x)
18. Example: Prove or disprove the validity of the following arguments using the rules of inference. (i) All men are fallible (ii) All kings are men (iii) Therefore, all kings are fallible.
19. Test the Validity of the Following argument:
   –Lions are dangerous animals, there are lions, and therefore there are dangerous animals.‖

MULTIPLE CHOICE QUESTIONS

1: Which of the following propositions is tautology?
   A.(p v q)→qB. p v (q→p) C.p v (p→q) D.Both (b) & (c)
   Option: C
2: Which of the proposition is p^ (~ p v q) is
   A.A tautology B.A contradiction C.Logically equivalent to p ^ q D.All of above
   Option: C
3: Which of the following is/are tautology?
   A.a v b → b ^ c B.a ^ b → b v c C.a v b → (b → c) D.None of these
   Option: B
4: Logical expression (A^ B) → (C' ^ A) → (A ≡ 1) is
   A.ContradictionB.Valid C.Well-formed formula D.None of these
   Option: D
5: Identify the valid conclusion from the premises Pv Q, Q → R, P → M, ¬M
   A.P ^ (R v R) B.P ^ (P ^ R) C.R ^ (P v Q) D.Q ^ (P v R)
   Option: D
6: Let a, b, c, d be propositions. Assume that the equivalence a ↔ (b v ¬b) and b

↔ c hold. Then truth value of the formula (a ^ b) → ((a ^ c) v d) is always

A.True B.False C.Same as the truth value of a D.Same as the truth value of b

Option: A

7: Which of the following is a declarative statement?

A. It's right B. He says C.Two may not be an even integer D.I love you

Option: B

8: P → (Q → R) is equivalent to

A. (P ^ Q) → R B.(P v Q) → R C.(P v Q) → ⅂R D.None of these

Option: A

9: Which of the following are tautologies?

A.((P v Q) ^ Q) ↔ Q B.((P v Q) ^ ⅂P) → Q C.((P v Q) ^ P) → P D.Both (a) & (b)

Option: D

10: If F1, F2 and F3 are propositional formulae such that F1 ^ F2 → F3 and F1 ^ F2→F3 are both tautologies, then which of the following is TRUE?

A.Both F1 and F2 are tautologies B.The conjuction F1 ^ F2 is not satisfiable C.Neither is tautologies D.None of these

Option: B

11. Consider two well-formed formulas in propositional logic
F1 : P →¬P F2 : (P →¬P) v (¬P →) Which of the following statement is correct? A.F1 is satisfiable, F2 is unsatisfiable B.F1 is unsatisfiable, F2 is satisfiable C.F1 is unsatisfiable, F2 is valid D.F1 & F2 are both satisfiable
Option: C

12: What can we correctly say about proposition P1 : (p v ¬q) ^ (q →r) v (r v p) A.P1 is tautology B.P1 is satisfiable C.If p is true and q is false and r is false, the P1 is true D.If p as true and q is true and r is false, then P1 is true Option: C

13: (P v Q) ^ (P → R)^ (Q →S) is equivalent to
A.S ^ R B.S → R C.S v R D.All of above
Option: C

14: The functionally complete set is
A.{ ¬, ^, v } B.{↓, ^ }C.{↑} D.None of these
Option: C

15: (P v Q) ^ (P→R) ^ (Q → R) is equivalent to
A.P B.Q C.R D.True = T
Option: C

16: ¬(P → Q) is equivalent to
A.P ^ ¬Q B.P ^ QC.¬P v Q D.None of these
Option: A

17: In propositional logic , which of the following is equivalent to p → q?
A.~p → q B.~p v q C.~p v~ q D.p →q
Option: B

18: Which of the following is FALSE? Read ^ as And, v as OR, ~as NOT, →as one way implication and ↔ as two way implication?
A.((x → y)^ x) →y B.((~x →y)^ (~x ^ ~y))→y C.(x → (x v y))D.((x v y) ↔(~x v ~y))
Option: D

19: Which of the following well-formed formula(s) are valid?
A.((P → Q)^(Q → R))→ (P → R) B.(P → Q) →(¬P → ¬Q)
C.(P v (¬P v ¬Q)) →P D.((P → R) v (Q → R)) → (P v Q}→R)
Option: A

20: Let p and q be propositions. Using only the truth table decide whether p ↔ q does not imply p → ¬q is
A.True B.False C.None D.Both A and B Option: A

UNIT-2
SET THEORY

Set:A set is collection of well defined objects.

In the above definition the words set and collection for all practical purposes are Synonymous. We have really used the word set to define itself.
Each of the objects in the set is called a member of an element of the set. The objects themselves can be almost anything. Books, cities, numbers, animals, flowers, etc. Elements of a set are usually denoted by lower-case letters. While sets are denoted by capital letters of English language.

The symbol ∈ indicates the membership in a set.
If –*a* is an element of the set *A*‖, then we write *a* ∈ *A*.
The symbol ∈ is read ―is a member of ‖ or ―is an element of ‖.
The symbol □ is used to indicate that an object is not in the given set. The symbol □ is read ―is not a member of ‖ or ―is not an element of ‖If *x* is not an element of the set *A* then we write *x* □ *A*.

Subset*:*
A set *A* is a subset of the set *B* if and only if every element of *A* is also an element of *B*. We also say that *A* is contained in *B*, and use the notation *A* □ *B*.

Proper Subset*:*
A set *A* is called proper subset of the set *B*. If (*i*) *A* is subset of *B* and (*ii*) *B* is not a subset *A* i.e., *A* is said to be a proper subset of *B* if every element of *A* belongs to the set *B*, but there is atleast one element of *B*, which is not in *A*. If *A* is a proper subset of *B*, then we denote it by *A* □ *B*.

Super set: If *A* is subset of *B*, then *B* is called a superset of *A*.

Null set: The set with no elements is called an empty set or null set. A Null set is designated by the symbol □ . The null set is a subset of every set, i.e., If *A* is any set then □ □ *A*.

Universal set:
In many discussions all the sets are considered to be subsets of one particular set. This set is called the universal set for that discussion. The Universal set is often designated by the script letter □ . Universal set in
not unique and it may change from one discussion to another.

Power set:
The set of all subsets of a set *A* is called the power set of *A*.
The power set of *A* is denoted by *P* (*A*). If *A* has *n* elements in it, then *P* (*A*) has 2^n elements:

Disjoint sets:
Two sets are said to be disjoint if they have no element in common.

Union of two sets:
The union of two sets *A* and *B* is the set whose elements are all of the elements in *A* or in *B* or in both. The union of sets *A* and *B* denoted by $A \cup B$ is read as –*A* union *B*.

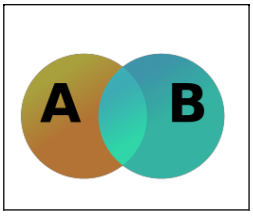
Intersection of two sets:
The intersection of two sets *A* and *B* is the set whose elements are all of the elements common to both *A* and *B*. The intersection of the sets of –*A* and –*B* is denoted by $A \cap B$ and is read as –*A* intersection *B*

Difference of sets:
If *A* and *B* are subsets of the universal set *U*, then the relative complement of *B* in *A*is the set of all elements in
A which are not in *A*. It is denoted by $A - B$ thus: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$

Complement of a set:
If U is a universal set containing the set A, then $U - A$ is called the complement of A. It is denoted by A^1 . Thus
$A^1 = \{x: x \square A\}$

Inclusion-Exclusion Principle:

The inclusion–exclusion principle is a counting technique which generalizes the familiar method of obtaining the number of elements in the unionof two finite sets; symbolically expressed as



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

Fig.Venn diagram showing the union of sets A and B

where A and B are two finite sets and $|S|$ indicates the cardinality of a set S (which may be considered as the number of elements of the set, if the set is finite). The formula expresses the fact that the sum of the sizes of the two sets may be too large since some elements may be counted twice. The double-counted elements are those in the intersection of the two sets and the count is corrected by subtracting the size of the intersection.

The principle is more clearly seen in the case of three sets, which for the sets A, B and C is given by

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

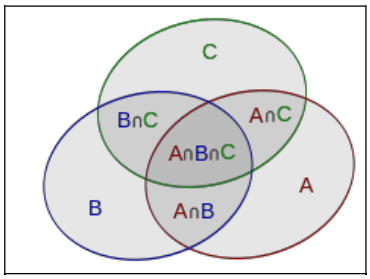


Fig.Inclusion–exclusion illustrated by a Venn diagram for three sets

This formula can be verified by counting how many times each region in the Venn diagram figure is included in the right-hand side of the formula. In this case, when removing the contributions of over-counted elements, the number of elements in the mutual intersection of the three sets has been subtracted too often,

so must be added back in to get the correct total.

In general, Let A1, · · · , Ap be finite subsets of a set U. Then,

$$|A_1 \cup A_2 \cup \ldots \cup A_p| = \sum_{1 \le i \le p} |A_i| - \sum_{1 \le i_1 < i_2 \le p} |A_{i_1} \cap A_{i_2}| +$$

$$\sum_{1 \le i_1 < i_2 < i_3 \le p} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \ldots + (-1)^{p-1} |A_1 \cap A_2 \cap \cdots \cap A_p|,$$

Example: How many natural numbers $n \le 1000$ are not divisible by any of 2, 3? Ans: Let $A_2 = \{n \in N \mid n \le 1000, 2|n\}$ and $A_3 = \{n \in N \mid n \le 1000, 3|n\}$.

Then, $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 500 + 333 - 166 = 667$.

So, the required answer is $1000 - 667 = 333$.

Example: How many integers between 1 and 10000 are divisible by none of 2, 3, 5, 7? Ans: For $i \in \{2, 3, 5, 7\}$, let $A_i = \{n \in N \mid n \le 10000, i|n\}$.

Therefore, the required answer is $10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$.

Relations

Definition: Any set of ordered pairs defines a *binary relation*.

We shall call a binary relation simply a relation. Binary relations represent relationships between elements of two sets. If R is a relation, a particular ordered pair, say $(x, y) \in R$ can be written as xRy and can be read as "x is in relation R to y".

Example: Give an example of a relation.
Solution: The relation "greater than" for real numbers is denoted by $'>'$. If x and y are any two real numbers such that $x > y$, then we say that $(x, y) \in >$. Thus the relation $>$ is $\{\} >= (x, y)$: x and y are real numbers and $x > y$
Example: Define a relation between two sets $A = \{5, 6, 7\}$ and $B = \{x, y\}$.

Solution: If $A = \{5, 6, 7\}$ and $B = \{x, y\}$, then the subset $R = \{(5, x), (5, y), (6, x), (6, y)\}$ is a relation from A to B.

Definition: Let S be any relation. The *domain* of the relation S is defined as the set of all first elements of the ordered pairs that belong to S and is denoted by $D(S)$.

$$D(S) = \{ x : (x, y) \in S, \text{ for some } y \}$$

The *range* of the relation S is defined as the set of all second elements of the ordered pairs that belong to S and is denoted by $R(S)$.

$$R(S) = \{ y : (x, y) \in S, \text{ for some } x\}$$

Example: $A = \{2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$. Define a relation from A to B by $(a, b) \in R$ if a divides b.
Solution: We obtain $R = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$.

Domain of $R = \{2, 3, 4\}$ and range of $R = \{3, 4, 6\}$.

Properties of Binary Relations in a Set

A relation R on a set X is said to be

- Reflexive relation if xRx or $(x, x) \in R$, $\forall x \in X$
- Symmetric relation if xRy then yRx, $\forall x, y \in X$
- Transitive relation if xRy and yRz then xRz, $\forall x, y, z \in X$
- Irreflexive relation if $x \not R x$ or $(x, x) \notin R$, $\forall x \in X$
- Antisymmetric relation if for every x and y in X, whenever xRy and yRx, then $x = y$.

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

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

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

(iv). If $R_4 = \{(1, 2), (2, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$ is an antisymmetric.

Example: Given $S = \{1, 2, ..., 10\}$ and a relation R on S, where $R = \{(x, y) | x + y = 10\}$. What are the properties of the relation R?

Solution: Given that

$S = \{1, 2, ..., 10\}$

$R = \{(x, y) | x + y = 10\}$

$R = \{(1, 9), (9, 1), (2, 8), (8, 2), (3, 7), (7, 3), (4, 6), (6, 4), (5, 5)\}$.

(i). For any $x \in S$ and $(x, x) \notin R$. Here, $1 \in S$ but $(1, 1) \notin R$.

$\Rightarrow$ the relation R is not reflexive. It is also not irreflexive, since

$(5, 5) \in R$. (ii). $(1, 9) \in R \Rightarrow (9, 1) \in R$

$(2, 8) \in R \Rightarrow (8, 2) \in R$.....

$\Rightarrow$ the relation is symmetric, but it is not antisymmetric. (iii). $(1, 9) \in R$ and $(9, 1) \in R$

$\Rightarrow (1, 1) \notin R$

$\Rightarrow$ The relation R is not transitive. Hence, R is symmetric.

Relation Matrix and the Graph of a Relation

Relation Matrix: A relation R from a finite set X to a finite set Y can be represented by a matrix is called the *relation matrix* of R.

Let $X = \{x_1, x_2, ..., x_m\}$ and $Y = \{y_1, y_2, ..., y_n\}$ be finite sets containing m and n elements, respectively, and R be the relation from A to B. Then R can be represented by an $m \times n$ matrix

$M_R = [r_{ij}]$, which is defined as follows:

$$r_{ij} = \begin{cases} 1, & \text{if } (x_i, y_j) \in R \\ 0, & \text{if } (x_i, y_j) \notin R \end{cases}$$

Example. Let $A = \{1, 2, 3, 4\}$ and $B = \{b_1, b_2, b_3\}$. Consider the relation $R = \{(1, b_2), (1, b_3), (3, b_2), (4, b_1), (4, b_3)\}$. Determine the matrix of the relation.

Solution: $A = \{1, 2, 3, 4\}$, $B = \{b_1, b_2, b_3\}$.

Relation $R = \{(1, b_2), (1, b_3), (3, b_2), (4, b_1), (4, b_3)\}$.

Matrix of the relation R is written as

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

Example: Let $A = \{1, 2, 3, 4\}$. Find the relation R on A determined by the matrix

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

Solution: The relation $R = \{(1, 1), (1, 3), (2, 3), (3, 1), (4, 1), (4, 2), (4, 4)\}$.

Properties of a relation in a set:

(i). If a relation is reflexive, then all the diagonal entries must be 1.

(ii). If a relation is symmetric, then the relation matrix is symmetric, i.e., $r_{ij} = r_{ji}$ for every i and j. (iii). If a relation is antisymmetric, then its matrix is such that if $r_{ij} = 1$ then $r_{ji} = 0$ for $i \neq j$.

Graph of a Relation: A relation can also be represented pictorially by drawing its *graph*. Let R be a relation in a set $X = \{x_1, x_2, ..., x_m\}$. The elements of X are represented by points or circles called *nodes*. These nodes are called *vertices*. If $(x_i, x_j) \in R$, then we connect the nodes x_i and x_j by means of an arc and put an arrow on the arc in the direction from x_i to x_j . This is called an *edge*. If all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, then we get a graph of the relation R.

Note: (i). If $x_i R x_j$ and $x_j R x_i$, then we draw two arcs between x_i and x_j with arrows pointing in both directions.

(ii). If $x_i R x_i$, then we get an arc which starts from node x_i and returns to node x_i. This arc is called a *loop*.

Properties of relations:

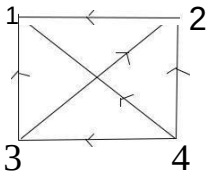
(i). If a relation is reflexive, then there must be a loop at each node. On the other hand, if the relation is irreflexive, then there is no loop at any node.

(ii). If a relation is symmetric and if one node is connected to another, then there must be a return arc from the second node to the first.

(iii). For antisymmetric relations, no such direct return path should exist. (iv). If a relation is transitive, the situation is not so simple.

Example: Let $X = \{1, 2, 3, 4\}$ and $R=\{(x, y)| x > y\}$. Draw the graph of R and also give its matrix. Solution: $R = \{(4, 1), (4, 3), (4, 2), (3, 1), (3, 2), (2, 1)\}$.

The graph of R and the matrix of R are



Graph of R

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

Partition and Covering of a Set

Let S be a given set and $A = \{A_1, A_2, \cdots, A_m\}$ where each A_i, $i = 1, 2, \cdots, m$ is a subset of S and

$$\bigcup_{i=1}^{m} A_i \subseteq S.$$

Then the set A is called a *covering* of S, and the sets $A_1, A_2, \cdots, A_m$ are said to *cover* S. If, in addition, the elements of A, which are subsets of S, are mutually disjoint, then A is called a

partition of S, and the sets $A_1, A_2, \cdots, A_m$ are called the *blocks* of the partition.

Example: Let $S = \{a, b, c\}$ and consider the following collections of subsets of S. $A = \{\{a, b\}, \{b, c\}\}$, $B = \{\{a\}, \{a, c\}\}$, $C = \{\{a\}, \{b, c\}\}$, $D = \{\{a, b, c\}\}$, $E = \{\{a\}, \{b\}, \{c\}\}$, and $F = \{\{a\}, \{a, b\}, \{a, c\}\}$. Which of the above sets are covering?

Solution: The sets A, C, D, E, F are covering of S. But, the set B is not covering of S, since their union is not S.

Example: Let $S = \{a, b, c\}$ and consider the following collections of subsets of S. $A = \{\{a, b\}, \{b, c\}\}$, $B = \{\{a\}, \{b, c\}\}$, $C = \{\{a, b, c\}\}$, $D = \{\{a\}, \{b\}, \{c\}\}$, and $E = \{\{a\}, \{a, c\}\}$.

Which of the above sets are covering?

Solution: The sets B, C and D are partitions of S and also they are covering. Hence, every partition is a covering.

The set A is a covering, but it is not a partition of a set, since the sets $\{a, b\}$ and $\{b, c\}$ are not disjoint. Hence, every covering need not be a partition.

The set E is not partition, since the union of the subsets is not S. The partition C has one block and the partition D has three blocks.

Example: List of all ordered partitions $S = \{a, b, c, d\}$ of

type (1, 2, 2). Solution:

$(\{a\}, \{b\}, \{c, d\})$, $(\{b\}, \{a\}, \{c, d\})$
$(\{a\}, \{c\}, \{b, d\})$, $(\{c\}, \{a\}, \{b, d\})$
$(\{a\}, \{d\}, \{b, c\})$, $(\{d\}, \{a\}, \{b, c\})$
$(\{b\}, \{c\}, \{a, d\})$, $(\{c\}, \{b\}, \{a, d\})$
$(\{b\}, \{d\}, \{a, c\})$, $(\{d\}, \{b\}, \{a, c\})$
$(\{c\}, \{d\}, \{a, b\})$, $(\{d\}, \{c\}, \{a, b\})$.

Equivalence Relations

A relation R in a set X is called an *equivalence relation* if it is reflexive, symmetric and transitive. The following are some examples of equivalence relations:

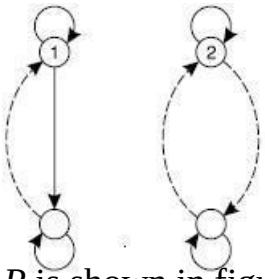
1. Equality of numbers on a set of real numbers.

2. Equality of subsets of a universal set.

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

Prove that R is an equivalence relation.

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



The corresponding graph of R is shown in figure:
Clearly, the relation R is reflexive, symmetric and transitive. Hence, R is an equivalence relation. Example: Let $X = \{1, 2, 3, ..., 7\}$ and $R = \{(x, y) | x - y$ is divisible by 3. Show that R is an equivalence relation.

Solution: (i). For any $x \in X$, $x - x = 0$ is divisible by 3.

$\therefore xRx$

$\Rightarrow R$ is reflexive.

(ii) For any $x, y \in X$, if xRy, then $x - y$ is divisible by 3.

$\Rightarrow -(x - y)$ is divisible by 3.

$\Rightarrow y - x$ is divisible by 3.

$\Rightarrow yRx$

Thus, the relation R is

symmetric. (iii). For any $x, y, z \in X$, let

xRy and yRz.

$\Rightarrow (x - y) + (y - z)$ is divisible by 3

$\Rightarrow x - z$ is divisible by 3

$\Rightarrow xRz$

Hence, the relation R is transitive.

Thus, the relation R is an equivalence relation.

Congruence Relation: Let I denote the set of all positive integers, and let m be

apositive integer. For $x \in I$ and $y \in I$, define R as $R = \{(x, y) | x - y$ is divisible by m

}

The statement $\|x - y$ is divisible by $m\|$ is equivalent to the statement that both x and y have the

same remainder when each is divided by m.

In this case, denote R by $\equiv$ and to write xRy as $x \equiv y \pmod{m}$, which is read as ‖x equals to y
modulo m‖. The relation $\equiv$ is called a *congruence relation*.
Example: $83 \equiv 13 \pmod 5$, since 83-13=70 is divisible by
5.
Example: Prove that the relation –congruence modulo m‖ over the set of positive integers is an equivalence relation.

Solution: Let N be the set of all positive integers and m be a positive integer.
We define the relation ‖congruence modulo m‖ on N as follows:
Let $x, y \in N$. $x \equiv y \pmod{m}$ if and only if $x - y$ is divisible by m.

Let $x, y, z \in N$.

Then (i). $x - x =$

$0.m$

$\Rightarrow x \equiv x \pmod{m}$ for all $x \in N$

(ii). Let $x \equiv y \pmod{m}$. Then, $x - y$ is divisible by m.

$\Rightarrow -(x - y) = y - x$ is divisible

by m. i.e., $y \equiv x \pmod{m}$

$\therefore$ The relation $\equiv$ is symmetric.

$\Rightarrow x - y$ and $y - z$ are divisible by m. Now $(x - y) + (y - z)$ is divisible by m. i.e., $x - z$ is divisible by m.

$\Rightarrow x \equiv z \pmod{m}$

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

Since the relation $\equiv$ is reflexive, symmetric and transitive, the relation *congruence modulo m* is an equivalence relation.

Example: Let R denote a relation on the set of ordered pairs of positive integers such that $(x,y)R(u, v)$ iff $xv = yu$. Show that R is an equivalence relation.

Solution: Let R denote a relation on the set of ordered pairs of positive integers.

Let x, y, u and v be positive integers. Given $(x, y)R(u, v)$ if and only if $xv = yu$. (i). Since $xy = yx$ is true for all positive integers

$\Rightarrow (x, y)R(x, y)$, for all ordered pairs (x, y) of positive integers.

$\therefore$ The relation R is reflexive. (ii). Let $(x, y)R(u, v)$

$\Rightarrow xv = yu \Rightarrow yu$

$= xv \Rightarrow uy = vx$

$\Rightarrow (u, v)R(x, y)$

$\therefore$ The relation R is symmetric.

(iii). Let x, y, u, v, m and n be positive integers Let $(x, y)R(u, v)$ and $(u, v)R(m, n)$

$\Rightarrow xv = yu$ and $un = vm$

$\Rightarrow xvun = yuvm$

$\Rightarrow xn = ym$, by canceling uv

$\Rightarrow (x, y)R(m, n)$

$\therefore$ The relation R is transitive.

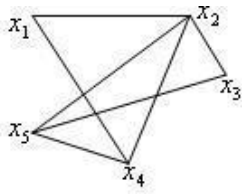
Since R is reflexive, symmetric and transitive, hence the relation R is an equivalence relation.

Compatibility Relations

Definition: A relation R in X is said to be a *compatibility relation* if it is reflexive and symmetric. Clearly, all equivalence relations are compatibility relations. A compatibility relation is sometimes denoted by ≈.

Example: Let $X = \{$ball, bed, dog, let, egg$\}$, and let the relation R be given by $R = \{(x, y) | x, y \in X \wedge xRy$ if x and y contain some common letter$\}$. Then R is a compatibility relation, and x, y are called compatible if xRy. Note: ball≈bed, bed≈egg. But ball≉egg.
Thus ≈ is not transitive.

Denoting ‖ball‖ by x_1, ‖bed‖ by x_2, ‖dog‖ by x_3, ‖let‖ by x_4, and ‖egg‖ by x_5, the graph of ≈ is

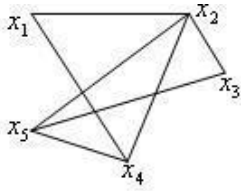


given as follows:

Maximal Compatibility Block:

Let X be a set and ≈ a compatibility relation on X. A subset $A \subseteq X$ is called a *maximal compatibility block* if any element of A is compatible to every other element of A and no element of $X - A$ is compatible to all the elements of A.

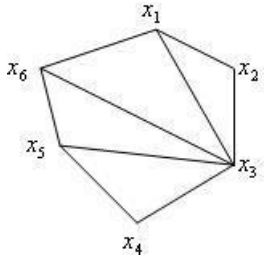
Example: The subsets $\{x_1, x_2, x_4\}$, $\{x_2, x_3, x_5\}$, $\{x_2, x_4, x_5\}$, $\{x_1, x_4, x_5\}$ are maximal compatibility blocks.



Example: Let the compatibility relation on a set $\{x_1, x_2, ..., x_6\}$ be given by the matrix:

x_2	1				
x_3	1	1			
x_4	0	0	1		
x_5	0	0	1	1	
x_6	1	0	1	0	1
	x_1	x_2	x_3	x_4	x_5

Draw the graph and find the maximal compatibility blocks of the relation. Solution:



The maximal compatibility blocks are $\{x_1, x_2, x_3\},\{x_1, x_3, x_6\},\{x_3, x_5, x_6\},\{x_3, x_4, x_5\}$.

Composition of Binary Relations

Let R be a relation from X to Y and S be a relation from Y to Z. Then a relation written as $R \circ S$ is called a *composite relation* of R and S where $R \circ S = \{(x, z) | x \in X, z \in Z,$ and there exists $y \in Y$ with $(x, y) \in R$ and $(y, z) \in S\}$.

Theorem: If R is relation from A to B, S is a relation from B to C and T is a relation from C to D
then $T \circ (S \circ R) = (T \circ S) \circ R$

Example: Let $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$. Find $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$, and $(R \circ R) \circ R$.

Solution: Given $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$.

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

$S \circ R = \{(4, 2), (3, 2), (1, 4)\} \neq R \circ S$

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

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

$R \circ R = \{(1, 2), (2, 2)\}$

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

Example: Let $A = \{a, b, c\}$, and R and S be relations on A whose matrices are as given below:

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

Find the composite relations $R \circ S$, $S \circ R$, $R \circ R$, $S \circ S$ and their matrices. Solution:

$R = \{(a, a), (a, c), (b, a), (b, b), (b, c), (c, b)\}$

$S = \{(a, a), (b, b), (b, c), (c, a), (c, c)\}$. From these, we find that

$R \circ S = \{(a, a), (a, c), b, a), (b, b), (b, c), (c, b), (c, c)\}$

$S \circ R = \{(a, a), (a, c), (b, b), (b, a), (b, c), (c, a), (c, b), (c, c)\}$

$R \circ R = R^2 = \{(a, a), (a, c), (a, b), (b, a), (b, c), (b, b), (c, a), (c, b), (c, c)\}$ $S \circ S = S^2 = \{(a, a), (b, b), (b, c), (b, a), (c, a), (c, c)\}$.

The matrices of the above composite relations are as given below:

$$M_{RO\,S} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}; \quad M_{SO\,R} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}; \quad M_{RO\,R} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix};$$

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

Transitive Closure

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

Example: Let the relation $R = \{(1, 2), (2, 3), (3, 3)\}$ on the set $\{1, 2, 3\}$. What is the transitive closure of R?

Solution: Given that $R = \{(1, 2), (2, 3), (3, 3)\}$.

The transitive closure of R is $R^+ = R \cup R^2 \cup R^3 \cup \cdots$ = R= $\{(1, 2), (2, 3), (3, 3)\}$

$R^2 = R \circ R = \{(1, 2), (2, 3), (3, 3)\} \circ \{(1, 2), (2, 3), (3, 3)\} = \{(1, 3), (2, 3), (3, 3)\}$

$R^3 = R^2 \circ R = \{(1, 3), (2, 3), (3, 3)\}$

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

$R^+ = R \cup R^2 \cup R^3 \cup R^4 \cup \ldots$

$= \{(1, 2), (2, 3), (3, 3)\} \cup \{(1, 3), (2, 3), (3, 3)\} \cup \{(1, 3), (2, 3), (3, 3)\} \cup \ldots$

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

Therefore $R^+ = \{(1, 2), (1, 3), (2, 3), (3, 3)\}$.

Example: Let $X = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 3), (3, 4)\}$ be a relation on X. Find R^+.

Solution: Given $R = \{(1, 2), (2, 3), (3, 4)\}$

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

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

$R^4 = \{(1, 4)\}$

$R^+ = \{(1, 2), (2, 3), (3, 4), (1, 3), (2, 4), (1, 4)\}$.

Partial Ordering

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

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

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

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

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

(i). Since $a \geq a$ for every integer a, the relation $\geq$ is reflexive. (ii). Let a and b be any two integers.

Let aRb and $bRa \Rightarrow a \geq b$ and $b \geq a$

$\Rightarrow a = b$

$\therefore$ The relation $'\geq'$ is antisymmetric. (iii).

Let a, b and c be any three integers.

Let aRb and $bRc \Rightarrow a \geq b$ and $b \geq c$

$\Rightarrow a \geq c$

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

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

Example: Show that the inclusion $\subseteq$ is a partial ordering on the set power set of a set S. Solution: Since (i). $A \subseteq A$ for all $A \subseteq S$, $\subseteq$ is reflexive.

(ii). $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$, $\subseteq$ is antisymmetric. (iii). $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$, $\subseteq$ is transitive.

Thus, the relation $\subseteq$ is a partial ordering on the power set of S.

Example: Show that the divisibility relation $'/'$ is a partial ordering on the set of positive integers. Solution: Let Z^+ be the set of positive integers.

Since (i). a/a for all $a \in Z^+$, $/$ is reflexive.

(ii). a/b and $b/a \Rightarrow a = b$, $/$ is antisymmetric. (iii). a/b and $b/c \Rightarrow a/c$, $/$ is transitive.

It follows that $/$ is a partial ordering on Z^+ and $(Z^+, /)$ is a poset.

Note: On the set of all integers, the above relation is not a partial order as a and $-a$ both divide each other, but $a = -a$. i.e., the relation is not antisymmetric.

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

Note: It is not necessary to have $x \leq y$ or $y \leq x$ for every x and y in a poset P . In fact, x may not be related to y, in which case we say that x and y are incomparable.

Examples:

(i). The poset $(Z, \leq)$ is a totally ordered.
Since $a \leq b$ or $b \leq a$ whenever a and b are integers.

(ii). The divisibility relation $/$ is a partial ordering on the set of positive integers.

Therefore $(Z^+, /)$ is a poset and it is not a totally ordered, since it contain elements that are incomparable, such as 5 and 7, 3 and 5.

Definition: In a poset $(P, \leq)$, an element $y \in P$ is said to *cover* an element $x \in P$ if x

$< y$ and if there does not exist any element $z \in P$ such that $x \leq z$ and $z \leq y$; that is, y covers $x \Leftrightarrow (x < y \wedge (x \leq z \leq y \Rightarrow x = z \vee z = y))$.

Hasse Diagrams

A partial order $\leq$ on a set P can be represented by means of a diagram known as Hasse diagram of $(P, \leq)$. In such a diagram,

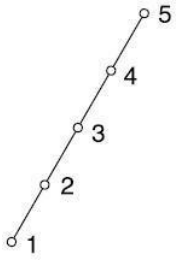
(i). Each element is represented by a small circle or dot.

(ii). The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn between x and y if y covers x.

(iii). If $x < y$ but y does not cover x, then x and y are not connected directly by a single line.

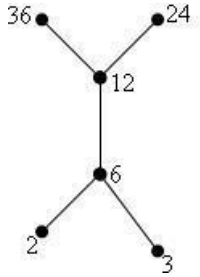
Note: For totally ordered set $(P, \leq)$, the Hasse diagram consists of circles one below the other. The poset is called a chain.

Example: Let $P = \{1, 2, 3, 4, 5\}$ and $\leq$ be the relation ‖less than or equal to‖ then the Hasse diagram is:



It is a totally ordered set.

Example: Let $X = \{2, 3, 6, 12, 24, 36\}$, and the relation $\leq$ be such that $x \leq y$ if x divides y. Draw the Hasse diagram of $(X, \leq)$. Solution: The Hasse diagram is is shown below:



It is not a total order set.

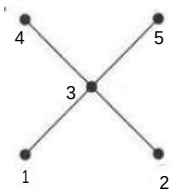
Example: Draw the Hasse diagram for the relation R on $A = \{1, 2, 3, 4, 5\}$ whose relation matrix given below:

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

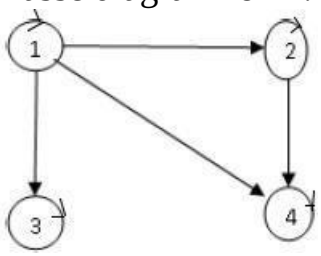
Solution:

R= {(1, 1), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (5.5)}.

Hasse diagram for M_R is


4
5
3
1
2

Example: A partial order R on the set $A = \{1, 2, 3, 4\}$ is represented by the following digraph. Draw the Hasse diagram for R.

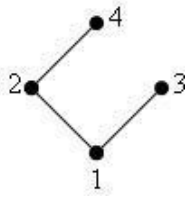


Solution: By examining the given digraph , we find that

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

We check that R is reflexive, transitive and antisymmetric. Therefore, R is partial order relation on A.

The hasse diagram of R is shown below:



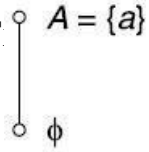
Example: Let A be a finite set and $\rho(A)$ be its power set. Let $\subseteq$ be the inclusion relation on the elements of $\rho(A)$. Draw the Hasse diagram of $\rho(A), \subseteq)$ for

- $A = \{a\}$
- $A = \{a, b\}$.

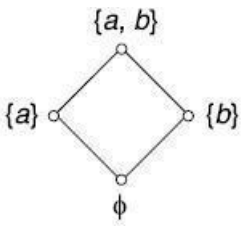
Solution: (i). Let $A = \{a\}$

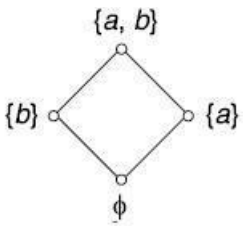
$$\rho(A) = \{\phi, a\}$$

Hasse diagram of $(\rho(A), \subseteq)$ is shown in F



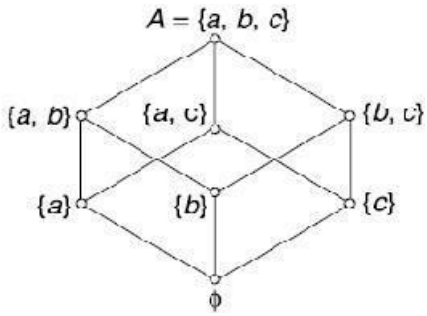
(ii). Let $A = \{a, b\}$. $\rho(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$. The Hasse diagram for $(\rho(A), \subseteq)$ is shown in fig:



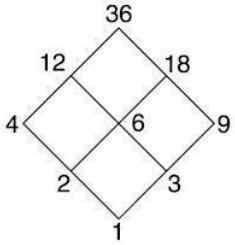


Example: Draw the Hasse diagram for the partial ordering $\subseteq$ on the power set $P(S)$ where $S = \{a, b, c\}$.
Solution: $S = \{a, b, c\}$.

$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.
Hasse diagram for the partial ordered set is shown in fig:



Example: Draw the Hasse diagram representing the positive divisions of 36 (i.e., D_{36}).
Solution: We have $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ if and only a divides b. The Hasse diagram for R is shown in Fig.



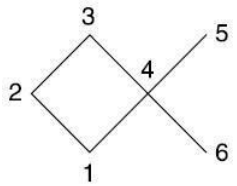
Minimal and Maximal elements(members): Let $(P, \leq)$ denote a partially ordered set. An element $y \in P$ is called a *minimal member* of P relative to $\leq$ if for no $x \in P$, is $x < y$.

Similarly an element $y \in P$ is called a maximal member of P relative to the partial ordering $\leq$ if

for no $x \in P$, is $y <$
x. Note:

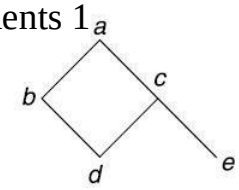
(i). The minimal and maximal members of a partially ordered set need not unique.
(ii). Maximal and minimal elements are easily calculated from the Hasse diagram. They are the *'top'* and *'bottom'* elements in the diagram.

Example:



In the Hasse diagram, there are two maximal elements and two minimal elements. The elements 3, 5 are maximal and the elements 1 and 6 are minimal.

Example: Let $A = \{a, b, c, d, e\}$ and let the partial order on A in the natural way.

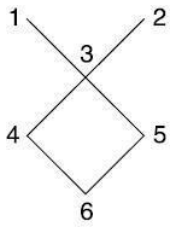


The element a is maximal.
The elements d and e are minimal.

Upper and Lower Bounds: Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$

is called an *upper bound* for A if for all $a \in A$, $a \leq x$. Similarly, any element $x \in P$ is called a

lower bound for *A* if for all $a \in A$, $x \leq a$. Example: $A = \{1, 2, 3, ..., 6\}$ be ordered as pictured in figure.

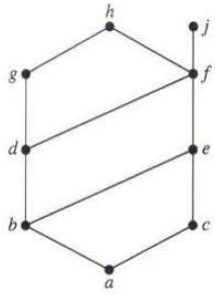


If $B = \{4, 5\}$ then the upper bounds of *B* are 1, 2, 3. The lower bound of *B* is 6.

Least Upper Bound and Greatest Lower Bound:

Let $(P, \leq)$ be a partial ordered set and let $A \subseteq P$. An element $x \in P$ is a *least upper bound* or *supremum* for *A* if *x* is an upper bound for *A* and $x \leq y$ where *y* is any upper bound for *A*. Similarly, the *the greatest lower bound* or *in mum* for *A* is an element $x \in P$ such that *x* is a lower bound and $y \leq x$ for all lower bounds *y*.

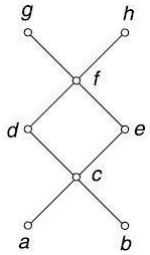
Example: Find the great lower bound and the least upper bound of $\{b, d, g\}$, if they exist in the



poset shown in fig:

Solution: The upper bounds of $\{b, d, g\}$ are *g* and *h*. Since $g < h$, *g* is the least upper bound. The lower bounds of $\{b, d, g\}$ are *a* and *b*. Since $a < b$, *b* is the greatest lower bound.

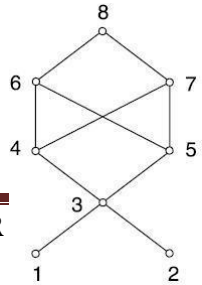
Example: Let $A = \{a, b, c, d, e, f, g, h\}$ denote a partially ordered set whose Hasse diagram is shown in Fig:



If $B = \{c, d, e\}$ then *f*, *g*, *h* are upper bounds of *B*. The element *f* is least upper bound.

Example: Consider the poset $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ whose Hasse diagram is shown in Fig and

let $B = \{3, 4, 5\}$



The elements 1, 2, 3 are lower bounds of *B*. 3 is greatest lower bound.

Functions

A function is a special case of relation.

Definition: Let X and Y be any two sets. A relation f from X to Y is called a function if for every x

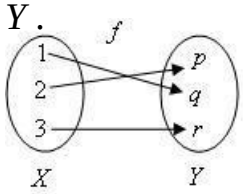
$\in X$, there is a unique element $y \in Y$ such that $(x, y) \in f$. Note: The definition of function requires that a relation must satisfies two additional conditions in order to qualify as a function. These conditions are as follows:

(i) For every $x \in X$ must be related to some $y \in Y$, i.e., the domain of f must be X and nor merely a subset of X.

(ii) Uniqueness, i.e., $(x, y) \in f$ and $(x, z) \in f \Rightarrow y = z$.

The notation $f : X \rightarrow Y$, means f is a function from X to Y .

Example: Let $X = \{1, 2, 3\}$, $Y = \{p, q, r\}$ and $f = \{(1, p), (2, q), (3, r)\}$ then $f(1) = p$, $f(2) = q$, $f(3) = r$. Clearly f is a function from X to Y .



Domain and Range of a Function: If $f : X \rightarrow Y$ is a function, then X is called the Domain of f and the set Y is called the codomain of f. The range of f is defined as the set of all images under f.

It is denoted by $f(X) = \{y|$ for some x in X, $f(x) = y\}$ and is called the image of X in Y . The Range

f is also denoted by Rf .

Example: If the function f is defined by $f(x)=x^2 + 1$ on the set $\{-2, -1, 0, 1, 2\}$, find the range of

f.

Solution: $f(-2) = (-2)^2 + 1 = 5$

$$f(-1) = (-1)^2 + 1 = 2$$

$$f(0) = 0 + 1 = 1$$

$$f(1) = 1 + 1 = 2$$

$$f(2) = 4 + 1 = 5$$

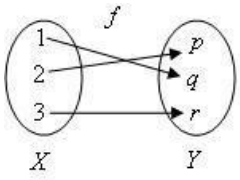
Therefore, the range of $f = \{1, 2, 5\}$.

Types of Functions

One-to-one(Injection): A mapping $f : X \rightarrow Y$ is called *one-to-one* if distinct elements of X are mapped into distinct elements of Y , i.e., f is one-to-one if

$$x1 \neq x2 \Rightarrow f(x1) \neq$$

(2) or equivalently $f(x1) = f(x2) \Rightarrow x1 = x2$ for



$x1, x2 \in X$.

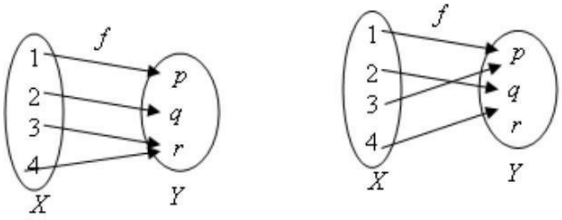
Example: $f : R \rightarrow R$ defined by $f(x) = 3x$, $\forall x \in R$ is one-one, since

$$f(x1) = f(x2) \Rightarrow 3x1 = 3x2 \Rightarrow x1 = x2, \forall x1, x2 \in R.$$

Example: Determine whether $f : Z \rightarrow Z$ given by $f(x) = x^2$, $x \in Z$ is a one-to-One function. Solution: The function $f : Z \rightarrow Z$ given by $f(x) = x^2$, $x \in Z$ is not a one-to-one function. This is because both 3 and -3 have 9 as their image, which is against the definition of a one-to-one function.

Onto(Surjection): A mapping $f : X \rightarrow Y$ is called *onto* if the range set $Rf = Y$.

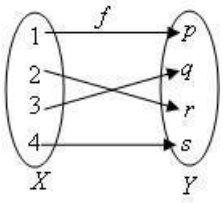
If $f : X \rightarrow Y$ is onto, then each element of Y is f-image of atleast one element of X. i.e., $\{f(x) : x \in X\} = Y$.
If f is not onto, then it is said to be *into*.



Surjective Not Surjective

Example: $f : R \rightarrow R$, given by $f(x) = 2x$, $\forall x \in R$ is onto.

Bijection or One-to-One, Onto: A mapping $f : X \rightarrow Y$ is called *one-to-one*, *onto* or *bijective* if it is both one-to-one and onto. Such a mapping is also called a one-to-one correspondence between X and Y .



Example: Show that a mapping $f : R \rightarrow R$ defined by $f(x) = 2x + 1$ for $x \in R$ is a bijective map from R to R.

Solution: Let $f : R \rightarrow R$ defined by $f(x) = 2x + 1$ for $x \in R$. We need to prove that f is a bijective map, i.e., it is enough to prove that f is one-one and onto.

- Proof of f being one-to-one
  Let x and y be any two elements in R such that $f(x) = f(y)$
  $\Rightarrow 2x + 1 = 2y + 1$

$\Rightarrow x = y$

Thus, $f(x) = f(y) \Rightarrow x = y$

This implies that f is one-to-one.

- Proof of f being onto
  Let y be any element in the codomain R

  $\Rightarrow f(x) = y$

  $\Rightarrow 2x + 1 = y$

  $\Rightarrow x = (y-1)/2$

Clearly, $x = (y-1)/2 \in R$

Thus, every element in the codomain has pre-image in the domain. This implies that f is onto
Hence, f is a bijective map.

Identity function: Let X be any set and f be a function such that $f : X \rightarrow X$ is defined by $f(x) = x$

for all $x \in X$. Then, f is called the identity function or identity transformation on X. It can be

denoted by I or I_X.

Note: The identity function is both one-to-one and onto.

Let $I_X(x) = I_X(y)$

$\Rightarrow x = y$

$\Rightarrow I_X$ is one-to-one

I_X is onto since $x = I_X(x)$ for all x.

Composition of Functions

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be two functions. Then the composition of f and g denoted by $g \circ f$, is the function from X to Z defined as

$$(g \circ f)(x) = g(f(x)), \text{ for all } x \in X.$$

Note. In the above definition it is assumed that the range of the function f is a subset of Y (the Domain of g), i.e., $Rf \subseteq Dg$. $g \circ f$ is called the left composition g with f.

Example: Let $X = \{1, 2, 3\}$, $Y = \{p, q\}$ and $Z = \{a, b\}$. Also let $f : X \rightarrow Y$ be f = $\{(1, p), (2, q), (3, q)\}$ and $g : Y \rightarrow Z$ be given by $g = \{(p, b), (q, b)\}$. Find $g \circ f$. Solution: $g \circ f = \{(1, b), (2, b), (3, b)$.

Example: Let $X = \{1, 2, 3\}$ and f, g, h and s be the functions from X to X given by

$f = \{(1, 2), (2, 3), (3, 1)\}$ $g = \{(1, 2), (2, 1), (3, 3)\}$
$h = \{(1, 1), (2, 2), (3, 1)\}$ $s = \{(1, 1), (2, 2), (3, 3)\}$

Find $f \circ f$; $g \circ f$; $f \circ h \circ g$; $s \circ g$; $g \circ s$; $s \circ s$; and $f \circ s$.

Solution:

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

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

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

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

$\therefore s \circ g = g \circ s = g$

$s \circ s = \{(1, 1), (2, 2), (3, 3)\} = s$

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

Thus, $s \circ s = s$, $f \circ g \neq g \circ f$, $s \circ g = g \circ s = g$ and $h \circ s = s \circ h = h$.

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

Solution: $f : R \to R$ is defined by $f(x) = x + 2$

f: $R \to R$ is defined by $g(x) = x - 2$

$h : R \to R$ is defined by $h(x) = 3x$

- $g \circ f : R \to R$

Let $x \in R$. Thus, we can write

$(g \circ f)(x) = g(f(x)) = g(x + 2) = x + 2 - 2 = x$

$\therefore (g \circ f)(x) = \{(x, x) | x \in R\}$

- $(f \circ g)(x) = f(g(x)) = f(x - 2) = (x - 2) + 2 = x$

  $\therefore f \circ g = \{(x, x) | x \in R\}$
- $(f \circ f)(x) = f(f(x)) = f(x + 2) = x + 2 + 2 = x + 4$

  $\therefore f \circ f = \{(x, x + 4) | x \in R\}$
- $(g \circ g)(x) = g(g(x)) = g(x - 2) = x - 2 - 2 = x - 4$

  $\Rightarrow g \circ g = \{(x, x - 4) | x \in R\}$
- $(f \circ h)(x) = f(h(x)) = f(3x) = 3x + 2$

  $\therefore f \circ h = \{(x, 3x + 2) | x \in R\}$
- $(h \circ g)(x) = h(g(x)) = h(x - 2) = 3(x - 2) = 3x - 6$

  $\therefore h \circ g = \{(x, 3x - 6) | x \in R\}$
- $(h \circ f)(x) = h(f(x)) = h(x + 2) = 3(x + 2) = 3x + 6$ $h \circ f =$

  $\{(x, 3x + 6) | x \in R\}$
- $(f \circ h \circ g)(x) = [f \circ (h \circ g)](x)$

  $f(h \circ g(x)) = f(3x - 6) = 3x - 6 + 2 = 3x - 4$

  $\therefore f \circ h \circ g = \{(x, 3x - 4) | x \in R\}$.

Example: What is composition of functions? Let f and g be functions from R to R, where R is a set of real numbers defined by $f(x) = x^2 + 3x + 1$ and $g(x) = 2x - 3$. Find the composition of functions: i) $f \circ f$ ii) $f \circ g$ iii) $g \circ f$.

Inverse Functions

A function $f : X \to Y$ is aid to be *invertible* of its inverse function f^{-1} is also function from the
range of f into X.

Theorem: A function $f : X \to Y$ is invertible $\Leftrightarrow$ f is one-to-one and onto.

Example: Let $X = \{a, b, c, d\}$ and $Y = \{(1, 2, 3, 4\}$ and let $f : X \to Y$ be given by f = $\{(a, 1), (b, 2), (c, 2), (d, 3)\}$. Is f^{-1} a function?

Solution: $f^{-1} = \{(1, a), (2, b), (2, c), (3, d)\}$. Here, 2 has two distinct images b and c.

Therefore, f^{-1} is not a function.

Example: Let R be the set of real numbers and $f : R \to R$ be given by $f = \{(x, x^2) | x \in R\}$. Is f^{-1} a function?

Solution: The inverse of the given function is defined as $f^{-1} = \{(x^2, x) | x \in R\}$. Therefore, it is not a function.

Theorem: If $f : X \to Y$ and $g : Y \to X$ be such that $g \circ f = I_X$ and $f \circ g = I_y$, then f and g are both invertible. Furthermore, $f^{-1} = g$ and $g^{-1} = f$.

Example: Let $X = \{1, 2, 3, 4\}$ and f and g be functions from X to X given by $f = \{(1, 4), (2, 1), (3, 2), (4, 3)\}$ and $g = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Prove that f and g are inverses of each other. Solution: We check that

$(g \circ f)(1) = g(f(1)) = g(4) = 1 = I_X(1)$, $(f \circ g)(1) = f(g(1)) = f(2) = 1 = I_X(1)$.

$(g \circ f)(2) = g(f(2)) = g(1) = 2 = I_X(2)$, $(f \circ g)(2) = f(g(2)) = f(3) = 2 = I_X(2)$.

$(g \circ f)(3) = g(f(3)) = g(2) = 3 = I_X(3)$, $(f \circ g)(3) = f(g(3)) = f(4) = 3 = I_X(3)$.

$(g \circ f)(4) = g(f(4)) = g(3) = 4 = I_X(4)$, $(f \circ g)(4) = f(g(4)) = f(1) = 4 = I_X(4)$.

Thus, for all $x \in X$, $(g \circ f)(x) = I_X(x)$ and $(f \circ g)(x) = I_X(x)$. Therefore g is inverse of f and f is inverse of g.

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

Solution: $f : R \to R$ is defined by $f(x) = x^3$; f: $R \to R$ is defined by $g(x) = x^{1/3}$

$(f \circ g)(x) = f(g(x)) = f(x^{1/3}) = x^{3(1/3)} = x = I_X(x)$ i.e., $(f \circ g)(x) = I_X(x)$

and $(g \circ f)(x) = g(f(x)) = g(x^3) = x^{3(1/3)} = x = I_X(x)$ i.e., $(g \circ f)(x) = I_X(x)$

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

., f and g are inverses of one other.

***Example: $f : R \to R$ is defined by $f(x) = ax + b$, for $a, b \in R$ and $a \neq 0$.

Show that f is invertible and find the inverse of f.

(i) First we shall show that f is one-to-one

Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$\Rightarrow ax_1 + b = ax_2 + b$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x1 = x2$

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

- To show that f is onto.

  Let $y \in R$(codomain) such that $y = f(x)$ for some $x \in R$.

  $\Rightarrow y = ax + b$

  $\Rightarrow ax = y - b$

  $\Rightarrow x = (y-b)/a$

Given $y \in R$(codomain), there exists an element $x = (y-b)/a \in R$ ~~such~~ that $f(x) = y$.

$\therefore f$ is onto

$\Rightarrow f$ is invertible and $f^{-1}(x) = (x-b)/a$

Example: Let $f : R \rightarrow R$ be given by $f(x) = x^3 - 2$. Find f^{-1}.

(i) First we shall show that f is one-to-one Let $x1, x2 \in R$ such that

$f(x1) = f(x2)$

$\Rightarrow x^3_1 - 2 = x^3_2 - 2 \Rightarrow x^3_1 = x^3_2$

$\Rightarrow x1 = x2$

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

- To show that f is onto.

  $\Rightarrow y = x^3 - 2$

  $\Rightarrow x^3 = y+2$

  $\Rightarrow x = \sqrt[3]{y + 2}$

  Given $y \in R$(codomain), there exists an element $x = \sqrt[3]{y + 2} \in R$ such that $f(x) = y$.

  $\therefore f$ is onto

  $\Rightarrow f$ is invertible and $f^{-1}(x) = \sqrt[3]{x + 2}$

Floor and Ceiling functions:

Let x be a real number, then the least integer that is not less than x is called the CEILING of x. The CEILING of x is denoted by $\lceil x \rceil$.

Examples: $\lceil 2.15 \rceil = 3, \lceil \sqrt{5} \rceil = 3, \lceil -7.4 \rceil = -7, \lceil -2 \rceil = -2$

Let x be any real number, then the greatest integer that does not exceed x is called the Floor of x. The FLOOR of x is denoted by $\lfloor x \rfloor$.

Examples: $\lfloor 5.14 \rfloor = 5$, $\lfloor \sqrt{5} \rfloor = 2$, $\lfloor -7.6 \rfloor = -8$, $\lfloor 6 \rfloor = 6$, $\lfloor -3 \rfloor = -3$

Example: Let f and g abe functions from the positive real numbers to positive real numbers defined by $f(x) = \lfloor 2x \rfloor$, $g(x) = x^2$. Calculate $f \circ g$ and $g \circ f$.

Solution: $f \circ g(x) = f(g(x)) = f(x^2) = \lfloor 2x^2 \rfloor$

$g \circ f(x) = g(f(x)) = g(\lfloor 2x \rfloor) = (\lfloor 2x \rfloor)^2$

Recursive Function

Total function: Any function $f : N^n \rightarrow N$ is called *total* if it is defined for every n-tuple in N^n. Example: $f(x, y) = x + y$, which is defined for all $x, y \in N$ and hence it is a total function.

Partial function: If $f : D \rightarrow N$ where $D \subseteq N^n$, then f is called a *partial function*. Example: $g(x, y) = x - y$, which is defined for only $x, y \in N$ which satisfy $x \geq y$.

Hence $g(x, y)$ is partial.

Initial functions:

The initial functions over the set of natural numbers is given by

- ***Zero function*** Z: $Z(x) = 0$, for all x.
- ***Successor function*** S: $S(x) = x + 1$, for all x.
- ***Projection function*** U_i^n: $U_i^n(x_1, x_2, ..., x_n) = x_i$ for all n tuples $(x_1, x_2, ..., x_n)$, $1 \leq i \leq n$.

Projection function is also called *generalized identity function*. For example, $U_1^1(x) = x$ for every $x \in N$ is the identity function.

$U_1^2(x, y) = x$, $U_2^3(2, 6, 9) = 2$, $U_3^3(2, 6, 9) = 6$, $U_3^3(2, 6, 9) = 9$.

Composition of functions of more than one variable:

The operation of composition will be used to generate the other function.

Let $f_1(x, y)$, $f_2(x, y)$ and $g(x, y)$ be any three functions. Then the composition of g with f_1 and f_2 is defined as a function $h(x, y)$ given by

$$h(x, y) = g(f_1(x, y), f_2(x, y)).$$

In general, let $f_1, f_2, ..., f_n$ each be partial function of m variables and g be a partial function of n variables. Then the composition of g with $f_1, f_2, ..., f_n$ produces a partial function h given by

$$h(x_1, x_2, ..., x_m) = g(f_1(x_1, x_2, ..., x_m), ..., f_n(x_1, x_2, ...x_m)).$$

Note: The function h is total iff $f_1, f_2, ..., f_n$ and g are total.

Example: Let $f_1(x, y) = x + y$, $f_2(x, y) = xy + y^2$ and $g(x, y) = xy$. Then

$$\begin{aligned} h(x, y) &= g(f_1(x, y), f_2(x, y)) \\ &= g(x + y, xy + y^2) \\ &= (x + y)(xy + y^2) \end{aligned}$$

Recursion: The following operation which defines a function $f(x_1, x_2, ..., x_n, y)$ of $n + 1$ variables by using other functions $g(x_1, x_2, .., x_n)$ and $h(x_1, x_2, ..., x_n, y, z)$ of n and $n + 2$ variables, respectively, is called *recursion*.

$$f(x_1, x_2, ..., x_n, 0) = g(x_1, x_2, ..., x_n)$$

$f(x1, x2, ..., xn, y + 1) = h(x1, x2, ..., xn, y, f(x1, x2, ..., xn, y))$ where y is the inductive variable.

Primitive Recursive: A function f is said to be *Primitive recursive* iff it can be obtained from the initial functions by a finite number of operations of composition and recursion.

*****Example:** Show that the function $f(x, y) = x + y$ is primitive recursive. Hence compute the value of $f(2, 4)$.

Solution: Given that $f(x, y) = x + y$.

Here, $f(x, y)$ is a function of two variables. If we want f to be defined by recursion, we need a function g of single variable and a function h of three variables. Now,

$$f(x, y + 1) = x + (y + 1)$$
$$= (x + y) + 1$$
$$= f(x, y) + 1.$$

Also, $f(x, 0) = x$.

We define $f(x, 0)$ as

$$f(x, 0) = x = U^1(x)$$
$$= S(f(x, y))$$
$$= S(U_3^3(x, y, f(x, y)))$$

If we take $g(x) = U1^1(x)$ and $h(x, y, z) = S(U3^3(x, y, z))$, we get $f(x, 0) = g(x)$ and $f(x, y + 1) = h(x, y, z)$.

Thus, f is obtained from the initial functions $U1^1$, $U3^3$, and S by applying composition once and recursion once.

Hence f is primitive recursive.

Here,

$$f(2, 0) = 2$$
$$f(2, 4) = S(f(2, 3))$$
$$= S(S(f(2, 2)))$$
$$= S(S(S(f(2, 1))))$$
$$= S(S(S(S(f(2, 0)))))$$
$$= S(S(S(S(2))))$$
$$= S(S(S(3)))$$
$$= S(S(4))$$
$$= S(5)$$
$$= 6$$

Example: Show that $f(x, y) = x * y$ is primitive recursion.

Solution: Given that $f(x, y) = x * y$.

Here, $f(x, y)$ is a function of two variables. If we want f to be defined by recursion, we need a function g of single variable and a function h of three variables. Now, $f(x, 0) = 0$ and

$$f(x, y + 1) = x * (y + 1) = x * y$$
- $f(x, y) + x$

We can write

$$f(x, 0) = 0 = Z(x) \text{ and}$$
$$f(x, y + 1) = f1(U3^3(x, y, f(x, y)), U1^3(x, y, f(x, y)))$$

where $f1(x, y) = x + y$, which is primitive recursive. By taking $g(x) = Z(x) = 0$ and h defined by $h(x, y, z) = f1(U3^3(x, y, z), U1^3(x, y, z)) = f(x, y + 1)$, we see that f defined by recursion. Since g and h are primitive recursive, f is primitive recursive.

Example: Show that $f(x, y) = x^y$ is primitive recursive function. Solution: Note that $x^0 = 1$ for $x \neq 0$ and we put $x^0 = 0$ for $x = 0$.
Also, $x^{y+1} = x^y * x$

Here $f(x, y) = x^y$ is defined as

$$f(x, 0) = 1 = S(0) = S(Z(x))$$

$f(x, y+1) = x * f(x, y)$

- $U_1^3(x, y, f(x, y)) * U_3^3(x, y, f(x, y))$

$h(x, y, f(x, y)) = f_1(U_1^3(x, y, f(x, y)), U_3^3(x, y, f(x, y)))$ where $f_1(x, y) = x * y$, which is primitive recursive.

$\therefore f(x, y)$ is a primitive recursive function.

Example: Consider the following recursive function definition: If $x < y$ then $f(x, y) = 0$, if $y \leq x$
then $f(x, y) = f(x - y, y) + 1$. Find the value of $f(4, 7)$, $f(19, 6)$.

Solution: Given

$$f(x, y) = \begin{cases} 0; x < y \\ f(x - y, y) + 1; y \geq x \end{cases}$$

$f(4, 7) = 0 \quad [\because 4 < 7]$

$f(19, 6) = f(19 - 6, 6) + 1$
$= f(13, 6) + 1$
$f(13, 6) = f(13 - 6, 6) + 1$
$= f(7, 6) + 1$
$f(7, 6) = f(7 - 6, 6) + 1$
$= f(1, 6) + 1$
$= 0 + 1$
$= 1$
$f(13, 6) = f(7, 6) + 1$
$= 1 + 1$
$= 2$
$f(19, 6) = 2 + 1$
$= 3$

Example: Consider the following recursive function definition: If $x < y$ then $f(x, y) = 0$, if $y \leq x$
then $f(x, y) = f(x - y, y) + 1$. Find the value of $f(86, 17)$

Permutation Functions

Definition: A *permutation* is a one-one mapping of a non-empty set onto itself.

Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set and p is a permutation on S, we list the elements of S and the corresponding functional values of $p(a_1), p(a_2), ..., p(a_n)$ in the following form:

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ p(a_1) & p(a_2) & \dots & p(a_n) \end{pmatrix}$$

If $p : S \rightarrow S$ is a bijection, then the number of elements in the given set is called the *degree* of its permutation.

Note: For a set with three elements, we have 3! permutations.

Example: Let $S = \{1, 2, 3\}$. The permutations of S are as follows:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; $P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Example: Let $S = \{1, 2, 3, 4\}$ and $p : S \to S$ be given by $f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 3$. Write this in permutation notation.

Solution: The function can be written in permutation notation as given below:

$$f=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

Identity Permutation: If each element of a permutation be replaced by itself, then such a permutation is called the *identity permutation.*

Example: Let $S = \{a_1, a_2, , a_n\}$.then $I=\begin{pmatrix}a_1&a_2&\dots&a_n\\a_1&a_2&\dots&a_n\end{pmatrix}$ is the identity permutation on S.

$$\begin{pmatrix}a\\a\end{pmatrix}\quad\begin{pmatrix}1&2&&n\end{pmatrix}$$

Equality of Permutations: Two permutations f and g of degree n are said to be equal if and only if $f(a) = g(a)$ for all $a \in S$.

Example: Let $S = \{1, 2, 3, 4\}$

$$f=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix};g=\begin{pmatrix}4&1&3&2\\4&3&2&1\end{pmatrix}$$

We have $f(1) = g(1) = 3$

$f(2) = g(2) = 1$

$f(3) = g(3) = 2$

$f(4) = g(4) = 4$

i.e., $f(a) = g(a)$ for all $a \in S$.

Product of Permutations: (or Composition of Permutations)

Let S={a,b,…h}and let $\begin{pmatrix}a&b&\dots&h\\f(a)&f(b)&\dots&f(h)\end{pmatrix}$ $\begin{pmatrix}a&b&\dots&h\\g(a)&g(b)&\dots&g(h)\end{pmatrix}$

We define the composite of f and g as follows:

$$f\circ g=\begin{pmatrix}a&b&\dots&h\\f(g(a))&f(g(b))&\dots&f(g(h))\end{pmatrix}$$

$$=\begin{pmatrix}a&b&\dots&h\\f(g(a))&f(g(b))&\dots&f(g(h))\end{pmatrix}$$

Clearly, $f \circ g$ is a permutation.

Example: Let $S = \{1, 2, 3, 4\}$ and let $f=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ and $g=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$ Find $f \circ g$ and $g \circ f$ in the permutation from.

Solution: $f\circ g=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$ $g\circ f=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$

Note: The product of two permutations of degree n need not be commutative.

Inverse of a Permutation:

If f is a permutation on $S = \{a_1, a_2, , a_n\}$ such that f $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b & \dots & & b \end{pmatrix}$

b

$\begin{pmatrix} 1 & 2 & & n \end{pmatrix}$

then there exists a permutation called the inverse f, denoted f^{-1} such that $f \circ f^{-1} = f^{-1} \circ f =$

I (the identity permutation on S)

$$\begin{pmatrix} 1 & b_1 & b_2 & \cdots & b_n \\ & a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

where f

Example: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, then find f^{-1}, and show that $f \circ f^{-1} = f^{-1} \circ f = I$

Solution: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Similarly, $f^{-1} \circ f = I. \Rightarrow f \circ f^{-1} = f^{-1} \circ f = I.$

Cyclic Permutation: Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set of n symbols. A permutation f defined on S is said to be *cyclic permutation* if f is defined such that

$f(a_1) = a_2, f(a_2) = a_3, ..., f(a_n - 1) = a_n$ and $f(a_n) = a_1$.

Example: Let $S = \{1, 2, 3, 4\}$.

Then $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 4)(2\ 3)$ is a cyclicpermutation.

Disjoint Cyclic Permutations: Let $S = \{a_1, a_2, ..., a_n\}$. If f and g are two cycles on S such that they have no common elements, then f and g are said to be disjoint cycles.

Example: Let $S = \{1, 2, 3, 4, 5, 6\}$.

If $f = (1\ 4\ 5)$ and $g = (2\ 3\ 6)$ then f and g are disjoint cyclic

permutations on S. *Note:* The product of two disjoint cycles is

commutative.

Example: Consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 1 & 7 & 6 & 2 \end{pmatrix}$

The above permutation f can be written as $f = (1\ 2\ 3\ 4\ 5)(6\ 7)$. Which is a product of two disjoint cycles.

Transposition: A cyclic of length 2 is called a

transposition. *Note:* Every cyclic permutation is the

product of transpositions.

Example: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} = (1\ 2\ 4)(3\ 5) = (1\ 4)(1\ 2)(3\ 5)$.

Inverse of a Cyclic Permutation: To find the inverse of any cyclic permutation, we write its elements in the reverse order.

For example, $(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1)$.

Even and Odd Permutations: A permutation *f* is said to be an *even permutation* if *f* can be expressed as the product of even number of transpositions.

A permutation *f* is said to be an *odd permutation* if *f* is expressed as the product of odd number of transpositions.

Note:

(i) An identity permutation is considered as an even permutation.

(ii) A transposition is always odd.

(iii) The product of an even and an odd permutation is odd. Similarly the product of an odd permutation and even permutations is odd.

Example: Determine whether the following permutations are even or odd permutations.

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 8 & 6 & 1 & 4 & 3 & 2 \end{pmatrix}$

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

Solution: (i). For $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} = (1\ 2\ 4) = (1\ 4)(1\ 2)$

$\Rightarrow f$ is an even permutation

(ii). For $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix}$

$= (1\ 2\ 5\ 6)(3\ 7\ 4\ 8) = (1\ 6)(1\ 5)(1\ 2)(3\ 8)(3\ 4)(3\ 7)$

$\Rightarrow g$ is an even permutation.

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} = (1\ 4\ 2\ 3) = (1\ 3)(1\ 2)(1\ 4)$

Product of three transpositions

$\Rightarrow h$ is an odd permutation.

Lattices

In this section, we introduce lattices which have important applications in the theory and design of computers.

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

Example: Let Z^+ denote the set of all positive integers and let R denote the relation 'division' in Z^+, such that for any two elements $a, b \in Z^+$, aRb, if a divides b. Then (Z^+, R) is a lattice in which the join of a and b is the least common multiple of a and b, i.e.

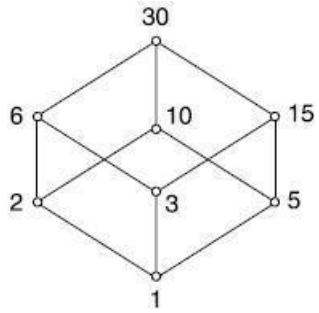
$$a \vee b = a \oplus b = \text{LCM of } a \text{ and } b,$$

and the meet of a and b, i.e. $a * b$ is the greatest common divisor (GCD) of a and b i.e.,

$$a \wedge b = a * b = \text{GCD of } a \text{ and } b.$$

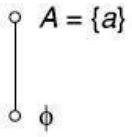
We can also write $a+b = a \vee b = a \oplus b$=LCM of a and b and $a.b = a \wedge b = a * b$=GCD of a and b.

Example: Let n be a positive integer and S_n be the set of all divisors of n If $n = 30$, $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Let R denote the relation division as defined in Example 1. Then (S_{30}, R) is a Lattice see Fig:

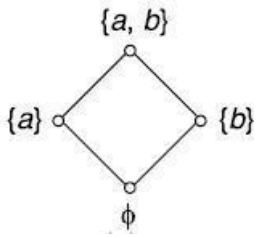


Example: Let A be any set and $P(A)$ be its power set. The poset $P(A), \subseteq)$ is a lattice in which the meet and join are the same as the operations $\cap$ and $\cup$ on sets respectively.

$S = \{a\}$, $P(A) = \{\phi, \{a\}\}$



$S = \{a, b\}$, $P(A) = \{\phi, \{a\}, \{a\}, S\}$.


{a, b}
{a}
{b}
ϕ

Some Properties of Lattice

Let $(L, \leq)$ be a lattice and $*$ and $\oplus$ denote the two binary operation meet and join on $(L, \leq)$. Then for any $a, b, c \in L$, we have

(L1): $a*a = a$, $(L1)'$: $a \oplus a = a$ (Idempotent laws)

$(L2)$: $b*a = b*a$, $(L2)'$: $a \oplus b = b + a$ (Commutative laws)

$(L3)$: $(a*b)*c = a*(b*c)$, $(L3)'$: $(a \oplus b) \oplus c = a \oplus (b + c)$ (Associative laws)

$(L4)$: $a*(a + b) = a$, $(L4)'$: $a \oplus (a*b) = a$ (Absorption laws).

The above properties $(L1)$ to $(L4)$ can be proved easily by using definitions of meet and join. We can apply the principle of duality and obtain $(L1)'$ to $(L4)'$.

Theorem: Let $(L, \leq)$ be a lattice in which $*$ and $\oplus$ denote the operations of meet and join respectively. For any $a, \in L$, $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Proof: We shall first prove that $a \leq b \Leftrightarrow a * b = b$.

In order to do this, let us assume that $a \leq b$. Also, we know that $a \leq a$. Therefore $a \leq a * b$. From the definition of $a * b$, we have $a * b \leq a$.

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

Next, assume that $a * b = a$; but it is only possible if $a \leq b$, that is, $a * b = a \Rightarrow a \leq b$. Combining these two results, we get the required equivalence.

It is possible to show that $a \leq b \Leftrightarrow a \oplus b = b$ in a similar manner.

Alternatively, from $a * b = a$, we have

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

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

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

By repeating similar steps, we can show that $a * b = a$ follows from $a \oplus b = b$. Therefore $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Theorem: Let $(L, \leq)$ be a lattice. Then $b \leq c \Rightarrow a * b \leq a * c$

$a \oplus b \leq a \oplus c$

Proof: By above theorem $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

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

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

$= a * (b * c)$

$= a * b$

$\therefore$ If b $\leq$ c then a $*$ b $\leq$ a $*$ c.Next, let $b \leq c \Rightarrow b \oplus c = c$.

To show that $a \oplus b \leq a \oplus c$. It sufficient to show that $(a \oplus b) \oplus (a \oplus c) = a \oplus c$.

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

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

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

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

$= a \oplus b$

$\therefore$ If $b \leq c$ then $a \oplus b \leq a \oplus c$.

Note: The above properties of a Lattice are called properties of Isotonicity.

Lattice as an algebraic system:

We now define lattice as an algebraic system, so that we can apply many concepts associated with algebraic systems to lattices.

Definition: A lattice is an algebraic system (L, ∗,⊕) with two binary operation _∗'and _⊕' on L which are both commutative and associative and satisfy absorption laws.

Bounded Lattice:

A bounded lattice is an algebraic structure (L,□ ,□ ,0,1) sucha that (L,□ ,□) is a lattice, and the constants 0,1∈ L satisfy the following:

1. for all x∈ L, x□ 1=x andx□ 1=1
2. for all x∈ L, x□ 0=0 andx□ 0=x.

The element 1 is called the upper bound, or top of L and the element 0 is called the lower bound or bottom of L.

Distributive lattice:

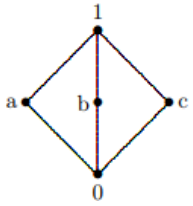
A lattice $(L,\vee,\wedge)$ is **distributive** if the following additional identity holds for all x, y, and z in L: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Viewing lattices as partially ordered sets, this says that the meet peration preserves nonempty finite joins. It is a basic fact of lattice theory that the above condition is equivalent to its dual

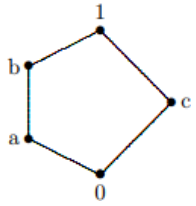
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ for all x, y, and z in L.

Example: Show that the following simple but significant lattices are not distributive.

a)



b)

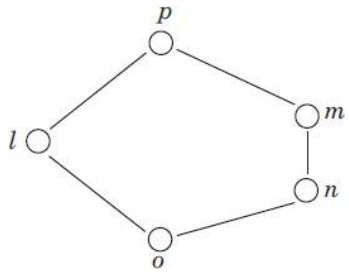


Solution a) To see that the diamond lattice is not distributive, use the middle elements of the lattice: a ∧ (b ∨ c) = a ∧ 1 = a, but (a ∧ b) ∨ (a ∧ c) = 0 ∨ 0 = 0, and a ≠0.

Similarly, the other distributive law fails for these three elements.

b) The pentagon lattice is also not distributive

Example: Show that lattice is not a distributive lattice.



Sol. A lattice is distributive if all of its elements follow distributive property so let we verify the distributive property between the elements *n*, *l* and *m*.

GLB(*n*, LUB(*l*, *m*)) = GLB(*n*, *p*) [∴ LUB(*l*, *m*) = *p*]
= *n* (LHS)

also LUB(GLB(*n*, *l*), GLB(*n*, *m*)) = LUB(*o*, *n*); [∴ GLB(*n*, *l*) = *o* and GLB(*n*, *m*) = *n*]
= *n* (RHS)

so LHS = RHS.

But GLB(*m*, LUB(*l*, *n*)) = GLB(*m*, *p*) [∴ LUB(*l*, *n*) = *p*]
= *m* (LHS)

also LUB(GLB(*m*, *l*), GLB(*m*, *n*)) = LUB(*o*, *n*); [∴ GLB(*m*, *l*) = *o* and GLB(*m*, *n*) = *n*]
= *n* (RHS)

Thus, LHS ≠ RHS hence distributive property doesn‘t hold by the lattice so lattice is not distributive.

Example: Consider the poset (X, ≤) where X = {1, 2, 3, 5, 30} and the partial ordered relation ≤

is defined as i.e. if x and y ∈X then x ≤ y means ‗x divides y‘. Then show that poset (I+, ≤) is a lattice.

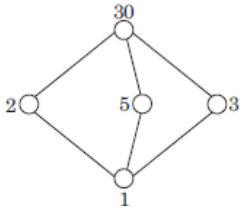
Sol. Since GLB(*x*, *y*) = *x* ∧ *y* = *lcm*(*x*, *y*)
and LUB(*x*, *y*) = *x* ∨ *y* = *gcd*(*x*, *y*)
Now we can construct the operation table I and table II for GLB and LUB

Table I

LUB	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

Table II

GLB	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30



respectively and the Hasse diagram is shown in Fig.

Test for distributive lattice, i.e.,

GLB(*x*, LUB(*y*, *z*)) = LUB(GLB(*x*, *y*), GLB(*x*, *z*))

Assume *x* = 2, *y* = 3 and *z* = 5, then

*RHS:*GLB(2, LUB(3, 5)) = GLB(2, 30) = 2

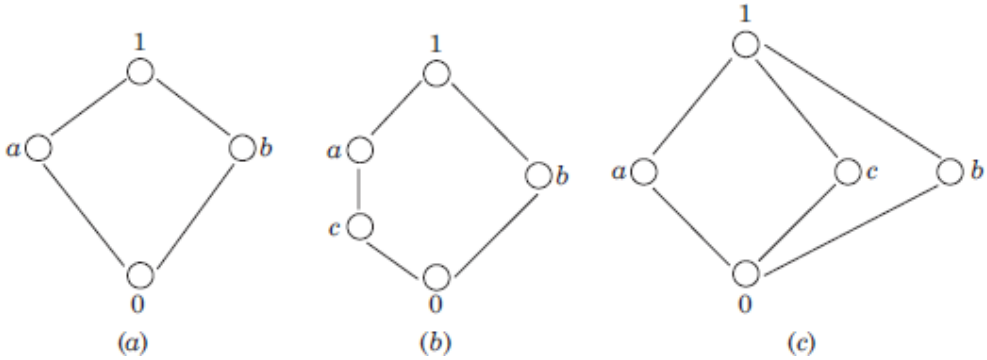
LHS: LUB(GLB(2, 3), GLB(2, 5)) = LUB(1, 1) = 1

Since$RHS \neq LHS$, hence lattice is not a distributive lattice.

Complemented lattice:

A complemented lattice is a bounded lattice (with least element 0 and greatest element 1), in which every element a has a complement, i.e. an element b satisfying $a \vee b = 1$ and $a \wedge b = 0$. Complements need not be unique.

Example: Lattices shown in Fig (a), (b) and (c) are complemented lattices.



Sol.

For the lattice (*a*) GLB(*a*, *b*) = 0 and LUB(*x*, *y*) = 1. So, the complement *a* is *b* and vise versa. Hence, a complement lattice.

For the lattice (*b*) GLB(*a*, *b*) = 0 and GLB(*c*, *b*) = 0 and LUB(*a*, *b*) = 1 and LUB(*c*, *b*) = 1; so both *a* and *c* are complement of *b*.
Hence, a complement lattice.

In the lattice (*c*) GLB(*a*, *c*) = 0 and LUB(*a*, *c*) = 1; GLB(*a*, *b*) = 0 and LUB(*a*, *b*) = 1. So, complement of *a* are *b* and *c*.
Similarly complement of *c* are *a* and *b* also *a* and *c* are complement of *b*. Hence lattice is a complement lattice.

Previous Questions

1. a) Let R be the Relation R= {(x,y)/ x divides y)} . Draw the Hasse diagram?
   b) Explain in brief about lattice?
   c) Define Relation? List out the Operations on Relations
2. Define Relation? List out the Properties of Binary operations?
3. Let the Relation R be R={(1,2) ,(2,3),(3,3)} on the set A= {1,2,3}. What is the Transitive Closure of R?
4. Explain in brief about Inversive and Recursive functions with examples?
5. Prove that (S, ≤) is a Lattice, where S= {1,2,5,10} and ≤ is for divisibility. Prove that it is also a Distributive Lattice?
6. Prove that (S,≤) is a Lattice, where S= {1,2,3,6} and ≤ is for divisibility. Prove that it is also a Distributive Lattice?
7. Let A be a given finite set and P(A) its power set. Let □ be the inclusion relation on the elements of P(A). Draw Hasse diagrams of (P(A), □) for A={a}; A={a,b}; A={a,b,c} and A={a,b.c.d}.
8. Let Fx be the set of all one-to-one onto mappings from X onto X, where X={1,2,3}. Find all the elements of Fx and find the inverse of each element.
9. Show that the function f(x) = x+y is primitive recursive.
10. Let X={2,3,6,12,24,36) and a relation ≤‘ be such that x≤ _if x divides y.

Draw the Hasse diagram of $(x,\leq)$.

11. If A={1,2,3,4} and P={{1,2},{3},{4}} is a partition of A, find the equivalence relation

determined by P.

12. Let X={1,2,3} and f, g, h and s be functions from X to X given by f={<1,2>, <2,3>, <3,1>} g={<1,2>, <2,1>, <3,3>}h={<1,1>, <2,2>, <3,1>} and s={<1,1>, <2,2>, <3,3>}. Find fog, fohog, gos, fos.
13. Let X={1,2,3,4} and R={<1,1>, <1,4>, <4,1>, <4,4>, <2,2>, <2,3>, <3,2>, <3,3>}. Write the matrix of R and sketch its graph.
14. Let X = {a,b,c,d,e} and let C = {{a,b},{c},{d,e}}. Show that the partition C defines an equivalence relation on X.
15. Show that the function f(x)= $x/2$ *when x iseven* is primitive recursive.

$$\begin{cases} (x-1)/2; & \textit{when } x \textit{ is odd} \end{cases}$$

16. If A={1,2,3,4} and R,S are relations on A defined by R={(1,2),(1,3),(2,4),(4,4)} S={(1,1),(1,2),(1,3),(1,4),(2,3),(2,4)} find R o S, S o R, R^2, S^2, write down there matrices.
17. Determine the number of positive integers n where 1≤n≤2000 and n is not divisible by2,3 or 5 but is divisible by 7.
18. Determine the number of positive integers n where 1≤n≤100 and n is not divisible by2,3 or 5.
19. Which elements of the poset /({2,4,5,10,12,20,25},/) are maximal and which are minimal?
20. Let X={(1,2,3} and f,g,h and s be functions from X to X given by f={(1,2),(2,3),(3,1)}, g={(1,2),(2,1),(3,3)}, h={(1,1),(2,2),(3,1) and s={(1,1),(2,2),(3,3)}.

Multiple choice questions

1. A__is an ordered collection of objects.
   a) Relation b) Function c) Set d) Proposition Answer: c
2. The set O of odd positive integers less than 10 can be expressed by___.
   a) {1, 2, 3} b) {1, 3, 5, 7, 9} c) {1, 2, 5, 9} d) {1, 5, 7, 9, 11} Answer: b
3. Power set of empty set has exactly_subset.
   a) One b) Two c) Zero d) Three Answer: a
4. What is the Cartesian product of A = {1, 2} and B = {a, b}?
   a) {(1, a), (1, b), (2, a), (b, b)} b) {(1, 1), (2, 2), (a, a), (b, b)}
   c) {(1, a), (2, a), (1, b), (2, b)} d) {(1, 1), (a, a), (2, a), (1, b)}
   Answer: c
5. The Cartesian Product B x A is equal to the Cartesian product A x B. Is it True or False?
   a) True b) False Answer: b

6. What is the cardinality of the set of odd positive integers less than 10? a) 10 b) 5 c) 3 d) 20
Answer: b

7. Which of the following two sets are equal?
a) A = {1, 2} and B = {1} b) A = {1, 2} and B = {1, 2, 3}
c) A = {1, 2, 3} and B = {2, 1, 3} d) A = {1, 2, 4} and B = {1, 2, 3}
Answer: c

8. The set of positive integers is_____.
a) Infinite b) Finite c) Subset d) Empty Answer: a

9. What is the Cardinality of the Power set of the set {0, 1, 2}.
a) 8 b) 6 c) 7 d) 9
Answer: a

10. The members of the set S = {x | x is the square of an integer and x < 100} is-----
a) {0, 2, 4, 5, 9, 58, 49, 56, 99, 12} b) {0, 1, 4, 9, 16, 25, 36, 49, 64, 81}
c) {1, 4, 9, 16, 25, 36, 64, 81, 85, 99} d) {0, 1, 4, 9, 16, 25, 36, 49, 64, 121}
Answer: b

11. Let R be the relation on the set of people consisting of (a,b) where aa is the parent of b. Let S be the relation on the set of people consisting of (a,b) where a and b are siblings. What are S∘ R and R∘ S?
A) (a,b) where a is a parent of b and b has a sibling; (a,b) where a is the aunt or uncle of b.
B) (a,b) where a is the parent of b and a has a sibling; (a,b) where a is the aunt or uncle of b.
C) (a,b) where a is the sibling of b's parents; (a,b) where aa is b's niece or nephew.
D) (a,b) where a is the parent of b; (a,b) where a is the aunt or uncle of b.

12. On the set of all integers, let $(x,y) \in R$ $(x,y) \in R$ *iff* $xy \geq 1$ $xy \geq 1$. Is relation R reflexive, symmetric, antisymmetric, transitive?
A) Yes, No, No, Yes B) No, Yes, No, Yes
C) No, No, No, Yes D) No, Yes, Yes, Yes E) No, No, Yes, No

13. Let R be a non-empty relation on a collection of sets defined by ARB if and only if $A \cap B = \emptyset$ Then (pick the TRUE statement)

C.R is an equivalence relation D.R is not relexive and not symmetric
A.R is relexive and transitive B.R is symmetric and not transitive
Option: B

14. Consider the divides relation, m | n, on the set A = {2, 3, 4, 5, 6, 7, 8, 9, 10}. The cardinality of the covering relation for this partial order relation (i.e., the number of edges in the Hasse diagram) is
(a) 4 (b) 6 (c) 5 (d) 8 (e) 7
Ans:e

15. Consider the divides relation, m | n, on the set A = {2, 3, 4, 5, 6, 7, 8, 9, 10}. Which of the following permutations of A is not a topological sort of this partial order relation?
(a) 7,2,3,6,9,5,4,10,8 (b) 2,3,7,6,9,5,4,10,8
(c) 2,6,3,9,5,7,4,10,8 (d) 3,7,2,9,5,4,10,8,6
(e) 3,2,6,9,5,7,4,10,8
Ans:c

16. Let A = {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} and consider the divides relation on A. Let C denote the length of the maximal chain, M the number of maximal elements, and m the number of minimal elements. Which is true?
(a) C = 3, M = 8, m = 6 *(b) C = 4, M = 8, m = 6 (c) C = 3, M = 6, m = 6 (d) C = 4, M = 6, m = 4 (e) C = 3, M = 6, m = 4*
Ans:a

17. What is the smallest N > 0 such that any set of N nonnegative integers must have two distinct integers whose sum or difference is divisible by 1000?
(a) 502 (b) 520 (c) 5002 (d) 5020 (e) 52002
Ans:a

18. Let R and S be binary relations on a set A. Suppose that R is reflexive, symmetric, and transitive and that S is symmetric, and transitive but is not reflexive. Which statement is always true for any such R and S?
    (a) R ∪ S is symmetric but not reflexive and not transitive.
    (b) R ∪ S is symmetric but not reflexive.
    (c) R ∪ S is transitive and symmetric but not reflexive

(d) R ∪ S is reflexive and symmetric. (e) R ∪ S is symmetric but not transitive. Ans:d

19. Let R be a relation on a set A. Is the transitive closure of R always equal to the transitive closure of R^2? Prove or disprove.

Solution: Suppose A = {1, 2, 3} and R = {(1, 2),(2, 3)}. Then R2 = {(1, 3)}. Transitive closure of R is R^* = {(1, 2),(2, 3),(1, 3)}. Transitive closure of R^2 is {(1, 3)}.

They are not always equal.

20. Suppose R1 and R2 are transitive relations on a set A. Is the relation R1 ∪ R2 necessariy a transitive relation? Justify your answer.

Solution: No. {(1, 2)} and {(2, 3)} are each transitive relations, but their union {(1, 2),(2, 3)} is not transitive.

21. Let D_{30} = {1, 2, 3, 4, 5, 6, 10, 15, 30} and relation I be partial ordering on D_{30}. The all lower bounds of 10 and 15 respectively are

A.1,3 B.1,5 C.1,3,5 D.None of these Option: B

22. Hasse diagrams are drawn for

A.partially ordered sets B.lattices C.boolean Algebra D.none of these Option: D

23. A self-complemented, distributive lattice is called

A.Boolean algebra B.Modular lattice C.Complete lattice D.Self dual lattice Option: A

24. Let D30 = {1, 2, 3, 5, 6, 10, 15, 30} and relation I be a partial ordering on D30. The lub of 10 and 15 respectively is

A.30 B.15 C.10 D.6 Option: A

25: Let X = {2, 3, 6, 12, 24}, and ≤ be the partial order defined by X ≤ Y if X divides Y. Number of edges in the Hasse diagram of (X, ≤) is

A.3 B.4 C.5 D.None of these Option: B

26. Principle of duality is defined as

A.≤ is replaced by ≥ B.LUB becomes GLB

C.all properties are unaltered when ≤ is replaced by ≥

D.all properties are unaltered when ≤ is replaced by ≥ other than 0 and 1 element. Option: D

27. Different partially ordered sets may be represented by the same Hasse diagram if they are A.same B.lattices with same order C.isomorphic D.order-isomorphic Option: D

28. The absorption law is defined as

A.a * (a * b) = b B.a * (a ⊕ b) = b C.a * (a * b) = a ⊕ b D.a * (a ⊕ b) = a Option: D

29. A partial order is deined on the set S = {x, a_1, a_2, a_3,..... a_n, y} as x ≤ a i for all i and a_i ≤ y for all i, where n ≥ 1. Number of total orders on the set S which contain partial order ≤ is

A.1 B.n C.n + 2 D.n ! Option: D

30. Let L be a set with a relation R which is transitive, antisymmetric and

reflexive and for any two elements a, b ∈ L. Let least upper bound lub (a, b) and the greatest lower bound glb (a, b) exist. Which of the following is/are TRUE ?

is a Poset B.L is a boolean algebra C.L is a lattice D.none of these Option: C

ALGEBRAIC STRUCTURES

Algebraic Systems with One Binary Operation Binary Operation

Let S be a non-empty set. If $f : S \times S \to S$ is a mapping, then f is called a binary operation or binary composition in S.

The symbols $+, \cdot, *, \oplus$ etc are used to denote binary operations on a set.

- For $a, b \in S \Rightarrow a + b \in S \Rightarrow +$ is a binary operation in S.
- For $a, b \in S \Rightarrow a \cdot b \in S \Rightarrow \cdot$ is a binary operation in S.
- For $a, b \in S \Rightarrow a \circ b \in S \Rightarrow \circ$ is a binary operation in S.
- For $a, b \in S \Rightarrow a * b \in S \Rightarrow *$ is a binary operation in S.

- This is said to be the closure property of the binary operation and the set S is said to be closed with respect to the binary operation.

Properties of Binary Operations

Commutative: $*$ is a binary operation in a set S. If for $a, b \in S$, $a * b = b * a$, then $*$ is said to be commutative in S. This is called commutative law.

Associative: $*$ is a binary operation in a set S. If for $a, b, c \in S$, $(a*b)*c = a*(b*c)$, then $*$ is said to be associative in S. This is called associative law.

Distributive: $\circ, *$ are binary operations in S. If for $a, b, c \in S$, (i) $a \circ (b * c) = (a \circ b) * (a \circ c)$, (ii) $(b * c) \circ a = (b \circ a) * (c \circ a)$, then $\circ$ is said to be distributive w.r.t the operation $*$. Example: N is the set of natural numbers.

(i) $+, \cdot$ are binary operations in N, since for $a, b \in N$, $a + b \in N$ and $a \cdot b \in N$. In other words N is said to be closed w.r.t the operations $+$ and $\cdot$.

(ii) $+, \cdot$ are commutative in N, since for $a, b \in N$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(iii) $+, \cdot$ are associative in N, since for $a, b, c \in N$, $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) is distributive w.r.t the operation $+$ in N, since for $a, b, c \in N$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

(v) The operations subtraction $(-)$ and division $(\div)$ are not binary operations in N, since for $3, 5 \in N$ does not imply $3 - 5 \in N$ and $\frac{3}{5} \in N$. Example: A is the set of even integers.

(i) $+, \cdot$ are binary operations in A, since for $a, b \in A$, $a + b \in A$ and $a \cdot b \in A$.

(i) $+, \cdot$ are commutative in A, since for $a, b \in A$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

(ii) $+, \cdot$ are associative in A, since for $a, b, c \in A$, $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iv) $\cdot$ is distributive w.r.t the operation + in A, since for $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

Example: Let S be a non-empty set and $\circ$ be an operation on S defined by $a \circ b = a$ for $a, b \in S$. Determine whether $\circ$ is commutative and associative in S.

Solution: Since $a \circ b = a$ for $a, b \in S$ and $b \circ a = b$ for $a, b \in S$.

$\Rightarrow a \circ b \neq b \circ a$.

$\therefore \circ$ is not commutative in S.

Since $(a \circ b) \circ c = a \circ c = a$

$a \circ (b \circ c) = a \circ b = a$ for $a, b, c \in S$.

$\therefore \circ$ is associative in S.

Example: $\circ$ is operation defined on Z such that $a \circ b = a + b - ab$ for $a, b \in Z$. Is the operation $\circ$ a binary operation in Z? If so, is it associative and commutative in Z?

Solution: If $a, b \in Z$, we have $a + b \in Z$, $ab \in Z$ and $a + b - ab \in Z$.

$\Rightarrow a \circ b = a + b - ab \in Z$.

$\therefore \circ$ is a binary operation in Z.

$\Rightarrow a \circ b = b \circ a$.

$\therefore \circ$ is commutative in Z.

No
w

$$(a \circ b) \circ c = (a \circ b) + c - (a \circ b)c$$
$$= a + b - ab + c - (a + b - ab)c$$
$$= a + b - ab + c - ac - bc + abc$$

and

$$a \circ (b \circ c) = a + (b \circ c) - a(b \circ c)$$
$$= a + b + c - bc - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac + abc$$
$$= a + b - ab + c - ac - bc + abc$$

$\Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$. $\therefore$
$\circ$ is associative in Z.

Example: Fill in blanks in the following composition table so that $\circ$ is associative in $S = \{a,b,c,d\}$.

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

Solution: $d \circ a = (c \circ b) \circ a$[$\because c \circ b = d$]

$= c \circ (b \circ a)$ [$\because \circ$ is associative]

$= c \circ b$

$= d$

$d \circ b = (c \circ b) \circ b = c \circ (b \circ b) = c \circ a = c$. $d \circ c = (c \circ b) \circ c = c \circ (b \circ c) = c \circ c = c$.

$d \circ d = (c \circ b) \circ (c \circ b)$
$= c \circ (b \circ c) \circ b$
$= c \circ c \circ b$
$= c \circ (c \circ b)$
$= c \circ d$
$= d$

Hence, the required composition table is

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d	d	c	c	d

Example: Let $P(S)$ be the power set of a non-empty set S. Let $\cap$ be an operation in $P(S)$. Prove that associative law and commutative law are true for the operation in $P(S)$.

Solution: P(S)= Set of all possible subsets of S. Let A,B $\in$ P(S).
Since A $\subseteq$ S, B $\subseteq$ S $\Rightarrow$ A $\cap$ B $\subseteq$ S $\Rightarrow$ A $\cap$ B $\in$ P(S).

$\therefore \cap$ is a binary operation in $P(S)$.

Also $A \cap B = B \cap A$

$\therefore \cap$ is commutative in $P(S)$.

Again $A \cap B$, $B \cap C$, $(A \cap B) \cap C$ and $A \cap (B \cap C)$ are subsets of S.

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$.

Since $(A \cap B) \cap C = A \cap (B \cap C)$

$\therefore \cap$ is associative in $P(S)$.

Algebraic Structures

Definition: A non-empty set G equipped with one or more binary operations is called an *algebraic structure* or an *algebraic system*.

If $\circ$ is a binary operation on G, then the algebraic structure is written as $(G, \circ)$. Example: $(N, +)$, $(Q, -)$, $(R, +)$ are algebraic structures.

Semi Group

Definition: An algebraic structure $(S, \circ)$ is called a *semi group* if the binary oper-ation $\circ$ is associative in S.

That is, $(S, \circ)$ is said to be a semi group if

(i) $a, b \in S \Rightarrow a \circ b \in S$ for all $a, b \in S$

(ii) $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b,$

$c \in S$. Example:

1. $(N, +)$ is a semi group. For $a, b \in N \Rightarrow a + b \in N$ and $a, b, c \in N \Rightarrow (a + b) + c$ =a+ $(b + c)$. 2. $(Q, -)$ is not a semi group. For 5,3/2 , 1 ∈ Q does not imply (5 – 3/2) −1 = 5 −(3/2 −1).

3. $(R, +)$ is a semi group. For $a, b \in R \Rightarrow a + b \in R$ and $a, b, c \in R \Rightarrow (a + b) + c$ = a+ $(b + c)$.

Example: The operation $\circ$ is defined by $a \circ b = a$ for all $a, b \in S$. Show that $(S, \circ)$ is a semi group. Solution: Let $a, b \in S \Rightarrow a \circ b = a \in S$.

$\therefore \circ$ is a binary operation in S. Let $a, b, c \in S$, $a \circ (b \circ c) = a \circ b = a$
$(a \circ b) \circ c = a \circ c = a$.

$\Rightarrow \circ$ is associative in S.

$\therefore (S, \circ)$ is a semi group.

Example: The operation $\circ$ is defined by $a \circ b = a + b - ab$ for all $a, b \in Z$. Show that $(Z, \circ)$ is a semi group.

Solution: Let $a, b \in Z \Rightarrow a \circ b = a + b - ab \in Z$.

$\therefore \circ$ is a binary operation in
Z. Let $a, b, c \in Z$.

$$(a \circ b) \circ c = (a + b - ab) \circ c$$
$$= a + b - ab + c - (a + b - ab)c$$
$$= a + b + c - ab - bc - ac + abc$$

$$a \circ (b \circ c) = a \circ (b + c - bc)$$
$$= a + (b + c - bc) - a(b + c - bc)$$
$$= a + b + c - bc - ab - ac +$$

$abc \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$.

$\Rightarrow \circ$ is associative in Z. $\therefore (Z, \circ)$ is semi group.

Example: $(P(S), \cap)$ is a semi group, where $P(S)$ is the power set of a non-empty set S. Solution: $P(S)$= Set of all possible subsets of S.

Let $A, B \in P(S)$.

Since $A \subseteq S, B \subseteq S \Rightarrow A \cap B \subseteq S \Rightarrow A \cap B \in P(S)$.

$\therefore \cap$ is a binary operation in $P(S)$. Let $A, B, C \in P(S)$.

$\therefore (A \cap B) \cap C, A \cap (B \cap C) \in P(S)$. Since $(A \cap B) \cap C = A \cap (B \cap C)$

$\therefore \cap$ is associative in $P(S)$.

Hence $(P(S), \cap)$ is a semi group.

Example: $(P(S), \cup)$ is a semi group, where $P(S)$ is the power set of a non-empty set S. Solution: $P(S)$= Set of all possible subsets of S.

Let $A, B \in P(S)$.

Since $A \subseteq S, B \subseteq S \Rightarrow A \cup B \subseteq S \Rightarrow A \cup B \in P(S)$.

$\therefore \cup$ is a binary operation in P (S). Let A, B, C $\in$ P (S).

$\therefore$ (A $\cup$ B) $\cup$ C, A $\cup$ (B $\cup$ C) $\in$ P (S). Since (A $\cup$ B) $\cup$ C = A $\cup$ (B $\cup$ C)

∴ ∪ is associative in P (S).

Hence (P (S), ∪) is a semi group.

Example: Q is the set of rational numbers, $\circ$ is a binary operation defined on Q such that $a \circ b = a - b + ab$ for $a, b \in Q$. Then $(Q, \circ)$ is not a semi group.

Solution: For $a, b, c \in Q$,

$$(a \circ b) \circ c = (a \circ b) - c + (a \circ b)c$$
$$= a - b + ab - c + (a - b + ab)c$$
$$= a - b + ab - c + ac - bc + abc$$
$$a \circ (b \circ c) = a - (b \circ c) + a(b \circ c)$$
$$= a - (b - c + bc) + a(b - cbc)$$
$$= a - b + c - bc + ab - ac + abc.$$

Therefore, $(a \circ b) \circ c \neq a \circ (b \circ c)$.

Example: Let $(A, *)$ be a semi group. Show that for a, b, c in A if $a * c = c * a$ and $b * c = c * b$, then $(a * b) * c = c * (a * b)$.

Solution: Given $(A, *)$ be a semi group, $a * c = c * a$ and $b * c = c * b$. Consider

$$(a * b) * c = a * (b * c) \quad [\because A \text{ is seme group}]$$
$$= a * (c * b) \quad [\because b * c = c * b]$$
$$= (a * c) * b \quad [\because A \text{ is seme group}]$$
$$= (c * a) * b \quad [\because a * c = c * a]$$
$$= c * (a * b) \quad [\because A \text{ is seme group}].$$

Homomorphism of Semi-Groups

Definition: Let $(S, *)$ and $(T, \circ)$ be any two semi-groups. A mapping $f : S \to T$ such that for any two elements $a, b \in S$, $f(a * b) = f(a) \circ f(b)$ is called a semi-group homomorphism.

Definition: A homomorphism of a semi-group into itself is called a semi-group endomorphism. Example: Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups and $f : S_1 \to S_2$ and $g : S_2 \to S_3$ be homomorphisms. Prove that the mapping of $g \circ f : S_1 \to S_3$ is a semigroup homomorphism.

Solution: Given that $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ are three semigroups and $f : S_1 \to S_2$ and $g : S_2 \to S_3$ be homomorphisms.

Let a, b be two elements of S_1.

$(g \circ f)(a *_1 b) = g[f(a *_1 b)]$

$= g[f(a) *_2 f(b)]$ ($\because f$ is a homomorphism)

$= g(f(a)) *_3 g(f(b))$ ($\because g$ is a homomorphism)

$= (g \circ f)(a) *_3 (g \circ f)(b)$

$\therefore g \circ f$ is a homomorphism.

Identity Element: Let S be a non-empty set and $\circ$ be a binary operation on S. If there exists an element $e \in S$ such that $a \circ e = e \circ a = a$, for $a \in S$, then e is called an *identity element* of S.

Example:

(i) In the algebraic system $(Z, +)$, the number 0 is an identity element.

(ii) In the algebraic system $(R, \cdot)$, the number 1 is an identity element.

Note: The identity element of an algebraic system is unique.

Monoid

Definition: A semi group $(S, \circ)$ with an identity element with respect to the binary operation $\circ$ is known as a *monoid*. i.e., $(S, \circ)$ is a monoid if S is a non-empty set and $\circ$ is a binary operation in S such that $\circ$ is associative and there exists an identity element w.r.t $\circ$.

Example:

1. $(Z, +)$ is a monoid and the identity is 0.
2. $(Z, \cdot)$ is a monid and the identity is 1.

Monoid Homomorphism

Definition: Let $(M, *)$ and $(T, \circ)$ be any two monoids, e_m and e_t denote the identity elements of $(M, *)$ and $(T, \circ)$ respectively. A mapping $f : M \rightarrow T$ such that for any two elements $a, b \in M$,

$f(a * b) = f(a) \circ f(b)$ and

$f(e_m) = e_t$

is called a monoid homomorphism.

Monoid homomorphism presents the associativity and identity. It also preserves commutative. If $a \in M$ is invertible and $a^{-1} \in M$ is the inverse of a in M, then $f(a^{-1})$ is the inverse of $f(a)$, i.e., $f(a^{-1}) = [f(a)]^{-1}$.

Sub Semi group

Let $(S, *)$ be a semi group and T be a subset of S. Then $(T, *)$ is called a sub semi group of $(S,$

$*)$ whenever T is closed under $*$. i.e., $a * b \in T$, for all $a, b \in T$.

Sub Monoid

Let $(S,*)$ be a monoid with e is the identity element and T be a non-empty subset of S. Then

$(T, *)$ is the sub monoid of $(S, *)$ if $e \in T$ and $a * b \in T$, whenever $a, b \in T$. Example:

1. Under the usual addition, the semi group formed by positive integers is a sub semi group of all integers.
2. Under the usual addition, the set of all rational numbers forms a monoid. We

denote it (Q,
+). The monoid (Z, +) is a submonid of (Q, +).
3. Under the usual multiplication, the set E of all even integers forms a semi group. This semi group is sub semi group of (Z, ·). But it is not a submonoid of (Z, ·), because $1 \neq E$.

Example: Show that the intersection of two submonoids of a monoid is a monoid. Solution: Let S be a monoid with e as the identity, and S_1 and S_2 be two submonoids of S. Since S_1 and S_2 are submonoids, these are monoids. Therefore $e \in S_1$ and $e \in S_2$.

Since $S_1 \cap S_2$ is a subset of S, the associative law holds in $S_1 \cap S_2$, because it holds in S. Accordingly $S_1 \cap S_2$ forms a monoid with e as the identity.

Invertible Element: Let $(S, \circ)$ be an algebraic structure with the identity element e in S w.r.t

$\circ$. An element $a \in S$ is said to be *invertible* if there exists an element $x \in S$ such that $a \circ x = x \circ a = e$.

Note: The inverse of an invertible element is unique.

From the composition table, one can conclude

1. Closure Property: If all entries in the table are elements of S, then S closed under $\circ$.
2. Commutative Law: If every row of the table coincides with the corresponding column, then $\circ$ is commutative on S.
3. Identity Element: If the row headed by an element a of S coincides with the top row, then a is called the identity element.
4. Invertible Element: If the identity element e is placed in the table at the intersection of the row headed by $'a'$ and the column headed by $'b'$, then $b^{-1} = a$ and $a^{-1} = b$.

Example: $A = \{1, \omega, \omega^2\}$.

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

From the table we conclude that

1. Closure Property: Since all entries in the table are elements of A. So, closure property is satisfied.
2. Commutative Law: Since 1^{st}, 2^{nd} and 3^{rd} rows coincides with 1^{st}, 2^{nd} and 3^{rd} columns respectively. So multiplication is commutative on A.
3. Identity Element: Since row headed by 1 is same as the initial row, so 1 is the identity element.
4. Inverses: Clearly $1^{-1} = 1$, $\omega^{-1} = \omega^2$, $(\omega^2)^{-1} = \omega$.

Groups

Definition: If G is a non-empty set and $\circ$ is a binary operation defined on G such that the following three laws are satisfied then $(G, \circ)$ is a group.

Associative Law: For $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$

Identity Law: There exists $e \in G$ such that $a \circ e = a = e \circ a$ for every $a \in G$, e is called an identity element in G.

Inverse Law: For each $a \in G$, there exists an element $b \in G$ such that $a \circ b = b \circ a = e$, b is called an inverse of a.

Example: The set Z of integers is a group w.r.t. usual addition.

(i) For $a, b \in Z \Rightarrow a + b \in Z$

(ii) For $a, b, c \in Z$, $(a + b) + c = a + (b + c)$

(iii) $0 \in Z$ such that $0 + a = a + 0 = a$ for each $a \in G$

∴ 0 is the identity element in Z.

(iv) For $a \in Z$, there exists $-a \in Z$ such that $a + (-a) = (-a) + a = 0$.

∴ $-a$ is the inverse of a. $(Z, +)$ is a group.

Example: Give an example of a monoid which is not a group.

Solution: The set N of natural numbers w.r.t usual multiplication is not a group. (i). For $a, b \in N \Rightarrow a \cdot b$.

(ii) For $a, b, c \in N$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) $1 \in N$ such that $1 \cdot a = a \cdot 1 = a$, for all $a \in N$.

∴ $(N, \cdot)$ is a monoid.

(iv) There is no $n \in N$ such that $a \cdot n = n \cdot a = 1$ for $a \in N$.

∴ Inverse law is not true.

∴ The algebraic structure $(N, \cdot)$ is not a group.

Example: $(R, +)$ is a group, where R denote the set of real numbers.

Abelian Group (or Commutative Group): Let $(G, *)$ be a group. If $*$ is com-mutative that is

$a * b = b * a$ for all $a, b \in G$ then $(G, *)$ is called an Abelian group. Example: $(Z, +)$ is an Abelian group.

Example: Prove that $G = \{1, \omega, \omega^2\}$ is a group with respect to multiplication where $1, \omega, \omega^2$ are cube roots of unity.

Solution: We construct the composition table as follows:

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

The algebraic system is $(G, \cdot)$ where $\omega^3 = 1$ and multiplication $\cdot$ is the binary opera-tion on G. From the composition table; it is clear that $(G, \cdot)$ is closed with respect to the oper-ation multiplication and the operation $\cdot$ is associative.

1 is the identity element in G such that $1 \cdot a = a = a \cdot 1, \quad \forall\, a \in G$.

Each element of G is invertible

1. $1 \cdot 1 = 1 \Rightarrow 1$ is its own inverse.
2. $\omega \cdot \omega^2 = \omega^3 = 1 \Rightarrow \omega^2$ is the inverse of ω and ω is the inverse of ω^2 in

G.

$\therefore (G, \cdot)$ is a group and $a \cdot b = b \cdot a, \forall a, b \in G$, that is commutative law holds in G with respect to multiplication.

$\therefore (G, \cdot)$ is an abelian group.

Example: Show that the set $G = \{1, -1, i, -i\}$ □ 1 is an abelian group with where $i =$ $\sqrt{}$respect to multiplication as a binary operation. Solution: Let us construct the composition table:

·	1	−1	i	$-i$
1	1	−1	i	$-i$
-1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	-1

From the above composition, it is clear that the algebraic structure $(G, \cdot)$ is closed and satisfies the following axioms:

Associativity: For any three elements $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Since

$1 \cdot (-1 \cdot i) = 1 \cdot -i = -i$

$(1 \cdot -1) \cdot i = -1 \cdot i = -i$

$\Rightarrow 1 \cdot (-1 \cdot i) = (1 \cdot -1) \cdot i$

Similarly with any other three elements of G the properties holds.

$\therefore$ Associative law holds in $(G, \cdot)$.

Existence of identity: 1 is the identity element in $(G, \cdot)$ such that $1 \cdot a = a = a \cdot 1, \forall a \in G$. Existence of inverse: $1 \cdot 1 = 1 = 1 \cdot 1 \Rightarrow 1$ is inverse of 1.

$(-1) \cdot (-1) = 1 = (-1) \cdot (-1) \Rightarrow -1$ is the inverse of (-1)

$i \cdot (-i) = 1 = -i \cdot i \Rightarrow -i$ is the inverse of i in G.

$-i \cdot i = 1 = i \cdot (-i) \Rightarrow i$ is the inverse of $-i$ in G. Hence inverse of every element in G exists.

Thus all the axioms of a group are satisfied.

Commutativity: $a \cdot b = b \cdot a, \forall a, b \in G$ hold in G.

$1 \cdot 1 = 1 = 1 \cdot 1; \quad -1 \cdot 1 = -1 = 1 \cdot -1$

$i \cdot 1 = i = 1 \cdot i; i \cdot -i = -i \cdot i = 1$ etc.

Commutative law is satisfied. Hence $(G, \cdot)$ is an abelian group.

Example: Prove that the set Z of all integers with binary operation $*$ defined by $a * b = a + b$

+ 1, $\forall\ a, b \in Z$ is an abelian group. Solution:

Closure: Let $a, b \in Z$. Since $a + b \in Z$ and $a + b + 1 \in Z$.

$\therefore Z$ is closed under

$*$. Associativity: Let $a, b,$

$c \in Z$.

Consider $(a * b) * c = (a + b + 1) * c$

$= a + b + 1 + c + 1$

$= a + b + c + 2$

also

$a * (b * c) = a * (b + c + 1)$

$= a + b + c + 1 + 1$

$= a + b + c + 2$

Hence $(a * b) * c = a * (b * c)$ for $a, b, c \in Z$.

Existence of Identity: Let $a \in Z$. Let $e \in Z$ such that $e * a = a * e = a$, i.e., $a + e + 1 = a$

$\Rightarrow e = -1$

$e = -1$ is the identity element in Z.

Existence of Inverse: Let $a \in Z$. Let $b \in Z$ such that $a * b = e$.

$\Rightarrow a + b + 1 =$

$-1\ b = -2 - a$

$\therefore$ For every $a \in Z$, there exits $-2-a \in Z$ such that $a*(-2-a) = (-2-a)*a = -1$.

$\therefore (Z, *)$ is an abelian group.

Example: Show that the set $Q+$ of all positive rational numbers forms an abelian group under the composition defined by $\circ$ such that $a \circ b = ab/3$ for $a, b \in Q+$.

Solution: $Q+$ of the set of all positive rational numbers and for $a, b \in Q+$, we have the operation $\circ$ such that $a \circ b = ab/3$.

Associativity: $a, b, c \in Q+ \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$.

Since $ab \in Q+$ and $ab/3 \in Q+$.

Associativity: $a, b, c \in Q+ \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$.

Since $(a \circ b) \circ c = (ab/3) \circ c = [ab/3 .c]/3 = a/3(bc/3) = a/3\ (b \circ c)$ $= a \circ (b \circ c)$. Existence of Identity: Let $a \in Q+$. Let $e \in Q+$ such that $e \circ a = a$.

i.e., $ea/3 = a$

$\Rightarrow ea - 3a = 0 \Rightarrow (e - 3)a = 0$

$\Rightarrow e - 3 = 0 \qquad (\because a \neq 0)$

$\Rightarrow e = 3$

$\therefore e = 3$ is the identity element in $Q+$.

Existence of Inverse: Let $a \in Q+$. Let $b \in Q+$ such that $a \circ b = e$.

$\Rightarrow ab/3 = 3$

$b = 9/a \qquad (\because a \neq 0)$

$\therefore$ For every $a \in Q+$, there exists $9/a \in Q+$ such that $a \circ 9/a = 9/a \circ a = 3$.

Commutativity: Let $a, b \in Q+ \Rightarrow a \circ b = b \circ a$.

Since $a \circ b$ = ab/3=ba/3 =

$b \circ a$. ($Q+, \circ$) is an abelian

group.

Exercises: 1. Prove that the set G of rational numbers other than 1 with operation $\oplus$ such that

$a \oplus b = a + b - ab$ for $a, b \in G$ is abelian group.

2. Consider the algebraic system $(G, *)$, where G is the set of all non-zero real numbers and $*$

is a binary operation defined by: $a * b = \frac{ab}{4}$, $\forall a, b \in G$. Show that $(G, *)$ is an

Addition modulo m

We shall now define a composite known as –addition modulo *m*| where *m* is fixed integer.

If *a* and *b* are any two integers, and *r* is the least non-negative reminder obtained by dividing the ordinary sum of *a* and *b* by *m*, then the addition modulo *m* of *a* and *b* is *r* symbolically

$$a +_m b = r, \quad 0 \le r < m.$$

Example: $20 +_6 5 = 1$, since $20 + 5 = 25 = 4(6) + 1$, i.e., 1 is the remainder when 20+5 is divisible by 6.

Example: $-15 +_5 3 = 3$, since $-15 + 3 = -12 = 3(-5) + 3$.

Multiplication modulo p

If *a* and *b* are any two integers, and *r* is the least non-negative reminder obtained by dividing the ordinary product of *a* and *b* by *p*, then the Multiplication modulo *p* of *a* and *b* is *r* symbolically

$$a \times_p b = r, \qquad 0 \le r < p.$$

Example: Show that the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group with respect to addition modulo 5.

Solution: We form the composition table as follows:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Since all the entries in the composition table are elements of *G*, the set *G* is closed with respect to addition modulo 5.

Associativity: For any three elements $a, b, c \in G$, $(a +_5 b) +_5 c$ and $a +_5 (b +_5 c)$ leave the same remainder when divided by 5.

i.e., $(a +_5 b) +_5 c = a +_5 (b +_5 c)$

$(1 +_5 3) +_5 4 = 3 = 1 +_5 (3 +_5 4)$ etc.

Existence of Identity: Clearly $0 \in G$ is the identity element, since we have

$0 +_5 9 = 4 = 9 +_5 0, \forall\ a \in G.$

Existence of Inverse: Each element in G is invertible with respect to addition modulo 5.

0 is its own inverse; 4 is the inverse of 1 and 1 is the inverse of 4.

2 is the inverse of 3 and 3 is the inverse of 2 with respect to addition modulo 5 in G. Commutativity: From the composition table it is clear that $a +_5 b = b +_5 a$, $\forall\ a, b \in G.$

Hence $(G, +_5)$ is an abelian group.

Example: Show that the set $G = \{1, 2, 3, 4\}$ is an abelian with respect to multipli-cation modulo 5.

Solution: The composition table for multiplication modulo 5 is

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From the above table, it is clear that G is closed with respect to the operation $\times_5$ and the binary composition $\times_5$ is associative; 1 is the identity element. Each element in G has a inverse.

1 is its own inverse 2 is the inverse of 3

3 is the inverse of 2

4 is the inverse of 4, with respect to the binary operation $\times_5$. Commutative law holds good in (G, $\times_5$).

Therefore (G, $\times_5$) is an abelian group.

Example: Consider the group, $G = \{1, 5, 7, 11, 13, 17\}$ under multiplication modulo 18. Construct the multiplication table of G and find the values of: 5^{-1}, 7^{-1} and 17^{-1}.

Example: If G is the set of even integers, i.e., $G = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ then prove that

G is an abelian group with usual addition as the operation. Solution: Let $a, b, c \in G$.

$\therefore$ We can take $a = 2x$, $b = 2y$, $c = 2z$, where x, $y, z \in Z$. Closure: $a, b \in G \Rightarrow a + b \in G$.

Since $a + b = 2x + 2y = 2(x + y) \in G$.

Associativity: $a, b, c \in G \Rightarrow a + (b + c) = (a + b) + c$

Since

$$\begin{aligned} a + (b + c) &= 2x + (2y + 2z) \\ &= 2[x + (y + z)] \\ &= 2[(x + y) + z] \\ &= (2x + 2y) + 2z \\ &= (a + b) + c \end{aligned}$$

Existence of Identity: $a \in G$, there exists $0 \in G$ such that $a + 0 = 0 + a = a$.

Since $a + 0 = 2x + 0 = 2x = a$ and $0 + a = 0 + 2x = 2x = a$

$\therefore$ 0 is the identity in G.

Existence of Inverse: $a \in G$, there exists $-a \in G$ such that $a+(-a) = (-a)+a = 0$. Since $a + (-a) = 2x + (-2x) = 0$ and $(-a) + a = (-2x) + 2x = 0$.

$\therefore$ $(G, +)$ is a group.

Commutativity: $a, b \in G \Rightarrow a + b = b + a$.
Since $a + b = 2x + 2y = 2(x + y) = 2(y + x) = 2y + 2x = b + a$.

$\therefore$ $(G, +)$ is an abelian group.

Example: Show that set $G = \{x | x = 2^a 3^b$ for $a, b \in Z\}$ is a group under multiplication.

Solution: Let $x, y, z \in G$. We can take $x = 2^p 3^q$, $y = 2^r 3^s$, $z = 2^l 3^m$, where $p, q, r, s, l, m \in Z$.

We know that (i). $p + r, q + s \in Z$

(ii). $(p + r) + l = p + (r + l)$, $(q + s) + m = q + (s + m)$.

Closure: $x, y \in G \Rightarrow x \cdot y \in G$.

Since $x \cdot y = (2^p 3^q)(2^r 3^s) = 2^{p+r} 3^{q+s} \in G$. Associativity: $x, y, z \in G \Rightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$ Since $(x \cdot y) \cdot z = (2^p 3^q 2^r 3^s)(2^l 3^m)$

$$= 2^{(p+r)+l} 3^{(q+s)+m}$$

$$= 2^{p+(r+l)} 3^{q+(s+m)}$$

$$= (2^p 3^q)(2^r 3^s 2^l 3^m)$$

$$= x \cdot (y \cdot z)$$

Existence of Identity: Let $x \in G$. We know that $e = 2^0 3^0 \in G$, since $0 \in Z$.

$\therefore x \cdot e = 2^p 3^q 2^0 3^0 = 2^{p+0} 3^{q+0} = 2^p 3^q = x$ and $e \cdot x = 2^0 3^0 2^p 3^q = 2^p 3^q = x$. $\therefore e \in G$ such that $x \cdot e = e \cdot x = x$

$\therefore e = 2^0 3^0$ is the identity element in G.

Existence of Inverse: Let $x \in G$.

Now $y = 2^{-p} 3^{-q} \in G$ exists, since $-p, -q \in Z$ such that

$x \cdot y = 2^p 3^q 2^{-p} 3^{-q} = 2^0 3^0 = e$ and $y \cdot x = 2^{-p} 3^{-q} 2^p 3^q = 2^0 3^0 = e$.

$\therefore$ For every $x = 2^p 3^q \in G$ there exists $y = 2^{-p} 3^{-q} \in G$ such that $x \cdot y = y \cdot x = e$. $\therefore (G, \cdot)$ is a group.

Example: Show that the sets of all ordered pairs (a, b) of real numbers for which $a \neq 0$ with the operation $*$ defined by $(a, b) * (c, d) = (ac, bc + d)$ is a group. Is the commutative?

Solution: Let $G = \{(a, b) | a, b \in R$ and $a \neq 0\}$. Define a binary operation $*$ on G by $(a, b) * (c, d) = (ac, bc + d)$, for all $(a, b), (c, d) \in G$. Now we show that $(G, *)$ is a group. Closure: $(a, b), (c, d) \in G \Rightarrow (a, b) * (c, d) = (ac, bc + d) \in G$.

Since $a \neq 0, c \neq 0 \Rightarrow ac \neq 0$.

Associativity: $(a, b), (c, d), (e, f) \in G \Rightarrow \{(a, b) * (c, d)\} * (e, f) = (a, b) * \{(c, d) * (e, f)\}$. Since $\{(a, b) * (c, d)\} * (e, f) = (ac, bc + d) * (e, f)$

$$= (ace, (bc + d)e + f)$$
$$= (ace, bce + de + f)$$

Also $(a, b) * \{(c, d) * (e, f)\} = (a, b) * (ce, de + f)$

$$= (a(ce), b(ce) + de + f)$$
$$= (ace, bce + de + f)$$

Existence of Identity: Let $(a, b) \in G$. Let $(x, y) \in G$ such that $(x, y) * (a, b) = (a,b) * (x, y) = (a, b)$

$$\Rightarrow (xa, ya + b) = (a, b)$$

$\Rightarrow xa = a, ya + b = b$

$\Rightarrow x = 1, (\because a \neq 0)$ and $ya = 0 \Rightarrow x = 1$ and $y = 0 (\because a \neq 0)$

$\Rightarrow (1, 0) \in G$ such that $(a, b) * (1, 0) = (a, b)$.

$\therefore (1, 0)$ is the identity in G.

Existence of Inverse: Let $(a, b) \in G$. Let $(x, y) \in G$ such that $(x, y) * (a, b) = (1, 0)$

$\Rightarrow (xa, ya + b) = (1, 0)$

$\Rightarrow xa = 1, ya + b = 0 \Rightarrow x = a^{\frac{1}{}}, y = \frac{-}{a}b$

$\therefore$ The inverse of (a, b) exits and it is (1/a,-b/a).

Commutativity: Let $(a, b), (c, d) \in G \Rightarrow (a, b) * (c, d) \neq (c, d) * (a, b)$

Since $(a, b) * (c, d) = (ac, bc + d)$ and $(c, d) * (a, b) = (ca, da + b)$.

$\therefore G$ is a group but not commutative group w.r.t $*$.

Example: If $(G, *)$ is a group then $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in$

G. Solution: Let $a, b \in G$ and e be the identity element in G.

Let $a \in G \Rightarrow a^{-1} \in G$ such that $a*a^{-1}=a^{-1}*a=e$ and $b \in G \Rightarrow b^{-1} \in G$ such that $b*b^{-1}=b^{-1} * b =$

e.

Now $a, b \in G \Rightarrow a * b \in G$ and $(a * b)^{-1} \in G$.

Consider

$(a*b)*(b^{-1}*a^{-1}) = a*[b*(b^{-1}*a^{-1})]$ (by associativity law)

$= a * [(b * b^{-1}) * a^{-1}]$

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

$= a * a^{-1}$ (e is the identity)

$= e$

and

$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * [a^{-1} * (a * b)]$

$= b^{-1} * [(a^{-1} * a) * b]$

$= b^{-1} * [e * b]$

$= b^{-1} * b$

$= e$

$\Rightarrow (a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e$

$(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Note:

1. $(b^{-1}a^{-1})^{-1} = ab$
2. $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$
3. If $(G, +)$ is a group, then $-(a + b) = (-b) + (-a)$
4. $-(a + b + c) = (-c) + (-b) + (-a)$.

Theorem: Cancelation laws hold good in G, i.e., for all $a, b, c \in G$ $a * b = a * c$ $\Rightarrow b = c$ (left cancelation law) $b * a = c * a \Rightarrow b = c$ (right cancelation law).

Proof: G is a group. Let e be the identity element in G.

$a \in G \Rightarrow a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Consider

$a * b = a * c$

$\Rightarrow a^{-1} * (a * b) = a^{-1}(a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ (by associative law)

$\Rightarrow e * b = e * c$ (a^{-1} is the inverse of a in G)

$\Rightarrow b = c$ (e is the identity element in G) and

$b * a = c * a$

$\Rightarrow (b * a)a^{-1} = (c * a) * a^{-1}$

$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1})$ (by associative law)

$\Rightarrow b * e = c * e$ ($\because a * a^{-1} = e$)

$\Rightarrow b = c$ (e is the identity element in G)

Note:

1. If G is an additive group, $a + b = a + c \Rightarrow b = c$ and $b + a = c + a \Rightarrow b = c$.

2. In a semi group cancelation laws may not hold. Let S be the set of all 2×2 matrices over integers and let matrix multiplication be the binary operation defined on S. Then S is a semi group of the above operation.

If $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$; $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$; $C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, then $A, B, C \in S$ and $AB = AC$, we observe that left cancellation law is not true in the semi group.

3. $(N, +)$ is a semi group. For $a, b, c \in N$

$a + b = a + c \Rightarrow b + c$ and $b + a = c + a$

$\Rightarrow b = c$. But $(N, +)$ is not a group.

In a semigroup even if cancellation laws holds, then semigroup is not a group.

Example: If every element of a group G is its own inverse, show that G is an abelian group. Solution: Let $a, b \in G$. By hypothesis $a^{-1} = a$, $b^{-1} = b$.

Then $ab \in G$ and hence $(ab)^{-1}$

$= ab$. Now

$$(ab)^{-1} = ab$$
$$\Rightarrow b^{-1}a^{-1} = ab$$
$$\Rightarrow ba = ab$$

$\therefore$ G is an abelian group.

Note: The converse of the above not true.
For example, $(R, +)$, where R is the set of real numbers, is abelian group, but no element except 0 is its own inverse.
Example: Prove that if $a^2 = a$, then $a = e$, a being an element of a group G. Solution: Let a be an element of a group G such that $a^2 = a$. To prove that $a = e$.
$a^2 = a \Rightarrow aa = a$

$\Rightarrow (aa)a^{-1} = aa^{-1} \Rightarrow a(aa^{-1}) = e$

$\Rightarrow ae = e$ [$\because aa^{-1} = e$] $\Rightarrow a = e$ [$\because ae = a$]

Example: In a group G having more than one element, if $x^2 = x$, for every $x \in G$. Prove that G is abelian.
Solution: Let $a, b \in G$. Under the given hypothesis, we have $a^2 = a$, $b^2 = b$, $(ab)^2 = ab$.

$\therefore a(ab)b = (aa)(bb) = a^2b^2 = ab = (ab)^2 = (ab)(ab) = a(ba)b$

$\Rightarrow ab = ba$ (Using cancelation laws)

$\therefore G$ is abelian.

Example: Show that in a group G, for $a, b \in G$, $(ab)^2 = a^2b^2 \Leftrightarrow G$ is abelian.

(May. 2012) Solution: Let $a, b \in G$, and $(ab)^2 = a^2b^2$. To prove that G is abelian.
Then
$(ab)^2 = a^2b^2$

$\Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow a(ba)b = a(ab)b$ (by Associative law) $\Rightarrow ba = ab$, (by cancellation laws)

$\Rightarrow G$ is abelian.

Conversely, let G be abelian. To prove that $(ab)^2 = a^2b^2$. Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$.
***Example: If a, b are any two elements of a group $(G, \cdot)$, which commute. Show that

1. a^{-1} and b commute
2. b^{-1} and a commute
3. a^{-1} and b^{-1} commute.

Solution: $(G, \cdot)$ is a group and such that

$ab = ba$.

1. $ab = ba \Rightarrow a^{-1}(ab) = a^{-1}(ba)$

$\Rightarrow (a^{-1}a)b = a^{-1}(ba)$

$\Rightarrow eb = (a^{-1}b)a$

$\Rightarrow b = (a^{-1}b)a$

$\Rightarrow ba^{-1} = [(a^{-1}b)a]a^{-1}$

$=(a^{-1}b)(aa^{-1})$

$=(a^{-1}b)e$

$=a^{-1}b$

$\Rightarrow a^{-1}$ and b commute.

1 $ab = ba \Rightarrow (ab)b^{-1} = (ba)b^{-1}$

$\Rightarrow a(bb^{-1}) = (ba)b^{-1} \Rightarrow ae = b(ab^{-1})$

$\Rightarrow a = b(ab^{-1})$

$\Rightarrow b^{-1}a = b^{-1}[b(ab^{-1})]$

$=(b^{-1}b)(ab^{-1})]$

$=e(ab^{-1})$

$=ab^{-1}$

$\Rightarrow b^{-1}$ and a commute.

2 $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1}\ b^{-1}\ a^{-1} = a^{-1}\ b^{-1}$

$\Rightarrow a^{-1}$ and b^{-1} are commute.

Order of an Element

Definition: Let $(G, *)$ be a group and $a \in G$, then the least positive integer n if it exists such that $a^n = e$ is called the order of $a \in G$.

The order of an element $a \in G$ is be denoted by $O(a)$.

Example: $G = \{1, -1, i, -i\}$ is a group with respect to multiplication. 1 is the identity in G. $1^1 = 1^2 = 1^3 = \cdots = 1 \Rightarrow O(1) = 1$.

$(-1)^2 = (-1)^4 = (-1)^6 = \cdots = 1 \Rightarrow O(-1) = 2$.

$i^4 = i^8 = i^{12} = \cdots = 1 \Rightarrow O(i) = 4$. $(-i)^4 = (-i)^8 = \cdots = 1 \Rightarrow O(-i) = 4$.

Example: In a group G, a is an element of order 30. Find order of a^5.

Solution: Given $O(a) = 30$

$\Rightarrow a^{30} = e$, e is the identity element of G. Let $O(a^5) = n$

$\Rightarrow (a^5)^n = e$

$\Rightarrow a^{5n} = e$, where n is the least positive integer. Hence 30 is divisor of $5n$.

$\therefore n = 6$.

Hence $O(a^5) = 6$

Sub Groups

Definition: Let $(G, *)$ be a group and H be a non-empty subset of G. If $(H, *)$ is itself is a

group, then $(H, *)$ is called sub-group of

$(G, *)$. Examples:

1. $(Z, +)$ is a subgroup of $(Q, +)$.

2. The additive group of even integers is a subgroup of the additive group of all integers.
3. $(N, +)$ is not a subgroup of the group $(Z, +)$, since identity does not exist in N under $+$.

Example: Let $G = \{1, -1, i, -i\}$ and $H = \{1, -1\}$.
Here G and H are groups with respect to the binary operation multiplication and H is a subset of G. Therefore $(H, \cdot)$ is a subgroup of $(G, \cdot)$.

Example: Let $H = \{0, 2, 4\} \subseteq Z_6$. Check that $(H, +_6)$ is a subgroup of $(Z_6, +_6)$. Solution: $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

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

$\therefore (Z_6, +_6)$ is a group.

H= $\{0, 2, 4\}$.

$+6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

The following conditions are to be satisfied in order to prove that it is a subgroup. (i). Closure: Let $a, b \in H \Rightarrow a +_6 b \in H$.

$0, 2 \in H \Rightarrow 0 +_6 2 = 2 \in H$.

(ii). Identity Element: The row headed by 0 is exactly same as the initial row.

$\therefore$ 0 is the identity element.

(iii). Inverse: $0^{-1} = 0, 2^{-1} = 4, 4^{-1} = 2$.

Inverse exist for each element of $(H, +_6)$.

$\therefore (H, +_6)$ is a subgroup of $(Z_6, +_6)$.

Theorem: If $(G, *)$ is a group and $H \subseteq G$, then $(H, *)$ is a subgroup of $(G, *)$ if and only if

(i) $a, b \in H \Rightarrow a * b \in H$;

(ii) $a \in H \Rightarrow a^{-1} \in$

H. Proof: The condition is necessary

Let $(H, *)$ be a subgroup of $(G, *)$.

To prove that conditions (i) and (ii) are satisfied.

Since $(H, *)$ is a group, by closure property we have $a, b \in H$

$\Rightarrow ab \in H$. Also, by inverse property $a \in H \Rightarrow a^{-1} \in H$.

The condition is sufficient:

Let (i) and (ii) be true. To prove that $(H, *)$ is a subgroup

of $(G, *)$. We are required to prove is: $*$ is associative in H

and identity $e \in H$.

That $*$ is associative in H follows from the fact that $*$ is associative in G. Since H

is nonempty, let $a \in H \Rightarrow a^{-1} \in H$ (by (ii))

$\therefore a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$ (by (i))

$\Rightarrow$ e $\in$ H ($\because$ $aa^{-1} \in H \Rightarrow aa^{-1} \in G \Rightarrow aa^{-1}$ = e, where e is the identity in G.)

$\Rightarrow$ e is the identity in

H. Hence H itself is a

group.

$\therefore$ H is a subgroup of G.

Example: The set S of all ordered pairs (a, b) of real numbers for which $a \neq 0$ w.r.t the operation $\times$ defined by $(a, b) \times (c, d) = (ac, bc + d)$ is non-abelian. Let H= $\{(1, b) | b \in R\}$ is a subset of S. Show that H is a subgroup of $(S, \times)$.

Solution: Identity element in S is (1, 0). Clearly $(1, 0) \in H$.

Inverse of (a, b) in S is $(1/a, -b/a)$ ($\because$

$a \neq 0$) Inverse of $(1, c)$ in S is (1, -c/1),

i.e., $(1, -c)$

Clearly $(1, c) \in H \Rightarrow (1, c)^{-1} = (1, -c) \in H$.

Let $(1, b) \in H$.

$(1, b) \times (1, c)^{-1} = (1, b) \times (1, -c)$

$= (1.1, b.1 - c) = (1, b - c) \in H$ ($\because b - c \in R$)

$\therefore (1, b), (1, c) \in H \Rightarrow (1, b) \times (1, c)^{-1} \in H \therefore$

H is a subgroup of $(S, \times)$.

Note: $(1, b) \times (1, c) = (1.1, b.1 + c)$

$=(1, b + c)$

$=(1, c + b)$

$=(1, c) \times (1, b)$

$\therefore H$ is an abelian subgroup of the non-abelian group $(S, \times)$.

Theorem: If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a

subgroup of
G.

Proof: Let H_1 and H_2 be two subgroups of a group G. Let e be the identity element in G.

$\therefore e \in H_1$ and $e \in H_2$. $\therefore e \in$

$H_1 \cap H_2$.

$\Rightarrow H_1 \cap H_2 \neq \phi$.

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$.

$\therefore a \in H_1$, $a \in H_2$ and $b \in H_1$, $b \in H_2$.

Since H_1 is a subgroup, $a \in H_1$ and $b \in H_1 \Rightarrow$

$ab^{-1} \in H_1$. Similarly $ab^{-1} \in H_2$.

$\therefore ab^{-1} \in H_1 \cap H_2$.

Thus we have, $a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$.

$\therefore H_1 \cap H_2$ is a subgroup of G.

Example: Let G be the group and $Z=\{x \in G | xy=yx$ for all $y \in G\}$. Prove that Z is a subgroup of
G.

Solution: Since $e \in G$ and $ey = ye$, for all $y \in G$. It follows that $e \in Z$. Therefore Z is non-empty.

Take any $a, b \in Z$ and any $y \in G$. Then

$$(ab)y = a(by)$$
$$= a(yb), \text{ since } b \in Z, by = yb$$
$$= (ay)b$$
$$= (ya)b$$
$$= y(ab)$$

This show that $ab \in Z$.

Let $a \in Z \Rightarrow ay = ya$ for all $y \in G$.

$\Rightarrow a^{-1}(ay)a^{-1} = a^{-1}(ya)a^{-1}$

$\Rightarrow (a^{-1}a)(ya^{-1}) = (a^{-1}y)(aa^{-1})$

$\Rightarrow e(ya^{-1}) = (a^{-1}y)e \Rightarrow a^{-1}y = ay^{-1}$

This shows that $a^{-1} \in Z$.

Thus, when $a, b \in Z$, we have $ab \in Z$ and

$a^{-1} \in Z$. Therefore Z is a subgroup of G.

This subgroup is called the *center* of G.

Homomorphism

Homomorphism into: Let $(G, *)$ and $(G', \cdot)$ be two groups and f be a mapping from G into

G'. If for $a, b \in G$, $f(a*b) = f(a) \cdot f(b)$, then f is called *homomorphism G into* G'.

Homomorphism onto: Let $(G, *)$ and $(G', \cdot)$ be two groups and f be a mapping from G onto G'. If for $a, b \in G$, $f(a*b) = f(a) \cdot f(b)$, then f is called *homomorphism*

G onto G'.

Also then G' is said to be a homomorphic image of G. We write this as $f(G)$ □ G'. **Isomorphism:** Let $(G, *)$ and $(G', \cdot)$ be two groups and f be a one-one mapping of G onto G'. If for $a, b \in G$, $f(a * b) = f(a) \cdot f(b)$, then f is said to be an isomorphism from G onto G'.

Endomorphism: A homomorphism of a group G into itself is called an *endomor-phism*. **Monomorphism:** A homomorphism into is one-one, then it is called an *monomor-phism*. **Epimorphism:** If the homomorphism is onto, then it is called *epimorphism*.

Automorphism: An isomorphism of a group G into itself is called an *automorphism*.

Example: Let G be the additive group of integers and G' be the multiplicative group. Then mapping $f : G \to G'$ given by $f(x) = 2^x$ is a group homomorphism of G into G'.

Solution: Since $x, y \in G \Rightarrow x + y \in G$ and $2^x, 2^y \in G' \Rightarrow 2^x \cdot 2^y \in G'$.

$\therefore f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$.

$\Rightarrow f$ is a homomorphism of G into G'.

Example: Let G be a group of positive real numbers under multiplication and G' be a group of all real numbers under addition. The mapping $f : G \to G'$ given by $f(x) = \log_{10} x$. Show that f is an isomorphism.

Solution: Given $f(x) = \log_{10} x$.

Let $a, b \in G \Rightarrow ab \in G$. Also, $f(a), f(b) \in G'$.

$\therefore f(ab) = \log_{10} ab = \log_{10} a + \log_{10} b = f(a) + f(b)$.

$\Rightarrow f$ is a homomorphism from G into G'. Let $x_1, x_2 \in G$ and $f(x_1) = f(x_2)$

$$\Rightarrow \log_{10} x_1 = \log_{10} x_2$$

$$\Rightarrow 10^{\log_{10} x_1} = 10^{\log_{10} x_2}$$

$\Rightarrow x_1 = x_2$

$\Rightarrow f$ is one-one.

$\Rightarrow f(10^y) = \log_{10}(10^y) = y$.

$\therefore$ For ever $y \in G'$, there exists $10^y \in G$ such that $f(10^y) = y$

$\Rightarrow f$ is onto.

$\therefore f$ an isomorphism from G to G'.

Example: If R is the group of real numbers under the addition and R^+ is the group of positive real numbers under the multiplication. Let $f : R \to R^+$ be defined by $f(x) = e^x$, then show that f is an isomorphism.

Solution: Let $f : R \to R^+$ be defined by $f(x) = e^x$.

f is one-one: Let $a, b \in G$ and $f(a) = f(b)$

$\Rightarrow e^a = e^b$

$\Rightarrow \log e^a = \log e^b$

$\Rightarrow a \log e = b \log e$

$\Rightarrow a = b$

Thus f is one-one.

f is onto: If $c \in R^+$ then $\log c \in R$ and $f(\log c) = e^{\log c} = c$

Thus each element of R^+ has a pre-image in R under f and hence f is onto.

f is Homomorphism: $f(a + b) = e^{a+b} = e^a.e^b = f(a).f(b)$ Hence f is an isomorphism.

Example: Let G be a multiplicative group and $f : G \to G$ such that for $a \in G$, $f(a) = a^{-1}$. Prove that f is one-one and onto. Also, prove that f is homomorphism if and only if G is commutative.

Solution: $f : G \to G$ is a mapping such that $f(a) = a^{-1}$,
for $a \in G$. (i). To prove that f is one-one.
Let $a, b \in G$. $\therefore a^{-1}, b^{-1} \in G$ and $f(a)$,
$f(b) \in G$. Now $f(a) = f(b)$

$\Rightarrow a^{-1} = b^{-1}$

$\Rightarrow (a^{-}1)^{-}1 = (b^{-}1)^{-}1$

$\Rightarrow a = b$

$\therefore f$ is one-one.

(ii). To prove that f is onto.
Let $a \in G$. $\therefore a^{-1} \in G$ such that $f(a^{-1}) = (a^{-1})^{-1} = a$.

$\therefore f$ is onto.

(iii). Suppose f is a homomorphism.

For $a, \in G$, $ab \in G$. Now $f(ab) = f(a)f(b)$

$\Rightarrow (ab)^{-1} = a^{-1}b^{-1} \Rightarrow b^{-}1a^{-}1 = a^{-}1b^{-}1$

$\Rightarrow (b^{-}1a^{-}1)^{-}1 = (a^{-}1b^{-}1)^{-}1$

$\Rightarrow (a^{-}1)^{-}1(b^{-}1)^{-}1 = (b^{-}1)^{-}1(a^{-}1)^{-}1$

$\Rightarrow ab = ba$

$\therefore G$ is abelian.

(iv). Suppose G is abelian $\Rightarrow ab = ba, \forall a, b \in G$.

For $a, b \in G$, $f(ab) = (ab)^{-1}$

$= b^{-}1a^{-}1$

$= a^{-}1b^{-}1$
$= f(a)f(b)$

$\therefore f$ is a homomorphism.

UNIT-3

ELEMENTARY COMBINATORICS

Combinatorics is a subfield of "discrete mathematics," so we should begin by asking what discrete mathematics means. The differences are to some extent a matter of opinion, and various mathematicians might classify specific topics differently.

"Discrete" should not be confused with "discreet," which is a much more commonly-used word. They share the same Latin root, "discretio," which has to do with wise discernment or separation. In the mathematical "discrete," the emphasis is on separateness, so "discrete" is the opposite of "continuous." If we are studying objects that can be separated and treated as a (generally countable) collection of units rather than a continuous structure, then this study falls into discrete mathematics.

In calculus, we deal with continuous functions, so calculus is not discrete mathematics. In linear algebra, our matrices often have real entries, so linear algebra also does not fall into discrete mathematics.

Text books on discrete mathematics often include some logic, as discrete mathematics is often used as a gateway course for upper-level math. Elementary number theory and set theory are also sometimes covered. Algorithms are a common topic, as algorithmic techniques tend to work very well on the sorts of structures that we study in discrete mathematics.

In Combinatorics, we focus on combinations and arrangements of discrete structures. There are five major branches of combinatorics that we will touch on in this course: enumeration, graph theory, Ramsey Theory, design theory, and coding theory. (The related topic of cryptog- raphy can also be studied in combinatorics, but we will not touch on it in this course.) We will focus on enumeration, graph theory, and design theory, but will briefly introduce the other two topics.

1A. Enumeration

Enumeration is a big fancy word for counting. If you've taken a course in probability and statistics, you've already covered some of the techniques and problems we'll be covering in this course. When a statistician (or other mathematician) is calculating the "probability" of a particular outcome in circumstances where all outcomes are equally likely, what they usually do is enumerate all possible outcomes, and then figure out how many of these include the outcome they are looking for.

EXAMPLE 1.1. What is the probability of rolling a 3 on a 6-sided die?

SOLUTION. To figure this out, a mathematician would count the sides of the die (there are six) and count how many of those sides display a three (one of them). She would conclude that the probability of rolling a 3 on a 6-sided die is 1/6 (one in six).

1

That was an example that you could probably figure out without having studied enumera- tion or probability, but it nonetheless illustrates the basic principle behind many calculations of probability. The object of enumeration is to enable us to count outcomes in much more complicated situations. This sometimes has natural applications to questions of probability, but our focus will be on the counting, not on the probability.

After studying enumeration in this course, you should be able to solve problems such as:

- If you are playing Texas Hold'em poker against a single opponent, and the two cards in your hand are a pair, what is the probability that your opponent has a higher pair?
- How many distinct Shidokus (4-by-4 Sudokus) are there?
- How many different orders of five items can be made from a bakery that makes three kinds of cookies?
- Male honeybees come from a queen bee's unfertilised eggs, so have only one parent (a female). Female honeybees have two parents (one male, one female). Assuming all ancestors were distinct, how many ancestors does a male honeybee have from 10 generations ago?

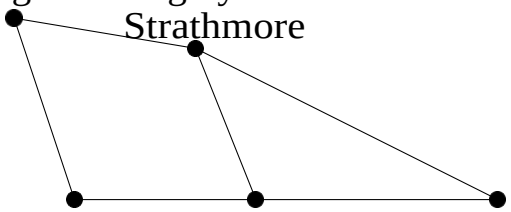
Although all of these questions (and many others that arise naturally) may be of interest to you, the reason we begin our study with enumeration is because we'll be able to use many of the techniques we learn, to count the other structures we'll be studying.

1B. Graph Theory

When a mathematician talks about graph theory, she is not referring to the "graphs" that you learn about in school, that can be produced by a spreadsheet or a graphing calculator. The "graphs" that are studied in graph theory are models of networks.

Any network can be modeled by using dots to represent the nodes of the network (the cities, computers, cell phones, or whatever is being connected) together with lines to represent the connections between those nodes (the roads, wires, wireless connections, etc.). This model is called a graph. It is important to be aware that only at a node may information, traffic, etc. may pass from one edge of a graph to another edge. If we want to model a highway network using a graph, and two highways intersect in the middle of nowhere, we must still place a node at that intersection. If we draw a graph in which edges cross over each other but there is no node at that point, you should think of it as if there is an overpass there with no exits from one highway to the other: the roads happen to cross, but they are not connecting in any meaningful sense.

EXAMPLE 1.2. The following diagram: Calgary Strathmore



Fort Macleod

Lethbridge Medicine

Hat is a graph.

Many questions that have important real-world applications can be modeled with graphs. These are not always limited to questions that seem to apply to networks. Some questions can be modeled as graphs by using lines to represent constraints or some other relationship between them (e.g. the nodes might represent classes, with a line between them if they cannot

be scheduled at the same time, or some nodes might represent students and others classes, with a line between a student and each of the classes he or she is taking).

After studying graph theory in this course, you should be able to solve problems such as:

- How can we find a good route for garbage trucks to take through a particular city?
- Is there a delivery route that visits every city in a particular area, without repetition?
- Given a collection of project topics and a group of students each of whom has expressed interest in some of the topics, is it possible to assign each student a unique topic that interests him or her?
- A city has bus routes all of which begin and end at the bus terminal, but with different schedules, some of which overlap. What is the least number of buses (and drivers) required in order to be able to complete all of the routes according to the schedule?
- Create a schedule for a round-robin tournament that uses as few time slots as possible. Some of these questions you may only be able to answer for particular kinds of graphs.

Graph theory is a relatively "young" branch of mathematics. Although some of the problems and ideas that we will study date back a few hundred years, it was not until the 1930s that these individual problems were gathered together and a unified study of the theory of graphs began to develop.

1C. Ramsey Theory

Ramsey theory takes its name from Frank P. Ramsey, a British mathematician who died in 1930 at the tragically young age of 26, when he developed jaundice after an operation.

Ramsey was a logician. A result that he considered a minor lemma in one of his logic papers now bears the name "Ramsey's Theorem" and was the basis for this branch of mathematics. Its statement requires a bit of graph theory: given c colours and fixed sizes $n_1, \ldots, n_c$, there is an integer $r = R(n_1, \ldots, n_c)$ such that for any colouring the edges of of a complete graph on r vertices, there must be some i between 1 and c such that there is a complete subgraph on n_i vertices, all of whose edges are coloured with colour i.

In addition to requiring some graph theory, that statement was a bit technical. In much less precise terms that don't require so much

background knowledge (but could be misleading in specific situations), Ramsey Theory asserts that if structure is big enough and contains a property we are interested in, then no matter how we cut it into pieces, at least one of the pieces should also have that property. One major theorem in Ramsey Theory is van der Waerden's Theorem, which states that for any two constants c and n, there is a constant V (c, n) such that if we take V (c, n) consecutive numbers and colour them with c colours, there must be an arithmetic progression of length n all of whose members have been coloured with the same colour.

EXAMPLE 1.3. Here is a small example of van der Waerden's Theorem. With two colours and a desired length of 3 for the arithmetic progression, we can show that V (2, 3) > 8 using the following colouring:

3456**78**910

(In case it is difficult to see, we point out that 3, 4, 7, and 8 are black, while 5, 6, 9, and 10 are grey, a different colour.) Notice that with eight consecutive integers, the difference in a three-term arithmetic progression cannot be larger than three. For every three-term arithmetic progression with difference of one, two, or three, it is straightforward to check that the numbers have not all received the same colour.

In fact, V (2, 3) = 9, but proving this requires exhaustive testing.

We will touch lightly on Ramsey Theory in this course, specifically on Ramsey's Theorem itself, in the context of graph theory.

1D. Design Theory

Like graph theory, design theory is probably not what any non-mathematician might expect from its name.

When researchers conduct an experiment, errors can be introduced by many factors (in- cluding, for example, the timing or the subject of the experiment). It is therefore important to replicate the experiment a number of times, to ensure that these unintended variations do not account for the success of a particular treatment. If a number of different treatments are being tested, replicating all of them numerous times becomes costly and potentially infeasible. One way to reduce the total number of trials while still maintaining the accuracy, is to test multiple treatments on each subject, in different combinations.

One of the major early motivations for design theory was this context: given a fixed number of total treatments, and a fixed number of treatments we are willing to give to any subject, can we find combinations of the possible treatments so that each treatment is given to some fixed number of subjects, and any pair of treatments is given together some fixed number of times (often just once). This is the basic structure of a block design.

EXAMPLE 1.4. Suppose that we have seven different fertilisers and seven garden plots on which to try them. We can organise them so that each fertiliser is applied to three of the plots, each garden plot receives 3 fertilisers, and any pair of fertilisers is used together on precisely one of the plots. If the different fertilisers are numbered one through seven, then a method for arranging them is to place fertilisers 1, 2, and 3 on the first plot; 1, 4, and 5 on the second; 1,
6, and 7 on the third; 2, 4, and 6 on the fourth; 2, 5, and 7 on the fifth; 3, 4, and 7 on the sixth; and 3, 5, and 6 on the last. Thus,

123	145	167
246	257	347
	356	

is a design.

This basic idea can be generalised in many ways, and the study of structures like these is the basis of design theory. In this course, we will learn some facts about when designs exist, and how to construct them.

After studying design theory in this course, you should be able to

solve problems such as: Is it possible for a design to exist with a particular set of parameters?

What methods might we use in trying to construct a design?

1E. Coding Theory

In many people's minds "codes" and "cryptography" are inextricably linked, and they might be hard-pressed to tell you the difference. Nonetheless, the two topics are vastly different, as is the mathematics involved in them.

Coding theory is the study of encoding information into different symbols. When someone uses a code in an attempt to make a message that only certain other people can read, this becomes cryptography. Cryptographers study strategies for ensuring that a code is difficult to "break" for those who don't have some additional information. In coding theory, we ignore the question of who has access to the code and how secret it may be. Instead, one of the primary concerns becomes our ability to detect and correct errors in the code.

Codes are used for many purposes in which the information is not intended to be secret. For example, computer programs are transformed into long strings of binary data, that a computer reinterprets as instructions. When you text a photo to a friend, the pixel and colour information are converted into binary data to be transmitted through radio waves. When you listen to an
.mp3 file, the sound frequencies of the music have been converted into binary data that your computer decodes back into sound frequencies.

Electronic encoding is always subject to interference, which can cause errors. Even when a coded message is physically etched onto a device (such as a dvd), scratches can make some parts of the code illegible. People don't like it when their movies, music, or apps freeze, crash, or skip over something. To avoid this problem, engineers use codes that allow our devices to automatically detect, and correct, minor errors that may be introduced.

In coding theory, we learn how to create codes that allow for error detection and correction, without requiring excessive memory or storage capacity. Although coding theory is not a focus of this course, designs can be used to create good codes. We will learn how to make codes from designs, and what makes these codes "good."

EXAMPLE 1.5. Suppose we have a string of binary information, and we want the computer to store it so we can detect if an error has arisen. There are two symbols we need to encode: 0 and 1. If we just use 0 for 0 and 1 for 1, we'll never know if a bit has been flipped (from 0 to 1 or vice versa). If we use 00 for 0 and 01 for 1, then if the first bit gets flipped we'll know there was an error (because the first bit should never be 1), but we won't notice if the second was flipped. If we use 00 for 0 and 11 for 1, then we will be able to detect an error, as long as at most one bit gets flipped, because flipping one bit of either code word will result in either 01 or 10, neither of which is a valid code word. Thus, this code allows us to detect an error. It does not allow us to correct an error, because even knowing that a single bit has been flipped, there is no way of knowing whether a 10 arose from a 00 with the first bit flipped, or from a 11 with the second bit flipped. We would need a longer code to be able to correct errors.

After our study of coding theory, you should be able to solve problems such as:

- Given a code, how many errors can be detected?
- Given a code, how many errors can be corrected?
- Construct some small codes that allow detection and correction of small numbers of errors.

EXERCISES 1.6. Can you come up with an interesting counting problem that you wouldn't know how to solve?

SUMMARY:

- enumeration
- graph theory
- Ramsey theory
- design theory
- • coding theory

Basic Counting Techniques

When we are trying to count the number of ways in which something can happen, sometimes the answer is very obvious. For example, if a doughnut shop has five different kinds of doughnuts for sale and you are planning to buy one doughnut, then you have five choices.

There are some ways in which the situation can become slightly more complicated. For example, perhaps you haven't decided whether you'll buy a doughnut or a bagel, and the store also sells three kinds of bagels. Or perhaps you want a cup of coffee to go with your doughnut, and there are four different kinds of coffee, each of which comes in three different sizes.

These particular examples are fairly small and straightforward, and you could list all of the possible options if you wished. The goal of this chapter is to use simple examples like these to demonstrate two rules that allow us to count the outcomes not only in these situations, but in much more complicated circumstances. These rules are the *product rule*, and the *sum rule*.

2A. The product rule

The product rule is a rule that applies when we there is more than one variable (i.e. thing that can change) involved in determining the final outcome.

EXAMPLE 2.1. Consider the example of buying coffee at a coffee shop that sells four varieties and three sizes. When you are choosing your coffee, you need to choose both variety and size. One way of figuring out how many choices you have in total, would be to make a table. You could label the columns with the sizes, and the rows with the varieties (or vice versa, it doesn't matter). Each entry in your table will be a different combination of

variety and size:

	Small	**Medium**	**Large**
Latte	small latte	medium latte	large latte
Mocha	small mocha	medium mocha	large mocha
Espresso	small espresso	medium espresso	large espresso
Cappuccino	small cappuccino	medium cappuccino	large cappuccino

As you can see, a different combination of variety and size appears in each space of the table, and every possible combination of variety and size appears somewhere. Thus the total number of possible choices is the number of entries in this table. Although in a small example like this we could simply count all of the entries and see that there are twelve, it will be more useful to notice that elementary arithmetic tells us that the number of entries in the table will be the number of rows times the number of columns, which is four times three.

In other words, to determine the total number of choices you have, we multiply the number of choices of variety (that is, the number of rows in our table) by the number of choices of size (that is, the number of columns in our table). This is an example of what we'll call the *product rule*.

We're now ready to state the product rule in its full generality.

THEOREM 2.2.Product Rule *Suppose that when you are determining the total number of outcomes, you can identify two different aspects that can vary. If there are* n_1 *possible outcomes for the first aspect, and for each of those possible outcomes, there are* n_2 *possible outcomes for the second aspect, then the total number of possible outcomes will be* n_1n_2.

In the above example, we can think of the aspects that can change as being the variety of coffee, and the size. There are four outcomes (choices) for the first aspect, and three outcomes (choices) for the second aspect, so the total number of possible outcomes is 4 3 = 12.

Sometimes it seems clear that there are more than two aspects that are varying. If this happens, we can apply the product rule more than once to determine the answer, by first identifying two aspects (one of which may be "all the rest"), and then subdividing one or both of those aspects. An example of this is the problem posed earlier of buying a doughnut to go with your coffee.

EXAMPLE 2.3. Kyle wants to buy coffee and a doughnut. The local doughnut shop has five kinds of doughnuts for sale, and sells four varieties of coffee in three sizes (as in Example 2.1). How many different orders could Kyle make?

SOLUTION. A natural way to divide Kyle's options into two aspects that can vary, is to consider separately his choice of doughnut, and his choice of coffee. There are five choices for the kind of doughnut he orders, so $n_1 = 5$. For choosing the coffee, we have already used the product rule in Example 2.1 to determine that the number of coffee options is $n_2 = 12$.

Thus the total number of different orders Kyle could make is $n_1 n_2 = 5 \cdot 12 = 60$.

Let's go through an example that more clearly involves repeated applications of the product rule.

EXAMPLE 2.4. Chloë wants to manufacture children's t-shirts. There are generally three sizes of t-shirts for children: small, medium, and large. She wants to offer the t-shirts in eight different colours (blue, yellow, pink, green, purple, orange, white, and black). The shirts can have an image on the front, and a slogan on the back. She has come up with three images, and five slogans.

To stock her show room, Chloë wants to produce a single sample of each kind of shirt that she will be offering for sale. The shirts cost her $4 each to produce. How much are the samples going to cost her (in total)?

SOLUTION. To solve this problem, observe that to determine how many sample shirts Chloë will produce, we can consider the size as one aspect, and the style (including colour, image, and slogan) as the other. There are $n_1 = 3$ sizes. So the number of samples will be three times n_2, where n_2 is the number of possible styles.

We now break n_2 down further: to determine how many possible styles are available, you

can divide this into two aspects: the colour, and the decoration (image and slogan). There are $n_{2,1} = 8$ colours. So the number of styles will be eight times $n_{2,2}$, where $n_{2,2}$ is the number of possible decorations (combinations of image and slogan) that are available.

We can break $n_{2,2}$ down further: to determine how many possible decorations are available, you divide this into the two aspects of image and slogan. There are $n_{2,2,1} = 3$ possible images, and $n_{2,2,2} = 5$ possible slogans, so the product rule tells us that there are $n_{2,2} = 3 \cdot 5 = 15$ possible combinations of image and slogan (decorations).

Putting all of this together, we see that Chloë will have to create $3(8(3 \cdot 5)) = 360$ sample t-shirts. As each one costs $4, her total cost will be $1440. □

Notice that finding exactly two aspects that vary can be quite artificial. Example 2.4 serves as a good demonstration for a generalisation of the product rule as we stated it above. In that example, it would have been

more natural to have considered from the start that there were four apparent aspects to the t-shirts that can vary: size; colour; image; and slogan. The total number of t-shirts she needed to produce was the product of the number of possible outcomes of each of these aspects: $3 \cdot 8 \cdot 3 \cdot 5 = 360$.

THEOREM 2.5.Product Rule for many aspects *Suppose that when you are determining the total number of outcomes, you can identify* k *different aspects that can vary. If for each* i *between 1 and* k *there are* n_i *possible outcomes for the* i*th aspect, then the total number of possible outcomes will be* $\prod_{i=1}^{k} n_i$ *(that is, the product as* i *goes from 1 to* k *of the* n_i*).*

Now let's look at an example where we are trying to evaluate a probability. Since this course is about counting rather than probability, we'll restrict our attention to examples where all outcomes are equally likely. Under this assumption, in order to determine a probability, we can count the number of outcomes that have the property we're looking for, and divide by the total number of outcomes.

EXAMPLE 2.6. Peter and Mary have two daughters. What is the probability that their next two children will also be girls?

SOLUTION. To answer this, we consider each child as a different aspect. There are two possible sexes for their third child: boy or girl. For each of these, there are two possible choices for their fourth child: boy or girl. So in total, the product rule tells us that there are $2 \cdot 2 = 4$ possible combinations for the sexes of their third and fourth children. This will be the denominator of the probability.

To determine the numerator (that is, the number of ways in which both children can be girls), we again consider each child as a different aspect. There is only one possible way for the third child to be a girl, and then there is only one possible way for the fourth child to be a girl. So in total, only one of the four possible combinations of sexes involves both children being girls.

The probability that their next two children will also be girls is 1/4. □

Notice that in this example, the fact that Peter and Mary's first two children were girls was irrelevant to our calculations, because it was already a known outcome, over and done with, so is true no matter what may happen with their later children. If Peter and Mary hadn't yet had any children and we asked for the probability that their first four children will all be girls, then our calculations would have to include both possible options for the sex of each of their first two children. In this case, the final probability would be 1/16 (there are 16 possible combinations for the sexes

of four children, only one of which involves all four being female).

EXERCISES 2.7. Use only the product rule to answer the following questions:

1) The car Jack wants to buy comes in four colours; with or without air conditioning; with five different options for stereo systems; and a choice of none, two, or four floor mats. If the dealership he visits has three cars in the lot, each with different options, what is the probability that one of the cars they have in stock has exactly the options he wants?
2) Candyce is writing a "Choose your own adventure" book in which she wants every possible choice to result in a different ending. If there are four points at which choices

must be made in every storyline, and there are three choices the first time but two every time after that, how many endings does Candyce need to write?

3) William is buying five books. For each book he has a choice of version: hardcover, paperback, or electronic. In how many different ways can he make his selection?

2B. The sum rule

The sum rule is a rule that can be applied to determine the number of possible outcomes when there are two different things that you might choose to do (and various ways in which you can do each of them), and you cannot do both of them. Often, it is applied when there is a natural way of breaking the outcomes down into cases.

EXAMPLE 2.8. Recall the example of buying a bagel *or* a doughnut at a doughnut shop that sells five kinds of doughnuts and three kinds of bagels. You are only choosing one or the other, so one way to determine how many choices you have in total, would be to write down all of the possible kinds of doughnut in one list, and all of the possible kinds of bagel in another list:

Doughnuts	**Bagels**
chocolate glazed	
	blueberry
chocolate iced	cinnamon
raisin	
honey cruller	
	plain
custard filled	
original glazed	

The total number of possible choices is the number of entries that appear in the two lists combined, which is five plus three.

In other words, to determine the number of choices you have, we add the number of choices of doughnut (that is, the number of entries in the first list) and the number of choices of bagel (that is, the number of entries in the second list). This is an example of the *sum rule*.

We're now ready to state the sum rule in its full generality.

THEOREM 2.9.Sum Rule *Suppose that when you are determining the total number of out- comes, you can identify two distinct cases with the property that every possible outcome lies in exactly one of the cases. If there are* n_1 *possible outcomes in the first case, and* n_2 *possible outcomes in the second case, then the total number of possible outcomes will be* $n_1 + n_2$.

It's hard to do much with the sum rule by itself, but we'll cover a couple more examples and then in the next section, we'll get into some more challenging examples where we combine the two rules.

Sometimes the problem naturally splits into more than two cases, with every possible out- come lying in exactly one of the cases. If this happens, we can apply the sum rule more than once to determine the answer. First we identify two cases (one of which may be "everything else"), and then subdivide one or both of the cases. Let's look at an example of this.

EXAMPLE 2.10. Mary and Peter are planning to have no more than three children. What are the possible combinations of girls and boys they might end up with, if we aren't keeping track of the order of the children? (By not keeping track of the order of the children, I mean that we'll consider having two girls followed by one boy as being the same as having two girls and one boy in any other order.)

SOLUTION. To answer this question, we'll break the problem into cases. First we'll divide the problem into two possibilities: Mary and Peter have no children; or they have at least one child. If Mary and Peter have no children, this can happen in only one way (no boys and no girls). If Mary and Peter have at least one child, then they have between one and three children. We'll have to break this down further to find how many outcomes are involved.

We break the case where Mary and Peter have between one and three children down into two cases: they might have one child, or they might have more than one child. If they have one child, that child might be a boy or a girl, so there are two possible outcomes. If they have more than one child, again we'll need to further subdivide this case.

The case where Mary and Peter have either two or three children

naturally breaks down into two cases: they might have two children, or they might have three children. If they have two children, the number of girls they have might be zero, one, or two, so there are three possible outcomes (the remaining children, if any, must all be boys). If they have three children, the number of girls they have might be zero, one, two, or three, so there are four possible outcomes (again, any remaining children must be boys).

Now we put all of these outcomes together with the sum rule. We conclude that in total, there are 1 + (2 + (3 + 4)) = 10 different combinations of girls and boys that Mary and Peter might end up with. □

Notice that it was artificial to repeatedly break this example up into two cases at a time. Thus, Example 2.10 serves as a good demonstration for a generalisation of the sum rule as we stated it above. It would have been more natural to have broken the problem of Mary and Peter's kids up into four cases from the beginning, depending on whether they end up with zero, one, two, or three kids. The total number of combinations of girls and boys that Mary and Peter might end up with, is the sum of the combinations they can end up with in each of these cases; that is, 1 + 2 + 3 + 4 = 10.

THEOREM 2.11.Sum Rule for many cases *Suppose that when you are determining the total number of outcomes, you can identify* k *distinct cases with the property that every possible outcome lies in exactly one of the cases. If for each* i *between 1 and* k *there are* n_i *possible outcomes in the* i*th case, then the total number of possible outcomes will be* $\sum_{i=1}^{k} n_i$ *(that is, the sum as* i *goes from 1 to* k *of the* n_i*).*

There is one other important way to use the sum rule. This application is a bit more subtle. Suppose you know the total number of outcomes, and you want to know the number of outcomes that *don't* include a particular event. The sum rule tells us that the total number of outcomes is comprised of the outcomes that *do* include that event, together with the ones that don't. So if it's easy to figure out how many outcomes include the event that interests you, then you can subtract that from the total number of outcomes to determine how many outcomes *exclude* that event. Here's an example.

EXAMPLE 2.12. There are 216 different possible outcomes from rolling a white die, a red die, and a yellow die. (You can work this out using the product rule.) How many of these outcomes involve rolling a one on two or fewer of the dice?

SOLUTION. Tackling this problem directly, you might be inclined to split it into three cases: outcomes that involve rolling no ones, those that involve rolling exactly one one, and those that involve rolling exactly two ones. If you try this, the analysis will be long and fairly involved, and will include both the product rule and the sum rule. If you are careful, you will be able to find the correct answer this way.

We'll use a different approach, by first counting the outcomes that we *don't* want: those that involve getting a one on all three of the dice. There is only one way for this to happen: all three of the dice have to roll ones! So the number of outcomes that involve rolling ones on two or fewer of the dice, will be $216 - 1 = 215$.

EXERCISES 2.13. Use only the sum rule to answer the following questions:

1) I have four markers on my desk: one blue and three black. Every day on my way to class, I grab three of the markers without looking. There are four different markers that could be left behind, so there are four combinations of markers that I could take with me. What is the probability that I take the blue marker?

2) Maple is thinking of either a letter, or a digit. How many different things could she be thinking of?

3) How many of the 16 four-bit binary numbers have at most one 1 in them?

2C. Putting them together

When we combine the product rule and the sum rule, we can explore more challenging questions.

EXAMPLE 2.14. Grace is staying at a bed-and-breakfast. In the evening, she is offered a choice of menu items for breakfast in bed, to be delivered the next morning. There are three kinds of items: main dishes, side dishes, and beverages. She is allowed to choose up to one of each, but some of them come with optional extras. From the menu below, how many different breakfasts could she order?

Menu

Mains	Sides	Beverages
pancakes	fruit cup	coffee
oatmeal	toast	tea
omelette		orange juice

waffl
es

SOLUTION. We see that the number of choices Grace has available depends partly on whether or not she orders an item or items that include optional extras. We will therefore divide our consideration into four cases:

1)Grace does not order any pancakes, waffles, or toast. 2)Grace orders pancakes or waffles, but does not order toast.

3)Grace does not order pancakes or waffles, but does order toast. 4)Grace orders toast, and also orders either pancakes or waffles.

In the first case, Grace has three possible choices for her main dish (oatmeal, omelette, or nothing). For each of these, she has two choices for her side dish (fruit cup, or nothing). For each of these, she has four choices for her beverage (coffee, tea, orange juice, or nothing). Using the product rule, we conclude that Grace could order 3 2 4 = 24 different breakfasts that do not include pancakes, waffles, or toast.

In the second case, Grace has two possible choices for her main dish (pancakes, or waffles). For each of these, she has two choices for her side dish (fruit cup, or nothing). For each of these, she has four choices for her beverage. In addition, for each of her choices of pancakes oraffles, she can choose to have maple syrup, or not (two choices). Using the product rule, we conclude that Grace could order 2 2 4 2 = 32 different breakfasts that include pancakes or waffles, but not toast.

In the third case, Grace has three possible choices for her main dish (oatmeal, omelette, or nothing). For each of these, she has only one possible side dish (toast), but she has four choices for what to put on her toast (marmalade, lemon curd, blackberry jam, or nothing). For each of these choices, she has four choices of beverage. Using the product rule, we conclude that Grace could order 3 4 4 = 48 different breakfasts that include toast, but do not include pancakes or waffles.

In the final case, Grace has two possible choices for her main dish (pancakes, or waffles). She has two choices for what to put on her main dish (maple syrup, or only butter). She is having toast, but has four choices for what to put on her toast. Finally, she again has four choices of beverage. Using the product rule, we conclude that Grace could order 2 2 4 4 = 64 different breakfasts that include toast as well as either pancakes or waffles.

Using the sum rule, we see that the total number of different breakfasts Grace could order is 24 + 32 + 48 + 64 = 168. □

Here's another example of combining the two rules.

EXAMPLE 2.15. The types of license plates in Alberta that are available to individuals (not corporations or farms) for their cars or motorcycles, fall into one of the following categories:

- vanity plates;
- regular car plates;
- veteran plates; or
- motorcycle plates.

None of these license plates use the letters I or O.

Regular car plates have one of two formats: three letters followed by three digits; or three letters followed by four digits (in the latter case, none of the letters A, E, I, O, U, or Y is used). Veteran plates begin with the letter V, followed by two other letters and two digits. Motorcycle plates have two letters followed by three digits.

Setting aside vanity plates and ignoring the fact that some three-letter words are avoided, how many license plates are available to individuals in Alberta for their cars or motorcycles?

SOLUTION. To answer this question, there is a natural division into four cases: regular car plates with three digits; regular car plates with four digits; veteran plates; and motorcycle plates.

For a regular car plate with three digits, there are 24 choices for the first letter, followed by 24 choices for the second letter, and 24 choices for the third letter. There are 10 choices for the first digit, 10 choices for the second digit, and 10 choices for the third digit. Using the product rule, the total number of license plates in this category is $24^3\ 10^3 = 13, 824, 000$.

For a regular car plate with four digits, there are 20 choices for the first letter, followed by 20 choices for the second letter, and 20 choices for the third letter. There are 10 choices for the first digit, 10 choices for the second digit, 10 choices for the third digit, and 10 choices for the fourth digit. Using the product rule, the total number of license plates in this category is $20^3\ 10^4 = 80, 000, 000$.

For a veteran plate, there are 24 choices for the first letter, followed by 24 choices for the second letter. There are 10 choices for the first digit, and 10 choices for the second digit. Using the product rule, the total number of license plates in this category is $24^2\ 10^2 = 57, 600$.

Finally, for a motorcycle plate, there are 24 choices for the first letter, followed by 24 choices for the second letter. There are 10 choices for the first digit, 10 choices for the second digit, and 10 choices for the third digit. Using the product rule, the total number of license plates in this category is $24^2 \cdot 10^3 = 576,000$.

Using the sum rule, we see that the total number of license plates is

$$13, 824, 000 + 80, 000, 000 + 57, 600 + 576, 000$$

which is 94, 457, 600. □

It doesn't always happen that the sum rule is applied first to break the problem down into cases, followed by the product rule within each case. In some problems, these might occur in the other order. Sometimes there may seem to be one "obvious" way to look at the problem, but often there is more than one equally effective analysis, and different analyses might

begin with different rules.

In Example 2.14, we could have begun by noticing that no matter what else she may choose, Grace has four possible options for her beverage. Thus, the total number of possible breakfast orders will be four times the number of possible orders of main and side (with optional extras). Then we could have proceeded to analyse the number of possible choices for her main dish and her side dish (together with the extras). Breaking down the choices for her main and side dishes into the same cases as before, we could see that there are 3 2 = 6 choices in the first case; $2 \cdot 2 \cdot 2 = 8$ choices in the second case; 3 4 = 12 choices in the third case; and 2 2 4 = 16 choices in the fourth case. Thus she has a total of 6 + 8 + 12 + 16 = 42 choices for her main and side dishes. The product rule now tells us that she has 4 42 = 168 possible orders for her breakfast.

Let's run through one more (simpler) example of using both the sum and product rules, and work out the answer in two different ways.

EXAMPLE 2.16. Kathy plans to buy her Dad a shirt for his birthday. The store she goes to has three different colours of short-sleeved shirts, and six different colours of long-sleeved shirts. They will gift-wrap in her choice of two wrapping papers. Assuming that she wants the shirt gift-wrapped, how many different options does she have for her gift?

SOLUTION. Let's start by applying the product rule first. There are two aspects that she can vary: the shirt, and the wrapping. She has two choices for the wrapping, so her total number of options will be twice the number of shirt choices that she has. For the shirt, we break her choices down into two cases: if she opts for a short-sleeved shirt then she has three choices (of colour), while if she opts for a long-sleeved shirt then she has six choices. In total she has 3 + 6 = 9 choices for the shirt. Using the product rule, we see that she has 2 9 = 18 options for her gift.

Alternatively, we could apply the sum rule first. We will consider the two cases: that she buys a short-sleeved shirt; or a long-sleeved shirt. If she buys a short-sleeved shirt, then she has three options for the shirt, and for each of these she has two options for the wrapping, making (by the product rule) 3 2 = 6 options of short-sleeved shirts. If she buys a long-sleeved shirt, then she has six options for the shirt, and for each of these she has two options for the wrapping, making (by the product rule) 6 2 = 12 options of long-sleeved shirts. Using the sum rule, we see that she has 6 + 12 = 18 options for her gift.

EXERCISES 2.17. How many passwords can be created with the following constraints: 1)The password is three characters long and contains two lowercase letters and one digit,

in some order.

2) The password is eight or nine characters long and consists entirely of digits.

3) The password is five characters long and consists of lowercase letters and digits. All of the letters must come before all of the digits in the password, but there can be any number of letters (from zero through five).

4) The password is four characters long and consists of two characters that can be either digits or one of 16 special characters, and two lowercase letters. The two letters can be in any two of the four positions.

5) The password is eight characters long and must include at least one letter and at least one digit.

6) The password is eight characters long and cannot include any character more than once.

EXERCISES 2.18.

1) There are 8 buses a day from Toronto to Ottawa, 20 from Ottawa to Montreal, and 9 buses directly from Toronto to Montreal. Assuming that you do not have to complete the trip in one day (so the departure and arrival times of the buses is not an issue), how many different schedules could you use in travelling by bus from Toronto to Montreal?

2) How many 7-bit ternary strings (that is, strings whose only entries are 0, 1, or 2) begin with either 1 or 01?

2D. Summing up

Very likely you've used the sum rule or the product rule when counting simple things, without even stopping to think about what you were doing. The reason we're going through each of them very slowly and carefully, is because whsen we start looking at more complicated problems, our uses of the sum and product rules will become more subtle. If we don't have a very clear understanding in very simple situations of what we are doing and why, we'll be completely lost when we get to more difficult examples.

It's dangerous to try to come up with a simple guideline for when to use the product rule and when to use the sum rule, because such a guideline will often go wrong in complicated situations. Nonetheless, a good question to ask yourself when you are trying to decide which rule to use is, "Would I describe this with the word 'and,' or the word 'or' ?" The word "and" is

generally used in situations where it's appropriate to use the product rule, while "or" tends to go along with the sum rule.

Let's see how this applies to each of the examples we've looked at in this chapter.

In Example 2.1, you needed to choose the size *and* the variety for your coffee. In Example 2.3, Kyle wanted to choose a doughnut *and* coffee. In Example 2.4, Chloë needed to determine the size *and* the colour *and* the image *and* the slogan for each t-shirt. In Example 2.6, we wanted to know the sex of Peter and Mary's third *and* fourth children. So in each of these examples, we used the product rule.

In Example 2.8, you needed to choose a bagel *or* a doughnut. In Example 2.10, Mary and Peter could have zero *or* one *or* two *or* three children. So in each of these examples, we used the sum rule.

You definitely have to be careful in applying this guideline, as problems can be phrased in a misleading way. We could have said that in Example 2.8, we want to know how many different kinds of doughnuts *and* of bagels there are, altogether. The important point is that you aren't choosing both of these things, though; you are choosing just one thing, and it will be either a doughnut, *or* a bagel.

In Example 2.14, Grace was choosing a main dish *and* a side dish *and* a beverage, so we used the product rule to put these aspects together. Whether or not she had extra options available for her main dish depended on whether she chose pancakes *or* waffles *or* oatmeal *or* omelette *or* nothing, so the sum rule applied here. (Note that we didn't actually consider each of these four things separately, since they naturally fell into two categories. However, we would have reached the same answer if we had considered each of them separately.) Similarly, whether or not she had extra options available for her side dish depended on whether she chose toast *or* not, so again the sum rule applied.

In Example 2.15, the plates can be regular (in either of two ways) *or* veteran *or* motorcycle plates, so the sum rule was used. In each of these categories, we had to consider the options for the first character *and* the second character (and so on), so the product rule applied.

Finally, in Example 2.16, the shirt Kathy chooses can be short-sleeved *or* long-sleeved, so the sum rule applies to that distinction. Since she wants to choose a shirt *and* gift wrap, the product rule applies to that combination.

EXERCISES 2.19. For each of the following problems, do you need to use the sum rule, the product rule, or both?

1) Count all of the numbers that have exactly two digits, and the numbers that have exactly four digits.

2) How many possible outcomes are there from rolling a red die and a yellow die? 3)How many possible outcomes are there from rolling

three dice, if you only count the
outcomes that involve at most one of the dice coming up as a one?

Permutations, Combinations, and the Binomial Theorem

The examples we looked at in Chapter 2 involved drawing things from an effectively infinite population – they couldn't run out. When you are making up a password, there is no way you're going to "use up" the letter b by including it several times in your password. In Example 2.4, Chloë's suppliers weren't going to run out of blue t-shirts after printing some of her order, and be unable to complete the remaining blue t-shirts she'd requested. The fact that someone has already had one daughter doesn't mean they've used up their supply of X chromosomes so won't have another daughter.

In this chapter, we'll look at situations where we are choosing more than one item from a finite population in which every item is uniquely identified – for example, choosing people from a family, or cards from a deck.

3A. Permutations

We begin by looking at permutations, because these are a straightforward application of the product rule. The word "permutation" means a rearrangement, and this is exactly what a permutation is: an ordering of a number of distinct items in a line. Sometimes even though we have a large number of distinct items, we want to single out a smaller number and arrange those into a line; this is also a sort of permutation.

DEFINITION 3.1. A **permutation** of n distinct objects is an arrangement of those objects into an ordered line. If $1 \leq r \leq n$ (and r is a natural number) then an ***r*-permutation** of n objects is an arrangement of r of the n objects into an ordered line.

So a permutation involves choosing items from a finite population in which every item is uniquely identified, and keeping track of the order in which the items were chosen.

Since we are studying enumeration, it shouldn't surprise you that what we'll be asking in this situation is *how many* permutations there are, in a variety of circumstances. Let's begin with an example in which we'll calculate the number of 3-permutations of ten objects (or in this case, people).

EXAMPLE 3.2. Ten athletes are competing for Olympic medals in women's speed skating (1000 metres). In how many ways might the medals end up being awarded?

SOLUTION. There are three medals: gold, silver, and bronze, so this question amounts to finding the number of 3-permutations of the ten athletes (the first person in the 3-permutation is the one who gets the gold medal, the second gets the silver, and the third gets the bronze). To solve this question, we'll apply the product rule, where the aspects that can vary are the winners of the gold, silver, and bronze medals. We begin by considering how many different athletes might get the gold medal. The answer is that any of the ten athletes might get that medal. No matter which of the athletes gets the gold medal, once that is decided we move our consideration to the silver medal. Since one of the athletes has already been awarded the gold medal, only nine of them remain in contention for the silver medal, so for any choice of athlete who wins gold, the number of choices for who gets the silver medal is nine. Finally, with the gold and silver medalists out of contention for the bronze, there remain eight choices for who might win that medal. Thus, the total number of ways in which the medals might be awarded is $10 \cdot 9 \cdot 8 = 720$. □

We can use the same reasoning to determine a general formula for the number of r- permutations of n objects:

THEOREM 3.3. *The number of* r*-permutations of* n *objects is* $n(n-1)\ldots(n-r+1)$.

PROOF. There are n ways in which the first object can be chosen (any of the n objects). For each of these possible choices, there remain $n-1$ objects to choose for the second object, etc. □

It will be very handy to have a short form for the number of permutations of n objects.

NOTATION 3.4. We use n! to denote the number of permutations of n objects, so

$$n! = n(n-1)\ldots 1.$$

By convention, we define $0! = 1$.

DEFINITION 3.5. We read n! as "***n* factorial**," so n factorial is $n(n-1)\ldots 1$.

Thus, the number of r-permutations of n objects can be re-written as $n!/(n\ r)!$. When $n = r$
this gives $n!/0! = n!$, making sense of our definition that $0! = 1$.

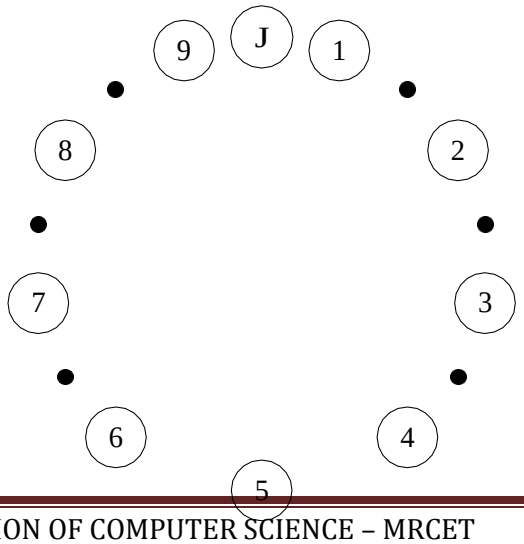
EXAMPLE 3.6. There are 36 people at a workshop. They are seated at six round tables of six people each for lunch. The Morris family (of three) has asked to be seated together (side-by- side). How many different seating arrangements are possible at the Morris family's table?

SOLUTION. First, there are 3! = 6 ways of arranging the order in which the three members of the Morris family sit at the table. Since the tables are round, it doesn't matter which specific seats they take, only the order in which they sit matters. Once the Morris family is seated, the three remaining chairs are uniquely determined by their positions relative to the Morris family (one to their right, one to their left, and one across from them). There are 33 other people at the conference; we need to choose three of these people and place them in order into the three vacant chairs. There are 33!/(33 3)! = 33!/30! ways of doing this. In total, there are 6(33!/30!) = 196, 416 different seating arrangements possible at the Morris family's table.

By adjusting the details of the preceding example, it can require some quite different thought processes to find the answer.

EXAMPLE 3.7. At the same workshop, there are three round dinner tables, seating twelve people each. The Morris family members (Joy, Dave, and Harmony) still want to sit at the same table, but they have decided to spread out (so no two of them should be side-by-side) to meet more people. How many different seating arrangements are possible at the Morris family's table now?

SOLUTION. Let's begin by arbitrarily placing Joy somewhere at the table, and seating everyone else relative to her. This effectively distinguishes the other eleven seats. Next, we'll consider the nine people who aren't in Joy's family, and place them (standing) in an order clockwise around the table



from her. There are 33!/(33 9)! ways to do this. Before we actually assign seats to these nine people, we decide where to slot in Dave and Harmony amongst them.

(In the above diagram, the digits 1 through 9 represent the nine other people who are sitting at the Morris family's table, and the J represents Joy's position.) Dave can sit between any pair of non-Morrises who are standing beside each other; that is, in any of the spots marked by small black dots in the diagram above. Thus, there are eight possible choices for where Dave will sit. Now Harmony can go into any of the remaining seven spots marked by black dots. Once Dave and Harmony are in place, everyone shifts to even out the circle (so the remaining black dots disappear), and takes their seats in the order determined.

We have shown that there are 33!/24! 8 7 possible seating arrangements at the Morris table. That's a really big number, and it's quite acceptable to leave it in this format. However, in case you find another way to work out the problem and want to check your answer, the total number is $783,732,837,888,000$.

EXERCISES 3.8. Use what you have learned about permutations to work out the following problems. The sum and/or product rule may also be required.

1) Six people, all of whom can play both bass and guitar, are auditioning for a band. There are two spots available: lead guitar, and bass player. In how many ways can the band be completed?
2) Your friend Garth tries out for a play. After the auditions, he texts you that he got one of the parts he wanted, and that (including him) nine people tried out for the five roles. You know that there were two parts that interested him. In how many ways might the cast be completed (who gets which role matters)?
3) You are creating an 8-character password. You are allowed to use any of the 26 lower- case characters, and you must use exactly one digit (from 0 through 9) somewhere in

   the password. You are not allowed to use any character more than once. How many different passwords can you create?

4) How many 3-letter "words" (strings of characters, they don't actually have to be words) can you form from the letters of the word STRONG? How many of those words contain an s? (You may not use a letter more than once.)

5) How many permutations of 0, 1, 2, 3, 4, 5, 6 have no adjacent even digits? For example, a permutation like 5034216 is not allowed because 4 and 2 are adjacent.

3B. Combinations

Sometimes the order in which individuals are chosen doesn't matter; all that matters is whether or not they were chosen. An example of this is choosing a set of problems for an exam. Although the order in which the questions are arranged may make the exam more or less intimidating, what really matters is which questions are on the exam, and which are not. Another example would be choosing shirts to pack for a trip (assuming all of your shirts are distinguishable from each other). We call a choice like this a "combination," to indicate that it is the collection of things chosen that matters, and not the order.

DEFINITION 3.9. Let n be a positive natural number, and $0 \leq r \leq n$. Assume that we have
n distinct objects. An ***r*-combination** of the n objects is a subset consisting of r of the objects.

So a combination involves choosing items from a finite population in which every item is uniquely identified, but the order in which the choices are made is unimportant.

Again, you should not be surprised to learn (since we are studying enumeration) that what we'll be asking is *how many* combinations there are, in a variety of circumstances. One signifi- cant difference from permutations is that it's not interesting to ask how many n-combinations there are of n objects; there is only one, as we must choose all of the objects.

Let's begin with an example in which we'll calculate the number of 3-combinations of ten objects (or in this case, people).

EXAMPLE 3.10. Of the ten athletes competing for Olympic medals in women's speed skating (1000 metres), three are to be chosen to form a committee to review the rules for future competitions. How many different committees could be formed?

SOLUTION. We determined in Example 3.2 that there are 10!/7! ways in which the medals can be assigned. One easy way to choose the committee would be to make it consist of the three medal-winners. However, notice

that if (for example) Wong wins gold, Šajna wins silver, and Andersen wins bronze, we will end up with the same committee as if Šajna wins gold, Andersen wins silver, and Wong wins bronze. In fact, what we've learned about permutations tells us that there are 3! different medal outcomes that would each result in the committee being formed of Wong, Šajna, and Andersen.

In fact, there's nothing special about Wong, Šajna, and Andersen – for any choice of three people to be on the committee, there are 3! = 6 ways in which those individuals could have been awarded the medals. Therefore, when we counted the number of ways in which the medals could be assigned, we counted each possible 3-member committee exactly 3! = 6 times. So the number of different committees is 10!/(7!3!) = 10 · 9 · 8/6 = 120.

We can use the same reasoning to determine a general formula for the number of r- combinations of n objects:

THEOREM 3.11. *The number of* r*-combinations of* n *objects is*

$$\frac{n!}{r!(n-r)!}.$$

PROOF. By Theorem 3.3, there are n!/(n r)! r-permutations of n objects. Suppose that we knew there are k unordered r-subsets of n objects (i.e. r-combinations). For each of these k unordered subsets, there are r! ways in which we could order the elements. This tells us that k · r! = n!/(n − r)!. Rearranging the equation, we obtain k = n!/(r!(n − r)!).

It will also prove extremely useful to have a short form for the number of r-combinations of n objects.

NOTATION 3.12. We use $\binom{n}{r}$ to denote the number of r-combinations of n objects, so

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

DEFINITION 3.13. We read $\binom{n}{r}$ as "***n* choose *r***," so n choose r is n!/[r!(n − r)!]. Notice that when r = n, we have

$$\binom{n}{r} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!0!} = \frac{n!}{n!} = 1,$$

coinciding with our earlier observation that there is only one way in which all of the n objects can be chosen. Similarly,

$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = 1;$$

there is exactly one way of choosing none of the n objects.

Let's go over another example that involves combinations.

EXAMPLE 3.14. Jasmine is holding three cards from a regular deck of

playing cards. She tells you that they are all hearts, and that she is holding at least one of the two highest cards in the suit (Ace and King). If you wanted to list all of the possible sets of cards she might be holding, how long would your list be?

SOLUTION. We'll consider three cases: that Jasmine is holding the Ace (but not the King); that she is holding the King (but not the Ace), or that she is holding both the Ace and the King.

If Jasmine is holding the Ace but not the King, of the eleven other cards in the suit of hearts she must be holding two. There are $\binom{11}{2}$ possible choices for the cards she is holding in this case.

Similarly, if Jasmine is holding the King but not the Ace, of the eleven other cards in the suit of hearts she must be holding two. Again, there are $\binom{11}{2}$ possible choices for the cards she is holding in this case.

Finally, if Jasmine is holding the Ace and the King, then she is holding one of the other eleven cards in the suit of hearts. There are $\binom{11}{1}$ possible choices for the cards she is holding in this case.

In total, you would have to list

$$\binom{11}{2} + \binom{11}{2} + \binom{11}{1} = \frac{11!}{2!9!} + \frac{11!}{2!9!} + \frac{11!}{1!10!} = \frac{11 \cdot 10}{2} + \frac{11 \cdot 10}{2} + 11 = 55 + 55 + 11 = 121$$

possible sets of cards.

Here is another analysis that also works: Jasmine has at least one of the Ace and the King, so let's divide the problem into two cases: she might be holding the Ace, or she might be holding the King but not the Ace. If she is holding two; these can be chosen in $\binom{12}{2} = 66$ ways. If she is holding the King but not the Ace, then of the twelve other hearts, she is holding the Ace, then as before, her other two cards can be chosen in $\binom{11}{2} = 55$ ways, for a total (again) of 121. □

A common mistake in an example like this, is to divide the problem into the cases that Jasmine is holding the Ace, or that she is holding the King, and to determine that each of these $\binom{12}{2}$ cases includes $\binom{11}{1} = 66$ possible combinations of cards, for a total of 132. The problem with this analysis is that we've counted the combinations that include both the Ace and the King twice: once as a combination that includes the Ace, and once as a combination that includes the King. If you do this, you need to compensate by subtracting at the end the number of combinations that have been counted twice: that is, those that include the Ace and the King. As we worked out in the example, there are $\binom{11}{1} = 11$ of these, making a total of $132 - 11 = 121$ combinations.

EXERCISES 3.15. Use what you have learned about combinations to work out the following problems. Permutations and other counting rules we've covered may also be required.

1) For a magic trick, you ask a friend to draw three cards from a standard deck of 52 cards. How many possible sets of cards might she have chosen?
2) For the same trick, you insist that your friend keep replacing her first draw until she draws a card that isn't a spade. She can choose any cards for her other two cards. How many possible sets of cards might she end up with? (Caution: choosing 5♦, 6♣, 3♠ in that order, is *not* different from choosing 6♣, 5♦, 3♠ in that order. You do *not* need to take into account that some sets will be more likely to occur than others.)
3) How many 5-digit numbers contain exactly two zeroes? (We insist that the number contain exactly 5 digits.)
4) Sandeep, Hee, Sara, and Mohammad play euchre with a standard deck consisting of 24 cards (A, K, Q, J, 10, and 9 from each of the four suits of a regular deck of playing cards). In how many ways can the deck be dealt so that each player receives 5 cards, with 4 cards left in the middle, one of which is turned face-up? The order of the 3 cards that are left face-down in the middle does not matter, but who receives a particular set of 5 cards (for example, Sara or Sandeep) does matter.
5) An ice cream shop has 10 flavours of ice cream and 7 toppings. Their *megasundae* consists of your choice of any 3 flavours of ice cream and any 4 toppings. (A customer must choose *exactly* three different flavours of ice cream and four different toppings.) How many

different megasundaes are there?

3C. The Binomial

Theorem Here is an algebraic example in which "n choose r" arises naturally. **EXAMPLE 3.16.** Consider

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

If you try to multiply this out, you must systematically choose the a or the b from each of the four factors, and make sure that you make every possible combination of choices sooner or later.

One way of breaking this task down into smaller pieces, is to separate it into five parts, depending on how many of the factors you choose as from (4, 3, 2, 1, or 0). Each time you choose 4 of the as, you will obtain a single contribution to the coefficient of the term a^4; each time you choose 3 of the as, you will obtain a single contribution to the term a^3b; each time you choose 2 of the as, you will obtain a single contribution to the term a^2b^2; each time you choose 1 of the as, you will obtain a single contribution to the term ab^3; and each time you choose 0 of the as, you will obtain a single contribution to the term b^4. In other words, the coefficient of a particular term a^ib^{4-i} will be the number of ways in which you can choose i of the factors from which to take an a, taking a b from the other 4 − i factors (where $0 \le i \le 4$).

$\binom{4}{4} = 1$ way

$\binom{4}{0}$

choose four factors from which to take as. (Clearly, you must choose an a from every one of the four factors.) Thus, the coefficient of a^4 will be 1.

If you want to take as from three of the four factors, Theorem 3.11 tells us that there are $\binom{4}{3} = 4$ ways in which to choose the factors from which you take the as. (Specifically, these four ways consist of taking the b from any one of the four factors, and the as from the other three factors). Thus, the coefficient of a^3b will be 4.

If you want to take as from two of the four factors, and bs from the other two, Theorem 3.11 tells us that there are $\binom{4}{2} = 6$ ways in which to choose the factors from which you take the as (then take bs from the other two factors). This is a small enough example that you could easily work out all six ways by hand if you wish. Thus, the coefficient of a^2b^2 will be 6.

If you want to take as from one of the four factors, Theorem 3.11 tells us that there are $\binom{4}{1} = 4$ ways in which to choose the factors from which you take the as. (Specifically, these four ways consist of taking the a from any one of the four factors, and the bs from the other three factors). Thus, the coefficient of ab^3 will be 4.

Finally, by Theorem 3.11, there is $\binom{4}{0} = 1$ way to choose zero factors from

which to take as. (Clearly, you must choose a b from every one of the four factors.) Thus, the coefficient of b^4 will be 1.

Putting all of this together, we see that

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

In fact, if we leave the coefficients in the original form in which we worked them out, we see that

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

This example generalises into a significant theorem of mathematics:

THEOREM 3.17.Binomial Theorem *For any* a *and* b, *and any natural number* n, *we have*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

One special case of this is that

$$(1 + x)^n = \sum_{r=0}^{n} \binom{n}{r} x^r.$$

PROOF. As in Example 3.16, we see that the coefficient of $a^r b^{n-r}$ in $(a+b)^n$ will be the number of ways of choosing r of the n factors from which we'll take the a (taking the b from the other n − r factors). By Theorem 3.11, there are $\binom{n}{r}$ ways of making this choice.

For the special case, begin by observing that $\binom{n}{r} = \binom{n}{n-r}$; then take a = x and b = 1 in the general formula. Use the fact that $1^{n-r} = 1$ for any integers n and r. □

Thus, the values $\binom{n}{r}$ are the coefficients of the terms in the Binomial Theorem.

DEFINITION 3.18. Expressions of the form $\binom{n}{r}$ are referred to as **binomial coefficients**.

There are some nice, simple consequences of the binomial theorem.

COROLLARY 3.19. *For any natural number* n*, we have*

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n.$$

PROOF. This is an immediate consequence of substituting a = b = 1 into the Binomial Theo- rem. □

COROLLARY 3.20. *For any natural number* n*, we have*

$$\sum_{r=0}^{n} \binom{n}{r} (-1)^{r-1} = 0.$$

PROOF. From the special case of the Binomial Theorem, we have

$$(1 + x)^n = \sum_{r=0}^{n} \binom{n}{r} x^r.$$

If we differentiate both sides, we obtain

$$n(1 + x)^{n-1} = \sum_{r=0}^{n} \binom{n}{r} x^{r-1}.$$

Substituting x = −1 gives the result (the left-hand side is zero). □

EXERCISES 3.21. Use the Binomial Theorem to evaluate the following:

1) $\sum_{i=1}^{n} \binom{n}{i} 2^i$.

i

2)the coefficient of $a^2b^3c^2d^4$ in $(a + b)^5(c + d)^6$. 3)the coefficient of $a^2b^6c^3$ in $(a + b)^5(b + c)^6$.

4)the coefficient of a^3b^2 in $(a + b)^5 + (a + b^2)^4$.

Countingwith Repetitions

In counting combinations and permutations, we assumed that we were drawing from a set in which all of the elements are distinct. Of course, it is easy to come up with a scenario in which some of the elements are indistinguishable. We need to know how to count the solutions to problems like this, also.

5A. Unlimited repetition

For many practical purposes, even if the number of indistinguishable elements in each class is not actually infinite, we will be drawing a small enough number that we will not run out. The bagel shop we visited in Example 2.8 is not likely to run out of one variety of bagel before filling a particular order. In standard card games, we never deal enough cards to a single player that they might have all of the cards of one suit and still be getting more cards.

This is the sort of scenario we'll be studying in this section. The set-up we'll use is to assume that there are n different "types" of item, and there are enough items of each type that we won't run out. Then we'll choose items, allowing ourselves to repeatedly choose items of the same type as many times as we wish, until the total number of items we've chosen is r. Notice that (unlike in Chapter 3), in this scenario r may exceed n.

We'll consider two scenarios: the order in which we make the choice matters, or the order in which we make the choice doesn't matter.

EXAMPLE 5.1. Chris has promised to bring back bagels for three friends he's studying with (as well as one for himself). The bagel shop sells eight varieties of bagel. In how many ways can he choose the bagels to give to Jan, Tom, Olive, and himself?

SOLUTION. Here, it matters who gets which bagel. We can model this by assuming that the first bagel Chris orders will be for himself, the second for Jan, the third for Tom, and the last for Olive. Thus, the order in which he asks for the bagels matters.

We actually saw back in Chapter 2 how to solve this problem. It's just an application of the product rule! Chris has eight choices for the first bagel;

for each of these, he has eight choices for the second bagel; for each of these, he has eight choices for the third bagel; and for each of these, he has eight choices for the fourth bagel. So in total, he has 8^4 ways to choose the bagels.

OK, so if the order in which we make the choice matters, we just use the multiplication rule. What about if order doesn't matter?

EXAMPLE 5.2. When Chris brought back the bagels, it turned out that he'd done a poor job of figuring out what his friends wanted. They all traded around. Later that night, they sent him to the doughnut store, but this time they told him to just bring back eight doughnuts and they'd figure out who should get which. If the doughnut store has five varieties, how many ways are there for Chris to fill this order?

SOLUTION. Let's call the five varieties chocolate, maple, boston cream, powdered, and jam- filled. One way to describe Chris' order would be to make a list in which we first write one **c** for each chocolate doughnut, then one **m** for each maple doughnut, then one **b** for each boston cream doughnut, then one **p** for each powdered doughnut, and finally one **j** for each jam-filled doughnut. Since Chris is ordering eight doughnuts, there will be eight letters in this list. Notice that there's more information provided by this list than we actually need. We know that all of the first group of letters are **c**s, so instead of writing them all out, we could simply put a dividing marker after all of the **c**s and before the first **m**. Similarly, we can put three more dividing markers in to separate the **m**s from the **b**s, the **b**s from the **p**s, and the **p**s from the **j**s. Now we have a list that might look something like this:

cc||bbb|ppp|

(Notice in this possible list, Chris chose no maple or jam-filled doughnuts.)

Now, we don't actually need to write down the letters **c**, **m**, **b** and so on, as long as we know how many spaces they take up; we know that any letters that appear before the first dividing marker are **c**s, for example. Thus, the following list gives us the same information as the list above:

___||_____|_____|

Similarly, if we see the list

|___|___|_____|_

we understand that Chris ordered no chocolate doughnuts; two maple doughnuts; two boston cream doughnuts; three powdered doughnuts; and one jam-filled doughnut.

So an equivalent problem is to count the number of ways of arranging eight underlines and four dividing markers in a line. This is something we already understand! We have twelve positions that we need to fill, and the problem is to know how many ways can we fill eight of the twelve positions with underlines (placing dividing markers in the other four positions). We

Solution: There are $\binom{12}{8}$ ways. □

This technique can be used to give us a general formula for counting the

number of ways of choosing r objects from n types of objects, where we are allowed to repeatedly choose objects of the same type.

THEOREM 5.3. *The number of ways of choosing* r *objects from* n *types of objects (with re- placement or repetition allowed) is*

$$\left(\begin{matrix} n+r-1 \\ r \end{matrix}\right).$$

PROOF. We use the same idea as in the solution to Example 5.2, above. Since there are n different types of objects, we will need $n-1$ dividing markers to keep them apart. Since are choosing r objects, we will need r underlines, for a total of $n+r-1$ positions to be filled.

We can choose the r positions in which the objects will go in $n+r-1$ ways, and then (in each case) put dividing markers into the remaining $n-1$ positions. Thus, $\binom{n+r-1}{r}$ ways there are to choose r objects from n types of objects, if repetition or replacement of choices is

Again, we will want to have a short form for this value.

NOTATION 5.4. We use $\binom{n}{r}$ to denote the number of ways of choosing r objects from n types of objects (with replacement or repetition allowed), so

$$\binom{n}{r} = \binom{n+r-1}{r}.$$

The reason we say "replacement or repetition" is because there is another natural model for this type of problem. Suppose that instead of choosing eight bagels from five varieties, Chris is asked to put his hand into a bag that contains five different-coloured pebbles, and draw one out; then replace it, repeatedly (with eight draws in total). If he keeps count of how many times he draws each of the rocks, the number of possible tallies he'll end up with is exactly the same as the number of doughnut orders in Example 5.2.

The following table summarises some of the key things we've learned about counting so far:

Table 5.1. The number of ways to choose *r* objects from *n* objects (or types of objects)

	repetition allowed	**repetition not allowed**
order matters	n^r	$\frac{n!}{(n-r)!}$
order doesn't matter	$\binom{n}{r}$	$\binom{n}{r}$

EXERCISES 5.5. Evaluate the following problems.

1) Each of the ten sections in your community band (trombones, flutes, and so on) includes at least four people. The conductor needs a quartet to play at a school event. How many different sets of instruments might end up playing at the event?

2) The prize bucket at a local fair contains six types of prizes. Kim wins 4 prizes; Jordan wins three prizes, and Finn wins six. Each of the kids plans to give one of the prizes he has won to his teacher, and keep the rest. In how many ways can their prizes (including the gifts to the teacher) be chosen? (It is important which gift comes from which child.)

3) There are three age categories in the local science fair: junior, intermediate, and senior. The judges can choose nine projects in total to advance to the next level of competition, and they must choose at least one project from each age group. In how many ways can the projects that advance be distributed across the age groups?

EXERCISES 5.6. Prove the following combinatorial identities:

1) For $k, n \geq 1$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n}{k-1}$.

2) For $k, n \geq 1$, $\binom{n}{k} = \binom{n+k-1}{k}$.

3) For $k, n \geq 1$, $\binom{k+1}{k} = \binom{n+k-1}{k}$.

4) For $1 \leq k \leq n$, $\binom{n-1}{k-n} = \binom{n}{k-1}$

EXERCISES 5.7. Solve the following problems.

1) Find the number of 5-lists of the form (x_1, x_2, x_3, x_4, x_5), where each x_i is a nonnegative integer and $x_1 + x_2 + x_3 + x_4 + 3x_5 = 12$.
2) We will buy 3 pies (not necessarily all different) from a store that sells 4 kinds of pie. How many different orders are possible? List all of the possibilities (using A for apple, B for blueberry, C for cherry, and D for the other one).
3) Suppose Lacrosse balls come in 3 colours: red, yellow, and blue. How many different combinations of colours are possible in a 6-pack of Lacrosse balls?
4) After expanding $(a + b + c + d)^7$ and combining like terms, how many terms are there? [Justify your answer without performing the expansion.]

5B. Sorting a set that contains repetition

In the previous section, the new work came from looking at combinations where repetition or replacement is allowed. For our purposes, we assumed that the repetition or replacement was effectively unlimited; that is, the store might only have 30 cinnamon raisin bagels, but since Chris was only ordering four bagels, that limit didn't matter.

In this section, we're going to consider the situation where there are a fixed number of objects in total; some of them are "repeated" (that is, indistinguishable from one another), and we want to determine how many ways they can be arranged (permuted). This can arise in a variety of situations.

EXAMPLE 5.8. When Chris gets back from the doughnut store run, he discovers that Mo- hammed, Jing, Karl, and Sara have joined the study session. He has bought two chocolate doughnuts, three maple doughnuts, and three boston cream doughnuts. In how many ways can the doughnuts be distributed so that everyone gets one doughnut?

SOLUTION. Initially, this looks a lot like a permutation question: we need to figure out the number of ways to arrange the doughnuts in some order, and give the first doughnut to the first student, the second doughnut to the second student, and so on.

The key new piece in this problem is that, unlike the permutations we've studied thus far, the two chocolate doughnuts are indistinguishable (as are the three maple doughnuts and the three boston cream doughnuts). This

means that there is no difference between giving the first chocolate doughnut to Tom and the second to Mohammed, and giving the first chocolate doughnut to Mohammed and the second to Tom.

One way to solve this problem is to look at it as a series of combinations of the people, rather than as a permutation question about the doughnuts. Instead of arranging the doughnuts, we can first choose which two of the eight people will receive the two chocolate doughnuts. Once that is done, from the remaining six people, we choose which three will receive maple doughnuts. Finally, the remaining three people receive boston cream doughnuts. Thus, the solution is $\binom{8}{2}\binom{6}{3}$.

Another approach is more like the approach we used to figure out how many r-combinations there are of n objects. In this approach, we begin by noting that we would be able to arrange the eight doughnuts in 8! orders if all of them were distinct. For any fixed choice of two people who receive the chocolate doughnuts, there are 2! ways in which those two chocolate doughnuts could have been distributed to them, so in the 8! orderings of the doughnuts, each of these choices for who gets the chocolate doughnuts has been counted 2! times rather than once. Similarly, for any fixed choice of three people who receive the maple doughnuts, there are 3! ways in which these three maple doughnuts could have been distributed to them, and each of these choices has been counted 3! times rather than once. The same holds true for the three boston cream doughnuts. Thus, the solution is 8!/(2!3!3!).

Since

$$\binom{8}{2}\binom{6}{3} = \frac{8!}{2!6!}\cdot\frac{6!}{3!3!} = \frac{8!}{2!3!3!},$$

we see that these solutions are in fact identical although they look different. □

This technique can be used to give us a general formula for counting the number of ways of arranging n objects some of which are indistinguishable from each other.

THEOREM 5.9. *Suppose that:*

- *there are* n *objects;*
- *for each* i *with* $1 \le i \le m$, r_i *of them are of type* i *(indistinguishable from each other); and*
- $r_1 + \ldots + r_m = n$.

Then the number of arrangements (permutations) of these n *objects is*

$$\frac{n!}{r_1!r_2!\ldots r_m!}.$$

PROOF. We use the same idea as in the solution to Example 5.8, above. Either approach will work, but we'll use the first. There will be n positions in the final ordering of the objects. We begin by choosing r_1 of these to hold the objects of type 1. Then we choose r_2 of them to hold the objects of type 2, and so on. Ultimately, we choose the final r_m locations (in $\sum_{r_m=1}^{r_m}$ possible way) to hold the objects of type m.

Using the product rule, the total number of arrangements is

$$\begin{aligned}
&\binom{n}{r_1}\binom{n-r_1}{r_2}\cdots\binom{n-r_1-\ldots-r_{m-1}}{r_m} \\
&= \frac{n!}{r_1!(n-r_1)!}\cdot\frac{(n-r_1)!}{r_2!(n-r_1-r_2)!}\cdot\ldots\cdot\frac{(n-r_1-\ldots-r_{m-1})!}{r_m!0!} \\
&= \frac{n!}{r_1!r_2!\ldots r_m!},
\end{aligned}$$

UNIT-4
RECURRENCE RELATIONS

Second Order Recurrence Relations

In the previous section we saw how to solve first order linear recurrence relations. This is when a_n is given by a linear formula of a_{n-1}, i.e.

$$a_n = p_n a_{n-1} + s_n$$

where p_n and s_n are given sequences. In this section and the next we look at *second order linear* recurrence relations when a_n is given by a linear formula of a_{n-1} and a_{n-2}, i.e

$$a_n = p_n a_{n-1} + q_n a_{n-2} + s_n$$

where p_n, q_n and s_n are given sequences. For simplicity we concentrate on the *constant coefficient* case when p_n and q_n don't vary with n, i.e.

(1) $$a_n = p a_{n-1} + q a_{n-2} + s_n$$

where p and q are just numbers. In this section we look at the situation where the recurrence relation is *homogeneous* which is when $r_n = 0$ for all n, i.e.

(2) $$a_n = p a_{n-1} + q a_{n-2}$$

In the next section we look at the *inhomogeneous* case (1).

We illustrate the method of solution of equations of the form (2) with the following example.

Example 1. Consider the equation

(3) $$a_n = a_{n-1} + 2a_{n-2}$$

along with the initial conditions

(4) $$a_0 = 2 \quad \text{and} \quad a_1 = 3$$

(3) is the special case of (2) when $p = 1$ and $q = 2$.

To solve equations of the form (2) we start by looking for solutions which have the special form

(5) $a_n = r^n$

where r is a number to be determined. To determine r we substitute into (2). We illustrate this with (3). If a_n is given by (3) then

(6) $a_{n-1} = r^{n-1}$

and

(7) $a_{n-2} = r^{n-2}$

Substituting (5), (6) and (7) into (3) gives

$$r^n = r^{n-1} + 2r^{n-2}$$

Divide this by r^{n-2} giving

$$r^2 = r + 2$$

or

$$r^2 - r - 2 = 0$$

This is called the *characteristic equation*. It is a quadratic equation. The roots are the values of r in the solutions $a_n = r^n$. To solve we either factor or use the quadratic formula. In this case we can factor.

$$(r - 2)(r + 1) = 0$$

This equation has two solutions

$$r_1 = 2 \quad \text{and} \quad r_2 = -1$$

Recall the r is a number such that (5) is a solution to (3). This gives the following two solutions to (3)

$$a_n = 2^n \quad \text{and} \quad a_n = (-1)^n$$

Neither of these solutions satisfy the initial conditions (4). In order to get a solution which satisfies (4) we need to take a *superposition* of these two solutions, i.e. multiply them by constants and add. We can do this because of the following

Superposition Principle. If a_n and b_n are two solutions of the equation (2)

then so are

$$a_n + b_n$$

$$Aa_n$$

$$Aa_n + Bb_n$$

for any constants A and B.

Proof. By hypothesis we have

(8) $$a_n = pa_{n-1} + qa_{n-2}$$

and

(9) $$b_n = pb_{n-1} + qb_{n-2}$$

If we add the equations (8) and (9) we get

$$(a_n + b_n) = p(a_{n-1} + b_{n-1}) + q(a_{n-2} + b_{n-2})$$

which shows that $a_n + b_n$ is a solution. If we multiply equation (8) by A we get

$$(Aa_n) = p(Aa_{n-1}) + q(Aa_{n-2})$$

which shows that Aa_n is a solution. If we multiply equation (8) by A and equation (9) by B and add we get

$$(Aa_n + Bb_n) = p(Aa_{n-1} + Bb_{n-1}) + q(Aa_{n-2} + Bb_{n-2})$$

which shows that $Aa_n + Bb_n$ is a solution. //

It follows from the superposition principle that $a_n = A\,2^n + B\,(-1)^n$ is a solution to (3) for any constants A and B. Now we choose the constants A and B to satisfy the initial conditions (4). Plugging in $n = 0$ we get

$$2 = a_0 = A\,2^0 + B\,(-1)^0 = A + B$$

Plugging in $n = 1$ we get

$$3 = a_1 = A\,2^1 + B\,(-1)^1 = 2A - B$$

This is a system of two equations and two unknowns. We multiply them by

numbers to get the coefficient of one of the unknowns the same and then add or subtract. In this case we can just add the equations

$$\begin{array}{rcl} A + B &=& 2 \\ \underline{2A - B} &=& \underline{3} \\ 3A &=& 5 \end{array} \quad \Rightarrow \quad A = \frac{5}{3} \quad \Rightarrow \quad B = 2 - A = 2 - \frac{5}{3} = \frac{1}{3}$$

So $a_n = \frac{5}{3}2^n + \frac{1}{3}(-1)^n$. If we were interested in the behavior for large n then $a_n = O(2^n)$.

If the roots of the characteristic equation are equal then $a_n = nr^n$ is also a solution where r is a root of the characteristic equation. Then the general solution is $a_n = Ar^n + Bnr^n$.

Example 2. Consider the equation

(10) $\quad a_n = 4a_{n-1} - 4a_{n-2}$

along with the initial conditions

(11) $\quad a_0 = 2 \quad$ and $\quad a_1 = 5$

Try $a_n = r^n$. Substituting into (10) gives

$$r^n = 4r^{n-1} - 4r^{n-2} \Rightarrow r^2 = 4r - 4 \Rightarrow r^2 - 4r + 4 = 0 \Rightarrow (r-2)^2 = 0$$

$\Rightarrow$

$$r_1 = r_2 = 2$$

So $a_n = 2^n$ is a solution. As indicated, when the roots of the characteristic equation are equal, then $a_n = nr^n$ is a solution. So in this case $a_n = n2^n$ is a solution. We can check this by plugging into (10). When we do this we get

$$n2^n \stackrel{?}{=} 4(n-1)2^{n-1} - 4(n-2)2^{n-2}$$

Dividing by 2^{n-2} gives

$$4n \stackrel{?}{=} 8(n-1) - 4(n-2) \Rightarrow 4n \stackrel{?}{=} 8n - 8 - 4n + 8$$

which is true.

We get the general solution by taking a superposition of $a_n = 2^n$ and $a_n = n2^n$. So $a_n = A\,2^n + Bn2^n$ is a solution to (10) for any constants A and B. Now we choose the constants A and B to satisfy the initial conditions (4). Plugging in $n = 0$ we get

$$2 \;=\; a_0 \;=\; A\,2^0 \;+\; B\,(0)\,2^0 \;=\; A$$

Plugging in $n = 1$ we get

$$5 \;=\; a_1 \;=\; A\,2^1 \;+\; B\,(1)\,2^1 \;=\; 2A \;+\; 2B \;=\; (2)(2) \;+\; 2B.$$

So $B = \frac{1}{2}$ and $a_n \;=\; 2\,2^n + \frac{1}{2}\,n2^n = (n + 4)2^{n-1}$. If we were interested in the behavior for large n then $a_n = O(n2^n)$.

Example 3 (Fibonacci sequence). Recall the Fibonacci sequence f_n is defined by the recurrence relation

(12) $$f_n \;=\; f_{n-1} \;+\; f_{n-2}$$

along with the initial conditions

(13) $$f_0 \;=\; 1 \qquad \text{and} \qquad f_1 \;=\; 1$$

To solve we look for solutions of the form $a_n = r^n$ where r determined by substituting int (12). Doing this gives

$$r^n \;=\; r^{n-1} \;+\; r^{n-2}$$

Divide this by r^{n-2} giving

$$r^2 \;=\; r \;+\; 1$$

or

$$r^2 \;-\; r \;-\; 1 \;=\; 0$$

This doesn't look easy to factor so we use the quadratic formula.

$$r \;=\; \frac{1 \pm \sqrt{1 + 4}}{2} \;=\; \frac{1 \pm \sqrt{5}}{2}$$

This equation has two solutions

$$r_1 = \frac{1+\sqrt{5}}{2} \approx \frac{1+2.24}{2} = 1.62$$

$$r_2 = \frac{1-\sqrt{5}}{2} \approx \frac{1-2.24}{2} = -0.62$$

This gives the following two solutions to (3)

$$f_n = \left(\frac{1+\sqrt{5}}{2}\right)^n \approx 1.62^n \quad \text{and} \quad f_n = \left(\frac{1-\sqrt{5}}{2}\right)^n \approx (-0.62)^n$$

By the superposition principle the general solution is

$$f_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$$

is a solution to (3) for any constants A and B. Now we choose the constants A and B to satisfy the initial conditions (13). Plugging in $n = 0$ we get

$$1 = f_0 = A + B$$

So $B = 1 - A$. Plugging in $n = 1$ we get

$$1 = f_1 = A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right)$$

Using $B = 1 - A$ gives

$$1 = \sqrt{5}\,A + \frac{1-\sqrt{5}}{2}$$

or

$$A = \frac{1+\sqrt{5}}{2\sqrt{5}} = \frac{5+\sqrt{5}}{10} \approx \frac{5+2.24}{10} = 0.724$$

$$B = 1 - A = 1 - \frac{5+\sqrt{5}}{10} = \frac{5-\sqrt{5}}{10} \approx \frac{5-2.24}{10} = 0.276$$

So

$$f_n = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n \approx 0.724\,(1.62)^n + 0.276\,(-0.62)^n$$

Note that $(-0.62)^n \to 0$ as $n \to \infty$, so $f_n \approx 0.724\,(1.62)^n$ for large n. In particular, $f_n = O\left(\left(\frac{1+\sqrt{5}}{2}\right)^n\right)$.

Can we make the formula $f_n \approx 0.724\,(1.62)^n$ a little easier to interpret? Let's write $1.62 = 10^{\log_{10}(1.62)}$. One has $\log_{10}(1.62) \approx 0.2 = 1/5$, so $1.62 \approx 10^{1/5}$ and $f_n \approx 0.724 \times 10^{n/5}$. One way to look at this is that each time n increases by 5 the value of f_n is multiplied by 10, i.e. one adds another digit to f_n. For example, $f_{25} \approx 0.725 \times 10^{25/5} = 72{,}500$ while $f_{30} \approx 0.725 \times 10^{30/5} = 725{,}000$. The actual values are $f_{25} = 75{,}025$ and $f_{30} = 832{,}040$.

One reason the Fibonacci numbers are important is because they are the worst case for the Euclidean algorithm. More precisely, suppose you use the Euclidean algorithm to find the greatest common divisor of $m = f_n$ and $p = f_{n+1}$. Then when you divide $m = f_n$ into $p = f_{n+1}$ you get a quotient of 1 and a remainder of f_{n-1}, since $f_{n+1} = f_n + f_{n-1}$. Then when you repeat the process with f_{n-1} and f_n you get a quotient of 1 and a remainder of f_{n-2}, so the next pair is f_{n-2} and f_{n-1}. This continues until you reach $f_1 = 1$ and $f_2 = 2$ where you stop since the remainder is 0. So, altogether, you had to n divisions.

Example 4. Let S_n be the number of n bit strings that don't contain two consecutive 1's. Find a formula for S_n.

We discussed this in section 5.1 where we saw that S_n satisfied the recurrence relation and initial conditions

$$S_n = \begin{cases} S_{n-1} + S_{n-2} & \text{if } n \geq 3 \\ 2 & \text{if } n = 1 \\ 3 & \text{if } n = 2 \end{cases}$$

This is the same recurrence relation as the Fibonacci sequence f_n except the initial conditions are different. In fact $S_1 = f_2$ and $S_2 = f_3$. It follows that $S_n = f_{n+1}$ for all n. So

$$S_n = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

$$= \frac{5 + 3\sqrt{5}}{10}\left(\frac{1 + \sqrt{5}}{2}\right)^n + \frac{5 - 3\sqrt{5}}{10}\left(\frac{1 - \sqrt{5}}{2}\right)^n$$

$$\approx 1.17\,(1.62)^n - 0.17\,(-0.62)^n$$

UNIT-5
GRAPH THEROY
TERMINOLOGY AND BASIC GRAPH THEORY

Introduction

This chapter presents an overview of basic graph theory, including its association with set theory. Graphs can be shown to be quite useful, especially as a mathematical tool for studying network problems. We shall begin our study with graph theory as applied to static problems in network theory, which are those problems that are related to the structure of the network. Static problems include the assessment of the impact of the loss of one or more communicating nodes or one or more communication links. We use graph theory in an attempt to create networks that are less vulnerable to such loss.

In another chapter of these notes, we shall consider the application of graph theory to dynamic problems, such as dynamic load balancing. We shall show that certain algorithms become unstable under dynamic conditions, in that they present alternating optimal solutions: try this, no try that, etc. This observation should serve as a caution not to trust results from static graph theory to work in all dynamic problem areas.

But first we must get started with the basic graph theory. We begin with the definition of sets and develop the idea of a graph as a set of vertices and a set of edges.

Terminology and notations used

A **graph** G is a finite non-empty set of objects called **vertices** together with a (possibly empty) finite set of unordered pairs of distinct vertices of G called **edges**. The **vertex set** of G is commonly denoted by V(G), and the **edge set** commonly denoted by E(G). The cardinality of the vertex set of a graph G is called the **order** of G, and the cardinality of the edge set is called the **size** of G. An ***(n, m)*-graph** G is a graph with ***n*** vertices and ***m*** edges; $|V(G)| = n$ and $|E(G)| = m$. Although graphs are formally defined in terms of sets, they are commonly depicted by figures in which the nodes

are depicted as circles (or ellipses) and the edges as lines between the circles.

The formal definition of a graph is based on set theory and utilizes the Cartesian product of sets, for which we present the standard definition. We begin by recalling that a **set** is an unordered collection of elements. For a set A, we write $\boldsymbol{a \in A}$ if element a is an member of set A and $\boldsymbol{a \notin A}$ if it is not. We sometimes define sets by a complete listing of the members of the set and sometimes by a description of the form $\{x \mid p(x)\}$, to be read as the set of all x such that $p(x)$ is true. Although it would be a bit strange, one can define the set of all odd integers as $\{ x \mid (x \text{ is an integer}) \text{ and } (x \text{ is an odd number}) \}$.

Let A and B be two arbitrary sets, defined over the same type of elements. We say that A is a **subset** of B, denoted as $A \subseteq B$, if every element that is in A is also in B; more formally: $A \subseteq B$ if and only if $a \in A$ implies $a \in B$. Two sets A and B are equal if and only if both $A \subseteq B$ and $B \subseteq A$. We say that A is a **proper subset** of B, denoted $A \subset B$, if $A \subseteq B$, but $A \neq B$.

Definition: For any two sets A and B, the **Cartesian product** of A and B, denoted by $A \times B$, is the set of pairs of elements defined by $A \times B = \{ (a, b) \mid a \in A, b \in B\}$; thus it is the set of pairs of elements (a, b) for which the first element is a member of set A and the second element is a member of set B.

As we shall soon see, one may take the Cartesian product of a set with itself. Thus we have
$A \times A = \{ (a_1, a_2) \mid a_1 \in A, a_2 \in A\}$. This work will use the Cartesian product sets for which the elements of the pair are distinct and unordered; thus $a_1 \neq a_2$ and (a_1, a_2) is considered the same element as (a_2, a_1). For example, consider A = {1, 2, 3, 4}, The set $A \times A$ has 16 elements; our work focuses on a subset of $A \times A$, $E \subset A \times A$, that can be listed as

E = { (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4) }.

Let X be an arbitrary set with a finite number of elements. The **cardinality** of X, denoted by |X|, is the number of elements in the set. If |X| = 0, the set is said to be the **empty set**, denoted by Φ. If |X| > 0, the set is said to be **non-empty**. We now define the basic set operations. For two sets A and B:

the **set intersection**, denoted $A \cap B$, is $A \cap B = \{ x \mid x \in A \text{ and } x \in B\}$,
the **set union**, denoted $A \cup B$, is $A \cup B = \{ x \mid x \in A \text{ or } x \in B\}$, and
the **set difference**, denoted A – B, is $A - B = \{ x \mid x \in A \text{ and } x \notin B\}$, and
the set **symmetric difference**, denoted $A \oplus B$, is $A \oplus B = (A \cup B) - (A \cap B)$;
that is, the set of elements either in set A or in set B, but not in both sets.

As an example, consider the following two sets, each a subset of the integers.

A = {2, 4, 6, 8, 10, 12, 14, 16, 18}
B = {3, 6, 9, 12, 15, 18}
Then $A \cap B$ = {6, 12, 18}
$A \cup B$ = {2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18}
A – B = {2, 4, 8, 10, 14, 16}
$A \oplus B$ = {2, 3, 4, 8, 9, 10, 14, 15, 16}.

These set operations are often illustrated using Venn diagrams, as shown below.

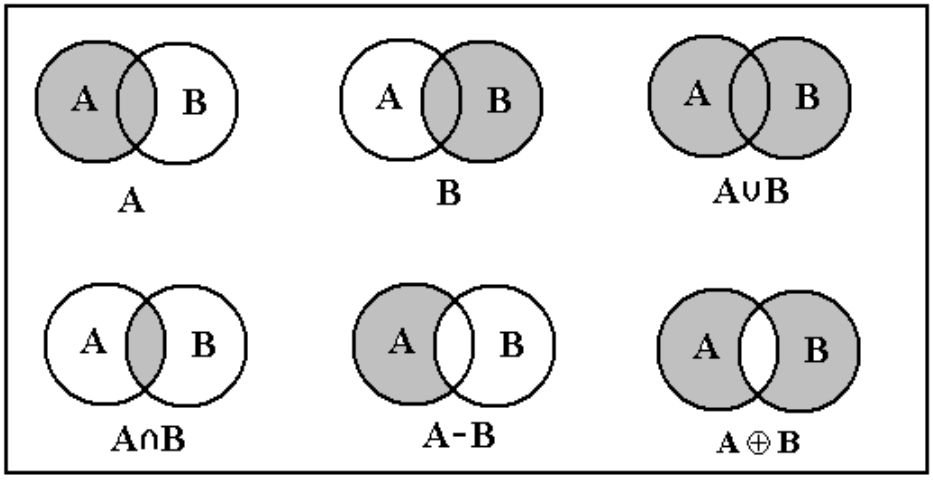


Figure 1: Venn Diagrams for Common Set Operations

Set Elements and Singleton Sets

At this point, it is important to make the distinction between elements of sets and the sets themselves. A set element can never be equal to a set. A **singleton set** is a set with one element. Singleton sets, unlike the empty set Φ, generally have no special significance in set theory and are mentioned only to clarify the notations used in the theory.

Consider the following set: F = {0, 1, 2, 3}, the set of integers modulo 4. The number 1 is an element of that set, so we can write $1 \in F$. Note that the element 1 is distinct from {1}, which is the set consisting of the single element 1. The following are true statements.

$1 \in F$	the element 1 is a member of the set F.
$1 \in \{1\}$	the element 1 is a member of this set also.
$\{1\} \subset F$	the set {1} is a proper subset of the set F.
$\{1\} \subseteq F$	the set {1} is a subset of the set F.
$\Phi \subseteq F$	the empty set is a subset of every set. In order to falsify this claim, one would have to show an element $x \in \Phi$, such that $x \notin F$. But the empty set has no members, so one cannot find such an element.

Note that we normally write subset inclusion as $X \subseteq Y$, unless it is important to state that X is a proper subset of set Y. We say $X \subseteq Y$ if either $X \subset Y$ or $X = Y$ is an acceptable condition.

The following statements are not correct and in many cases violate the conventions of set theory.

$1 \subset F$	an element cannot be a subset of any set. Elements are **members** of sets.
$1 = \{1\}$	an element can never be equal to a set; the two are different object types.
$\{1\} \in F$	F is a set of elements, so another set cannot be a member of F.
$\{1\} = F$	Obviously we have $\{1\} \subseteq F$, but $F \subseteq \{1\}$ is shown to be false by noting that $2 \in F$, but $2 \notin \{1\}$.

Sets of Sets

Just so the student knows it can be done, we can define a set containing other sets as members. Thus we can define G = { {0}, {1}, {2}, {3} }. Note that G is not

equal to F, as F has four integers as members and G has four singleton sets as members. In this case, we can properly write that $\{1\} \in G$, as the set G contains the element {1}.

Power Sets

We shall normally avoid sets that contain other sets as members. There is one important set of sets that we should discuss – the power set. We define the term and give an example.

For a given set X, the **power set of X**, denoted **P(X)**, is the set of all subsets of X.

If A = {0, 1, 2, 3}, as above, then

P(A) = { Φ , {0}, {1}, {2}, {3}, {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4},
{1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2, 3, 4} }

It can be proven that if |X| = K, then $|P(X)| = 2^K$; here |A| = 4 and $|P(A)| = 16 = 2^4$.

We now restate the definition of a graph, using the more precise terminology.
Definition: A graph G is a finite non-empty set of vertices, denoted V(G), together with a (possibly empty) finite set $E \subseteq V(G) \times V(G)$ of unordered pairs. As before, we let $|V(G)| = n$
and $|E(G)| = m$ and speak of an (n, m)-graph, usually called G.

The definition above is a bit too general for use in association with graph theory, so we immediately restrict it a bit. We introduce the idea of simple graphs, which is the type of graphs normally implied by the term "graph". A **simple graph** is a graph without edges connecting any vertex to itself. The graph in the next figure is not simple, as it has edges connecting vertex 1 to itself and vertex 4 to itself.

The graph at right is also described as follows
V(G) = {1, 2, 3, 4}
E(G) = { (1, 1), (1, 4), (2, 3), (2, 4), (4, 4) }

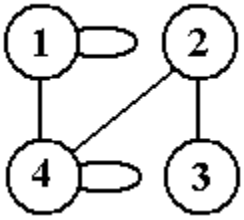


Figure 2: Two Representations of a Not-Simple Graph

We shall restrict our study of graphs to simple graphs. While graphs with loops are valuable in a number of studies, they are not useful in the analysis of networks and do present a number of difficulties that we would like to avoid. So – only simple graphs.

For a set of n objects, there are $n \bullet (n-1)$ ordered pairs of distinct elements; that is pairs (i, j), with $i \neq j$, in which the element (i, j) is different from the element (j, i).
For a set of n objects, there are $\binom{n}{2} = \frac{n \bullet (n-1)}{2}$ unordered pairs of distinct objects, in which the element (i, j) is considered to be the same as the element (j, i). We have two options, depending on whether the edge set contains ordered or unordered pairs.

Directed graphs correspond to edge sets that contain ordered pairs.
Undirected graphs correspond to edge sets that contain unordered pairs.

Consider the figure below, which shows an undirected graph and a directed graph.

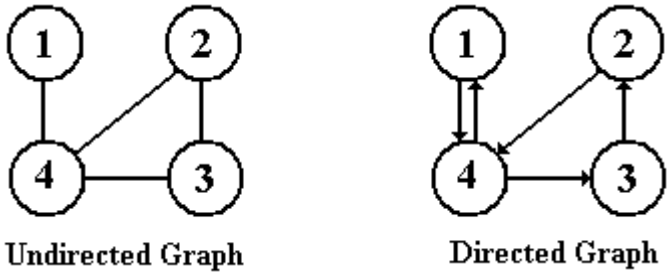


Figure 3: Two Sample Graphs On the Same Vertex Set

Each of the graphs in the figure has the vertex set V = {1, 2, 3, 4}. The edge set of the directed graph is E = { (1, 4), (2, 4), (3, 2), (4, 1), (4, 3)}. The edge set of the undirected graph is
E = { (1, 4), (2, 3), (2, 4), (3, 4) }. Note that in the undirected graph, the following edges are implicitly listed: (3, 2), (4, 1), (4, 2), (4, 3), as the pairs representing the edges are unordered. Thus, the pairs (1, 4) and (4, 1) are considered equivalent in an undirected graph and each represents the same edge. In a directed graph each of the ordered pairs (1, 4) and (4, 1) represents a distinct edge.

The student should note that it is always possible to create a directed graph that is equivalent to an undirected graph; one need only "double up" each edge in the undirected graph. The following figure shows an undirected graph and its equivalent directed graph.

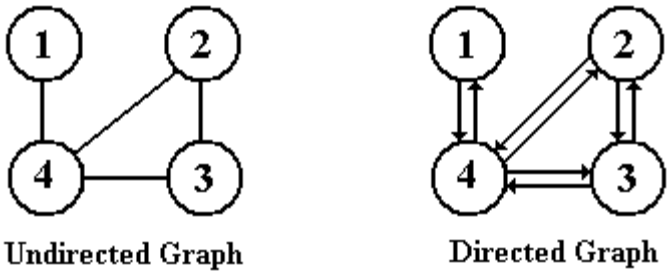


Figure 4: An Undirected Graph and the Equivalent Directed Graph

For the moment we shall restrict our discussions to undirected simple graphs, which we shall call "graphs" with no further distinction. As noted above, the edge set for an undirected graph with vertex set given by V(G) = {1, 2, …, *n*}. E(G) is a subset of V(G) × V(G) that contains only unordered pairs of distinct elements. For a set of *n* objects, there are $\binom{n}{2} = \frac{n \bullet (n-1)}{2}$ unordered pairs of distinct objects, this is the maximum size of the edge set for an (*n*, *m*)-graph. Thus we have the following limits on the number of edges in a simple undirected graph G.

Proposition 1: Let G be a simple undirected graph, with |V(G)| = *n*.

Then $0 \le |E(G)| \le \binom{n}{2} = \frac{n \bullet (n-1)}{2}$.

The complement of a graph G, denoted G_C, is the graph with the vertex set V(G) and edge set defined by $E(G_C) = \{ (u, v) \mid u \in V(G), v \in V(G), (u, v) \notin E(G) \}$. If G is an (*n*, *m*)-graph, then G_C is an (*n*, *n*•(*n* – 1)/2 – *m*)-graph.

In much of graph theory, the vertices of the graphs are labeled by integers, so that a four-vertex graph would have V(G) = {1, 2, 3, 4}. The set of possible edges for such a graph would be
{ (1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4) }. Consider two (4, 3)-graphs, a graph and its complement. First we give a rather formal definition of the two graphs.

G = (V(G), E(G) | V(G) = {1, 2, 3, 4}, E(G) = {(1, 2), (1, 3), (1, 4)}
G_C = (V(G), E(G) | V(G) = {1, 2, 3, 4}, E(G) = {(2, 3), (2, 4), (3, 4)}

While this is a sufficient definition of the two graphs, most people prefer the visual representation of the graphs. Here are standard representations of G and G_C.

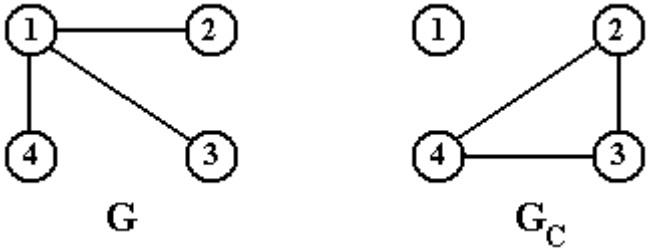


Figure 5: A Graph and Its Complement

Two graphs often have the same structure, differing only in the way their vertices and edges are labeled or in the way they are drawn. To make this idea more exact and to develop a way to focus on the essential structure of graphs, we introduce the concept of **graph isomorphism**. Two graphs G_1 and G_2 are said to be **isomorphic**, denoted by $G_1 \cong G_2$, if there exists a one-to-one mapping Φ from $V(G_1)$ onto $V(G_2)$ such that the mapping preserves the adjacency, that is to say that $(u, v) \in E(G_1)$ if and only if $(\Phi(u), \Phi(v)) \in E(G_2)$. Were we to push a point, we would note that graph isomorphism forms equivalence classes on graphs: if $G_1 \cong G_2$ and $G_2 \cong G_3$, then $G_1 \cong G_3$. The next figure shows two graphs that are labeled and drawn differently, but are isomorphic.

Figure 6: Two Isomorphic Graphs

The two graphs in Figure 6 are isomorphic under the following transformation: $\Phi(1) = A$, $\Phi(2) = B$, $\Phi(3) = C$, and $\Phi(4) = D$. The edge lists of the two graphs show this.

Graph on left: (1, 2), (1, 4), (2, 3), and (3, 4)
Graph on right: (A, B), (A, D), (B, C), and (C, D).

If we take the graph on left and apply the transformation to its vertex labels, we arrive at the edge list (A, B), (A, D), (B, C), and (C, D). This is precisely the edge list of the graph on the right, as expected. Thus, the two graphs are isomorphic.

The basic use of the idea of graph isomorphism is that we can view isomorphic graphs as identical and ask questions only about graphs that are not isomorphic. We use isomorphism to define a method of classifying graphs. For integers $n > 0$ and $m \geq 0$, let $\boldsymbol{\Gamma(n)}$ denote the collection of all non-isomorphic graphs with n vertices and $\boldsymbol{\Gamma(n, m)}$ denote the collection of all non-isomorphic graphs on n vertices and m edges. The next figure shows the sets $\Gamma(n)$ for $1 \leq n \leq 4$. Note that the set $\Gamma(1)$ has only one member – a single graph with one vertex and no edges incident on it; an isolated vertex.

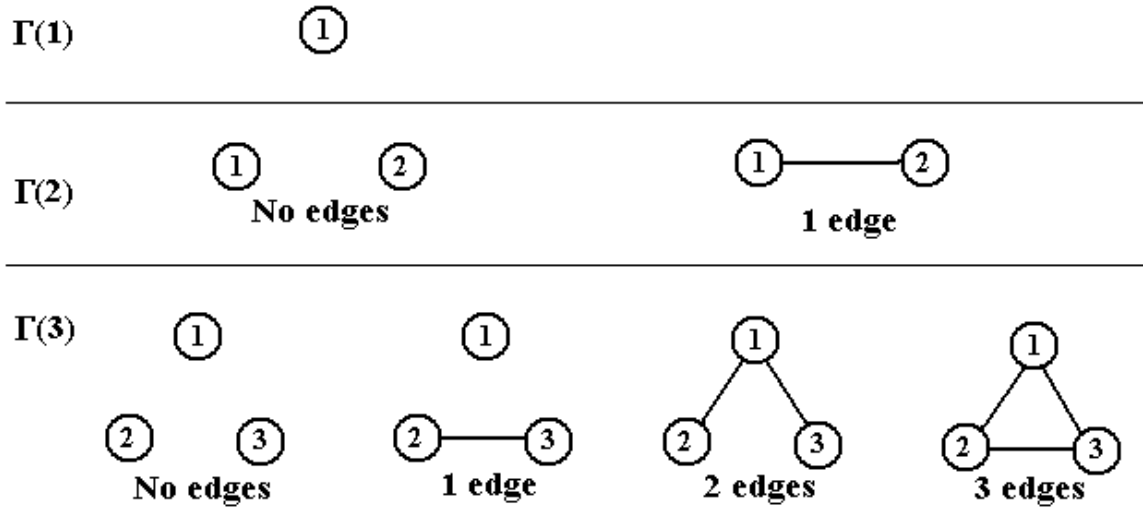


Figure 7: The sets Γ(1), Γ(2), and Γ(3)

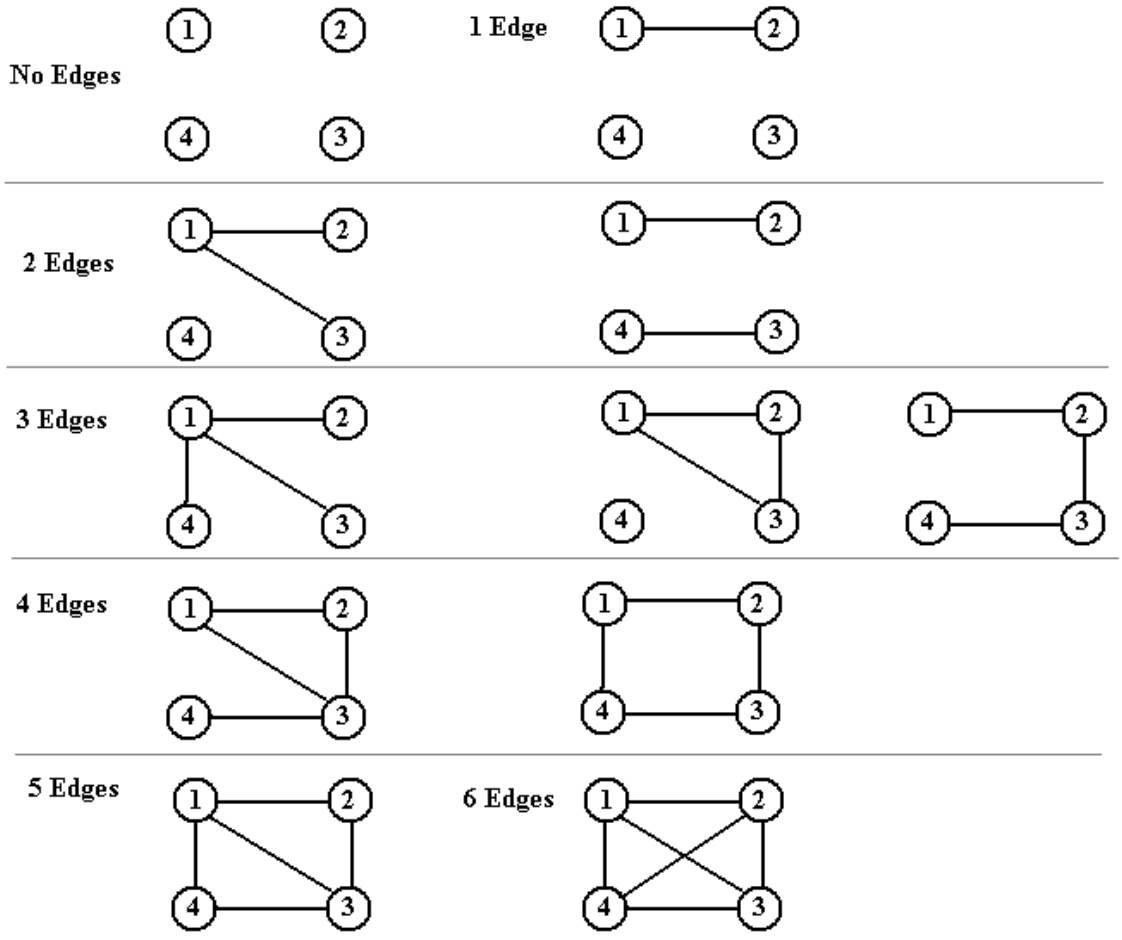


Figure 8: The Eleven Members of Γ(4)

Notation: At this point, we make a change in the way we refer to vertices. In our previous discussions, we used the "pure mathematics" approach to describing graphs, in which vertices were denoted by an integer in the range 1 to |V(G)|

inclusive and edges were denoted by unordered pairs of integers. In our studies, we normally use different labels for graphs, normally labeling the vertices as v_1, v_2, …., v_n for a graph with n vertices. When discussing a few vertices, we might give them labels, such as u, v, and w. Similarly, in discussing edges, we might use notation such as (u, v) or (v_i, v_j). The student should note that there is no theoretical significance to this; it is just one of many conventional notations used in describing graphs.

An edge (u, v) is said to join the vertices u and v. If $(u, v) \in E(G)$, then vertices u and v are said to be **adjacent**; u is adjacent to v, and v is adjacent to u. The edge (u, v) is said to be **incident** on its end vertices u and v. Again, in simple graphs we assume $u \neq v$.

The **degree** of a vertex v in G, denoted either as d_v or $d(v)$, is the number of edges incident on the vertex v. Since each edge incident on the vertex v causes another vertex to be adjacent to v, we might say that the degree of the vertex is the number of vertices adjacent to it. The two definitions are entirely equivalent. Occasionally, when a vertex is a part of two or more different graphs, we use the full notation $d_G(v)$ to indicate the degree of a vertex v in the graph G. Normally such precision is not required.

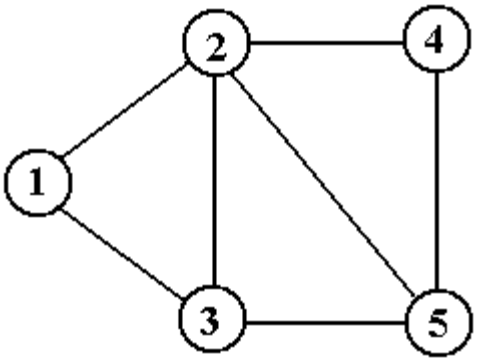


Figure 9: Illustration of Vertex Degrees

In this figure, $d_1 = d(v_1) = 2$, $d_2 = d(v_2) = 4$, $d_3 = d(v_3) = 3$, $d_4 = d(v_4) = 2$, and $d_5 = d(v_5) = 3$. Note that $\sum_{j=1}^{n} d_j = 2 + 4 + 3 + 2 + 3 = 14 = 2 \bullet m$. This is not a coincidence.

A vertex of zero degree is called an **isolated vertex** in that it has no edges incident on it and thus is not adjacent to any other vertex. At this point it will be convenient to state a few lemmas and theorems related to vertex degree.

Lemma 2: Let G be an (n, m)-graph and let $v \in V(G)$. Then $0 \leq d(v) \leq (n - 1)$.

Proof: The assertion that $d(v) \geq 0$ comes from the fact that $d(v)$ is a counting

number.
If $v \in V(G)$, there are only $(n-1)$ other vertices in V(G) to which v may be adjacent, thus it follows that $d(v) \leq (n-1)$.

Theorem 3: Let G be an (n, m)-graph with $V(G) = \{v_1, v_2, \ldots, v_n\}$. Let the degree of vertex v_j be given by $d_j = d(v_j)$. Then $\sum_{j=1}^{n} d_j = 2 \bullet m$.

Proof: Every edge in G is incident on two vertices; hence, when the degrees of the vertices are summed, each edge is counted twice. This completes the proof.

Theorem 4: Let G be an (n, m)-graph, with $m \geq n$. Then G has at least two vertices of degree $d(v) \geq 2$.
Proof: Assume that G has only one vertex with degree $d(v) \geq 2$. By Lemma 2, we have
$d(v) \leq (n-1)$, so we let the one vertex of degree greater than 1 have degree $(n-1)$. The maximum value of $\sum_{j=1}^{n} d_j$ is then $1 \bullet (n-1) + (n-1) \bullet 1 = 2 \bullet (n-1)$, being generated by the one vertex of degree $(n-1)$ and the $(n-1)$ vertices of degree 1. As a result of theorem 3, we have
$m \leq (n-1)$, which contradicts the assumption that $m \geq n$.

A graph G is called **regular** if all of its vertices have the same degree and is called **pseudoregular** if the degrees of its vertices differ by at most one. For a vertex v, define $N(v)$, the **open neighborhood** of v, as the set of vertices adjacent to v. As each edge incident on a vertex v connects it to an adjacent vertex, it follows immediately that $|N(v)| = d(v)$. The **closed neighborhood** of a vertex, denoted $N[v]$, adds the vertex itself to its open neighborhood; $N[v] = N(v) \cup \{v\}$. Note that $\{v\}$ is the set containing only one element – the vertex v.

A regular graph in which all vertices have degree k is called ***k*-regular**. The 3-regular graphs are called **cubic** and have been studied extensively.

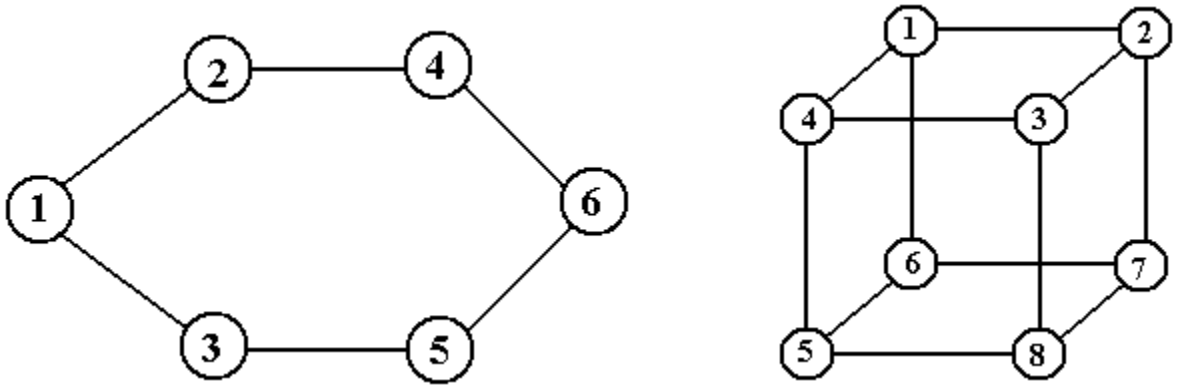


Figure 10: A 2-regular and a 3-regular graph

Note that in the above figure, that the 3-regular graph has been drawn so that its vertices appear at the corner of a cube. This is one of the reasons for the name "cubic". The next topic to be discusses considers the number of vertices that are adjacent to each of two distinct vertices.

Let u and v be two distinct vertices in (n, m)-graph G. The **codegree** of the two vertices, denoted by **codeg(u, v)**, is the number of vertices adjacent to both u and v. In set notation, we can write $\text{codeg}(u, v) = |N(u) \cap N(v)|$. We now give an upper limit on the codegree of two vertices.

Lemma 5: Let u and v be two distinct vertices in (n, m)-graph G.
Then $0 \leq \text{codeg}(u, v) \leq (n - 2)$.

Proof: The assertion that $\text{codeg}(u, v) \geq 0$ comes from the observation that it is a counting number. The upper limit comes from the observation that there are only $(n - 2)$ other vertices in G, so that $|N(u) \cap N(v)| \leq (n - 2)$.

We now place a lower limit on the codegree of two adjacent vertices.

Lemma 6: Let x and y be two adjacent vertices in an (n, m)-graph G. Then
$d(x) + d(y) \leq \text{Codeg}(x, y) + n$.

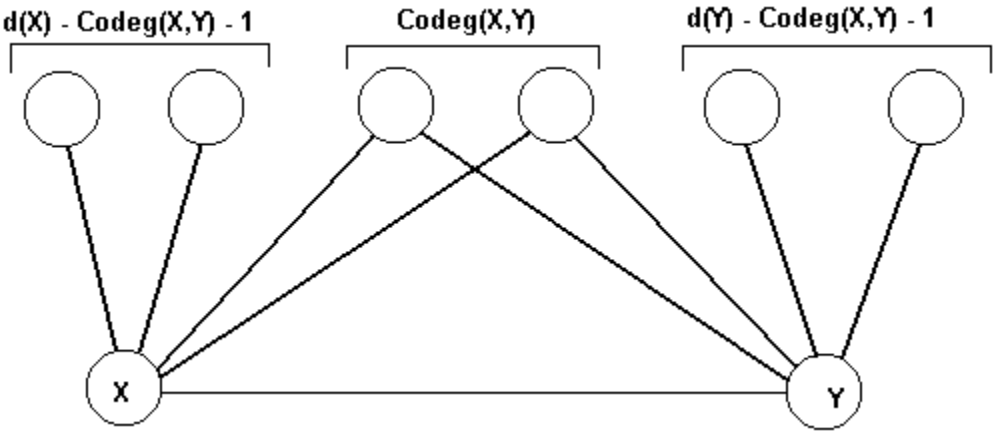


Figure 11: The Degrees and Codegree of Two Adjacent Vertices

Proof: Consider the two adjacent vertices x and y in the above diagram. Other than vertex y, there are $d(x) - 1$ vertices adjacent to vertex x, of which $d(x) - Codeg(x, y) - 1$ are adjacent to vertex x but not vertex y and $Codeg(x, y)$ are adjacent to both x and y. The number of vertices (other than x or y) that are adjacent to either vertex x or vertex y or both is given by
$d(x) - Codeg(x, y) - 1 + Codeg(x, y) + d(y) - Codeg(x, y) - 1 = d(x) + d(y) - Codeg(x, y) - 2$. But other than vertices x and y there are only $(n - 2)$ other vertices in the graph G, so we have
$d(x) + d(y) - Codeg(x, y) - 2 \leq (n - 2)$ or $d(x) + d(y) \leq Codeg(x, y) + n$.

A **subgraph** of a graph G us a graph having all of its nodes and edges in G. Thus, H is a subgraph of G if and only if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. A subgraph of G is a **spanning subgraph** if it contains all of the nodes of G. Thus H is a spanning subgraph of G if $V(H) = V(G)$ and $E(H) \subseteq E(G)$. For any sets U of nodes in G, $U \subseteq V(G)$, the **induced subgraph** <U> is the maximal subgraph with vertex set U. Put another way, the induced subgraph <U> is the graph with vertex set U $\subseteq V(G)$, with any two vertices being adjacent in <U> if and only if they are adjacent in G. We say more on induced subgraphs later in this chapter.

Let u and v be vertices in a graph G, with u and v not necessarily distinct. A ***u*-*v* walk** of G is a finite, alternating sequence of vertices and edges starting with u and ending with v: thought of as $u = u_0, e_1, u_1, e_2, \ldots, u_{s-1}, e_s, u_s = v$, such that $e_i = (u_{i-1}, u_i)$. The number s, the number of edges in the sequence, is called the **length** of the walk. A ***u*-*v* path** is a u-v walk in which no vertex is repeated. A **cycle** is a u-v walk in which all vertices are distinct with the sole exception that $u = v$. Paths and cycles, as special cases of walks, have obvious definitions for their lengths. A graph G is said to be **connected** if there exists a path between every pair of distinct vertices in the graph, otherwise it is **disconnected**. For a connected graph G, we define the **distance** $d(u, v)$ as the minimum of the lengths of all u-v paths connecting the 2 vertices u and v. A path of minimum length between two vertices is sometimes called a **geodesic**.

A **connected component**, or simply a **component**, of a graph G is a maximal connected subgraph of G. If a graph is connected, it has only one component; otherwise it has two or more components. For any vertex $v \in V(G)$, the component containing v is formed by adding v to the set of all vertices reachable by a path from v.

The following figure shows a graph with three components.

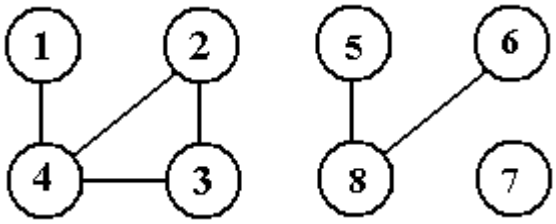


Figure 12: A Disconnected Graph With Three Components

The three components of the graph in this example are {1, 2, 3, 4}, {5, 6, 8}, and {7}. Note that there is a path from vertex 1 to vertex 3, so the two vertices are in the same component of the graph. Since there is no path from vertex 1 to vertex 5, they are in different components.

Recalling that a cycle is a path through a graph beginning and ending on the same vertex, we give the following definition of a graph without cycles.
Definition: An **acyclic graph** is a graph that does not contain a cycle.

Definition: A **tree** is a connected acyclic graph.

Definition: A **rooted tree** is a tree in which one vertex has been distinguished and called the **root**. Most trees of interest in computer science are rooted trees.

Trees play only a small part in the analysis of networks. The one tree of greatest importance for networks is the **star graph**, also called $K_{1,n-1}$ (see below). The next figure shows two of the smaller star graphs $K_{1,2}$ (also called a P_3, see below) and $K_{1,4}$. Note that we, as computer science people, see each tree as a rooted tree with the root vertex (or root node) being vertex 1.

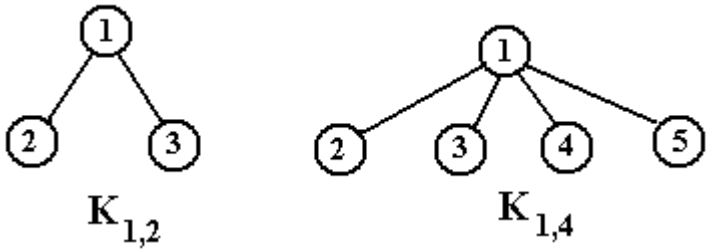


Figure 13: Two Star Graphs

Recalling that a subgraph H of graph G is a spanning subgraph if V(H) = V(G) and $E(H) \subseteq E(G)$. If H is a spanning subgraph of G and H happens to be a tree, then H is said to be a spanning tree of the graph G.

Upon reflection, one should realize that a graph G may have many distinct spanning trees; indeed it is almost obvious that a graph G has a unique spanning tree if and only if G is itself a tree. The next figure shows a graph and its three spanning trees.

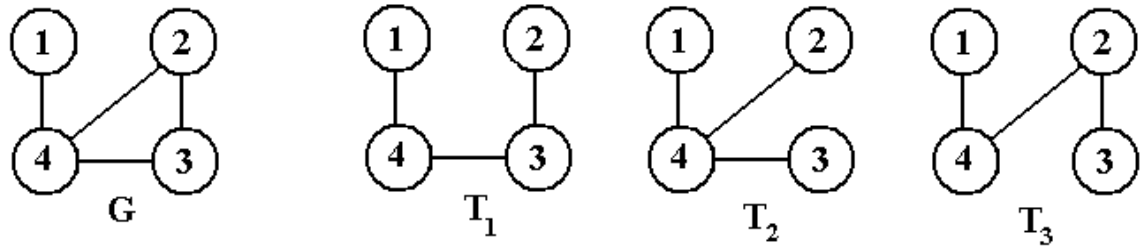


Figure 14: A Graph G and Its Spanning Trees

In the example above, we see a (4, 4)-graph G (4 vertices and 4 edges) and its 3 spanning trees T_1, T_2, and T_3. As we shall prove soon, a tree on four vertices must have exactly three edges. In the above example there are three edges that can be removed to yield a tree; removal of edge (1, 4) will cause the graph to be disconnected. Note that each of T_1 and T_3 is isomorphic to the graph P_4 – a path on

four vertices, while T_2 is isomorphic to $K_{1,3}$ – the star graph on 4 vertices.

We will soon quote one of the basic theorems regarding trees, but need to begin with a definition and a simple lemma. The definition serves to eliminate trivial exceptions from our theorems on trees.

Definition: A **nontrivial tree** is a tree with at least two vertices.

Lemma 7: Every nontrivial tree has at least two vertices of degree 1.
Proof: Let P be a longest path in a nontrivial tree T and let *u* and *v* be the end-nodes of the path P. Since T is acyclic, *u* and *v* each have only one neighbor in P, and since P is a longest path each has no neighbors in T – P (else the path could be extended). Thus there must be at least two vertices of degree one in a nontrivial tree.

Before we quote the "big theorem" we must explain a new bit of terminology. Let G be an
(*n*, *m*)-graph on at least two vertices, and let *u* and *v* be vertices that are not adjacent in G. Then by G + (*u*, *v*) we denote the (*n*, *m + 1*)-graph formed from G by adding making the two vertices *u* and *v* to be adjacent by adding the edge (*u*, *v*). Another term often used is G + *e*, denoting the addition of a new edge to a graph G.

Theorem 8: The following statements are equivalent.

1. G is a tree with *n* vertices and *m* edges.
2. Every two distinct vertices of G are connected by a unique path.
3. G is connected and $m = n - 1$.
4. G is acyclic and $m = n - 1$.
5. G is acyclic and if any two nonadjacent vertices of G are joined by an edge *e*, then G + *e*, the graph with one edge added, has exactly one cycle.

Proof: This is a well-known result. The theorem as stated is a slight rewording of Theorem 1.2 in reference [R01]. We shall adapt the proof from that reference and show the proof as an example of how graph theorists think. If the statements are all equivalent, then they must either be all true or all false for a given graph. The strategy for a proof of equivalence is quite simple; we just prove that any one statement implies all of the other statements. In this case we shall show a circular equivalence; thus $1 \Rightarrow 2$, $2 \Rightarrow 3$, $3 \Rightarrow 4$, $4 \Rightarrow 5$, and $5 \Rightarrow 1$.

Proof that $1 \Rightarrow 2$
Since G is a tree, it is a connected graph without cycles. Since G is connected, every two distinct nodes in G are connected by a path. Suppose two distinct nodes *u* and *v* in G that are connected by two distinct paths P and P*. Let *w* be the first node of path P (as we traverse from *u* to *v*) such that *w* is on both P and P*, but its successor on P is not on P*. Note that $w = v$ is allowed in this proof. We then follow path P from *u* to *w* and path P* backwards from *w* to *u* to form a cycle. Thus the assumption of two distinct paths between any two vertices implies that the graph contains cycles and cannot be a tree.

Proof that 2 $\Rightarrow$ 3

If every distinct pair of nodes in G is connected by a unique path, then G is connected by definition. We prove that $n = m + 1$ by induction. Reference to figures 7 and 8 of this work will show that the statement is true for $n = 2$, 3, and 4. It is also vacuously true for $n = 1$. Now assume that the result is true for all graphs with fewer than n vertices.

Suppose that G is a graph with n nodes ($n \geq 2$), m edges, and let v be one of the nodes of degree one in G (see Lemma 6). Then G – v, the graph obtained by removing the vertex v and the edge incident on it from G, has $(n – 1)$ vertices, one less than G, and still satisfies property 2. By the inductive hypothesis G – v has $m = (n – 1) – 1$, thus the number of edges in G is $m = (n – 1)$.

Proof that 3 $\Rightarrow$ 4
Assume that G has a cycle of length p. Then there are p vertices and p edges on the cycle, and for each of the $(n - p)$ vertices not on the cycle there is an incident edge on a geodesic from that vertex to a vertex in the cycle. Each such edge is different, so $(n - p) + p = n \geq m$, which is a contradiction.

Proof that 4 $\Rightarrow$ 5
Since G is acyclic, each component of G is a tree. If there are k components, then each component has one more vertex than edge and $n = m + k$, so the assumption that
$n = m + 1$ implies that $k = 1$ and that G is connected. Thus G is a tree and there is exactly one path connecting any two nodes in G. If we add an edge (u, v) to G, that edge together with the unique path in G joining u and v forms a cycle. The cycle is unique because the path is unique.

Proof that 5 $\Rightarrow$ 1
For this proof, we need a new notation. Let u and v be two non-adjacent vertices in a graph G. The graph G + (u, v) is the graph created by adding the edge (u, v) to G. If G is an (n, m)-graph, then G + (u, v) is an $(n, m + 1)$-graph. In general, we use the notation
G + e to indicate the graph generated from G by adding some new edge to G.

The graph G must be connected, for otherwise an edge e could be added joining two nodes in different components, and the graph G + e would be acyclic. Thus G is connected and acyclic, thus G is a tree.

We use the above theorem on trees to derive a result of importance to this work.
Lemma 9: Let G be an (n, m)-graph with $m < (n - 1)$. Then G is disconnected.
Proof: Let G be an (n, m)-graph with $m = (n - k)$, with $k \geq 2$. If G is connected, then there is a path between any two distinct vertices $u, v \in V(G)$. Select u and v as non-adjacent vertices and add the edge $e = (u, v)$. We now have an $(n, (n - k + 1))$-graph that contains a cycle, beginning at u, going to v, and returning to u by the existing path. If $k > 2$, repeat the above step $(k - 2)$ times, noting only that the addition of new edges does not remove the first cycle created. We then have an $(n, (n - 1))$-graph that is connected but contains a cycle. This contradicts Theorem 8 and thus we conclude that the original graph G could not have been a connected graph. The interested reader will find another proof of this lemma in the discussion of Theorem 1.3.1 in [R02]. It is important to note that $m < (n - 1)$ does not require that the graph have isolated vertices. The reader should examine the two (4, 2)-graphs shown in Figure 8, only one of which has an isolated vertex. A graph with an isolated vertex must be disconnected, but there are very

many disconnected graphs that have no isolated vertices.

For a connected graph G, we define e(*v*), the **eccentricity** of vertex *v*, as the maximum of the distances from *v* to the other vertices in the graph. The **radius** of a connected graph G, denoted rad(G), is the minimum value of the eccentricity of its vertices, while the **diameter** of the graph, denoted diam(G), is the maximum value of the eccentricity of its vertices. Before we quote a familiar theorem relating the radius and diameter of a graph, we give an example.

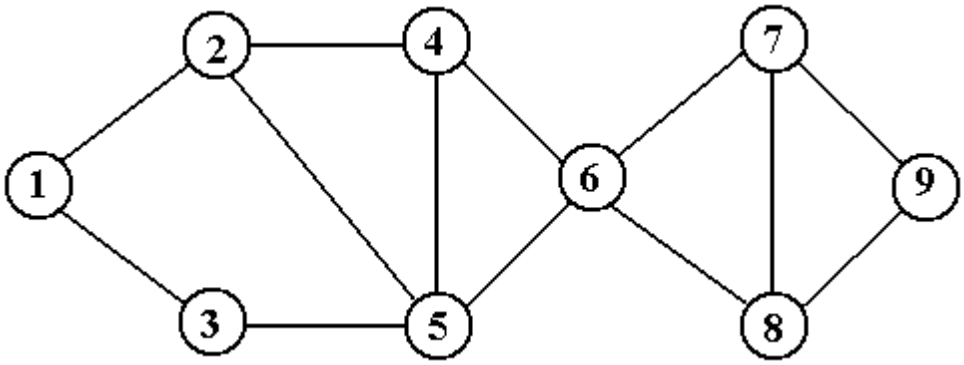


Figure 15: A Graph with Radius 3 and Diameter 5

In order to compute the radius and diameter of the graph, we first compute the eccentricity of each vertex. We construct the distance matrix for the graph.

Vertex	d(v, 1)	d(v, 2)	d(v, 3)	d(v, 4)	d(v, 5)	d(v, 6)	d(v, 7)	d(v, 8)	d(v, 9)	**e(v)**
1	0	1	1	2	2	3	4	4	5	**5**
2	1	0	2	1	1	2	3	3	4	**4**
3	1	2	0	2	1	2	3	3	4	**4**
4	2	1	2	0	1	1	2	2	3	**3**
5	2	1	1	1	0	1	2	2	3	**3**
6	3	2	2	1	1	0	1	1	2	**3**
7	4	3	3	2	2	1	0	1	1	**4**
8	4	3	3	2	2	1	1	0	1	**4**
9	5	4	4	3	3	2	1	1	0	**5**

Note that the maximum of the vertex eccentricities is 5; this is the diameter of the graph. The minimum of the vertex eccentricities is 3; this is the radius of the graph. A **central vertex** is a vertex with eccentricity equal to the radius of the graph. The **center of a graph**, denoted Z(G), is the set of all central vertices; here Z(G) = {4, 5, 6}. Since the radius of the graph is defined to be the minimum of the eccentricities of the vertices, it should be obvious that there is at least one vertex of

minimum eccentricity, and thus the center Z(G) has at least one element.

Theorem 10: For every connected graph G, rad(G) ≤ diam(G) ≤ 2 • rad(G).
Proof: The inequality rad(G) ≤ diam(G) arises from the definition that the radius is the minimum of a set of numbers while the diameter is the maximum of the same set of numbers. In order to verify the second inequality, select vertices *u* and *v* in G such that d(*u*, *v*) = diam(G). Let *w* be any vertex in Z(G), the center of G. Then d(*u*, *w*) ≤ e(*w*) and d(*v*, *w*) ≤ e(*w*), where
e(*w*) = rad(G). It can be shown that d(*u*, *v*) ≤ d(*u*, *w*) + d(*w*, *v*) for any three vertices *u*, *v*, and *w*, so we have d(*u*, *v*) ≤ d(*u*, *w*) + d(*w*, *v*) = 2 • e(*w*) = 2 • rad(G).

An (*n*, *m*)-graph G is called ***k*-partite**, $1 < k \leq n$, if the vertices of G can be partitioned into *k* vertex sets $V_1, V_2, \ldots, V_k$ such that no two vertices in the same set are connected by an edge in G. The vertex sets are called **parts** of V(G). For k = 2, we have a 2-partite graph, more commonly called a **bipartite graph**. A 3-partite graph is also called a **tripartite graph**.

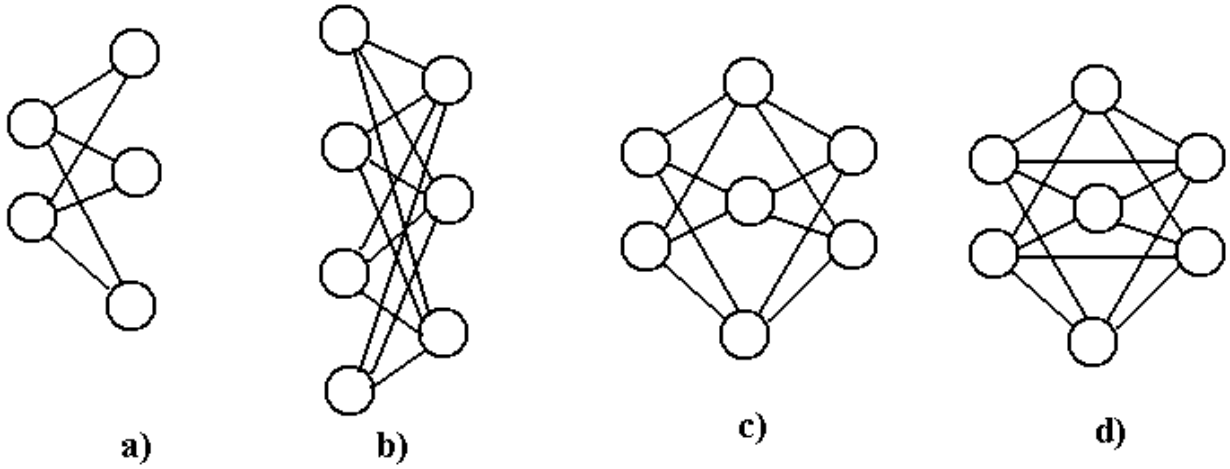


Figure 16: Some Bipartite Graphs and a Tripartite Graph

Fig 16a is $K_{2,3}$. Both fig 16b and 16c are $K_{3,4}$ – fig 16c is just drawn funny. Note that the vertices on the left and right side in fig 16c are not adjacent. Fig 16d is not a complete graph.

Before continuing, we note that any tree is also a bipartite graph. We show this fact by constructing the two vertex parts of the graph. Let T be a tree on *n* vertices and hence (*n* – 1) edges. Select one vertex, call it *u*, and place it in the vertex part called V_1. Place every vertex at distance 1 from *u* into vertex part V_2, every vertex distance 2 from *u* into vertex part V_1, and in general every vertex at odd distance from *u* into V_2 and at even distance from *u* into V_1. Since Theorem 8 assures us that the path from any vertex to *u* is unique, we do not try to place any vertex into

both V_1 and V_2. We now show that no two vertices in a vertex part can be adjacent. Suppose that *v* and *w* are two vertices in a vertex part that are adjacent. We have paths from u to both *v* and *w*, thus creating the cycle from the path from *u* to *w*, the edge (*w*, *v*) and the path from *v* to *u*. But the tree T is acyclic, so that vertices in the same vertex part cannot be adjacent and T is bipartite. In a rooted tree, think of one vertex part as all vertices at an odd distance from the root vertex and the other vertex part as the rest of the vertices.

A graph G is called **complete** if every pair of its vertices is connected by an edge. By $\mathbf{K}_n$ we denote a complete graph on *n* vertices. $\mathbf{C}_n$ denotes the **cycle on *n* vertices**, and $\mathbf{P}_n$ denotes the **path on *n* vertices**. Note that for $n \geq 2$, K_n has $n\bullet(n - 1)/2$ edges, C_n has n edges and P_n has $(n - 1)$ edges. K_3, which is isomorphic to C_3, is called the **triangle graph**, or **triangle**. K_1 denotes the empty graph on one vertex, it is a graph with one isolated vertex and no edges.

G is called a **complete *k*-partite** graph if it is *k*-partite and whenever two vertices are in different parts of the graph they are connected by an edge in E(G). A complete 2-partite graph is called **complete bipartite** and is denoted by $K_{a,b}$, where the number of vertices in the two vertex parts is *a* and *b* respectively. $\mathbf{K_{1,n-1}}$ denotes a **star graph** on *n* vertices with $(n - 1)$ edges. $K_{1,n-1}$ is a complete bipartite graph; it is also a tree. Note that $K_{1,2}$ is isomorphic to P_3. Note that there is only one connected graph on two vertices; it can be called either $K_{1,1}$ or K_2 or P_2, but not C_2 as a cycle must have at least three vertices.

For an arbitrary graph G, *n*G denotes *n* copies of the graph G. Let nK_1 denote the empty graph on *n* vertices. Then we have $m(nK_1) = 0$; $nK_1 \in \Gamma(n,0)$. The maximum number of edges in a graph in $\Gamma(n)$ equals $m(K_n) = n\bullet(n - 1)/2$.

There are many ways to combine graphs to produce new graphs. We shall consider only one binary operator – the **union**. This is defined as follows.
Definition: The union of two graphs G_1 and G_2, denoted $G = G_1 \cup G_2$, is that graph with
$V(G) = V(G_1) \cup V(G_2)$ and $E(G) = E(G_1) \cup E(G_2)$.

Note that one can use this union operator as an alternate definition of the graph nG, based on a recursive definition: $2G = G \cup G$, and $nG = (n - 1)G \cup G$. One important graph for our consideration will be $G = K_{1,n-j} \cup (j - 1)K_1$. For $n = 6$ and $j = 3$, we have the graph in the following figure. The graph has two isolated vertices.

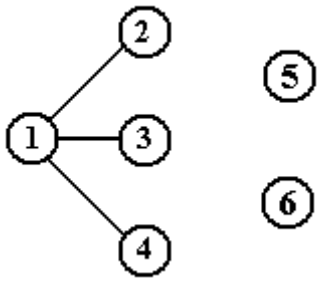


Figure 17: The (6, 3)-Graph $K_{1,3} \cup 2K_1$.

The **vertex connectivity** or simply **connectivity** of a connected graph G, denoted **κ(G)** is the minimum number of vertices the removal of which from G yields either an isolated vertex or a disconnected graph. If $\kappa(G) \geq r$, then the graph G is said to be **r-connected**. The **edge connectivity** of a graph G, denoted **λ(G)** is the minimum number of edges the removal of which results in a disconnected graph.

Let G be an (n, m)-graph with vertices $v_1, v_2, \ldots, v_n$ having degrees $d_1, d_2, \ldots d_n$, where
$d_i = d(v_i)$. We label the vertices so that $d_1 \geq d_2 \geq \ldots \geq d_n$ to get a sequence called the **degree sequence** of G, denoted by **D(G)** = $(d_1, d_2, \ldots, d_n)$. By **Δ(G)** we denote the maximum degree in G, and by **δ(G)** we denote the minimum degree in G. If the degree sequence D(G) is presented in the as above, then $\Delta(G) = d_1$ and $\delta(G) = d_n$. By **DSS(G)** we denote the sum of the squares of the vertex degrees of a graph G. In other words, for an (n, m)-graph G with degree sequence given by D(G) = $(d_1, d_2, \ldots, d_n)$, we have $DSS(G) = \sum_{1}^{n} (d_j)^2$.

We now consider two degree sequences, both for (n, m)-graphs and define a useful concept, called **degree sequence dominance**.

Definition: Let $D(G) = (d_1, d_2, \ldots, d_n)$ and $D(H) = (d'_1, d'_2, \ldots, d'_n)$ denote the degree sequences of (n, m)-graphs G and H, respectively. D(G) is said to **dominate** D(H) if $\sum_{i=1}^{j} d_i \geq \sum_{i=1}^{j} d'_i$ for all $j = 1, 2, \ldots, n$ with strict inequality for at least one value of j.

The importance of degree sequence dominance arises from its relation to the sum of the squares of the degrees of the vertices, as seen in the following proposition.

Proposition 11: Let G and H be two (n, m)-graphs such that the degree sequence of G dominates the degree sequence of H. Then DSS(G) > DSS(H).

Proof: Let $D(G) = (d_1, d_2, \ldots, d_n)$ and $D(H) = (d'_1, d'_2, \ldots, d'_n)$ denote the degree sequences of
(n, m)-graphs G and H, respectively. Since the degree sequence of G dominates that of H, there must be at least one index k, $1 \le k \le n$, such that $d_k > d'_k$.
Let k be the smallest index for which $d_k > d'_k$ and let $d_k = d'_k + d$, with $d > 0$.

Since the degree sequence is ordered, we have $d'_k \ge d'_j$ for all $j > k$. Since the two degree sequences add to the same sum, we must have $\sum_{i=k+1}^{n} d_i = \sum_{i=k+1}^{n} d'_i + d$.

We alter the degree sequence of H by adding the value to d to d'_k, increasing DSS(H) by
$2d \bullet d'_k + d^2$. Decreasing d'_{k+1} to balance the sum then decreases the new value of DSS(H) by
$d^2 - 2d \bullet d'_{k+1}$, yielding a net change of $2d \bullet d'_k + 2d \bullet d'_{k+1}$, which is a positive number. Thus by modifying the degree sequence of H to make it look more like that of G, we have increased the value of DSS(H). One can easily see that these changes to make the degree sequence of H identical to that of G continually increase DSS(H). Thus we must have started with DSS(H) < DSS(G).

A **sparse graph** is an (n, m)- graph for which $m \le \lfloor n^2/4 \rfloor$, and a **dense graph** is an (n, m)-graph for which $m > \lfloor n^2/4 \rfloor$, where $\lfloor x \rfloor$ is the largest integer not greater than the real number x.
$\lfloor n^2/4 \rfloor = (n^2/4)$ if and only if n is an even integer.

For graphs G and H, let *H(G) denote the number of induced subgraphs of G which are isomorphic to H and #H(G) denote the number of (not necessarily induced) subgraphs of G which are isomorphic to H. Thus $\#P_3(G)$ and $*P_3(G)$ denote the number of subgraphs and the number of induced subgraphs, respectively, of G isomorphic to P_3, the path on three vertices. $\#K_3(G)$ denotes the number of subgraphs isomorphic to K_3, the triangle. Because all triangles as subgraphs are induced, $\#K_3(G) = *K_3(G)$; we use $*K_3(G)$ to denote the number of triangles in a graph G. Any graph for which $*K_3(G) = 0$ is said to be **triangle-free** or **K_3-free**. We shall see that bipartite graphs are K_3-free.

Recall that a **bipartite graph** is an (n, m)-graph G with the property that V(G) can be broken into two disjoint sets V_1 and V_2, such that a vertex in V_1 is adjacent only to vertices in V_2 and a vertex in V_2 is adjacent only to vertices in V_1. We now

prove one result of major importance to our work: that bipartite graphs do not contain a K_3. We do this by first proving the more general result and then applying an obvious definition.

Theorem 12: A graph G is bipartite if and only if all of its cycles are even.

Proof: This proof is quite important, so is quoted almost verbatim from Theorem 1.3 in Distances in Graphs [R01]. If G is bipartite, then its vertex set V can be partitioned into two sets V_1 and V_2 so that every edge of G joins a vertex in V_1 with a vertex in V_2. Thus every cycle [of length k] $v_1, v_2, \ldots, v_k, v_1$ in G necessarily has its oddly subscripted vertices in V_1, say, and the others in V_2, and so its length is even. [Otherwise, we would have the edge (v_k, v_1) connecting two vertices in V_1, contradicting our hypothesis.]

For the converse, we assume without loss of generality that G is connected (for otherwise we can consider the components of G separately). Take any vertex $v_1 \in V(G)$ and let [vertex set] V_1 consist of v_1 and all vertices at even distance from v_1, while [vertex set] $V_2 = V - V_1$. Since all cycles of G are even, every edge of G joins a vertex of V_1 with a vertex of V_2. For suppose there is an edge (u, v) joining two vertices of V_1. Then the union of geodesics [shortest paths] from v_1 to v and from v_1 to u together with the edge (u, v) contains an odd cycle, a contradiction.

We now present the important result as a corollary to the above theorem.
Corollary 13: A bipartite graph does not contain a K_3 (triangle).
Proof: We have just shown that a bipartite graph does not contain any cycle of odd length. Specifically, it does not contain a C_3 (a cycle on three vertices), which is isomorphic to a K_3 (complete graph on three vertices).

In terms that we shall use later, we have just shown that if G is a bipartite graph then
$*K_3(G) = \#K_3(G) = 0$.

We now link sparse and dense graph to graphs containing triangles by use of a famous theorem due to Turan. Turan's work is considered the first theorem in an important area of graph theory, called extremal graph theory, which we now discuss briefly.

Extremal Graph Theory
The study of extremal graphs is generally the study of the largest or smallest graphs that have certain properties. The best reference on the topic is the book Extremal Graph Theory by Bollobas [R03], a book that is rare and hard to find.

The book contains references to many of the original papers in the subject; unfortunately many of them were written in Hungarian and have yet to be translated.

For these notes, we focus on extremal graph theory of complete subgraphs; that is subgraphs that are isomorphic to a complete graph K_n. We quote from chapter VI of Bollobas [R03] to introduce the subject.

> Given a graph F_1, what is ex(n; F_1), the maximum number of edges of a graph of order n [having n vertices] not containing F_1 as a subgraph. … [The] best known extremal result of graph theory [is] Turan's theorem. This result, proved in 1940 and always considered to be the first extremal theorem, answers this question above in the case $F_1 = K_r$.

Turan's theorem is based on specific complete q-partite graphs, denoted $T_q(n)$.
Definition: Given natural numbers n and q, denote by $T_q(n)$ the complete q-partite graph with $\lfloor n/q \rfloor$, $\lfloor (n+1)/q \rfloor$, … $\lfloor (n+q-1)/q \rfloor$ vertices in each of the vertex sets. Note that $T_q(n)$ is the unique complete q-partite graph of order n whose vertex sets have size as equal as possible. For convenience, we number the vertex parts beginning with 0, so that vertex part k has size $\lfloor (n+k)/q \rfloor$, $0 \le k \le (q-1)$.

It is a standard result that a q-partite graph of order n having $n_0, n_1, .. n_{q-1}$ vertices in its vertex parts has at most $\binom{n}{2} - \sum_{0}^{q-1} \binom{n_k}{2}$ edges. $T_q(n)$ is the unique q-partite graph of order n, denoted by $t_q(n)$. Turan also proved in 1941 that every other graph of order n and size $t_{r-1}(n)$ contains a K_r as a subgraph.

For this research the most important Turan graph will be $T_2(n)$, the complete bipartite graph with vertex parts of size $\lfloor n/2 \rfloor$ and $\lfloor (n+1)/2 \rfloor$.

Theorem 14: Let r and n be natural numbers, $r \ge 2$. Then every graph of order n and size greater than $t_{r-1}(n)$ contains a K_r, a complete graph of order r. Furthermore, $T_{r-1}(n)$ is the only graph of order n and size $t_{r-1}(n)$ that does not contain a K_r.
Proof: See the proof of theorem 1.1 in chapter VI of reference [R03].

Of special interest to much research is the largest graph that contains no K_3.
Lemma 15: The largest graph with n vertices that contains no triangle is the complete bipartite graph $K_{a,b}$, with $n = a + b$ and $|a - b| \le 1$.

Proof: See Theorem 4.1.2 in the book Pearls in Graph Theory [R02]. This is also a special case of Theorem 14, just above.

Remark: The complete bipartite graph $K_{a,b}$ has $m = a \bullet b$ edges. If $a > b$, then we have two possibilities for graphs satisfying theorem 15: $a = b$ and $a = b + 1$. If $a = b$, then
$n = 2 \bullet b$ and $m = b^2 = n^2/4$. If $a = b + 1$, then $n = 2 \bullet b + 1$ and $m = b \bullet (b + 1) = b^2 + b$. Also we have $n^2 = (2 \bullet b + 1)^2 = 4 \bullet b^2 + 4 \bullet b + 1$, so $m = \lfloor n^2/4 \rfloor$. The graph $K_{a,b}$, as described above is the largest sparse graph and we conclude that all dense graphs must contain triangles.

Corollary 16: If G is an acyclic graph, it must be a sparse graph.
Proof: If G is not a sparse graph, it is a dense graph that must contain a triangle or
$K_3 \approx C_3$, which is a cycle. Hence G is not acyclic.

We add another interesting result that might be of use in later work.
Theorem 17: If $n \geq (r + 1)$ then every (n, m)-graph with $m = t_{r-1}(n) + 1$ contains a K_{r+1} from which an edge as been omitted.
Proof: See the proof of theorem 1.2 in Chapter VI of reference [R03].

Another Count of Subgraphs
Another important count is $S_3(G)$, the number of induced three-vertex connected subgraphs of G. P_3, the path on three vertices, and K_3, the triangle, are the only connected graphs on three vertices, so $S_3(G) = {}^*P_3(G) + {}^*K_3(G)$ for any graph G.

An (n, m)-graph is said to be $\#P_3$-optimal if it maximizes $\#P_3(G)$ for all $G \in \Gamma(n, m)$, the set of all (n, m)-graphs. $^*P_3$-optimal and S_3-optimal graphs are those graphs which maximize the counts $^*P_3(G)$ and $S_3(G)$ respectively.

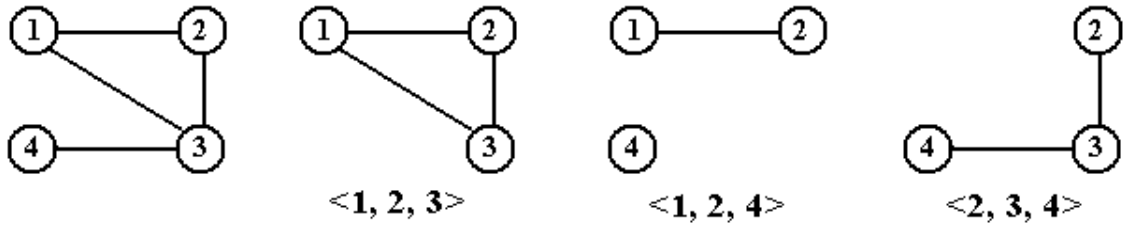


Figure 18: A Graph and Its 3-Vertex Induced Subgraphs

In the example above, we see a (4, 4)-graph and the subgraphs induced on the three distinct three-vertex subsets of {1, 2, 3, 4}. The subgraph <1, 2, 3> is a K_3, which contains three non-induced P_3's, one centered on each of its vertices. The graph

<1, 2, 4> is $K_1 \cup K_2$, also called a K_1K_2. The subgraph <2, 3, 4> is an induced P_3.

As was mentioned above, there are three non-induced P_3's in the above graph – one centered at vertex 1, one centered at vertex 2, and one centered at vertex 3. As a result we have one induced P_3 and three non-induced P_3's, for a total of four. Thus, for this graph we have $*P_3(G) = 1$, $*K_3(G) = 1$, $S_3(G) = 2$, and $\#P_3(G) = 4$.

Proposition 18: For any graph G, $\#P_3(G) = *P_3(G) + 3 \bullet *K_3(G)$.
Proof: Let *u*, *v*, and *w* be the vertices of a triangle in G. There is a P_3 centered on each of the vertices *u*, *v*, and *w*. Since none of these is an induced P_3, each triangle contributes 3 to the count $\#P_3(G)$ but 0 to the count $*P_3(G)$. The conclusion then follows by noting that each induced P_3 contributes 1 to the count of $\#P_3(G)$ and 1 to the count of $*P_3(G)$. In order to drive this point home, let's take another look at figure 18, presented above, focusing on the triangle induced by vertices 1, 2, and 3. Note that none of the P_3's defined on these 3 vertices is induced, as each lacks one edge incident only on vertices in the set {1, 2, 3}.

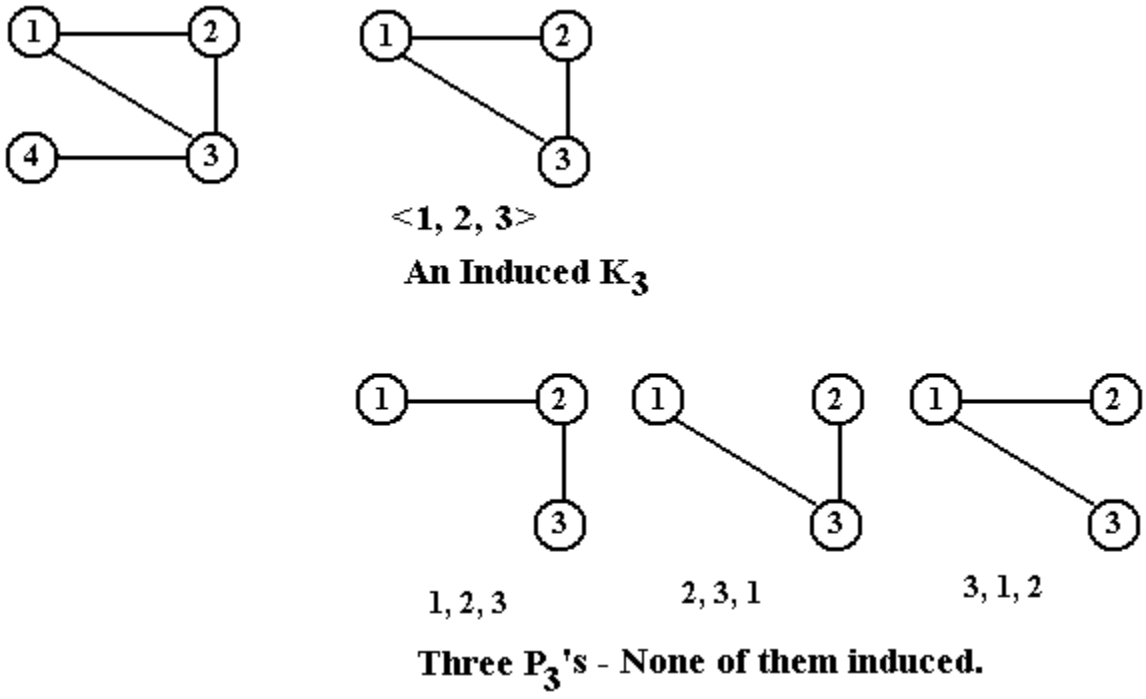


Figure 19: A Graph and Some of Its 3-Vertex Subgraphs

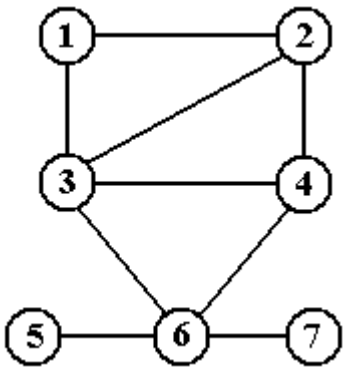
WEIGHTED GRAPHS

We now introduce the concept of a weighted graph – a graph in which there are weights associated with the edges. These weights can represent distances, costs, capacities, or any other measure that is associated with an edge and that can be quantified as a real number. For most weighted graphs, the weights are represented as non-negative integers, although negative edge weights appear to be used for some applications. To this author's knowledge, no work has been done on graphs with edge weights represented as complex numbers.

We begin with a formal definition of a weighted graph, and then move on to a more natural discussion of the concept in terms of drawings and adjacency matrices.

Definition: A ***weighted graph*** G is a triple (V, E, W) in which V is a non-empty set of vertices, $E \subseteq V \times V$ is a set of edges (the graph can be directed or undirected), and W is a function from the edge set **E** into **R**, the set of real numbers. For any edge $e \in E$, w(e) is the weight of e. In networks, the edge weights often represent the link transmission capacities.

We shall immediately revert to the standard practice of representing all edge weights as non-negative integers, most commonly using only positive integers. It can be proven that for most cases, this restriction does not present any difficulties. We shall begin with a simple undirected graph, in which all edges can be said to have a weight of one and then develop an example of the same graph with weighted edges. This example is taken, almost verbatim, from an excellent textbook [R04] by Sara Baase and Alan Van Gelder.



	1	**2**	**3**	**4**	**5**	**6**	**7**
1	0	1	1	0	0	0	0
2	1	0	1	1	0	0	0
3	1	1	0	1	0	1	0
4	0	1	1	0	0	1	0
5	0	0	0	0	0	1	0
6	0	0	1	1	1	0	1
7	0	0	0	0	0	0	1

Figure 20: An Undirected Graph and Its Adjacency Matrix

We now add edge weights to this example, making it a weighted graph. Note that the only change to the adjacency matrix representation is to replace the 1 by the

weight of the edge. Suppose that A is the adjacency matrix of a graph. We have two cases.

Unweighted Graph

A_{IJ} = 0 if no edge

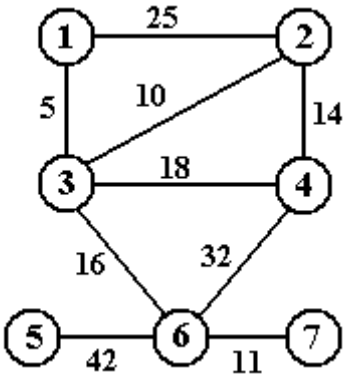
A_{IJ} = 1 if (I, J) is an edge

Weighted Graph

A_{IJ} = 0 if no edge

A_{IJ} = weight(I, J) if (I, J) is an edge

We now present a weighted graph that has the same underlying undirected graph as the example in the figure above. Note that the adjacency matrix is different, it now has the weights.



	1	**2**	**3**	**4**	**5**	**6**	**7**
1	0	25	5	0	0	0	0
2	25	0	10	14	0	0	0
3	5	10	0	18	0	16	0
4	0	14	18	0	0	32	0
5	0	0	0	0	0	42	0
6	0	0	16	32	42	0	11
7	0	0	0	0	0	11	0

Figure 21: A Weighted Graph and Its Adjacency Matrix.

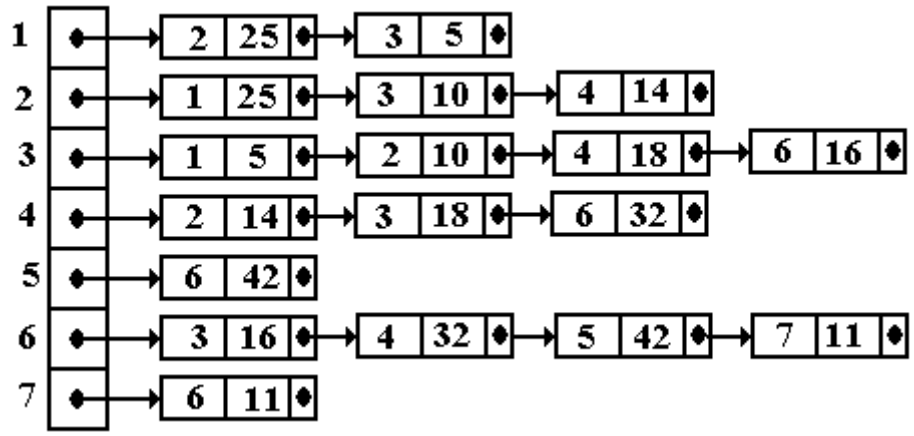


Figure 22: The Adjacency List Representation of the Same Weighted Graph

Note that the vertices in the list are kept in sorted order. This is a convention only and is not necessary. Ordered lists are easier to search, but take more time for insertion.

At this point we should note that the above adjacency matrix will cause some graph algorithms to malfunction. The problem arises when the edges represent distances

or costs or some such quantity that one might want to minimize. The problem, which does not occur in the adjacency list representation, is due to the fact that a 0 is used to represent an edge that is not present. Consider a silly algorithm attempting to develop a minimum cost Hamiltonian circuit of the above graph. It might select $1 \to 4 \to 5 \to 3 \to 7 \to 2 \to 6 \to 1$ as the route with a total weight of 0. This is, of course, an impossible route as none of these edges exist.

It is easy to see that the problem does not occur when one uses the adjacency list representation of the graph. Edges that are not present simply do not have entries in the linked lists representing the open neighborhoods of each vertex. The problem is avoided.

It is also easy to see that the problem does not occur when one is using a graph to model some problem in which the edges represent flow capacities, available communication circuits, or some other measure to be maximized. In that case an edge that does not exist is identical to an edge of zero capacity; neither can be used to solve the problem.

When one is considering an adjacency matrix representation of a graph modeling a problem for which sums of edge weights are to be minimized, it is necessary to place a large value in the matrix elements that indicate non-existent edges between distinct vertices. Note that almost all algorithms will detect that a diagonal element A[K][K] of a matrix is not to be used as the graph contains no loops, so only the entries for non-existent edges must be adjusted.

Many books suggest placing ∞ as an element in the adjacency matrix to represent the weight for the non-existent edges. This is great for drawings, but presents problems in the application of an algorithm, because most computers lack a consistent representation for ∞. The approach commonly suggested is to take a very large number and use that. Here is another suggestion that will work for most algorithms.

1) Beginning with the adjacency matrix having 0's represent each non-existent edge,
   sum all the edge weights. The sum is twice the total of the edge weights, as every
   edge is summed twice.
2) Multiply that number by two and use that value to represent non-existent edges.

In the above example, the sum of the values of the adjacency matrix is 346, indicating a total edge weight of 173. We double the value of 346 to get 692 and use either that value or any larger value to represent a non-existent edge. The use of this number is based on the observation that no path through the graph will have a

total distance greater than the sum of all the weights of all the edges, so here we use a number four times as big to keep the algorithms from picking any of these non-existent edges. The array below is the adjacency matrix using this approach.

0	25	5	692	692	692	692
25	0	10	14	692	692	692
5	10	0	18	692	16	692
692	14	18	0	692	32	692
692	692	692	692	0	42	692
692	692	16	32	42	0	11
692	692	692	692	692	11	0

Figure 23: The Adjusted Adjacency Matrix