Mathematics – III (CS)

Courseware Material

SiliconTech

Silicon Institute of Technology

Prepared by

The Special Academic Group Autonomy (SAGA)

FOREWORD

This is the third iteration of our own courseware material prepared by the members of SAGA, the special academic group, autonomy. The contents have been carefully developed according to the autonomous syllabus, and should augment material presented during lectures; it is hoped that it will be useful for the students and serve as a ready reference for faculty members.

This year-long task was aimed at preparing contents for all second year subjects of the autonomous B.Tech. curriculum. The subjects included are Mathematics III for Electric Sciences, Mathematics III for Computer Sciences, Mathematics IV for Electrical Sciences, Circuit Theory, Analog Electronic Circuits, Digital Electronic Circuits, Signals and Systems, Basics of Instrumentation, Measurements and Instrumentation, Transducers and Measurements, Electrical Machines, Control Systems Engineering, Basics of Mechanical Engineering, OOP using Java, Design and Analysis of Algorithms, Database Management Systems, Computer Organization and Architecture, Engineering Economics, Biology for Engineers and Universal Human Values & Professional Ethics.

Faculty members from all the departments contributed to task in a year-long sustained effort. They are, in no particular order, Susmita Biswal, Tusar Parida, Swarupa Roy, Dhananjaya Tripathy, Sanghamitra Das, Biranchi Rath, Amulya Roul, Satyabrata Das, Narayan Nayak, Sudhansu Biswal, Debangana Das, Tapas Maji, Anita Mohanty, Pratap Chandra Mohanty, Nivedita Pati, Ipsita Das, Manas Ranjan Singh, Subhashree Prusty, Samaleswari Nayak, Soumya Ranjan Dash, Bikram Misra, Sanjeev Dash, Tarini Mishra, Mahendra Agasty, Janmejay Senapati, Kumari Anamika and Rupa Kanungo.

Then entire group worked tirelessly and diligently throughout the year to get the task successfully completed. Sincere thanks to the group for a job well done.

I am hopeful that these contents will come in handy and will be extensively used. They are meant as additional resources to complement classroom teaching. If there are any errors, I would be grateful if they are brought to my notice so that we can correct them in future editions.

Dr. Jaideep Talukdar, Principal

Silicon Institute of Technology, Bhubaneswar

August 2023

PROPORTIONAL LOGIC

Proposition : Any declarative statement which is either true or false.

ex "Today is Monday"

p : "I love that dress."

q : "2+2 = 22"

☆ FACTS are NOT propositions.

Logical Connectives or Logical Operators

1. Negation ($\bar{p}$, $\neg p$, $\sim p$) : Let p be a proposition, the negation of p is the statement "It is not the case that p".

TRUTH TABLE

p	$\neg p$
T	F
F	T

ex $\neg p$: "It is not the case that today is Monday"

OR

$\neg p$: "Today is not Monday."

2. Conjunction ($\wedge$) : Let p and q be two propositions. The conjunction of p and q is the proposition "p and q".

TRUTH TABLE

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

☆ Conjunction is commutative.

$$p \wedge q \equiv q \wedge p$$

☆ BUT can also act as conjunction in place of AND.

ex "$2+2 = 4$ but $2-1 \neq 3$"

"We are visiting Puri but not visiting the beach."

★★★ AND does NOT act as conjunction always.

ex "I opened a book and started reading it."

Here commutativity fails as the statement cannot b

✗ "I started reading a book and then opened it".

DE MORGAN'S LAW : $\neg(p \wedge q) = \neg p \vee \neg q$

3. Disjunction ($\vee$) : Let p and q be two proposition

The disjunction of p and q is $p \vee q$.

TRUTH TABLE

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

ex " 1+2 = 3 or 1-2 = 1 " = T

" Secure A grade or O grade " = T

★ Disjunction is also commutative.

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

DE MORGAN'S LAW : $\neg(p \vee q) = \neg p \wedge \neg q$

★★ Conjunction and disjunction – both are distributiv

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

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

4. Exclusive OR ($\oplus$) : Let p and q be two propositions. The exclusive or of p and q, den by $p \oplus q$ is the proposition "There is true whe exactly one of p and q is true and false otherw

Teacher's Signature..................

TRUTH TABLE

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

ex "Today is Monday or Tuesday".
"I will sing or study."
"The lift will go up or down."

Conditional Statements

Implication ($\rightarrow$): Let p and q be two propositions. The implication of p and q, denoted by $p \rightarrow q$ is the proposition "If p then q".

TRUTH TABLE

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

ex ★ "If you score O grade, you will be awarded."
"If the sun rises, the day begins."

$p \rightarrow q$

Premise / Antecedant / Hypothesis

Conclusion / Consequence

p is sufficient for q
q is necessary for p

A necessary condition for p is q

iff ($\leftrightarrow$)
(biconditional)

Scanned by CamScanner

A sufficient condition for q is p.

If p, then q ; If p, q ; q follows from p.

q if p
p only if q
q when p
q whenever p

Imp. $p \to q$

Contrapositive	$\neg q \to \neg p$
Inverse	$\neg p \to \neg q$
Converse	$q \to p$

Q State the converse, contrapositive and inverse of these conditional statements.

1. If it snows tonight, then I will stay at home.

Here p : it snows tonight
q : I will stay at home

Contrapositive ~~Inverse~~ If I won't stay at home then it ~~won~~ doesn't snow tonight.

Inverse If it won't snow tonight then I won't stay at home.

Converse If I stay at home then it will/may snow tonight.

2. I go to the beach whenever it is a sunny summer day.

Here p : it is a sunny summer day
q : I go to the beach

Teacher's Signature..............

Converse: If I go to the beach then it should be a sunny summer day.

Inverse: If it isn't a sunny summer day then I don't go to the beach.

Contrapositive: If I don't go to the beach then it may not be a sunny summer day.

OR

It isn't a sunny summer day whenever I do not go to the beach.

3. When I stay up late, it is necessary that I sleep until noon.

Here, p : I stay up late

q : I sleep until noon.

Converse: If I sleep until noon, then I must have stayed up late.

Inverse: If I do not stay up late, then I do not sleep until noon.

Contrapositive: If I do not sleep until noon, then I haven't stayed up late.

Compound Propositions

Two compound propositions are said to be equivalent if they have the same truth values.

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

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

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

Teacher's Signature ....

Biconditional / Bi-implication

Let p and q be two propositions, the biconditional statement $p \leftrightarrow q$ is the proposition "p iff q".

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

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$
T	T	T	T	T
T	F	F	~~F~~ T	F
F	T	T	F	F
F	F	T	T	T

Q. Let p and q be two propositions.

p : It is below freezing

q : It is snowing

Write these propositions using p and q and ~~co~~ logical connectives.

i) It is below freezing and snowing

$p \wedge q$

ii) It is below freezing and not snowing

$p \wedge \neg q$

iii) It is not below freezing and not snowing

$\neg p \wedge \neg q$

iv) It is either snowing or freezing (or both)

$p \vee q$

v) If it is below freezing, it is also snowing.

$p \to q$

vi) It is either below freezing or it is snowing, but it is not snowing if it is below freezing.

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

vii) That it is below freezing is necessary and sufficient for it to be snowing.

$p \leftrightarrow q$

Q Let p and q be the propositions.

p : You drive over 65 miles per hour

q : You get a speeding ticket

Write these propositions using p and q and logical connectives.

i) You don't drive over 65 miles per hour.

$\neg p$

ii) You drive over 65 miles / hour but you don't get a speeding ticket.

$p \wedge \neg q$

iii) You will get a speeding ticket if you drive over 65 miles / hour.

$p \rightarrow q$

iv) If you do not drive over 65 miles / hour then you do not get a speeding ticket.

$\neg p \rightarrow \neg q$

v) Driving over 65 miles / hour is sufficient for getting a speeding ticket.

$p \rightarrow q$

vi) Whenever you get a speeding ticket, you are driving over 65 miles per hour.

~~p~~ ~~q~~ : 65 miles per hour

q ~~p~~ : You get a speeding ticket

$q \rightarrow p$

Precedance Rule

$\exists, \forall$

1 $\neg$

2 $\wedge$

3 $\vee$

4 $\rightarrow$

5 $\leftrightarrow$

Q Construct the truth table for the following.

1. $(p \to q) \vee (\neg p \to q)$

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

2. $(p \to q) \wedge (\neg p \to r)$

p	q	$p \to q$	$\neg p$	r	$\neg p \to r$
T	T	T	F		
T	F	F	F		
F	T	T	T		
F	F	T	T		

×

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

Q Let p, q and r be the propositions.

p: You have flu

q: You miss the final examination

r: You pass the course

Express each of these as a

1. $p \to q$

If you have flu, then you will miss the final exam.

2. $\neg q \leftrightarrow r$

You will pass the course iff you don't miss the final exam.

3. $q \to \neg r$

If you ~~pass~~ miss the final exam then you won't pass the course.

4. $p \vee q \vee r$

You have flu or miss the final exam or you pass the course.

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

If you have flu or if you ~~pass~~ miss the final exam, you will not pass the course.

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

If you have flu and you miss the final exam or ~~if~~ you don't miss the final exam or you pass the course

Propositional Equivalences

Tautology

A compound proposition that is always true no matter what the truth values of the proposition that occur in it is considered tautology.

ex $p \vee \neg p$

Contradiction

A compound proposition which is always false.

ex $p \wedge \neg p$

Contingency

It is neither a tautology nor a contradiction.

Logical Equivalences : Two compound propositions (x, y) are said to be logically equivalent if $x \leftrightarrow y$ is a tautology.

ex Let $x : p \leftrightarrow q$

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

x	y	$x \leftrightarrow y$
T	T	T
F	F	T
F	F	T
T	T	T

Laws

1. De - Morgan's Law

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

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

2. Commutative Law

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

$p \wedge q \equiv q \wedge p$

3. Associative Law

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

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

4. **Distributive Law**

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

5. **Dominance Law**

$$p \vee T \equiv T$$
$$p \wedge F \equiv F$$

6. **Identity Law**

$$p \wedge T \equiv p$$
$$p \vee F \equiv p$$

7. **Idempotent Law**

$$p \vee p \equiv p$$
$$p \wedge p \equiv p$$

8. **Negation Law**

$$p \vee \neg p \equiv T$$
$$p \wedge \neg p \equiv F$$

9. **Double Negation Law**

$$\neg(\neg p) \equiv p$$

10. **Absorption Law**

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

Absorption Law

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

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

Q. Prove i) $p \to q \equiv \neg p \vee q$

ii) $p \to q \equiv \neg q \to \neg p$

p	q	$p \to q$	$\neg p$	$\neg p \vee q$	$\neg q \to \neg p$
T	T	T	F	T	T
T	F	F	F	F	F
F	T	T	T	T	T
F	F	T	T	T	T

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

Q. What is the negation of "If you work hard, you will pass the exam".

You work hard and you don't pass the exam.

★ DON'T USE IF-THEN IN THIS CASE. USE ONLY WHEN ($\to$) IS THERE.

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

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

Q. Show that ~~negation of~~ $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$

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

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

$\equiv \neg p \wedge (p \wedge \neg q)$ (Double Negation Law, De-Morgan's Law)

$\equiv (\neg p \wedge p) \wedge \neg q$ (Associative Law)

$\equiv F \wedge \neg q$

$\equiv \neg(T \vee q) \neq \neg T = F$

Teacher's Signature.........

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

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

$\equiv \neg(T \wedge (p \vee q)) \equiv \neg(p \vee q)$ (Idempotent, Identity, Dominance)

$\equiv \neg p \wedge \neg q$

(Hence, proved)

Q Prove that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology

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

$\equiv \cancel{(p \wedge q) \rightarrow} \neg(p \wedge q) \vee (p \vee q)$

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

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

$\equiv T \vee T$

$\equiv T$

Q Show that $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$

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

$\equiv (\neg p \vee q) \vee (\neg p \vee r)$ ($\because x \rightarrow y \equiv \neg x \vee y$)

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

$\equiv \neg(p \wedge p) \vee (q \vee r)$ (De Morgan's Law)

$\equiv \neg p \vee (q \vee r)$ (Idempotent Law)

$\equiv p \rightarrow (q \vee r)$ (R.H.S.)

Q Prove that $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ is tautology

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

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

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

$\equiv (\neg p \wedge r) \vee F \longrightarrow (\neg p \vee r)$

$\equiv (\neg p \wedge r) \longrightarrow (\neg p \vee r)$

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

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

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

$\equiv T \vee T \equiv T$

Scanned by CamScanner

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

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

$\equiv \neg(T \wedge (p \vee q)) \equiv \neg(p \vee q)$ (Idempotent / Identity / Domination)

$\equiv \neg p \wedge \neg q$

(Hence, proved)

Q Prove that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology

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

$\equiv \cancel{(p \wedge q) \rightarrow}\ \neg(p \wedge q)\ \vee\ (p \vee q)$

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

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

$\equiv T \vee T$

$\equiv T$

Q Show that $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$

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

$\equiv (\neg p \vee q) \vee (\neg p \vee r)$ $(\because x \rightarrow y \equiv \neg x \vee y)$

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

$\equiv \neg(p \wedge p) \vee (q \vee r)$ (De Morgan's Law)

$\equiv \neg p \vee (q \vee r)$ (Idempotent Law)

$\equiv p \rightarrow (q \vee r)$ (R.H.S.)

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

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

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

$\equiv (\neg p \vee F) \vee (\neg p \vee q \wedge r) \rightarrow (p \rightarrow r)$ (Negation)

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

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

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

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

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

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

$\equiv (T \wedge \neg q \vee \neg r) \vee r$ (Negation)

$\equiv \neg q \vee (\neg r \vee r)$ (Identity)

$\equiv \neg q \vee T$ (Negation)

$\equiv T$ (Dominance)

$\rightarrow r) \rightarrow (p \rightarrow r)$ is tautolog

p	q	r	A: $p \to q$	B: $q \to r$	$A \wedge B$	C: $p \to r$	$(A \wedge B) \to r$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Q $(p \to q) \to r \not\equiv p \to (q \to r)$ Prove

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

Q What is the truth value of $(p \to q) \wedge \bar{q}$ when
p - T & q - T F

Q What is the truth value of $(\neg p \vee \neg q) \to q$ if $p \to q$

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

T F

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

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

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

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

$\equiv T \wedge F \equiv F$

(Ans.)

Q Write the inverse, converse and contrapositive of "We will go for movie if it doesn't rain or we do not go swimming".

Here, $(\neg p \rightarrow q) \vee (\neg r)$

p: It rains

q: We will go for movie

r: We ~~do not~~ go swimming

"If it does not rain, or we do not go swimming then we will go for movie."

p: It does not rain

q: We do not go swimming

r: We will go for movie

$(p \vee q) \rightarrow r$

Contrapositive: $\neg r \rightarrow \neg(p \vee q) \equiv \neg r \rightarrow (\neg p \wedge \neg q)$

If we do not go for movie then it should rain and we should go swimming.

Converse If we go for movie then neither will it rain nor would we go swimming.

Inverse If we go swimming and it rains then we should not go for movie.

Q What is the contrapositive of "If the flood destroys my house or the fire destroys my house, then the insurance company will pay me."

$(p \vee q) \rightarrow r$

Here p: flood destroys my house

q: fire destroys my house

r: insurance company will pay me

CONTRAPOSITIVE If the insurance company will not pay me then the flood and fire will not destroy my house.

Teacher's Signature.............

Predicates and Quantifiers

Predicate: It is a part of the statement which describes the behaviour of the object or the relationship among them.

Domain of discourse / universe of discourse : Domain of the subject.

ex • $P(x)$: $\underbrace{x}_{\text{sub.}}$ $\underbrace{\text{is a student of this class.}}_{\text{predicate}}$

where $x \in$ ~~stu~~ people — domain of discourse

• $Q(x)$: $x \geq 5$ where $x \in Z$

$Q(0)$: F $\longrightarrow$ PROPOSITION

★ Giving value to statement's subject part makes it proposition.

• $R(x,y,z)$: $x+y=z$

Q $Q(x,y)$: $x = y+3$.

What are the truth values of the propositions

$Q(1,2)$: F

$Q(3,0)$: T

Q $R(x,y,z)$: $x+y=z$

$R(1,2,3) \equiv$ T

$R(0,0,1) \equiv$ F

★ $P(x_1, x_2, x_3, \ldots x_n)$ is called the propositional function P having n numbers or n-ary predicate or n-place predicate.

Teacher's Signature..................

Universal Quantification : The universal quantification of $P(x)$ is the statement "$P(x)$ for all values of x" in the domain.

$\forall$: universal quantifier

Existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$".

Q Let $P(x)$ be the statement $P(x): x+1 > x$. What is the truth value of $P(x)$ where the domain consists of all real numbers.

$\forall x\, P(x)$ is true.

Q What is the truth value for (i) $\exists x\, P(x)$ where $P(x)$ is the statement $x^2 < 10$ and the domain consists of positive integers not exceeding 4.

Here, $x = 1, 2, 3, 4$.

$P(1): 1 < 10$ (T), $P(2): 4 < 10$ (T),

$P(3): 9 < 10$ (T), $P(4): 16 \nless 10$ (F)

(i) $P(1) \vee P(2) \vee P(3) \vee P(4) \equiv T \vee T \vee T \vee F$

$\equiv T$.

(ii) $\forall x\, P(x)$

$P(1) \wedge P(2) \wedge P(3) \wedge P(4) \equiv T \wedge T \wedge T \wedge F$

$\equiv F$

$$\boxed{\begin{aligned} \neg(\forall x\, P(x)) &\equiv \exists x(\neg P(x)) \\ \neg(\exists x\, P(x)) &\equiv \forall x(\neg P(x)) \end{aligned}}$$

→ DE MORGAN'S LAW FOR QUANTIFIERS

~~Ex $\neg(P(1) \wedge P(2) \wedge \ldots P(10)) \equiv \neg P(1) \vee \neg P(2) \vee \ldots \neg P(10)$~~

Teacher's Signature ....

Q Let $P(x): x = x^2$. If the domain consists of integers, what are the truth values of

a> $P(0)$ T
b> $P(1)$ T
c> $P(-1)$ F
d> $P(2)$ F
e> $\exists x\, P(x)$ T
f> $\forall x\, P(x)$ F

Q Domain consists of all real numbers.

a> $\exists x\,(x^3 = -1)$ T
b> $\exists x\,(x^4 < x^2)$ T
c> $\forall x\,((-x)^2 = x^2)$ T
d> $\forall x\,(2x > x)$ F

Q What do these statements mean for all real no.s?

a> $\forall x < 0\ (x^2 > 0)$
The square of a negative number is always positive

b> $\forall y \neq 0\ (y^3 \neq 0)$
The cube of a non-zero number is always non-zero

c> $\exists x > 0\ (x^2 = 2)$
There exists a positive square root of 2.

Uniqueness quantifier: $\exists!\, x P(x)$

$$\exists \underset{\substack{\downarrow \\ \text{bound}}}{x}\ \underbrace{(x + y = 5)}_{\text{scope}}$$

y = free (here)

Prove the De-Morgan's law for quantifiers

i> $\neg(\forall x P(x)) \equiv \exists x(\neg P(x))$

$\neg(\forall x P(x))$ is T

$\Leftrightarrow$ $\forall x P(x)$ is F $\quad (P(x_1) \wedge P(x_2) \wedge \dots P(x_n) \equiv F)$

$\Leftrightarrow$ $P(x_i)$ is F for some x_i

$\Leftrightarrow$ $\neg P(x_i)$ is T for some x_i

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

ii> $\neg(\exists x P(x)) \equiv \forall x(\neg P(x))$

$\neg(\exists x P(x))$ is T

$\Leftrightarrow$ $\exists x P(x)$ is F

$\Leftrightarrow$ $P(x_i)$ is F for ~~some~~ all x_i

$\Leftrightarrow$ $\neg P(x_i)$ is T for ~~some~~ all x_i

$\Leftrightarrow$ $\forall x(\neg P(x))$ is T

Imp Q Show that $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$

$\forall$: for each, for any

$\forall x(P(x) \wedge Q(x))$ is T

$\Leftrightarrow$ $(P(x_1) \wedge Q(x_1)) \wedge (P(x_2) \wedge Q(x_2)) \dots$ is T

$\Leftrightarrow$ $P(x_i) \wedge Q(x_i)$ is T for any x_i

$\Leftrightarrow$ $P(x_i)$ is T for each x_i and

$\Leftrightarrow$ $Q(x_i)$ is T for all x_i

$\Leftrightarrow$ $(\forall x P(x)) \wedge (\forall x Q(x))$ is T

Q $\exists x(P(x) \wedge Q(x)) \not\equiv (\exists x P(x)) \wedge (\exists x Q(x))$. Prove

Let $\exists x(P(x) \wedge Q(x))$ be T for some x.

$\Rightarrow$ $[P(x_1) \wedge Q(x_1)] \vee [P(x_2) \wedge Q(x_2)] \vee \dots$ is T.

$\Rightarrow$ $[P(x_1) \vee P(x_2) \vee P(x_3) \vee \dots] \wedge [Q(x_1) \wedge Q(x_2) \wedge \dots]$ is T

$\Rightarrow$ $P(x_i)$ is T for some x_i $\wedge$ $Q(x_i)$ is T for any x_i

$\Rightarrow$ $(\exists x P(x)) \wedge (\forall x Q(x))$ is T

$\not\equiv$ $(\exists x P(x)) \wedge (\exists x Q(x))$.

Teacher's Signature..........................

$\forall x(P(x) \vee Q(x)) \not\equiv (\forall x P(x)) \vee (\forall x Q(x))$

$\forall x(P(x) \vee Q(x))$ is T

$\Rightarrow (P(x_1) \vee Q(x_1)) \wedge (P(x_2) \vee Q(x_2)) \ldots$ is T

$\Rightarrow P(x_i) \vee Q(x_i)$ is T for any x_i

$\Rightarrow \neg(P(x_i) \vee Q(x_i))$ is F for any x

$\Rightarrow \forall x(\neg P(x))$ is F ~~and~~ or $\forall x(\neg Q(x))$ is F

$\not\equiv (\forall x(P(x)) \vee (\forall x Q(x))$

Imp. $\exists x(P(x) \vee Q(x)) \equiv (\exists x P(x)) \vee (\exists x Q(x))$

$\exists x(P(x) \vee Q(x))$ is T. for some x.

$\Leftrightarrow (P(x_1) \vee Q(x_1)) \vee (P(x_2) \vee Q(x_2)) \vee \ldots$ is T

$\Leftrightarrow [P(x_1) \vee P(x_2) \vee P(x_3) \ldots] \vee [Q(x_1) \vee Q(x_2) \vee Q(x_3) \vee \ldots]$ is T

$\Leftrightarrow P(x_i) \vee Q(x_i)$ is T for some x_i.

$\Leftrightarrow (\exists x P(x)) \vee (\exists x Q(x))$ is T.

Q Write the negations of i> $\forall x(x^2 > x)$

ii> $\exists x(x^2 = 2)$

i> $\neg(\forall x(x^2 > x)) \equiv \exists x(\neg(x^2 > x))$

$\equiv \exists x(x^2 \leq x)$

ii> $\neg(\exists x(x^2 = 2)) \equiv \forall x(\neg(x^2 = 2))$

$\equiv \forall x(x^2 \neq 2)$

Q Express the statement "Every student in this class has studied calculus using predicates and quantifiers".

$S(x)$: x is a student of this class

$T(x)$: x has studied calculus

Hence, $\forall x(S(x) \wedge T(x))$ X → NOT VALID

$\forall x(S(x) \rightarrow T(x))$ (Ans.)

Not every person in world is a student of this class

Teacher's Signature...

Q Express the statements using quantifiers and predicates.

1. "Some student in this class has visited Mexico".
2. "Every student in this class has visited Canada or Mexico".

$M(x)$: x has visited Mexico

$C(x)$: x has visited Canada

$P(x)$: x is a student of this class.

i> $\exists x\,(P(x) \land M(x))$

ii> $\forall x\,(P(x) \rightarrow (M(x) \lor C(x)))$.

★ With $\exists$ don't use $\rightarrow$, use $\land$ instead. Because in $\rightarrow$ case, (F, T) case also becomes F which means even if $P(x)$ is F in $P(x) \rightarrow Q(x)$, the result will be F which is not valid.

★ With $\forall$, use $\rightarrow$.

Q Translate each of these statements using logical expression using predicates, quantifiers and logical connectives.

1. No one is perfect
2. Not everyone is perfect
3. All your friends are perfect
4. At least one of your friend is perfect
5. Everyone is your friend and is perfect
6. Not everyone is your friend or someone is not perfect

Ans $P(x)$: x is perfect

$F(x)$: x is your friend

2. $\neg(\forall x\, P(x)) \equiv \exists x\,(\neg P(x))$

1. $\forall x\,(\neg P(x))$

3. $\forall x\,(F(x) \rightarrow P(x))$

4. $\exists x\,(F(x) \land P(x))$

5. $\forall x\,(F(x) \land P(x))$

6. $\neg(\forall x\,(F(x))) \lor (\exists x\,(\neg P(x)))$

$\equiv \exists x\,(\neg F(x)) \lor \exists x\,(\neg P(x))$

$\equiv \exists x\,(\neg F(x) \lor \neg P(x))$

Teacher's Signature.........

Q Translate these statements into English.

$C(x)$: x is a comedian

$F(x)$: x is funny

Domain consists of all people.

a) $\forall x\,(C(x) \rightarrow F(x))$

Every comedian is funny.

b) $\forall x\,(C(x) \wedge F(x))$

Everyone is a comedian and funny

c) $\exists x\,(C(x) \rightarrow F(x))$

There is a person such that ~~Some comedians are~~ if he/she is comedian, he(s) is funny.

d) $\exists x\,(C(x) \wedge F(x))$

There exists someone who is a comedian & funny.

OR

Some comedians are funny.

Q Suppose that the domain of the propositional functi P(x) consists of the integers 1, 2, 3, 4, 5, express these statements without using quantifiers, instead using only negation, conjunction and disjunctions

1. $\exists x\, P(x)$

$P(1) \vee P(2) \vee P(3) \vee P(4) \vee P(5)$

2. $\forall x\, P(x)$

$P(1) \wedge P(2) \wedge P(3) \wedge P(4) \wedge P(5)$

3. $\neg \exists x\, P(x) \equiv \forall x\,(\neg P(x))$

$\neg(P(1) \vee P(2) \vee P(3) \vee P(4) \vee P(5))$

Teacher's Signature..............

iv) $\neg \forall x\, P(x) \equiv \exists x (\neg P(x))$

$\neg (P(1) \wedge P(2) \wedge P(3) \wedge P(4) \wedge P(5))$

v) $\forall x (x \neq 3 \rightarrow P(x)) \vee (\exists x\, \neg P(x))$

$(P(1) \wedge P(2) \wedge P(4) \wedge P(5)) \vee (\neg P(1) \vee \neg P(2) \vee \neg P(3)$
$\vee \neg P(4) \vee \neg P(5))$

Q Show that $\neg \forall x (P(x) \longrightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x))$

Let $\neg \forall x (P(x) \rightarrow Q(x))$ be T.

$\Leftrightarrow$ $\exists x \neg (P(x) \rightarrow Q(x))$ is T (D.M. Law)

$\Leftrightarrow$ $\exists x (P(x) \wedge \neg Q(x))$ is T ($\because \neg(p \rightarrow q) \equiv p \wedge \neg q$)

Nested Quantifiers

Two quantifiers are said to be nested, if one lies within the scope of the other.

ex $\forall x (\forall y (x + y = y + x))$

Imp. $\forall x\, \exists y (x + y = 5)$ TRUE

$\exists x\, \forall y (x + y = 5)$ FALSE

$\hookrightarrow$ Let $x = 10$, for any $y \Rightarrow y = 5$ (say)

$\therefore$ $x + y = 10 + 5 \neq 5$. FALSE.

Hence, order in which the quantifiers appear in nested case is important.

Q $Q(x, y, z)$: "$x + y = z$",

i) $\forall x\, \forall y\, \exists z\, Q(x, y, z)$ T

ii) $\exists z\, \forall x\, \forall y\, Q(x, y, z)$ F

Q 1. The sum of two positive integers is always positive.

$\forall x\, \forall y (((x > 0) \wedge (y > 0)) \longrightarrow (x + y > 0))$

2. $\forall x \forall y\,((x>0) \wedge (y<0) \rightarrow (xy<0))$
The product of a positive and negative real number is negative.

Q "The difference of two negative integers is not necessarily negative". Translate it using predicates, quantifiers and connectives.
~~Let~~ $\exists x\, \exists y\, ((x<0) \wedge (y<0) \wedge \neg(x-y<0))$
$\equiv \quad \exists x\, \exists y\, ((x<0) \wedge (y<0) \wedge (x-y \geq 0))$

Expl^n "The diff. of two negative integers is negative."
$\forall x \forall y\, ((x<0) \wedge (y<0) \rightarrow (x-y<0))$
The negation of the above statement is the question
$\therefore \quad \neg(\forall y \forall x\, ((x<0) \wedge (y<0)) \rightarrow (x-y<0))$
$\equiv \quad \exists x \exists y\, ((x<0) \wedge (y<0) \wedge \neg(x-y<0))$

Q i) Translate 'Every real number except 0 has a multiplicative inverse.'
$\forall (x - \{0\})\, (x\ \cancel{\wedge y} \rightarrow (xy=1))$
$\exists y$)

A multiplicative inverse of a real number x is y such that $xy=1$.

$\forall x\, \exists y\, ((x \neq 0)\ \cancel{\wedge y} \rightarrow xy=1)$

ii) $\forall x\, (C(x) \vee \exists y\, (C(y) \wedge F(x,y)))$
$C(x)$: x has a computer
$F(x,y)$: x & y are friends.
Everyone has a computer or has a friend who has a computer.

Teacher's Signature.............

iii> Express this statement, "If a person is a female and is a parent, then this person is someone's mother"

$F(x)$: Person is female

$P(x)$: Person is parent

$M(x,y)$: Person is someone's mother

~~$F(x) \wedge P(x) \longrightarrow M(x)$~~

$\forall x \, (F(x) \wedge P(x) \longrightarrow \exists y \, (M(x,y)))$

$\longrightarrow$ $M(x,y)$: x is the mother of y.

iv> "There is a woman who has taken a flight on every airline in the world."

v> $\neg(i)$

$\neg \left(\forall x \, \exists y \, (x \neq 0 \longrightarrow xy = 1) \right)$

$\equiv \quad \forall y \, \exists x \, ((x \neq 0) \wedge (xy \neq 1))$

Limit : Every thing converging to one point.

vi> $\neg(\forall (\epsilon > 0) \, \exists (\delta > 0) \, (0 < |x-a| < \delta \longrightarrow |f(x) - L| < \epsilon)$

(definition of limit)

$\equiv \quad \exists (\epsilon > 0) \, \forall (\delta > 0) (0 < |x-a| < \delta \ \wedge \ |f(x) - L| \geq \epsilon$

Express each of these statements using predicates, quantifiers and logical connectives.

1. The product of two negative R no.s is positive.
2. The difference of a real no. and itself is 0.
3. A negative real no doesn't have a square root that is a real no.

1. $\forall x \, \forall y \, (x < 0 \ \wedge \ y < 0 \longrightarrow xy > 0)$
2. $\forall x \, \forall y \, (x = y \ \wedge \ x - y \longrightarrow 0)$ or $\forall x (x - x = 0$
3. ~~$\forall x \, \forall y \, (x < 0 \ \wedge \ \sqrt{x} \longrightarrow \neg y)$~~

3. $\forall (x < 0) \longrightarrow \neg (\exists y \, (y^2 = x))$

Ans iv) "There is a woman who has taken a flight on every airline in the world."

Let $W(x)$: x is a woman

$F(x)$: x has taken a flight

$A(x,y)$: x has travelled in airline y.

$\exists x \forall y \, (W(x) \wedge F(x) \wedge A(x,y))$

Q Express these mathematical statements using....

1. $\exists x \forall y \, (xy = y)$

The product of two real numbers may be equal to any one of those two numbers in some cases.

OR

There exists a multiplicative identity for all real numbers.

2. $\exists x \exists y \, ((x^2 > y) \wedge (x < y))$

There exist real numbers x and y such that $x^2 >$ but $x < y$.

3. $\forall x \forall y \exists z \, (x + y = z)$

The sum of any two real numbers there exist a particular element z.

Rules of Inference

	Rule of Inference	Tautology	Name
1.	p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
2.	$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
3.	$p \to q$ $q \to r$ $\therefore p \to r$	$(p \to q) \wedge (q \to r)$ $\to (p \to r)$	Hypothetical Syllogism
4.	$\neg p$ $p \vee q$ $\therefore q$	$\neg p \wedge (p \vee q) \to q$	Disjunctive Syllogism
5.	p $\therefore p \vee q$	$p \to p \vee q$	Addition
6.	$p \wedge q$ $\therefore p$ $\therefore q$	$(p \wedge q) \to p$ $(p \wedge q) \to q$	Simplification
7.	p q $\therefore p \wedge q$	$(p) \wedge (q) \to p \wedge q$	Conjunction
8.	$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$(p \vee q) \wedge (\neg p \vee r)$ $\to q \vee r$	Resolution

Argument : An argument is a sequence of propositions.

* All but the final propositions are called premises and the final proposition is called conclusion.
* An argument is valid ~~in particular~~ if no matter ~~what pro~~ which particular proposition ~~is~~ are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true. If it is not valid then it is called as fallacy.

Q "If it snows today, then we will go skiing." Suppose that the above conditional statement and its hypothesis "It is snowing today" are true. Show if the conclusion "We will go skiing." true.

p : It snows today
q : we will go skiing

① $p \to q$ (premise)
② p (premise)
③ q (Modus ponens using ① and ②)

Q Determine whether the argument given here is valid and determine whether its conclusion must be true because of the validity of the argument
" If $\sqrt{2} > 3/2$, then $(\sqrt{2})^2 > (3/2)^2$ "
We know that $\sqrt{2} > 3/2$
Consequently, $(\sqrt{2})^2 = 2 > (3/2)^2 = 9/4$

p : $\sqrt{2} > 3/2$ ~~(premise)~~
q : $(\sqrt{2})^2 > (3/2)^2$

1. $p \to q$ (premise) (F)
2. p (premise)
3. q (modus ponens using 1 & 2)

The argument is valid but the conclusion is false because ~~it~~ one of the premises itself is F.

Q Show that the hypotheses

1 "If I get the job and work hard, then I will get promoted."

2 "If I get promoted, then I will be happy."

3 "I will not be happy"

imply the conclusion "Either I will not get the job or I will not work hard."

p: I get a job

q: I work hard

r: I will get promoted

s: I will be happy

1. $(p \wedge q) \to r$ (premise)
2. $r \to s$ (premise)
3. $(p \wedge q) \to s$ (Hypothetical Syllogism using 1 & 2)
4. $\neg s$ (premise)
5. $\neg(p \wedge q)$ (Modus tollens using 3 & 4)
6. $\neg p \vee \neg q$ (De-Morgan's law for 5) (conclusion)

Hence, the argument is a valid argument.

Q Is the following argument valid?

"If you do every problem in this book, then you will learn DM".

"You learned DM."

"Therefore you did every problem in this book."

Ans p: You do every problem in this book

q: You ~~will~~ learn discrete mathematics

1. $p \to q$ (premise)
2. q (premise)
3. p (conclusion)

The conclusion is not true, hence this is a fallacy

Q Show that the hypotheses $(p \wedge q) \vee r$, $r \to s$ imply the conclusion $p \vee s$.

1. $(p \wedge q) \vee r$ (hypothesis)
2. $r \to s$ (hypothesis)
3. ② $\equiv$ $\neg r \vee s$
4. $(p \wedge q) \vee s$ (resolution of ① and ③)
5. $\equiv (p \vee s) \wedge (q \vee s)$ (distributive law)
6. $(p \vee s)$ (simplification of ⑤)

Q Show that the hypotheses

i) "It is not sunny this afternoon and it is colder than yesterday."

ii) "We will go swimming only if it is sunny."

iii) "If we do not go swimming, then we take a canoe trip"

iv) "If we take a canoe trip, then we will be home by sunset"

lead to the conclusion "We will be home by sunset".

p: It is sunny this afternoon

q: It is colder than yesterday

r: We go swimming

s: We take a canoe trip

t: We will be home by sunset.

1. $\neg p \wedge q$ (premise)
2. $r \to p$ (premise)
3. $\neg r \to s$ (premise)
4. $s \to t$ (premise)
5. $\neg p$ (Simplification of 1)
6. $\neg r$ (Modus tollens of 5 and 2)
7. s (Modus ponens of 3 and 6)
8. t (Modus ponens of 4 and 7)

Q Show that the hypotheses i> "If you send me an email message, then I will finish writing program."

ii> "If you do not send me email message, then I will go to sleep early."

iii> "If I go to sleep early, then I will wake up feeling refreshed." lead to the conclusion "If I do not finish writing the program, I will wake up feeling refreshed."

p : You send me an email message

q : I finish writing program.

r : I sleep early

s : I wake up feeling refreshed.

1. $p \to q$ (premise)
2. $\neg p \to r$ (premise) $\neg q \to$
3. $r \to s$ (premise)
4. $\neg q \to \neg p$ (contrapositive of 1)
5. $\neg q \to r$ (Hypothetical syllogism of 2 and 4)
6. $\neg q \to s$ (" " of 3 and 5)

Q Use rules of inferences to provide a formal proof for the following argument.

Teacher's Signature..................

$\bar{a} \to (b \to \bar{c})$

$\bar{a} \vee d$

$\bar{x} \to b$

$\bar{d}$

$\therefore c \to x$

Sol

$\neg a \to (b \to \neg c)$ (premise)

$\equiv \neg(b \to \neg c) \to \neg(\neg a)$

① $\equiv (b \wedge c) \to a$

② $\neg a \vee d \equiv a \to d$ (premise)

③ $\neg x \to b$ (premise)

~~4~~ $a \to \neg x$ (Hypothetical syllogism of ② & ③)

⑤ $\neg d$ (premise)

⑥ $(b \wedge c) \to d$ (Hypothetical syllogism of ① & ②)

⑦ $\neg(b \wedge c)$ (Modus tollens of ⑤ & ⑥)

$\equiv b \vee \neg c$ (negation rule)

~~8~~ $\neg x \to (b \wedge c)$ (Hypothetical syllogism of ③ & ⑥)

$\equiv x \vee (b \wedge c)$

$\equiv (x \vee b) \wedge (x \vee c)$

---

① $\neg a \vee d$ (premise)

② $\neg d$ (premise)

③ $\neg a$ (Disjunctive syllogism of ① and ②)

④ $\neg a \to (b \to \neg c)$

$\equiv a \vee (b \to \neg c)$ ($\because p \to q \equiv \neg p \vee q$)

⑤ $b \to \neg c$ (Disjunctive syllogism of ③ and ④)

$\equiv \neg b \vee \neg c$ ($\because$

⑥ $\neg x \to b \equiv x \vee b$ ~~$x \vee \neg b$~~ $\neg b \to x$ (contrapositive)

⑦ $\neg c \vee x$ (resolution)

8 $\equiv c \to x$ (~~contrapositive of ⑦~~)

Determine whether the following argument is valid using rules of inference.

"If I graduate this semester, then I will have passed the physics course."

"If I do not study physics for 10 hours a week, then I won't pass physics."

"If I study physics for 10 hours a week, then I cannot play cricket."

"Therefore, if I play cricket, I will not graduate this semester."

Let p : I graduate this semester

q : I pass the physics course

r : I study physics for 10 hours a week

s : I play cricket

1. $p \rightarrow q$ (Premise)
2. $\neg r \rightarrow \neg q$ (Premise)
3. $r \rightarrow \neg s$ (Premise)
4. $\neg q \rightarrow \neg p$ (contrapositive of 1)
5. $\neg r \rightarrow \neg p$ (Hypothetical Syllogism of 2 & 4)
6. $r \vee \neg p$ ($\because a \rightarrow b \equiv \neg a \vee b$, using 5)
7. $\neg r \vee \neg s$ (using 3)
8. $\neg s \vee \neg p$ (Resolution of 6 & 7)
9. $s \rightarrow \neg p$ ($\because \neg a \vee b \equiv a \rightarrow b$, using 8)

Hence, the given conclusion is valid.

Rules of inference for Quantified statements

Rule of inference	Name
1. $\forall x\, P(x)$ $\therefore\ P(a)$	Universal Instantiation
2. $P(a)$ for arbitrary a $\therefore\ \forall x\, P(x)$	Universal Generalization
3. $\exists x\, P(x)$ $\therefore\ P(a)$ for some a	Existential Instantiation
4. $P(a)$ for some a $\therefore\ \exists x\, P(x)$	Existential Generalisation

Q Determine whether the argument is valid.
"All students in this class understand logic."
"Mandy is a student of this class."
"Therefore Mandy understands logic."

$P(x)$: x is a student of this class
$Q(x)$: x understands logic

i $\forall x(P(x) \rightarrow Q(x))$ (Premise)
ii $P(\text{Mandy})$ (Premise)
iii $P(\text{Mandy}) \rightarrow Q(\text{Mandy})$ (Universal Instantiation)
iv) $Q(\text{Mandy})$ (Modus ponens of iii and ii)

Q Show that the premises
"A student in this class has not read the book."
"Everyone in this class passed the first exam."
imply the conclusion
"Someone who passed the first exam has not read the book."

$P(x)$: x is a student of this class
$Q(x)$: x has not read the book
$R(x)$: x passed the ~~exo~~ first exam.

1 $\exists x\,(P(x) \wedge Q(x))$ (Premise)
2 $P(a) \wedge Q(a)$ for some a (Existential Instantiation of 1)
3 $\forall x\,(P(x) \rightarrow R(x))$ (Premise)
4 $P(a) \longrightarrow R(a)$ (Universal Instantiation using 3)
5 $P(a), Q(a)$ (Simplification of 2)
6 $R(a)$ (Modus ponens using 4 and 5)
7 $Q(a) \wedge R(a)$ (Conjunction using 6 and 7)
8 $\exists x.\,(Q(x) \wedge R(x))$ (Existential generalisation using 4).

If the order of premises in question is altered, then $\forall x$ appears before $\exists x$. In this case 4 can not be concluded. As a chosen for $\forall x$ is arbitrary, it may or ~~one~~ may not be true for $\exists x$ case. Hence in such cases, always consider $\exists x$ before $\forall x$.

Q Check the validity of the arguments.
"Everyone in New Jersey lives within 50 miles of the ocean"
i & ii) "Someone in New Jersey has never seen the ocean."
"Therefore, someone who lives within 50 miles of the ocean has never seen the ocean."

$P(x)$: x lives ~~within 50 miles of ocean~~ in NJ
$Q(x)$: x lives within 50 miles of ocean
$R(x)$: x has never seen ocean

3 $\forall x\,(P(x) \rightarrow Q(x))$ (premise)
4 $P(a) \rightarrow Q(a)$ (universal instantiation using 3)
1 $\exists x\,(P(x) \wedge R(x))$ (premise)
2 $P(a) \wedge R(a)$ for some a
(existential instantiation using 1)

5 $R(a), P(a)$ (Simplification of 2)
6 $Q(a)$ (Modus ponens using 4 and 5)
7 $Q(a) \wedge R(a)$ (Conjunction using 6 & 7)
8 $\exists x \, (Q(x) \wedge R(x))$
(Existential generalisation of 7)

Basic rules of inference for quantified statements

	Rules	Name
1	$\forall x \, (P(x) \rightarrow Q(x))$ $P(a)$ $\therefore Q(a)$	Universal Modus Ponens
2	$\forall x \, (P(x) \rightarrow Q(x))$ $\neg Q(x)$ $\therefore \neg P(x)$	Universal Modus Tollens

Assgn 22/8 1.5 → Q 9, 10, 13, 14, 15

Q Assume that " ~~for~~ $\forall$ positive integers n, if $n > 4$, then $n^2 <$ … is True. Show that $100^2 < 2^{100}$.

$P(n): n > 4$

$Q(n): n^2 < 2^n$

1 $\forall n \, (P(n) \rightarrow Q(n))$
$P(100)$
$Q(100)$ (universal modus ponens)
$\therefore$ the conclusion is true.

Introduction to Proofs

Give a direct proof of the theorem "if n is an ~~non~~ odd integer, then n^2 is odd."

$P(n)$: n is odd

$Q(n)$: n^2 is odd

If n is odd, $n = 2k+1$ where $k \in \mathbb{Z}$

$\Rightarrow n^2 = (2k+1)^2$

$\Rightarrow n^2 = 4k^2 + 4k + 1$

$\Rightarrow n^2 = 4(k^2+k)+1$ which is odd.

$\therefore n^2$ is odd.

Prove that if m and n are perfect squares, then nm is also a perfect square.

If m is a perfect square, $m = k_1^2$ where $k_1 \in \mathbb{Z}$

Similarly, for n, $n = k_2^2$, $k_2 \in \mathbb{Z}$.

$mn = k_1^2 \cdot k_2^2$

$\Rightarrow mn = (k_1 k_2)^2$

As k_1 and k_2 are integers, $\therefore k_1 k_2$ is also an intege

$\therefore$ mn is a perfect square.

Prove that if n is an integer and $3n+2$ is odd, then n is odd.

Taking the contrapositive of the given statement, "if n is even, then $3n+2$ is even."

If n is even, then $n = 2k$, $k \in \mathbb{Z}$.

$\Rightarrow 3n = 3(2k) = 6k$.

$\Rightarrow 3n+2 = 6k+2$

$\Rightarrow 3n+2 = 2(3k+1)$ is even.

Prove that if $n = ab$ where a & b are +ve integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Teacher's Signature......................

$(n = ab) \rightarrow ((a \le \sqrt{n}) \vee (b \le \sqrt{n}))$

$\equiv ((a > \sqrt{n}) \wedge (b > \sqrt{n})) \longrightarrow (n \ne ab)$

$\Rightarrow \quad ab > n \Rightarrow ab \ne n$

$p \rightarrow q$

p	q	$p \rightarrow q$
0	0	T
0	1	T
1	0	F
1	1	T

If p – F & $p \rightarrow q$ – T

VACUOUS PROOF

If q – T then $p \rightarrow q$ – T

Vacuous Proof

A proof of the conditional statement $p \rightarrow q$ that uses the fact that p is false is vacuous proof.

Trivial Proof

A proof of $p \rightarrow q$ that uses q is true is trivial proof

Show that the proposition $P(0)$ is true where
$P(n)$: "If $n > 1$, then $n^2 > n$" where $n \in \mathbb{Z}$.

$P(0)$: If $0 > 1$ then $0^2 > 0$

$p : 0 > 1$, $q : 0^2 > 0$

Since p is F, $p \rightarrow q$ is true using vacuous proof.

Let $P(n)$: "If a and b are positive integers with $a \ge b$, then $a^n \ge b^n$."

Prove that $P(0)$ is true.

$P(0)$: If $a \ge b$, then $\underbrace{a^0 \ge b^0}_{q}$ where $a, b \in \mathbb{Z}^+$

Here $q : a^0 \ge b^0$

q is T hence $(a \ge b) \rightarrow (a^0 \ge b^0)$ is true using trivial proof

Teacher's Signature..........

Prove that $\sqrt{2}$ is irrational.
Let $\sqrt{2}$ be rational.
Hence, let $\sqrt{2} = p/q$ for $p, q \in \mathbb{Z}$, $q \neq 0$, (p,q)-
Squaring both sides, $(\sqrt{2})^2 = (p/q)^2$

$$\Rightarrow \quad p^2/q^2 = 2$$
$$\Rightarrow \quad p^2 = 2q^2$$
$$\Rightarrow \quad p^2 \text{ is even}$$
$$\Rightarrow \quad p \text{ is even}$$
$$\Rightarrow \quad \text{if } p \text{ is odd, } p^2 \text{ is odd.}$$

Let $p = 2k+1$ for $k \in \mathbb{Z}$.
$\Rightarrow p^2 = (2k+1)^2 = 4k^2 + 2k + 1$ which is odd.
$\Rightarrow p^2 = 2(2k^2+k)+1 = 2r+1$ for $r = 2k^2+k$

$$(2k)^2 = 2q^2$$
$\Rightarrow q^2 = 2k^2 \Rightarrow q^2$ is even
$\Rightarrow q$ is even.
~~Ho~~ Therefore, p and q have a common factor 2.
$\therefore$ GCD of p and $q \neq 1$.
Hence, this is a contra~~positive~~diction.
$\therefore \sqrt{2}$ is irrational.

Q Prove by contradiction that if $3n+2$ is odd, n is odd
Assume, $p: (3n+2)$ is odd
$q:$ n is even
$\neg(p \rightarrow q) \equiv p \wedge \neg q$ (to prove)
Proof: If n is even, $n = 2k$, $k \in \mathbb{Z}$
$\Rightarrow 3n+2 = 3(2k)+2$
$\Rightarrow 3n+2 = 2(3k+1)$
$\Rightarrow 3n+2$ is even
- But it has been assumed that $3n+2$ is odd, which

is now contradicted.
Hence, for $3n+2$ to be odd, n is odd.

Q Prove the theorem "If n is a +ve integer, then n is odd iff n^2 is odd."

~~p : n is a positive integer~~

Assume
p: n is odd
q: n^2 is odd.

To prove $p \leftrightarrow q$

Proof $p \rightarrow q$

Let $n = 2k+1$, $k \in Z$

$\Rightarrow n^2 = 2(2k^2+k)+1$

$\Rightarrow n^2$ is odd.

$q \rightarrow p$

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

Hence, if n is even, $n = 2k$, $k \in Z$

$\Rightarrow n^2 = (2k)^2 = 2(2k^2)$

$\Rightarrow n^2$ is even.

$\therefore$ $q \rightarrow p$ is true as well.

Q Show that these statements about the integer n are equivalent.

$p1$: n is even

$p2$: $n-1$ is odd

$p3$: n^2 is even

Statements are equivalent means $p1 \rightarrow p2$, $p2 \rightarrow p3$, $p3 \rightarrow p1$.

Proof $p1 \rightarrow p2$

Let $n = 2k$, $k \in Z$

$\Rightarrow n-1 = 2k-1$ which is odd.

Teacher's Signature..................

$p2 \rightarrow p3$

Let $n-1 = 2k-1$ for $k \in \mathbb{Z}$

$\Rightarrow n = (2k-1)+1 = 2k$ which is odd.

$\Rightarrow n^2 = (2k)^2 = 2(2k)$ which is even.

$p3 \rightarrow p1 \equiv \neg p1 \rightarrow \neg p3$

Let n be odd $\Rightarrow n = 2k+1$, $k \in \mathbb{Z}$

$\Rightarrow n^2 = 2(2k^2+k)+1$ which is odd

Exhaustive Proofs

Some theorems can be proved by examining a relatively small number of examples. Such theorems' proofs are called exhaustive proofs.

Q Prove $(n+1)^3 \geq 3^n$ for n being a positive integer and $n \leq 4$.

This can be checked for $n = 1, 2, 3, 4$.

$n=1$	$(1+1)^3 \geq 3^1 \Rightarrow 2^3 \geq 3^1$	$\Rightarrow 8 \geq 3$	TRUE
$n=2$	$(2+1)^3 \geq 3^1$	$\Rightarrow 27 \geq 3$	TRUE
$n=3$	$(3+1)^3 \geq 3^1$	$\Rightarrow 64 \geq 3$	TRUE
$n=4$	$(4+1)^3 \geq 3^1$	$\Rightarrow 125 \geq 3$	TRUE

So by the method of exhaustive proofs, it is true.

Proof by Cases

Q Prove that if n is an integer, then $n^2 \geq n$.

CASE I $n=0$, $0^2 \geq 0$ is TRUE

CASE II $n<0$, $(-n)^2 \geq (-n) \Rightarrow n^2 \geq -n$ is TRUE

CASE III $n>0$, $n^2 \geq n$ is TRUE as square of every positive integer is greater than or equal to it.

Q Prove that $|xy| = |x||y|$ for $x, y \in \mathbb{R}$.

We know that $|a| = \begin{cases} a, & a > 0 \\ -a, & a < 0 \end{cases}$

CASE I $\quad x > 0, \; y > 0$

$|xy| = x \cdot y = |x| \cdot |y|$ is TRUE $(\because x = |x|)$

CASE II $\quad x > 0, \; y < 0$

$|xy| = x(-y) = -xy = |x||y|$

CASE III $\quad x < 0, \; y < 0$

$|xy| = (-x)(-y) = xy = |x||y|$ is TRUE.

CASE IV $\quad x < 0, \; y > 0$

$|xy| = (-x)y = |x||y|$

Existence Proofs $\quad \exists(x)\, P(x)$

Constructive $\qquad\qquad$ Non-constructive

An existence proof of $\exists x\, P(x)$ can be given by finding an element 'a' such that $P(a)$ is true. Such an existence proof is called constructive.

We can not find an element 'a' such that $P(a)$ is true but rather prove that $\exists x\, P(x)$ is true by some other way.

Q Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

$$1729 = 9^3 + 10^3$$
$$= 1^3 + 12^3$$

Q Show that there exist irrational numbers x and y such that x^y is rational.

Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Hence, $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$

$= (\sqrt{2})^2 = 2$

Let $x = \sqrt{2}$, $y = \sqrt{2}$ then $x^y = \sqrt{2}^{\sqrt{2}}$
If x^y is rational, then problem is solved.
But if x^y is irrational, then let $x = \sqrt{2}^{\sqrt{2}}$ & $y = \sqrt{2}$
which makes $x^y = 2$.

Q If x is rational and y is irrational, then x^y is irrational.
[Let $x = 5$ and $y = \pi$, then $x^y = 5^{\pi}$] X

Let $x = 2$ and $y = \sqrt{2}$, $\therefore x^y = 2^{\sqrt{2}}$
If $2^{\sqrt{2}}$ is irrational, problem is solved.
If irrational, then $x = 2^{\sqrt{2}}$ and $y = \sqrt{2}/4$ which makes $x^y = (2^{\sqrt{2}})^{\sqrt{2}/4} = \sqrt{2}$ which is irrational.
Hence, proved. (NON CONSTRUCTIVE)

Q Show that if a and b are real numbers with $a \neq b$, then there is a unique real number R such that $ar + b = 0$.

Uniqueness Proof

Let us assume that there is a number s which also satisfies the relation $as + b = 0$.

$$\therefore \quad ar + b = as + b$$
$$\Rightarrow \quad ar = as$$
$$\Rightarrow \quad r = s$$

Hence, the real number r is unique.

PRINCIPLE OF MATHEMATICAL INDUCTION

Prove that $1+2+3+\dots+n = \frac{n(n+1)}{2}$, $n \in Z^+$

Let $P(n): 1+2+3+\dots+n = \frac{n(n+1)}{2}$

BASIS STEP $P(1) = \frac{1(1+1)}{2} = 1$ is true.

INDUCTIVE STEP Let $P(k)$ be true for $k \in Z^+$.

$\Rightarrow P(k): 1+2+3+\dots+k = \frac{k(k+1)}{2}$ — (1)

Now, $P(k+1): 1+2+3+\dots+k+(k+1)$

$= \frac{k(k+1)}{2} + (k+1)$ (using (1))

$= (k+1)(1+k/2)$

$= \frac{(k+1)(k+2)}{2}$ which is true

Q Prove that $1^2+2^2+3^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$

Let $P(n): 1^2+2^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$

$P(1): \frac{1(1+1)(2\cdot 1+1)}{6} = \frac{1(2)(3)}{6} = 1$ is T

Let $P(k)$ be true for $k \in Z^+$.

$\therefore P(k): 1^2+2^2+3^2+\dots+k^2 = \frac{k(k+1)(2k+1)}{6}$ — (1)

Now, $P(k+1): 1^2+2^2+\dots+k^2+(k+1)^2$

$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$ using (1)

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

$= \frac{k(k+1)(2k+1+6k+6)}{6}$

Teacher's Signature..........

$$= \frac{k(k+1)(2k+3+6k+4)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

$$= \frac{(k+1)(k+2)(2(k+1)+1)}{6}$$

is T

Q Prove that $1^3+2^3+3^3+\dots+n^3 = \left[\frac{n(n+1)}{2}\right]^2$

Let $P(n): 1^3+2^3+3^3+\dots+n^3 = \left[\frac{n(n+1)}{2}\right]^2$

$P(1): \left[\frac{1(1+1)}{2}\right]^2 = 1^2 = 1$ is T.

Let $P(k)$ be true for $k \in Z^+$.

$\Rightarrow P(k): 1^3+2^3+\dots+k^3 = \left[\frac{k(k+1)}{2}\right]^2$

Now, $P(k+1) = 1^3+2^3+3^3+\dots+k^3+(k+1)^3$

$$= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$$

$$= \left[\frac{(k+1)(k+2)}{2}\right]^2$$

is T.

Q For a non-negative integers, $a+ar+ar^2+\dots+ar^n = \frac{ar^{n+1}-1}{r-1}, r \neq$

$P(0): ar^0 = a(1) = a$

RHS: $\frac{ar^1-1}{r-1} = a\left(\frac{r-1}{r-1}\right) = a$

Hence as RHS = LHS, $P(0)$ is true.

Let $P(k)$ be true $\Rightarrow$ $a+ar+ar^2+\dots+ar^k = \frac{ar^{k+1}-1}{r-1}$

Now, $P(k+1): a+ar+ar^2+\dots+ar^k+ar^{(k+1)}$

$$= \frac{ar^{k+1}-1}{r-1} + ar^{(k+1)} = \frac{ar^{k+2}-1}{r-1}$$ is T.

Q Use induction to prove the inequality $n < 2^n$ for all $n \in \mathbb{Z}^+$.

Let $P(n) : n < 2^n$

For $n = 1$, $P(1)$: LHS $= 1$, RHS $= 2^1$

$\therefore 1 < 2$ true.

Let $P(K)$ be true $\Rightarrow K < 2^K$ be true

Claim : $P(K+1)$ is true $\Rightarrow (K+1) < 2^{(K+1)}$ is T.

Proof : $K < 2^K$

$\Rightarrow K+1 < 2^K + 1$ (Adding 1 both sides) ~~$\Rightarrow K+1 < 2^K + 2$~~

$\Rightarrow K+1 < 2^K + 2^K$ $(\because 1 < 2^K)$

~~$K+1$~~ $= 2 \cdot 2^K$

$= 2^{K+1}$

$\Rightarrow K+1 < 2^{K+1}$

$\therefore$ $P(K+1)$ is true, hence the inequality is true.

Q $P(n) : 2^n < n!$, $n \geq 4$

For $n = 4$, $P(4)$: LHS $= 2^4 = 16$

RHS $= 4! = 24$

Hence, $P(4)$ is true as $16 < 24$.

Assuming $P(K)$ to be true i.e. $2^k < k!$

Claim $2^{(K+1)} < (K+1)! \Rightarrow 2^{K+1} < (K+1)K!$

Proof $2^K < K!$

$\Rightarrow 2^K (K+1) < (K+1)K!$

$\Rightarrow 2^K \cdot 2^{k} < (K+1)!$ $(\because 2^k < k! \Rightarrow 2^k < k(k-1)\ldots$ $\Rightarrow 2^k < k+1)$

$\Rightarrow 2^{k+1} < (k+1)!$

$2^K < k!$

$\Rightarrow 2 \cdot 2^k < 2k!$

$\Rightarrow 2^{k+1} < (k+1)k!$ $(\because 2 < k+1)$

$\Rightarrow 2^{k+1} < (k+1)!$

$2^{k+1} = 2^k \cdot 2 < (2^k(k+1) < (k+1)!$

Teacher's Signature

Q $P(n): 3 + 3\cdot5 + 3\cdot5^2 + \dots + 3\cdot5^n = \frac{3(5^{n+1}-1)}{4}$ $(n \geq 0)$.

~~$P(1): 3\cdot5^1 =$ LHS $= 3 + (3\cdot5)^1$~~

~~RHS $= 3(5^2-1)/4 = 3(24/4) = 18$~~

$P(0)$: 3 (LHS) = 3 (RHS).

Q $\frac{1^2}{1\cdot3} + \frac{2^2}{3\cdot5} + \dots + \frac{n^2}{(2n-1)(2n+1)} = \frac{n(n+1)}{2(2n+1)}$

for ~~non-negative~~ +ve n.

$P(1)$: LHS $= \frac{1}{(2-1)(2+1)} = \frac{1}{3}$, RHS $= \frac{2}{2(3)}$

Hence $P(1)$ is true.

Let $P(k)$ be true i.e. $\frac{1^2}{1\cdot3} + \frac{2^2}{3\cdot5} + \dots + \frac{k^2}{(2k-1)(2k+1)}$

CLAIM $P(k+1)$: $\frac{1^2}{1\cdot3} + \frac{2^2}{3\cdot5} + \dots + \frac{(k+1)^2}{(2k+1)(2k+3)} = \frac{(k+1)(k+2)}{2(2k+3)}$

PROOF $\frac{1^2}{1\cdot3} + \frac{2^2}{3\cdot5} + \dots + \frac{k^2}{(2k-1)(2k+1)} + \frac{(k+1)^2}{(2k+1)(2k+3)}$

$= \frac{(k+1)(k+2)}{2(2k+3)} + \frac{(k+1)^2}{(2k+1)(2k+3)}$

$= \frac{(k+1)}{(2k+3)}\left[\frac{k+2}{2} + \frac{k+1}{2k+1}\right]$

$= \left(\frac{k+1}{2k+3}\right)\left(\frac{2k^2+4k+k+2+2k+2}{2(2k+1)}\right)$

$= \left(\frac{k+1}{2k+3}\right)\left(\frac{2k^2+7k+4}{2(2k+1)}\right) = \frac{(k+1)}{(2k+3)} \frac{\cancel{(2k+1)}(k+2)}{2\cancel{(2k+1)}}$

Teacher's Signature..................

$$= \frac{(k+1)(k+2)}{2(2k+3)} = P(k+1)$$

Hence the given statement is true.

Q Prove that if n is a +ve integer, then 133 divides $11^{n+1} + 12^{2n-1}$.

Let $P(n): 11^{n+1} + 12^{2n-1} = 133m, \quad m \in Z^+$

For $n=1$, $P(1)$: LHS $= 11^{(1+1)} + 12^{(2(1)-1)} = 11^2 + 12 = 133$

RHS $= 133(1) = 133$.

Let $P(k)$ be true i.e. $11^{k+1} + 12^{2k-1} = 133m$

Claiming $P(k+1)$: $11^{k+2} + 12^{2k+1} = 133m$ to be true

PROOF $\cancel{11^{k+2} + 12^{2k+1}}$

$= \cancel{11^{k+1} \cdot 11 + 12^{2k-1} \cdot 12^2}$

$11^{(k+2)} + 12^{(2k+1)}$

$= 11(11^{(k+1)} + 12^{(2k-1)}) - 11 \cdot 12^{(2k-1)} + 12^{(2k+1)}$

$= 11(133m) - 11 \cdot 12^{(2k-1)} + 12^2 \cdot 12^{(2k-1)}$

$= 11(133m) + 12^{(2k-1)}(12^2 - 11)$

$= 11(133m) + 133(12^{2k-1})$

$= 133[11m + 12^{2k-1}]$

$\Rightarrow P(k+1)$ is true. Hence $P(n)$ is true.

Q Prove that $P(n): 1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{n^2} < 2 - \frac{1}{n}, \; n \geq 2$

$P(2)$: LHS $= 1 + \frac{1}{4} = \frac{5}{4}$, RHS $= 2 - \frac{1}{2} = \frac{3}{2} = \frac{6}{4}$

As $5/4 < 6/4 \Rightarrow P(2)$ is true.

Let $P(k)$ be true. $\Rightarrow 1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{k^2} < 2 - \frac{1}{k}$

CLAIM $P(k+1): 1 + \frac{1}{4} + \frac{1}{9} + \dots + \frac{1}{k^2} + \frac{1}{(k+1)^2} < 2 - \frac{1}{k+1}$

Teacher's Signature........

LHS $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2}$

$< 2 - \frac{1}{k} + \frac{1}{(k+1)^2} = \frac{2 - (k^2+3k+1)}{k(k+1)^2}$

Increase in LHS $= \frac{1}{(k+1)^2}$

Increase in RHS $= \left(2 - \frac{1}{k+1}\right) - \left(2 - \frac{1}{k}\right)$

$= \frac{1}{k} - \frac{1}{k+1} = \frac{1}{k(k+1)}$

Now, $k < k+1$

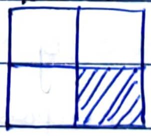
$\Rightarrow \frac{1}{k} > \frac{1}{k+1}$

$\Rightarrow \frac{1}{k(k+1)} > \frac{1}{(k+1)^2}$

$\Rightarrow$ Increase in RHS > Increase in LHS

Hence, the inequality is true.

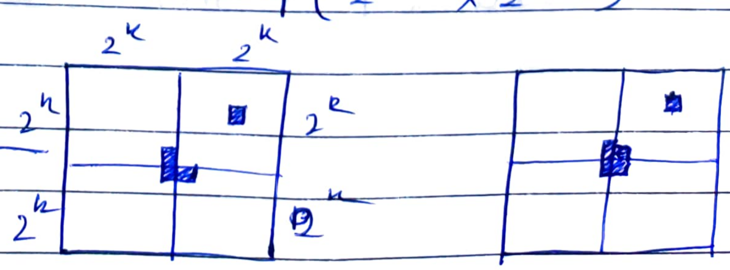
Q Let n be a positive integer so that every $2^n \times 2^n$ checkerboard is similar to a chess board. ~~If~~ with one square removed can be tiled by triminoes.

For $n = 1$, 2×2  $\rightarrow$ covered by triminoes

Assuming $P(k)$ be true : $2^k \times 2^k$ can be covered using triminoes.

Claim : $2^{k+1} \times 2^{k+1} = 4(2^{k+1} \times 2^{k+1})$

Assumption true for each box $\leftarrow$



Q Show that any integer ~~is~~ composed of 3^n identical digits is divisible by 3^n.

For $n=1$, the possible combinations are
111, 222, 333, ... , 999 – all divisible by 3!.
Hence, P(1) is true.
Let P(k) be true $\Rightarrow \underbrace{kk\ldots k}_{3^k \text{ times}}$ is divisible by 3^k

Claim: $P(k+1)$: $\underbrace{(k+1)(k+1)\ldots(k+1)}_{3^{k+1} \text{ times}} = 3^{k+1} z$.

For $n=1$, we note that any 3 digit integer with 3 identical digits is divisible by 3.
Let $m \neq 3l$, mmm be the number.
Then, sum of digits in mmm $= 3m =$ divisible by 3.
Let us assume that an integer composed of 3^k identical digits is divisible by 3^k.

CLAIM An integer composed of 3^{k+1} identical digits is divisible by 3^{k+1}

PROOF Let x be the number composed of 3^{k+1} identical digits, then $x = y \times z$ where
y is an integer composed of 3^k identical digits and $z = 10^{2(3k)} + 10^{3k} + 1$.
We know, y is divisible by 3^k, and z is divisible by 3. Hence, x will be divisible by 3^{k+1}

P(1)
P(2)
⋮
P(k)

Q Prove th
product
2 =
3 =
4 =
5 =
Hence,
For P

Q Prove
can be
12
13
14
15
Hence
CASE I:
Repl
will
CASE
The
is th
5s
by

Strong Induction

$P(1)$ $\quad\quad (P(1) \wedge P(2) \ldots \wedge P(k)) \rightarrow P(k+1)$

$P(2)$

$\vdots$

$P(k)$

Q Prove that any integer > 1 can be expressed as product of primes.

$2 = 2 \times 1$ $\quad\quad$ $6 = 2 \times 3$

$3 = 3 \times 1$ $\quad\quad$ $7 = 1 \times 7$

$4 = 2 \times 2$ $\quad\quad$ $8 = 2 \times 2 \times 2$

$5 = 5 \times 1$ $\quad\quad$ $9 = 3 \times 3$.

Hence, $P(2), P(3) \ldots P(k)$ are true.

For $P(k+1)$, $\quad x = y \times z$

y: expressed as product of primes

z: expressed as product of primes

Q Prove that every amount of postage of 12 cents or more can be formed using just 4 cent and 5 cent stamps

$12 = 4 + 4 + 4$

$13 = 4 + 4 + 5$

$14 = 4 + 5 + 5$

$15 = 5 + 5 + 5$

Hence $P(12), P(13) \ldots P(15) \ldots P(k)$ are true.

CASE I: Combination of 4s and 5s.

Replace ~~the~~ one 4 by 5 and the postage value will increase by +1.

CASE II: If there are only 5s in the existing value, The min. number of 5s we have here is 3 as it is the least multiple of 5 possible here. When ~~three~~ 5s are replaced by four 4s, the value increases by +1. Hence replace just three 5s with four 4s.

CHAPTER 5

BASICS OF COUNTING

Product Rule

If one experiment has 'm' possible outcomes, and another has 'n' possible outcomes, then the[re] are mn possible outcomes where both of these experiments take place.

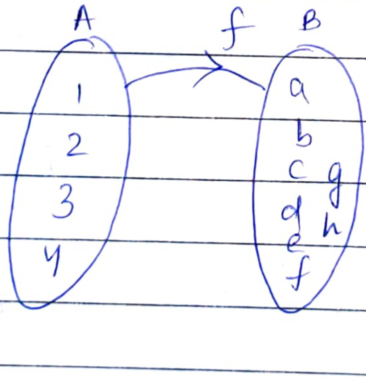
Sum Rule

If one experiment has 'm' possible outcomes, and another has 'n' possible outcomes, then the[re] are 'm+n' possible outcomes where exactly one of these experiments takes place.

Q Find the number of four digit numbers that contain no repeated digits.

8 8 6 7

Q How many one to one functions are there from a set with 'm' elements to a set with 'n' eleme[nts]



$m \leq n$

$n(n-1)(n-2)\cdots(n-m-$

Q A student can choose a computer project from one of three lists. The three lists contain 23, 15 and 19 projects respectively. No project is on more than one list. How many possible projects are there to choose from?

No. of possible projects $= 23 + 15 + 19$

Teacher's Signature.......................

Pigeonhole Principle

(Dirichlet Drawer Problem)

If k is a positive integer and k+1 or more objects are placed into k boxes, then there is at least one box, containing two or more of the objects.

Generalised Pigeonhole Principle:

If N objects are placed into K boxes, then there is at least one box containing at least $\lceil N/K \rceil$ objects.

ex For 27 ~~letto~~ words, at least two will begin with the same letter.

Q Among 100 people, how many will be born in same moth?

$$\left\lceil \frac{100}{12} \right\rceil = 9$$

Q How many cards must be selected from a standard deck of 52 cards to guarantee that at

1. least 3 cards are of the same suite?
2. How many must be selected to guarantee that at least 3 hearts are selected?

Ans 1 Here N = ?

$$\left\lceil \frac{N}{4} \right\rceil \geq 3$$

$$\frac{4 \times {}^{13}C_3}{{}^{52}C_3}$$

$\Rightarrow$ N = 9

2 While drawing cards there is a possibility that we will get everything else except hearts. At some point of time, all the cards except hearts will be exhausted. Hence, now every card picked will be a card.

$$\therefore N = \underbrace{(13+13+13)}_{\text{exhausted from other suites}} + \underbrace{3}_{\text{hearts}} = 42 \quad \text{(Ans)}$$

Q Suppose you selected 6 consecutive numbers. Prove that if they are divided by 5, ~~at~~ two of them yield the same remainder.

If divided by 5, the possible remainders 0, 1, 2, 3, 4.
Hence, ~~the~~ at least one element must yield repeated rem.

Q A drawer contains a dozen of black and a dozen of white — all unmatched socks. A man takes out socks at random in dark.

(ii) How many socks he must take out to be sure that he has at least three ~~sock~~ black socks?

(i) How many socks he must take out to be sure that he has at least 2 socks of the same colour?

Ans (i) 3

Any two of them must be of the same colour.

(ii) If he gets all whites and no blacks at beginning
Hence, $12 + 3 = 15$.

Q How many numbers will be selected from $\{1, 2, 3, 4, 5, 6\}$ to guarantee that at least one pair of these no.s add up to 7.

The pairs that add up to 7 : (1, 6), (2, 5), (3, 4).

Hence $N = 4$ as even if at first one element is selected from each of the above sets, ~~to~~ on selecting any fourth element, there will exist a pair that add up to 7.

Q $\{1, 3, 5, 7, 9, 11, 13, 15\}$ for sum 16.
Pairs : (1, 15), (3, 13), (5, 11), (7, 9).
Hence, $N = 5$

Q During a month with 30 days, a football team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must have played exactly 14 games.

Let a_i be the number of games the team has played on or before the ith day.

$a_1, a_2, a_3, \ldots\ldots a_{30}$ $\quad 1 \leq a_j \leq 45$ — (i)

$a_1+14, a_2+14, \ldots\ldots a_{30}+14$ $\quad 15 \leq a_j+14 \leq 59$ — (ii)

Here sequence (i) is an increasing sequence.

Hence sequence (ii) will also be increasing.

$a_{30} = 45$.

As in total number of terms possible in the two sequences $= 30+30 = 60$, but the limit is upto 59

Hence there is at least one repeatation.

$\therefore \quad a_i = a_j + 14 \Rightarrow a_i - a_j = 14$

The duration is from $(j+1)$th day to ith day. (Ans)

6}

PERMUTATIONS & COMBINATIONS

How many permutations of the ~~string~~ letters $\boxed{ABC}DEFGH$ contain the string ABC?

$6! = 720$

Q How many possibilities are there for the first, second and third positions in a horse race with 12 horses if all orders of finish are possible?

$12 \times 11 \times 10 = 1320$

Q Suppose that there are 9 faculty members in the mathematics department, and 11 in the CS dept. How many ways are there to select a committee to

Teacher's Signature..........

develop a discrete mathematics course if the committee is to be consisted of 3 faculties from the mathematics dept. and 4 from the CSE dept.

Sol $\quad {}^9C_3 \times {}^{11}C_4 = \frac{9\times8\times7}{3\times2} \times \frac{11\times10\times9\times8}{4\times3\times2}$

$= 84 \times 330 = 27,720$

Q How many subsets with more than two elements does a set with 100 elements contain?

$2^{100} - {}^{100}C_1 - {}^{100}C_2 - 1$ → empty set $\qquad 2^{100} - {}^{100}C_1 - {}^{100}C_2 - 1$

$= 2^{100} - 5051$

$= 1.26765 \times 10^{30}$.

Q How many ways are there for 8 men and 5 women to stand in a line so that no two women stand next to each other?

Binomial Coefficients

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}xy^{n-1} + \dots + \binom{n}{n}x^ny^0$$

$$= \sum_{r=0}^{\infty} x^r y^{n-r}\binom{n}{r}$$

Q i) What is the coefficient of x^5y^8 in $(x+y)^{13}$.

$r = 5$

Coefficient $= {}^nC_5 = {}^{13}C_5 = 1287$

ii) x^7 in $(1+x)^{13}$ $\qquad$ Here $n - r = 7 \Rightarrow r = 6$ $\therefore {}^{13}C_6$

$\hookrightarrow \sum_{r=0}^{\infty} \binom{n}{r} 1^r x^{n-r}$

Teacher's Signature....................

iii) x^7 in $(1-x)^{13} = \sum_{r=0}^{n} 1^r (-x)^{n-r} \binom{n}{r}$

$\therefore$ coeff $= \binom{13}{6}(-1)^6 = {}^{13}C_6$

iv) $x^{12}y^{13}$ in $(2x-3y)^{25} = \sum_{r=0}^{n} \binom{25}{r}(2x)^r(-3y)^{25-r}$

$r = 12$ $\qquad = \sum \binom{25}{r} 2^r x^r (-3)^{25-r} y^{25-r}$

Coeff $= {}^{25}C_{12} \cdot 2^{12} (-3)^{13}$

v) $x^{101} y^{99}$ in $(2x-3y)^{200}$

Here $r = 101$

$\therefore$ coeff $= {}^{25}C_{101} \cdot 2^{101} (-3)^{99}$

Q How many strings of length r can be formed from the ~~the~~ english alphabet?

26^r

THEOREM 1 The number of r permutations on a set of n objects with repeatation allowed is n^r

THEOREM 2 There are ${}^{n+r-1}C_r$ r combinations from a set of n elements when repeatation is allowed.

Q Suppose that a cookie shop has four different types of cookies. How many different ways can six cookies be chosen?

$r = 6$, $n = 4$ $\qquad \therefore$ no. of ways $= {}^9C_{\cancel{6}} = \cancel{126}\ 84$

Q How many different solutions does $x_1 + x_2 + x_3 = 11$ have where $x_1, x_2, x_3 \geq 0$?

Here, $n = 3$, $r = 11$

$\therefore$ there are $C(3+11-1, 11) = C(13, 11) = 78$

Q $x_1 + x_2 + x_3 = 11$, $x_1 \geq 1$.

Here $r = 10$,

$c(3+10-1, 10)$

Q $x_1 + x_2 + x_3 = 11$, $x_1 \geq 1$, $x_2 \geq 2$, $x_3 \geq 3$

$c(3+5-1, 5)$ $11-6=5$

Q $x_1 + x_2 + x_3 = 11$, $x_1 \geq 4$, $x_2 \geq 5$, $x_3 \geq 3$.

No possible combinations

Q How many different strings can be made by reordering letters of the word "SUCCESS".

$$\frac{7!}{2!\,3!}$$

Q How many numbers less than 10,000 will have the sum of the digits ≤ 19.

$x_1 + x_2 + x_3 + x_4 = 19$, $x_1 \geq 0$, $x_2 \geq 0$, $x_3 \geq 0$, $x_4 \geq 0$

CHAPTER 6

RECURRENCE RELATION

A recurrence relation for a sequence $\{a_n\}$ is an equation that expresses $\{a_n\}$ in terms of one or more of the previous terms of the sequence till $a_0, a_1, \ldots a_n$ for all integers n, $n \geq n_0$ and n_0 is a non-negative integer.

A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation

Q Determine whether $\{a_n\}$ with $a_n = 3n$, $a_n = 2^n$, $a_n = 5$ are solutions of the recurrence relations $a_n = 2a_{n-1} - a_{n-2}$ $n = 2, 3, 4, 5 \ldots$

For $a_n = 3n$; $3n = 2(3(n-1)) - 3(n-2)$

$= 6n - 6 - 3n + 6 = 3n$

Hence $a_n = 3n$ is a solution.

For $a_n = 2^n$; $2^n = 2 \cdot 2^{n-1} - 2^{n-2}$

$= 2^n - 2^{n-2}$ X

Hence $a_n = 2^n$ is not a solution.

For $a_n = 5$; $5 = 2(5) - 5 = 5$

Hence $a_n = 5$ is a solution.

Q A young pair of rabbits (one of each sex) is placed on an island. A pair of rabbits does not breed until they are two months old. After they are two months old, each pair of rabbits produces another pair each month. Find the recurrence relation for the number of pairs of rabbits on the island after n months, assuming that no rabbits ever died.

Let f_n be the number of pairs of rabbits after n month.

Teacher's Signature........................

	MONTH	f_n
Pair 1	1	1
Pair 1	2	1
Pair 1 + Pair 2	3	2
Pair 1 + 2 + 3	4	3
Pair 1 + 2 + 3 + 4 + 5	5	5

$\therefore \; f_n = f_{n-1} + f_{n-2}$, $f_1 = 1$, $f_2 = 1$.

Homogeneous linear Recurrence Relation with Constant Coefficient

The general form of a homogeneous linear recurrence relation of degree k is given by

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + c_3 a_{n-3} + \cdots + c_k a_{n-k}, \quad \text{(i)}$$

$$c_k \neq 0.$$

Let $a_n = r^n$ be the solution of (i)

Considering the first two RHS terms

$$r^n = c_1 r^{n-1} + c_2 r^{n-2}$$

$$\Rightarrow r^n - c_1 r^{n-1} - c_2 r^{n-2} = 0$$

$$\Rightarrow r^n \left(1 - \frac{c_1}{r} - \frac{c_2}{r^2}\right) = 0$$

As $r^n \neq 0$, $1 - \frac{c_1}{r} - \frac{c_2}{r^2} = 0$

$$\Rightarrow \boxed{r^2 - c_1 r - c_2 = 0} \rightarrow \text{characteristic equation}$$

Case I $\quad r_1 \neq r_2 \Rightarrow$ Solution is $\boxed{a_n = A r_1^n + B r_2^n}$

Case II $\quad r_1 = r_2 = r \Rightarrow$ Solution is $\boxed{a_n = (A + Bn) r^n}$

If a_0, a_1 are given,

$1, 1, 2, -2, 3, 3, 3.$

$$a = (A_1 + A_2 n) 1^n + B \cdot 2^n + C(-2)^n + (D_1 + D_2 n + D_3 n^2)(n^3)$$

Teacher's Signature..................

Q Solve the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2}, n \geq 2$

$a_0 = 1, a_1 = 0$ (i)

$a_n - 5a_{n-1} + 6_{n-1} = 0$

Let $a_n = r^n$ be the solition of (i)

$r^n - 5r^{n-1} + 6r^{n-2} = 0$

$\Rightarrow r^n \left(1 - \frac{5}{r} + \frac{6}{r^2}\right) = 0$

$\Rightarrow \boxed{r^2 - 5r + 6 = 0} \Rightarrow r = 2, 3$

$\therefore$ solution is $a_n = A2^n + B3^n$

For $n = 0$, $a_0 = A + B \Rightarrow A + B = 1$ —(ii)

For $n = 1$, $a_1 = 2A + 3B = 0 \Rightarrow 2A + 3B = 0$ —(iii)

$A = 3, B = -2$.

Q $a_n = \frac{a_{n-2}}{4}, n \geq 2, a_0 = 1, a_1 = 0$.

$\cancel{a_n - \frac{a_{n-2}}{4} = 0 \Rightarrow 3a_n - 2 = 0}$ —(i)

Let $a_n = \cancel{\lambda^n}$ be the solution of (i).

$\cancel{\lambda^n - 5\lambda^{n-1}}$ 3λ

$a_n - \frac{a_{n-2}}{4} = 0 \Rightarrow 4a_n - a_{n-2} = 0$ —(i)

Let $a_n = r^n$ be the solution of (i).

For $n = 2$, $a_2 - \frac{a_0}{2} = 0 \Rightarrow r^2 - \frac{1}{4} = 0$

$\Rightarrow r = \pm(1/2)$

$\therefore$ the solution is $a_n = A\left(\frac{1}{2}\right)^n + B\left(-\frac{1}{2}\right)^n$

For $n = 0$, $A + B = 0$

$3n^2)$ $n = 1$, $\frac{A}{2} - \frac{B}{2} = 1$

Teacher's Signature....................

Q $a_n = a_{n-1} + a_{n-2}$ $a_0 = 1,\ a_1 = 1$

$\Rightarrow a_n - a_{n-1} - a_{n-2} = 0$

Let r^n be the solution.

$\therefore r^n - r^{n-1} - r^{n-2} = 0$

$\Rightarrow r^n\left(1 - \frac{1}{r} - \frac{1}{r^2}\right) = 0$

$\Rightarrow 1 - \frac{1}{r} - \frac{1}{r^2} = 0 \Rightarrow \frac{r^2 - r - 1}{r^2} = 0$

$\Rightarrow r^2 - r - 1 = 0$

$\Rightarrow r = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$

$\therefore$ Solution is $a_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n$

For $n = \cancel{0}1$, $1 = A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right)$

$\Rightarrow A + \sqrt{5}(A-B) + B = 2$ — (i)

$n = 0$, $A + B = 1$ —— (ii)

Solving, $(A-B)\sqrt{5} + A + B = 2$

$\Rightarrow (A-B)\sqrt{5} + 1 = 2$

$\Rightarrow \sqrt{5}(A-B) = 1$

$\Rightarrow A - B = 1/\sqrt{5}$

$\Rightarrow A - 1 + A = 1/\sqrt{5} \Rightarrow 2A = \frac{1}{\sqrt{5}} + 1 = \frac{1+\sqrt{5}}{\sqrt{5}}$

$\Rightarrow A = \frac{1+\sqrt{5}}{2\sqrt{5}}$

$B = 1 - A = 1 - \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right)$

$\Rightarrow B = \frac{\sqrt{5}-1}{2\sqrt{5}}$

Q $a_n = 2a$

$a_n - 2a_n$

Let r^n

$r^n - 2$

$\Rightarrow r^n ($

$\Rightarrow r^3 - 2$

$\Rightarrow r^3 -$

$\Rightarrow (r-1$

$\Rightarrow r = 1$

$\therefore a_n$

$\Rightarrow$

Non -

Consta

$a_n =$

1.

2. $a_0 + a$

3. $A\alpha^n$

4. $A\alpha$

Q $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$, $a_0 = 7$, $a_1 = -4$, $a_2 = 8$

$a_n - 2a_{n-1} - 5a_{n-2} + 6a_{n-3} = 0$

Let r^n be the solution.

$r^n - 2r^{n-1} - 5r^{n-2} + 6r^{n-3} = 0$

$\Rightarrow r^n\left(1 - \frac{2}{r} - \frac{5}{r^2} + \frac{6}{r^3}\right) = 0$

$\Rightarrow \frac{r^3 - 2r^2 - 5r + 6}{r^3} = 0$

$\Rightarrow r^3 - 2r^2 - 5r + 6 = 0$

$\Rightarrow (r-1)(r+2)(r-3) = 0$

$\Rightarrow r = 1, -2, 3.$

$\therefore a_n = A \cdot 1^n + B(-2)^n + C \cdot 3^n$

$\Rightarrow A = 3, \quad B = -1, \quad C = 5.$

Non-homogeneous linear Recurrence Relations with Constant Coefficient

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + F(n)$

$$a_n = a_n^{(h)} + a_n^{(p)}$$

	$F(n)$	Choice of $a_n^{(p)}$
1.	$A\alpha^n$	$C \cdot \alpha^n$ provided, α is not a characteristic roo
2.	$a_0 + a_1 n + a_2 n^2 + \dots + a_k n^k$	$C_0 + C_1 n + C_2 n^2 + \dots + C_k n^k$ Provided 1 is not a characteristic root
3.	$A\alpha^n + a_0 + a_1 n + \dots + a_k n^k$	$C \cdot \alpha^n + C_0 + C_1 n + \dots + C_k n^k$ provided 1 & α are not characteristic root
4.	$A\alpha^n(a_0 + a_1 n + \dots + a_k n^k)$	$\alpha^n(C_0 + C_1 n + \dots + C_k n^k)$ provided α cannot be a characteristic root

Modification

If $r = 2, 3$, $a_n^{(p)} = c \cdot 2^n \cdot n^1$

$r = 2, 2$, $a_n^{(p)} = c \cdot 2^n \cdot n^2$

Multiplicity = no. of times a root is repeated =

Hence,

If α is a root of the equation, then multiply n^i

Q $a_n = 3a_{n-1} + 2^n$, $a_0 = 1$

$a_n - 3a_{n-1} = 2^n$

Characteristic equation : $r - 3 = 0$.

$\Rightarrow r = 3$

$a_n^{(h)} = A \cdot 3^n$

Let $a_n^{(p)} = c \cdot 2^n$

$\therefore c \cdot 2^n - 3c \cdot 2^{n-1} = 2^n$

$\Rightarrow 2^n \left(c - \frac{3c}{2}\right) = 2^n$

$\Rightarrow c\left(1 - \frac{3}{2}\right) = 1 \Rightarrow c\left(-\frac{1}{2}\right) = 1$

$\Rightarrow c = -2$.

Now, $a_n = a_n^{(h)} + a_n^{(p)}$

$a_n = A \cdot 3^n - 2 \cdot 2^n$

$a_0 = 1$ (given)

$\Rightarrow a_0 = A - 2 \Rightarrow A - 2 = 1 \Rightarrow A = 3$.

$\therefore a_n = 3 \cdot 3^n - 2 \cdot 2^n$

$\Rightarrow a_n = 3^{n+1} - 2^{n+1}$

Q $a_n = 4a_{n-1} - 4a_{n-2} + (n+1)$

$\Rightarrow a_n - 4a_{n-1} + 4a_{n-2} = n+1$

Characteristic equation : $r^2 - 4r + 4 = 0$

$\Rightarrow (r-2)^2 = 0$

$\Rightarrow r = 2, 2$.

Teacher's Signature..........

$$a_n^{(h)} = (A+Bn)\cdot 2^n$$

Let $a_n^{(p)} = c_0 + c_1 n$

$$a_n^{(p)} - 4a_{n-1}^{(p)} + 4a_{n-2}^{(p)} = (n+1)$$

$\Rightarrow c_0 + c_1 n - 4[c_0 + c_1(n-1)] + 4[c_0 + c_1(n-2)] = (n+1)$

$\Rightarrow c_0 + n(c_1 - 4c_1 + 4c_1) + 4c_1 - 8c_1 = n+1$

$\Rightarrow (c_1 - \cancel{8c_1})n + (c_0 - 4c_1) = n+1.$

$\therefore \quad c_0 - 4\cancel{c_1}^{1} = 1 \quad , \quad c_1 = 1$

$\Rightarrow c_0 = 1+4 = 5$

Now,

$$a_n = a_n^{(p)} + a_n^{(h)}$$

$$\Rightarrow \quad = (n+5) + (A+Bn)2^n$$

Q $a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n$

$\Rightarrow a_n - 4a_{n-1} + 4a_{n-2} = (n+1)2^n$

Characteristic equation : $r^2 - 4r + 4 = 0$

$\Rightarrow r = 2, 2.$

$\therefore a_n^{(h)} = (A+Bn)2^n$

Let $a_n^{(p)} = 2^n(c_0 + c_1 n)n^2 \qquad \alpha = 2$

$a_n^{(p)} - 4a_{n-1}^{(p)} + 4a_{n-2}^{(p)} = 2^n(n+1)$

$\Rightarrow$ ~~$2^n(c_0+c_1n)n^2 - 4.2^n(c_0+c_1n)n^2 + 4.2^n(c_0+c_1n)n^2$~~

$2^n(c_0 + c_1 n)n^2 - \overbrace{4.2^{n-1}}^{2^{n+1}}(c_0 + c_1(n-1))(n-1)^2$

$+ \underbrace{4.2^{n-2}}_{2^n}(c_0 + c_1(n-2))(n-2)^2 = 2^n(n+1)$

$\Rightarrow \cancel{2^n}(c_0 + c_1 n)n^2 - \cancel{2^n}.2(c_0 + c_1 n - c_1)(n^2 - 2n + 1)$

$+ \cancel{2^n}(c_0 - 2c_1 + c_1 n)(n^2 - 4n + 4) = \cancel{2^n}(n+1)$

$\Rightarrow n^2(c_0 + c_1 n) - 2n^2(c_0 - c_1 + c_1 n) + n^2(c_0 - 2c_1 + c_1 n)$

$- 2n(c_0 + c_1 n - c_1) - 4n(c_0 - 2c_1 + c_1 n) +$

$(c_0 - c_1 + c_1 n) + 4(c_0 - 2c_1 + c_1 n) = n+1$

$\Rightarrow n^2[c_0 + c_1 n - 2c_0 + 2c_1 - 2c_1 n + c_0 - 2c_1 + c_1 n] =$

$\Rightarrow n^2(0) = 0$.

$-2n(c_0 - c_1 + c_1 n + 2c_0 - \cancel{8}4c_1 + 2c_1 n) = n$

$\Rightarrow -2(3c_0 - 5c_1 + 3c_1 n) = 1$

$\Rightarrow 3c_0 - 5c_1 + 3c_1 n = -0.5$ ——— (i)

$c_0 - c_1 + c_1 n + 4c_0 - 8c_1 + 4c_1 n = 1$

$\Rightarrow 5c_0 - 9c_1 + 5c_1 n = 1$ ——— (ii)

$\Rightarrow (3c_0 - 5c_1 + 3c_1 n) + (2c_0 - 4c_1 + 2c_1 n) = 1$

$\Rightarrow 2c_0 - 4c_1 + 2c_1 n = 1.5$

$\Rightarrow c_0 - 2c_1 + c_1 n = 0.75$

$\Rightarrow c_1 n = 2c_1 - c_0 - 0.75$

$\Rightarrow n = 2 - \frac{c_0}{c_1} - \frac{0.75}{c_1}$ ——— (iii)

Hence, $3c_0 - 5c_1 + 3c_1\left(2 - \frac{c_0}{c_1} - \frac{0.75}{c_1}\right) = -0.5$

$\Rightarrow \cancel{3c_0} - 5c_1 + 6c_1 - \cancel{3c_0} - \frac{9}{4} = -\frac{1}{2}$

$\Rightarrow \cancel{c_1 = \frac{9}{4} - \frac{1}{2} = \frac{7}{4}}$

$c_0 = 1, \quad c_1 = 1/6$

$\therefore \quad a_n^p = 2^n(1 + n/6)n^2$

The solution is $a_n = a_n^h + a_n^p$

$\Rightarrow \boxed{a_n = (A + Bn)2^n + n^2\left(1 + \frac{n}{6}\right)n^2}$

(Ans.)

Q $a_n = -5a_{n-1} - 6a_{n-2} + 42\cdot4^n$ $a_1 = 56$, $a_2 = 278$

$\Rightarrow a_n + 5a_{n-1} + 6a_{n-2} - 42\cdot4^n = 0$.

$r^n + 5r^{n-1} + 6r^{n-2} = \cancel{42\cdot4^n}\ 0$

$\Rightarrow r^2 + 5r + 6 = 0$ is characteristic equation

$\Rightarrow (r+3)(r+2) = 0$

$\Rightarrow r = -2, -3$.

$\therefore a_n^{(h)} = A(-2)^n + B(-3)^n$

$a_n^{(P)} = c\cdot4^n$

Hence,

$c\cdot4^n + 5c\cdot4^{n-1} + 6c\cdot4^{n-2} = 42\cdot4^n$

$\Rightarrow 4^n c\left(1 + \frac{5}{4} + \frac{6}{4^2}\right) = 42\cdot4^n$

$\Rightarrow \left(\frac{16+20+6}{16}\right)c = 42$ ~~$\Rightarrow 2c = 42$~~

$\Rightarrow c = 16$

$a_n = a_n^{(h)} + a_n^{(P)}$ is the solution.

$\Rightarrow a_n = (-2)^n A + (-3)^n B - 42\cdot4^{n+2}$

For $n=1$, $-2A - 3B - 42\cdot4^{3} = 56$

For $n=2$, $4A + 9B - 42\cdot4^4 = 278$

On solving, $A = 1$, $B = 2$

$\therefore$ the solution is $a_n = (-2)^n + 2(-3)^n + 4^{n+2}$

(Ans.)

Q $a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3$, $a_0 = 1$, $a_2 = 5$

$\Rightarrow a_n - 4a_{n-1} + 3a_{n-2} = 2^n + n + 3$.

The characteristic equation:

$r^2 - 4r + 3 = 0 \Rightarrow r = 1, 3$.

$a_n^{(h)} = A(1)^n + B(3)^n$

$= A + 3^n B$.

$a_n^{(p)} = c\cdot2^n + (c_0 + c_1 n)n$

Teacher's Signature.........

$$c\cdot 2^n + n(c_0+c_1 n) - 4\left[c\cdot 2^{n-1} + (n-1)(c_0+c_1 n - c_1)\right] + 3\left[c\cdot 2^{n-2} + (n-2)(c_0 - 2c_1 + c_1 n)\right] = 2^n + n$$

$$\Rightarrow c\cdot 2^n + c_1 n^2 + c_0 n - c\cdot 2^{n+1} - 4n(c_0 - c_1) + 4c_1 n^2 + 4c_1 n + 3c\cdot 2^{n-2} + 4c_0 + 4c_1 + 3c_1 n^2 + 3(c_0-2c_1)n - 6c_1 n - 6(c_0 - 2c_1)$$

$$\Rightarrow 2^n(c - 2c + 0.75c) + n^2(c_1 + 4c_1 + 3c_1) + n(c_0 + 4c_1 + 3c_0 - 6c_1 - 6c_1 - 4c_0 + 4c_1) + (4c_0 + 4c_1 - 6c_0 + 12c_1) = 2^n + n + 3$$

$$\Rightarrow c - 2c + 0.75c = 1$$
$$\Rightarrow -0.25c = 1 \Rightarrow c = -4.$$

~~$c_1 + 4c_1 + 3c_1 = 0 \Rightarrow$~~

$$-4c_1 = 1 \Rightarrow c_1 = -1/4.$$

$$4c_0 - 4(-1/4) - 6c_0 + 12(-1/4) = 3$$
$$\Rightarrow 4c_0 + 1 - 6c_0 - 3 = 3 \Rightarrow -2c_0 = 5 \Rightarrow c_0 = -5/2$$
$$\therefore c = -4,\ c_0 = -5/2,\ c_1 = -1/4.$$

$\therefore$ $a_n = a_n^{(h)} + a_n^{(p)}$ is solution

$$\Rightarrow a_n = A + B\cdot 3^n - 2^{n+2} - (2.5 + 0.25n)n$$

$n=0$, $A + B - 4 = 1 \Rightarrow A + B = 5$ — (i)

$n=2$, $A + 9B - 16 - (5 + \cancel{0.5}\,1) = 5 \Rightarrow A + 9B = 27$ — (ii)

Solving (i) & (ii), $A = \cancel{2.3125}\ 9/4$, $B = \cancel{2.6875}\ \frac{11}{4}$

Hence the solution is

$$a_n = \frac{9}{4} + \frac{11}{4}\cdot 3^n - 2^{n+2} - 2.75n$$

(Ans)

Teacher's Signature........

Q $a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3} + F(n)$

$\Rightarrow a_n - 6a_{n-1} + 12a_{n-2} - 8a_{n-3} = F(n)$

The characteristic equation is

$r^3 - 6r^2 + 12r - 8 = 0$

$\Rightarrow r = 2, 2, 2$

a) $F(n) = n^2$

$a_n^{(P)} = C_0 + C_1 n + C_2 n^2$

b) $F(n) = 2^n$

$a_n^{(P)} = c \cdot 2^n \cdot n^3$

c) $F(n) = n \cdot 2^n$

$a_n^{(P)} = 2^n (C_0 + C_1 n) n^3$

d) $F(n) = (-2)^n$

$a_n^{(P)} = c(-2)^n$

e) $F(n) = n^2 \cdot 2^n$

$a_n^{(P)} = 2^n (C_0 + C_1 n + C_2 n^2) n^3$

f) $F(n) = n^3 (-2)^n$

$a_n^{(P)} = (-2)^n (C_0 + C_1 n + C_2 n^2 + C_3 n^3)$

g) $F(n) = 3$

$a_n^{(P)} = C_0$

Q $a_n = 8a_{n-2} - 16a_{n-4} + F(n)$

$\Rightarrow a_n - 8a_{n-2} + 16a_{n-4} = F(n)$

$r^4 - 8r^2 + 16 = 0$ is characteristic equation

$\Rightarrow k^2 - 8k + 16 = 0 \Rightarrow k = 4, 4$

$\Rightarrow r = 2, 2, -2, -2$

Teacher's Signature........................

a) $F(n) = n^3$

$a_n^{(P)} = \{c_0 + c_1 n + c_2 n^2 + c_3 n^3\}$

b) $F(n) = (-2)^n$

$a_n^{(P)} = c(-2)^n \cdot n^2$

c) $F(n) = n \cdot 2^n$

$a_n^{(P)} = 2^n (c_0 + c_1 n) n^2$

d) $F(n) = n^2 4^n$

$a_n^{(P)} = 4^n (c_0 + c_1 n + c_2 n^2)$

e) $F(n) = (n^2 - 2)(-2)^n$

$a_n^{(P)} = (-2)^n (c_0 + c_1 n + c_2 n^2) n^2$

f) $F(n) = n^4 . 2^n$

$a_n^{(P)} = 2^n (c_0 + c_1 n + c_2 n^2 + c_3 n^3 + c_4 n^4) n^2$

g) $F(n) = 2$

$a_n^{(P)} = c_0$

Generating function

$G(x)$ is an infinite series.

$$G(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

$$= \sum_{n=0}^{\infty} a_n x^n$$

1, 1, 1, 1 . . . .

$$G(x) = 1 + 1x + 1x^2 + \dots$$

$$\Rightarrow \boxed{G(x) = \frac{1}{1-x}}$$ CLOSED FORM

3, 3, 3, 3 . . . .

$$G(x) = 3 + 3x + 3x^2 + \dots$$

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

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

Q Find a closed form of generating function for the sequence 0, 2, 2, 2, 2, 2, 2, 0, 0, 0 . . .

$$G(x) = 0 + 2x + 2x^2 + \dots 2x^6 + 0 \dots$$

$$= 2x + 2x^2 + \dots + 2x^6$$

$$= 2x \,(1 + x + x^2 + \dots x^5)$$

$$= 2x \cdot \frac{1(x^6 - 1)}{x - 1}$$

Q $\binom{7}{0}, \binom{7}{1}, \binom{7}{2}, \dots \binom{7}{7}, 0, 0 \dots$

$$G(x) = {}^7C_0 + {}^7C_1 x + {}^7C_2 x^2 + \dots + {}^7C_7 x^7$$

$$= (1+x)^7$$

Q: Use generating function to solve the recurrence

$a_k = 7a_{k-1}$, $a_0 = 5$

~~$r - 7 = 0 \Rightarrow r = 7$~~

Multiplying x^k on both sides,

$x^k a_k = 7x^k a_{k-1}$

$$\sum_{k=1}^{\infty} x^k a_k = \sum_{k=1}^{\infty} 7x^k a_{k-1}$$

Since $G(x) = \sum_{k=0}^{\infty} a_k x^k = a_0 + a_1 x + a_2 x^2 + \dots$

$\therefore \sum_{k=1}^{\infty} x^k a_k = G(x) - a_0$.

Therefore, $\sum_{k=1}^{\infty} x^k a_k = \sum_{k=1}^{\infty} 7x^k a_{k-1}$

$\Rightarrow G(x) - a_0 = 7(a_0 x + a_1 x^2 + a_2 x^3 + \dots)$

$\Rightarrow G(x) - a_0 = 7x(a_0 + a_1 x + a_2 x^2 + \dots)$

$\Rightarrow G(x) - 5 = 7x\, G(x)$

$\Rightarrow G(x)(1 - 7x) = 5$

$\Rightarrow G(x) = \dfrac{5}{1-7x}$

$\Rightarrow G(x) = 5 \cdot \dfrac{1}{1-7x} = 5(7x)^k$

Comparing the coefficients,

$G(x) = 5(7x)^k$

$\Rightarrow \sum_{k=0}^{\infty} a_k x^k = 5 \sum_{k=0}^{\infty} (7x)^k$

$$\boxed{a_k = 5 \cdot 7^5}$$

(Ans.)

Q $a_k = 3a_{k-1} + 2$, $a_0 = 1$.

Multiplying x^k both sides,

$x^k a_k = x^k 3a_{k-1} + 2x^k$

$\Rightarrow \sum_{k=1}^{\infty} x^k a_k = \sum_{k=1}^{\infty} x^k . 3a_{k-1} + \sum_{k=1}^{\infty} 2x^k$

$\Rightarrow G(x) - a_0 = 3(a_0 x + a_1 x^2 + \dots) + 2(x + x^2 + \dots)$

$\Rightarrow G(x) - \cancel{a_0}\,1 = 3x\,G(x) + 2x\left(\frac{1}{1-x}\right)$

$\Rightarrow G(x)(1-3x) = 1 + \frac{2x}{1-x} = \frac{1+x}{1-x}$

$\Rightarrow G(x) = \frac{1+x}{(1-3x)(1-x)}$ ——— (i)

$\Rightarrow G(x) = \frac{A}{1-x} + \frac{B}{1-3x}$ ——— (ii)

Using partial fraction in (ii) with (i),

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

$\Rightarrow A + B - x(3A + B) = 1 + x$

$\Rightarrow A + B = 1 \quad \Rightarrow \quad A = -1$

$3A + B = -1 \qquad B = 2$

$\therefore G(x) = \frac{2}{1-3x} - \frac{1}{1-x}$

$\Rightarrow \sum_{k=0}^{\infty} a_k x^k = 2\sum_{k=1}^{\infty}(3x)^k - \sum_{k=1}^{\infty} x^k$

Comparing the coefficient of x^k,

$a_k = 2 \cdot 3^k - 1$. (Ans)

Q $a_k = 5a_{k-1} - 6a_{k-2}$, $a_0 = 6$, $a_1 = 30$

Multiplying x^k both sides,

$x^k a_k = 5x^k a_{k-1} - 6x^k a_{k-2}$

$\Rightarrow \sum_{k=2}^{\infty} x^k a_k = 5\sum_{k=2}^{\infty} x^k a_{k-1} - 6\sum_{k=2}^{\infty} x^k a_{k-2}$

$\Rightarrow G(x) - a_1x - a_0 = 5(a_1x^2 + a_2x^3 + \dots) - 6(a_0x^2 + a_1$

$\Rightarrow G(x) - a_1x - a_0 = 5x(a_1x + a_2x^2 + \dots) - 6x^2(a_0 + a_1x +$

$\Rightarrow G(x) - 30x - 6 = 5x(G(x) - 6) - 6x^2 G(x)$

$\Rightarrow G(x)(1 - 5x + 6x^2) = \cancel{30x} + 6 - \cancel{30x}$

$$\Rightarrow G(x) = \frac{6}{6x^2 - 5x + 1} = \frac{6}{(2x-1)(3x-1)} = \frac{6}{(1-2x)(1-}$$

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

$A(1-3x) + B(1-2x) = 6$

$\Rightarrow A + B - x(3A + 2B) = 6$

$\Rightarrow A + B = 6$

$3A + 2B = 0 \Rightarrow (3A + 3B) - B = 0 \Rightarrow 18 - B = 0$

$\Rightarrow B = 18, \quad A = 6 - 18 = -12$

$$\therefore G(x) = \frac{18}{1-3x} - \frac{12}{1-2x}$$

$$\Rightarrow \sum_{k=2}^{\infty} x^k a_k = 18 \sum_{k=2}^{\infty} (3x)^k - 12 \sum_{k=2}^{\infty} (2x)^k$$

Comparing the coefficient of x^k,

$a_k = 18 \cdot 3^k - 12 \cdot 2^k$ (Ans)

Q $a_n = a_{n-1} + 2a_{n-2} + 2^n$, $a_0 = 4$, $a_1 = 12$

$$G(x) - a_1x - a_0 = x[G(x) - a_0] + 2x^2 G(x) + \frac{1}{1-2x}$$

$$\Rightarrow G(x) - 12x - 4 = xG(x) - 4x + 2x^2 G(x) + \frac{1}{1-2x} - (1+2x)$$

Extended Binomial Coefficient

$\binom{u}{k}$ where $u \in R$ and $k \geq 0$.

$$\boxed{\binom{u}{k} = \frac{u(u-1)(u-2)\ldots\ldots[u-(k-1)]}{k!}}$$

Extended Binomial Theorem

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k$$

Q Prove that $\binom{-n}{r} = (-1)^r \, c(n+r-1, r)$.

$$\binom{-n}{r} = \frac{-n(-n-1)(-n-2)\ldots\ldots(-n-(r-1))}{r!}$$

$$= \frac{(-1)^r n(n+1)(n+2)\ldots\ldots[n+(r-1)]}{r!}$$

Multiplying $1, 2, 3, \ldots\ldots (n-1)$.

$$\binom{-n}{r} = (-1)^r \frac{1.2.3.\ldots(n-1)n(n+1)\ldots(n+r-1)}{1.2.3.\ldots(n-1)\ldots r!}$$

$$= (-1)^r \frac{(n+r-1)!}{(n-1)!\, r!}$$

$$= (-1)^r \, c(n+r-1, r) \qquad \left(\because {}^{n}C_{r} = \frac{n!}{(n-r)!\, r!}\right)$$

$(1+2x)$

$$\therefore \boxed{\binom{-n}{r} = (-1)^r \, c(n+r-1, r)}$$

Q i> $(1+x)^{-2}$ ~~= (+~~

$$= \sum_{k=0}^{\infty} \binom{-2}{k} x^k$$

-3

$$= \binom{-2}{0} + \binom{-2}{1} x + \binom{-2}{2} x^2 + \ldots\ldots$$

$$= 1 - 2x + \frac{2.3}{2!} x^2 - \frac{2.3.4}{3!} x^3 + \ldots\ldots$$

ii> $(1+x)^{-3} = \sum_{k=0}^{\infty} \binom{-3}{k} x^k$

$= \binom{-3}{0} + \binom{-3}{1} x + \binom{-3}{2} x^2 + \dots$

$= 1 - 3x + \frac{3.4}{2!} x^2 - \frac{3.4.5}{3!} x^3 + \dots$

$$\boxed{(1+x)^{-n} = 1 - nx + \frac{n(n+1)}{2!} x^2 - \frac{n(n+1)(n+2)}{3!} x^3 \dots}$$

Q Find coefficient of x^{10} in $(x^3 + x^4 + x^5 + \dots)^3$.

$(x^3 + x^4 + x^5 + \dots)^3$

$= x^9 (1 + x + x^2 + \dots)^3$

$= x^9 \left(\frac{1}{1-x}\right)^3$

$= x^9 (1-x)^{-3}$

$= x^9 (1 \cancel{+} {}^{-3}C_1 x + {}^{-3}C_2 x^2 \cancel{+} \dots)$

Coefficient of x^{10}, $= {}^{-3}C_1$

$= (-1)^1 c(3+1-1, 1)(-1)$

$= -({}^{3}C_1)(-1)$

$= 3$.

Q Find coefficient of x^{10} in $1/(1-x)^3$.

$(1-x)^{-3}$

$= 1 - 3x + \frac{3.4}{2!} x^2 - \frac{3.4.5}{3!} x^3 + \dots$

$= \sum_{r=0}^{\infty} {}^{-3}C_r (-x)^r$

For $r = 10$, coefficient $= (-1)^{10} c(3+10-1, 10$

$= {}^{12}C_{10}$

$= \frac{12 \times 11}{2}$

$= 66$

Teacher's Signature..............

Q Find coefficient of x^{10} in $\frac{x^4}{(1-x)^3}$

$= x^4 (1-x)^{-3}$

$= x^4 \sum_{r=0}^{\infty} {}^{-3}C_r (-x)^r$

For $r = 6$, coeff of $x^{10} = (-1)^6 \; {}^{-3}C_6$

$= C(3+6-1, 6)$

$= C(8,6)$

$= \frac{8!}{6!\,2!} = \frac{8 \times 7}{2} = 28$

Q Find the number of solution of $e_1 + e_2 + e_3 = 17$ where $e_1, e_2, e_3 \geq 0$, $2 \leq e_1 \leq 5$, $3 \leq e_2 \leq 6$, $4 \leq e_3 \leq 7$

$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$

For x^{17} : $x^7 \cdot x^5 \cdot x^5$

: $x^7 \cdot x^4 \cdot x^4$

: $x^6 \cdot x^6 \cdot x^5$ coeff $= 3$

No. of solutions $= 3$.

Q In how many different ways can 8 identical cookies be distributed among 3 distinct children if each child receives at least 2 cookies and no more than 4 cookies?

$c_1 + c_2 + c_3 = 8$, $2 \leq c_1, c_2, c_3 \leq 4$.

$(x^2 + x^3 + x^4)^3$

For x^8 : $3\,(x^2 \cdot x^2 \cdot x^4)$

: $3\,(x^3 \cdot x^3 \cdot x^2)$

Coefficient of $x^8 = 6$

No. of ways $= 6$

Teacher's Signature..................

Q Use generating functions to determine the number of different ways in which 10 identical balloons can be given to 4 children if each receives at least 2.

$n = 4$, $r = 10$.

If each receives at least 2, hence it means out of 10, 8 have already been distributed.

Now only 2 are remaining.

$r = 2$

No. of ways $= C(n+r-1, r)$

$= C(4+2-1, 2) = {}^5C_2 = 10$

Q Use generating functions to find the number of r combinations from a set of n elements when repeatation is allowed.

$(1+x+x^2+x^3+\dots)^n$

$= \left(\dfrac{1}{1-x}\right)^n = (1-x)^{-n}$

The coefficient of $x^r = (-1)^r\, C(n+r-1, r)(-1)^r$

$= C(n+r-1, r)$

Q In how many ways can we select 20 pens from an unlimited supply of indistinguishable pens of red, blue and black colours with even number of blue pens?

Here $n = 3$, $r = 20$ = no. of combinations

$\underbrace{(1+x+x^2+\dots)}_{\text{RED}}\underbrace{(1+x+x^2+\dots)}_{\text{BLACK}}\underbrace{(1+x^2+x^4+\dots)}_{\text{BLUE}}$

$= \left(\dfrac{1}{1-x}\right)\left(\dfrac{1}{1-x}\right)\left(\dfrac{1}{1-x^2}\right)$

$= \dfrac{1}{(1-x)^2} \cdot \dfrac{1}{(1-x^2)}$

$$\Rightarrow (x^2 + x^3 + \dots)^4$$
$$= x^8 (1 + x + x^2 + \dots)^4$$
$$= x^8 (1 - x)^{-4}$$

The coefficient of x^{10} in $(x^2 + x^3 + \dots)^4$ is equal to the coefficient of x^2 in $(1-x)^{-4}$.

$\therefore$ coefficient $= \binom{-4}{2}(-1)^2$

$$= (-1)^2 \, C(4+2-1, 2)(-1)^2$$

No. of ways $=$ 10 ways

CONTD...

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

$$\Rightarrow \frac{1}{(1-x)^3(1+x)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{(1-x)^3} + \frac{D}{1+x}$$

Using partial fraction,

$\cancel{A(1-x)^2 + B(1-x)}$

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

$\Rightarrow A(1-2x+x^2)(1+x) + B(1-x^2) + C(1+x) + D(1-x^3-3x+3x^2) = 1$

$\Rightarrow A(1-2x+x^2+x-2x^2+x^3) + B(1-x^2) + C(1+x) + D(1-x^3-3x+3x^2) = 1$

$\Rightarrow A(x^3-x^2-x+1) + B(1-x^2) + C(1+x) + D(1-x^3-3x+3x^2) = 1$

$\Rightarrow$ $A - D = 0 \Rightarrow A = D$

$-A - B + 3D = 0 \Rightarrow B = 2D$

$-A + C - 3D = 0 \Rightarrow C = 4D$

$A + B + C + D = 1 \Rightarrow 8D = 1 \Rightarrow D = 1/8$

$\therefore A = D = \frac{1}{8}, \quad B = \frac{1}{4}, \quad C = \frac{1}{2}$

$$\frac{1}{8(1-x)} - \frac{1}{2(1-x)^2} + \frac{1}{2(1-x)^3} + \frac{1}{8(1+x)}$$

The coefficient of x^{20} is

$$\frac{1}{8} - \frac{1}{2}\binom{-2}{20}(-1)^{20} + \frac{1}{2}\binom{-3}{20}(-1)^{20} + \frac{1}{8}(-1)^{20}$$

Now, $\binom{-2}{20} = (-1)^{20}\, c\,(2+\cancel{8}\,20-1,\ 20) = 21$

$\binom{-3}{20} = (-1)^{20}\, c\,(3+20-1,\ 20) = 231$

$\therefore$ coeff $= \frac{231}{2} - \frac{21}{2} = 105.$

Inclusion - Exclusion Principle

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

Q How many positive integers < 1000 are divisible by 7 or 11 ?

Let A : Set of numbers divisible by 7.

B : " " " " " 11.

$\therefore n(A) = \left\lfloor \frac{1000}{7} \right\rfloor = 142$

$n(B) = \left\lfloor \frac{1000}{11} \right\rfloor = 90$

$\therefore n(A \cap B) = \left\lfloor \frac{1000}{77} \right\rfloor = 12$

$\therefore n(A \cup B) = 142 + 90 - 12 = 220$

$n(A' \cap B') = 1000 - 220 = 780$

Q Find the number of positive integers not exceeding 100 that are either even or divisible by 5.

Let A : Set of numbers divisible by 2 or even

B : Set of numbers divisible by 5.

$|A| = \left\lfloor \frac{100}{2} \right\rfloor = 50$

$|A \cap B| = \left\lfloor \frac{100}{10} \right\rfloor = 10$

$|B| = \left\lfloor \frac{100}{5} \right\rfloor = 20$

$\therefore |A \cup B| = 50 + 20 - 10 = 60$

$\therefore$ not divisible either by 2 or 5 $= 100 - 60 = 40$

Q A total of 12~~00~~32 students have taken a course in spanish, 879 in french, 114 in Russian. Further, 103 have taken courses in both spanish and french, 23 in both spanish and Russian and 14 in french and Russian. If 2092

Teacher's Signature.....................

students have taken at least one of spanish, french and russian, how many have taken in all languages?

$$|A \cup B \cup C| = |A| + |B| + |C| - |AB| - |AC| - |BC| + |ABC|$$

Here,

$$|S \cup R \cup F| = |S| + |R| + |F| - |SR| - |SF| - |RF| + |SRF|$$

Given, $2092 = 1232 + 114 + 879 - 23 - 103 - 14 + |SRF|$

$\Rightarrow |SRF| = 7$

$$|A' \cap B' \cap C'| = N - |A \cup B \cup C|$$

Application of Inclusion - Exclusion Principle

$$|P_1' P_2' P_3'| = N - |P_1 \cup P_2 \cup P_3|$$
$$= N - |P_1| - |P_2| - |P_3| + |P_1 P_2| + |P_2 P_3| + |P_1 P_3| - |P_1 P_2 P_3|$$

Q How many primes are there from 1 to 100?

THEOREM

A composite integer is divisible by its prime not exceeding its square root.

Here, any composite number between 1 to 100 is divisible by primes between $\sqrt{100} = 10$ i.e. by 2, 3, 5, 7.

Let P_1 : Numbers divisible by 2

P_2 : " " " 3

P_3 : " " " 5

P_4 : " " " 7

Now, $|P_1' P_2' P_3' P_4'| = N - |P_1 \cup P_2 \cup P_3 \cup P_4|$

Here, $N = 99$ as "1" is neither prime nor composi

$\therefore |P_1' P_2' P_3' P_4'|$ ~~= 99~~

$= 99 - |P_1| - |P_2| - |P_3| - |P_4| + |P_1 P_2| + |P_1 P_3| + |P_1 P_4| + |P_2 P_3| + |P_2 P_4| + |P_3 P_4| - |P_1 P_2 P_3| - |P_1 P_2 P_4| - |P_1 P_3 P_4| - |P_2 P_3 P_4| + |P_1 P_2 P_3 P_4|$

$= 99 - \lfloor 100/2 \rfloor - \lfloor 100/3 \rfloor - \lfloor 100/5 \rfloor - \lfloor 100/7 \rfloor + \lfloor 100/6 \rfloor + \lfloor 100/10 \rfloor + \lfloor 100/14 \rfloor + \lfloor 100/15 \rfloor + \lfloor 100/21 \rfloor + \lfloor 100/35 \rfloor - \lfloor 100/30 \rfloor - \lfloor 100/42 \rfloor - \lfloor 100/70 \rfloor - \lfloor 100/105 \rfloor + \lfloor 100/210 \rfloor$

RF/

$= 99 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 + 0$

$= 21$

Hence, there are 21 primes (which does not include 2, 3, 5, 7 itself).

$\therefore$ No. of primes $= 21 + 4 = 25$.

Q How many solutions does $x_1 + x_2 + x_3 = 11$ have where x_1, x_2, x_3 are non-negative integers with $x_1 \leq 3$, $x_2 \leq 4$, $x_3 \leq 6$.

Without any constraints, $sol^n = C(n+r-1, r)$

$n = 3, r = 11$ $\quad = C(3+11-1, 11)$

$\Rightarrow N = 78$

$P_1 : x_1 \geq 4$, $\quad P_2 : x_2 \geq 5$, $\quad P_3 : x_3 \geq 7$

$|P_1' P_2' P_3'| = N - |P_1 \cup P_2 \cup P_3|$

$= N - |P_1| - |P_2| - |P_3| + |P_1 P_2| + |P_1 P_3| + |P_2 P_3| - |P_1 P_2 P_3|$

~~= 78~~

For P_1, $r = 11 - 4 = 7$. $\Rightarrow |P_1| = C(3+7-1, 7)$
$= 36$

For P_2, $r = 11 - 5 = 6 \Rightarrow |P_2| = C(3+6-1, 6)$
$= 28$

For P_3, $r = 11-7 = 4 \Rightarrow |P_3| = C(3+4-1, 4) =$

For $P_2 P_1$, $r = 11-4-5 = 2 \Rightarrow |P_2 P_3| = C(3+2-1, 2) = 6$

$P_1 P_3$, $r = 11-4-7 = 0 \Rightarrow |P_1 P_3| = C(3+0-1, 0) = 1$

$P_2 P_3$, $r = 11-5-7 = -1 < 0$ which is not possible

Hence, $|P_2 P_3| = 0$.

Similarly, $|P_1 P_2 P_3| = 0$

$\therefore |P_1' P_2' P_3'| = 78 - 36 - 28 - 15 + 6 + 1 = 6$.

Hence 6 solutions are possible.

Q How many solutions does $x_1 + x_2 + x_3 = 13$ have where x_1, x_2, x_3 are non-negative integers less than 6?

$P_1 : x_1 \geq 6$, $P_2 : x_2 \geq 6$, $P_3 : x_3 \geq 6$

$N = C(3+13-1, 13) = 105$

$|P_1| = C(3+7-1, 7) = C(9,7) = 36 = |P_2| = |P_3|$

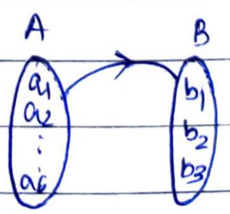
~~$|P_2|$~~ $|P_1 P_2| = C(3+1-1, 1)$

Q How many onto functions are there from a set with 6 elements to a set with 3 elements?

Let $P_1 : b_1$ is not in range

$P_2 : b_2$ " " " "

$P_3 : b_3$ " " " "



No. of possible functions $= 3^6$

$$|P_1' P_2' P_3'| = N - |P_1 \cup P_2 \cup P_3|$$

$$= N - |P_1| - |P_2| - |P_3| + |P_1 P_2| + |P_2 P_3| + |P_1 P_3| - |P_1 P_2 P_3|$$

$$= 3^6 - 2^6 - 2^6 - 2^6 + 1^6 + 1^6 + 1^6 - 0$$

$$= 3^6 - 3 \cdot 2^6 + 3$$

$$= 3^6 - C(3,1) \cdot 2^6 + C(3,2) = 540$$

Q How many onto functions are possible from a set of 7 elements to a set of 5 elements?

$|P_1' P_2' P_3' P_4' P_5'| = 5^7 - C(5,1)\cdot 4^7 + C(5,2)\cdot 3^7 - C(5,3)\cdot 2^7 + C(5,4)\cdot 1^7$

$=$

$$\boxed{\begin{array}{c} m \text{ elements} \longrightarrow n \text{ elements} \\ n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - C(n,3)(n-3)^m + \cdots\cdots C(n,n-1)\cdot 1^m \end{array}}$$

Q How many ways are there to assign 5 different jobs to 4 different students if every student is assigned at least one job?

Here, $m = 5$, $n = 4$, onto function

Every student has a pre-image here.

No. of ways $= 4^5 - C(4,1)\cdot 3^5 + C(4,2)\cdot 2^5 - C(4,3)\cdot 1^5$

$= 240$

Derangements

A derangement is a permutation of objects that leaves no object at its original position.

$$\boxed{\text{No. of derangements} = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots (-1)^n \frac{1}{n!}\right]}$$

Q How many derangements are there for a set of 7 elements?

$= 7!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \frac{1}{6!} - \frac{1}{7!}\right] = 1854$

Q What is the probability that none of 10 people receive the correct hat if a hat-check person hands their hats back randomly?

Q1 In how many ways can 8 distinct balls be distributed into 3 distinct urn if each urn must contain at least one ball?

Q2 Find the number of solutions of the equation $x_1 + x_2 + x_3 + x_4 = 17$ where $x_1, x_2, x_3, x_4 \geq 0$ such that $x_1 \leq 3$, $x_2 \leq 4$, $x_3 \leq 5$, $x_4 \leq 8$.

CH 5

RELATION

Binary Relation: It is a subset of the cartesian product.

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

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

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

If $R = \{(a,b) \mid a < b\}$

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

Relation on a set: A relation from a set to itself $(A \to A)$ or $A \times A$ subset.

Reflexive Relation: A relation is said to be reflexive when $(a,a) \in R \ \forall a \in A$.

ex $A = \{1, 2, 3\} \Rightarrow R: \{(1,1), (2,2), (3,3)\}$ is reflexive.

But for $A = \{1, 2, 3\}$, $R: \{(1,1), (3,3)\}$ is not reflexive

$\boxed{\text{Power set of A has } 2^{n^2} \text{ elements as } |A \times A| = n^2}$

Symmetric Relation: If $(a,b) \in R$ then $(b,a) \in R$

ex For $A = \{1, 2, 3\}$, $R: \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$ is symmetric.

Irreflexive Relation: If a set is not reflexive.

ex Some may not be there as in $R: \{(1,1), (3,3)\}$

Assymetric Relation: If $(a,b) \in R$ but $(b,a) \notin R$.

Antisymmetric Relation: If $(a,b) \in R$ & $(b,a) \in R$ then $a = b$.

ex $/, \leq$

Transitive Relation: If $(a,b) \in R$, $(b,c) \in R$ ~~and~~ then $(a,c) \in R$.

Equivalence Relation: Reflexive + Sym + Transitive

Q Is the relation divides on the set of positive integers, symmetric, assymetric ?

$R = \{ (a,b) \mid a/b \}$

Reflexive, since $(a,a) \in Z^+$

Symmetric, not symmetric / anti-symmetric.

Transitive: $(a/b) \in R$, $(b/c) \in R \Rightarrow (a/c) \in R$

Partially ordered ~~relati~~ relation: If relation is

ex $R = \{ (a,b) : a/b \}$

$R = \{ (a,b) : a \leq b \}$

$R = \{ A \subseteq B, B \subseteq A)$

i> Reflexive

2> symmetric

iii> Transitive

iv> Antisymmetric

Totally ordered relation: A relation is said to be ~~partially~~ totally ordered if it is partially ordered and $\forall a, b \in A$, aRb or bRa.

ex $R = \{ (a,b), a \leq b \}$ $\forall a, b \in Z^+$.

Circular relation: If $(a,b) \in R$ and $(b,c) \in R$ then $(c,a) \in R$.

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

$\equiv (a \neq b) \rightarrow ((a,b) \notin R \vee (b,a) \notin R)$

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

R_1: $\{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4$

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

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

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

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

R_6: $\{(3,4)\}$

R1 Irreflexive as $(3,3)$ is not present.

R2 Symmetric, transitive, circular

R3 Equivalence

R4 Assymmetric, anti-symmetric, irreflexive, transitive

R5 Reflexive, Transitive, assymmetric, anti-symmetric

R6 Assymmetric, anti-symmetric, transitive

(p is F hence $p \to q$ is T.)

Q $A = \{a, b, c\}$

$R1 = \{(a,b), (a,c)\}$

$R2 = \{(a,a), (b,b), (c,c)\}$

R1 Irreflexive, assymmetric, transitive, anti-symmetric

R2 Reflexive, symmetric, transitive i.e. equivalence, anti-symmetric

Q Consider these relations on a set of integers ~~$\{a,b\}$~~,

R1: $\{(a,b) \mid a \leq b\}$

R2: $\{(a,b) : a > b\}$

R3: $\{(a,b) : a = b \text{ or } a = -b\}$

R4: $\{(a,b) : a = b\}$

R5: $\{(a,b) : a = b+1\}$

R6: $\{(a,b) : a+b \leq 3\}$

R1 Reflexive, transitive

R2 Irreflexive, transitive, assymmetric, anti-symm

R3 Reflexive, symmetric, transitive i.e. equivalence, not anti-symmetric

R4 equivalence, anti-symmetric

R5 Irreflexive, assymmetric, anti-symmetric

R6 Irreflexive, symmetric, not transitive,

$(2,1),(1,2) \rightarrow \cancel{(2,2)}$

Q $R_1 \cup R_2$

$R_1 \cap R_2$

$R_1 - R_2$

$R_2 - R_1$ Write for $\{1,2,3,4\}$

7.1 $\boxed{R_1 \oplus R_2 = (R_1 \cup R_2) - (R_1 \cap R_2)}$

Q R is the relation from $\{1,2,3\}$ to $\{1,2,3,4\}$ and $S: \{1,2,3,4\} \longrightarrow \{0,1,2\}$.

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

$S: \{(1,0),(2,0),(3,1),(3,2),(4,1)\}$

What is the composite of R and S?

$S \circ R = \{(1,0),(1,1),(2,1),(2,2),(3,0),(3,1),(2,2)\}$

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

$R^2 \circ R = R^3 \longrightarrow$ Consider R first
Then R^2.

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

Inverse Relation: $R^{-1} = \{(b,a) \mid (a,b) \in R\}$

Complementary Relation: $\bar{R} = \{(a,b) \mid (a,b) \notin R\}$
All ordered pairs from the cartesian product that are not in R.

n-ary Relation: Let $A_1, A_2, A_3 \ldots A_n$ be sets. An n-ary relation on these sets is a subset of $A_1 \times A_2 \times A_3 \times \ldots A_n$. The sets $A_1, A_2, A_3 \ldots A_n$ are called the domains of the relation and n is called as the degree.

Q Let R be the relation on $Z \times Z \times Z$ consisting of all triples (a,b,c) in which a,b,c form an arithmetic progression. Will these triples belong to R?

$(1,3,5) \in R$

$(2,5,9) \notin R$

Teacher's Signature............

Q Let R be the relation on $Z \times Z \times Z^+$ consisting of triples (a, b, m) where a, b, m are integers with $m \geq 1$. Given $R: a \equiv b \pmod{m}$

$= m / (a-b)$.

$(8,2,3) \in R$ $\quad$ $(7,2,3) \notin R$

$(-1,9,5) \in R$ $\quad$ $(-2,-8,5) \notin R$

$(14,0,7) \in R$ $\quad$ $(11,0,6) \notin R$

Number of reflexive relations on a set with n elements $= 2^{(n^2-n)}$

as there will be n fixed elements which need to present in order to become reflexive. And out of $|A \times A| = n^2$ elements, n have already been fixed. Adding even one more element to those fixed n elements does not ruin its reflexivity. Hence there will be $2^{(n^2-n)}$ possible elements (subsets) that can be manipulated ~~and~~ to find reflexive relations

Representing Relations using Matrices

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

$R: A \to B$, $A = \{1,2,3\}$, $B = \{1,2\}$

$$m_{ij} = \begin{array}{c|cc} & 1 & 2 \\ \hline 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 1 & 1 \end{array} \qquad m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

★ Reflexive : All diagonal elements 1

★ Symmetric : If the matrix is symmetric

★ Anti-symmetric : Complementary elements (except diagonal elements) should be diff.

Teacher's Signature..............

Q $M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ Reflexive, Symmetric
Not anti-symmetric

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

$M_{R1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $M_{R2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

$M_{R_1 \wedge R_2} = M_{R_1} \wedge M_{R_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$M_{S \circ R} = M_R \cdot M_S$

Q $M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, $M_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ $M_{S \circ R} = ?$

$M_{S \circ R} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$

$M_{R^2} = M_R \cdot M_R$

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

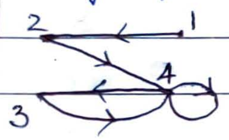
Directed Graphs

A directed graph or digraph consists of a set of vertices (nodes) together with a set E of ordered pairs of elements of V called <u>edges</u> or arcs. 1.

The vertex 'a' is called the initial vertex of the edge (a,b) and the vertex 'b' is called the terminal vertex of the edge. 2.

A graph $G = (V, E)$

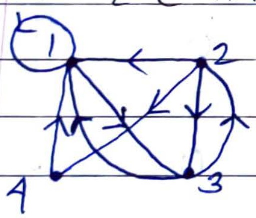
ex



$V = \{1, 2, 3, 4\}$

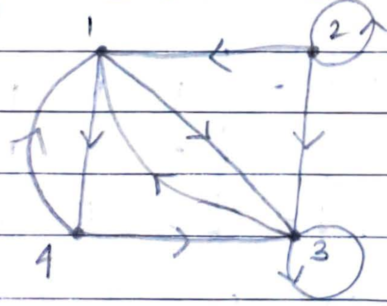
$E = \{\{1,2\}, \{2,4\}, \{4,3\}, \{3,4\},$ 4.
$\underbrace{\{4,4\},}_{\text{Self node}}\}$

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



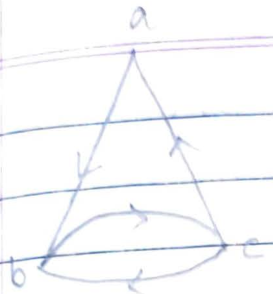
Reflexive : Self loops at all vertices
Symmetric : Cycle between 2 points 1.
Anti-symmetric : Half-cycle for all edges
i.e. if $\{1,2\}$ is present, $\{2,1\}$ is absent

Q Draw the diagraph for relation on
$R = \{(1,3), (1,4), (2,1), (2,2), (2,3), (3,1), (3,3), (4,1), (4,3)\}$



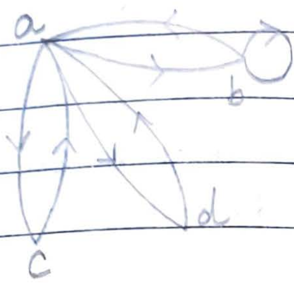
Irreflexive, Assymmetric,
not anti-symmetric,
not Transitive $(1,3), (3,1) \in R$ 2.
but $(1,1) \notin R$

1.



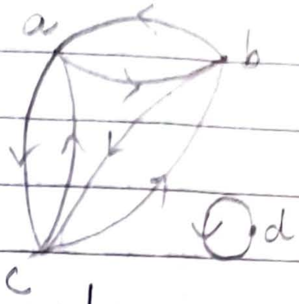
Irreflexive
Asymmetric
Circular

2.



Irreflexive
Symmetric

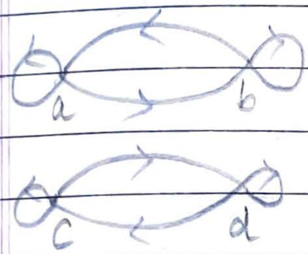
3.



↓

Irreflexive
Symmetric

4.



Reflexive
Symmetric
Transitive
Equivalence

Closure of Relations

1. Reflexive Closure :
The reflexive closure of the relation R is the smallest relation containing R having reflexive propety.

$A = \{1, 2, 3\}$
$R = \{(1,2), (2,3), (3,3)\}$
$R_f = \{(1,2), (2,3), (3,3), (2,2), (1,1)\}$

$$R_f = R \cup \Delta$$

where $\Delta = \{(a,a) \mid a \in A\}$

2. Symmetric Closure
The reflexive closure of the relation R is the smallest relation containing R with symmetric property.

$$R_s = R \cup R^{-1}$$

Teacher's Signature.........

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

3. Transitive Closure

It is the smallest relation containing R with transitive property.

If R is a relation on a set A with n elements, then the transitive closure is $R_t = R \cup R^2 \cup R^3 \ldots \cup R^n$

ex $A = \{1, 2, 3\}$, ~~$R = \{(1,2), (2,1), (3,2), (3,3)\}$~~

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

$R_t = R \cup R^2 \cup R^3$

So, $R^2 = R \circ R$

$= \{(1,3), (2,3), (3,3)\}$ $\left[\begin{matrix}\{(1,2), (2,3), (3,3)\} \\ \{(1,2), (2,3), (3,3)\}\end{matrix}\right.$

$R^3 = R^2 \circ R$

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

$\therefore R_t = R \cup R^2 \cup R^3$

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

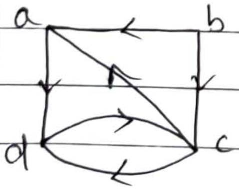
V. Imp. [LQ]

WARSHALL'S ALGORITHM

– Used to find transitive closure

Q Find the transitive closure using Warshall's algorithm

i>



$$M_R = W_0 \quad \begin{array}{c c} & \begin{matrix} a & b & c & d \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \end{matrix} & \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

COL ROW

b, c d

$(b,d), (c,d) \longrightarrow W_1$

Teacher's Signature..........

$$\begin{array}{l} bad \\ cad \end{array} \quad W_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$W_2 = W_1$
as no incoming paths to b.

b, d   a, d

$$W_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

bca, bcd, bcad, dcd, dca

<u>col</u>   <u>Row</u>
a, b, c, d   a, c, d

Order taken is imp.
First <u>col.</u>, then <u>row</u>.

$$W_4 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

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

$$W_0 = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 1 & 0 & 0 & 0 \end{array}, \quad W_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

2, 4   2

1, 2, 4   1, 2, 3

$$W_2 = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 1 & 1 & 0 \\ 2 & 1 & 1 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 1 & 1 & 1 & 0 \end{array}, \quad W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

1, 2, 4   4

1, 2, 3, 4   1, 2, 3, 4

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Teacher's Signature......................

iii) $A = \{a, b, c, d, e\}$

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

$$W_0 = \begin{array}{c|ccccc} & a & b & c & d & e \\ \hline a & 0 & 0 & 1 & 0 & 0 \\ b & 0 & 0 & 0 & 1 & 0 \\ c & 1 & 0 & 0 & 0 & 0 \\ d & 0 & 1 & 0 & 0 & 0 \\ e & 0 & 0 & 0 & 1 & 0 \end{array} \quad , \quad W_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

c c d d

$$W_2 = \begin{array}{c|ccccc} & a & b & c & d & e \\ \hline a & 0 & 0 & 1 & 0 & 0 \\ b & 0 & 0 & 0 & 1 & 0 \\ c & 1 & 0 & 1 & 0 & 0 \\ d & 0 & 1 & 0 & 1 & 0 \\ e & 0 & 0 & 0 & 1 & 0 \end{array} \quad , \quad W_3 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

a,c a,c b,d,e b,d

$$W_4 = \begin{array}{c|ccccc} & a & b & c & d & e \\ \hline a & 1 & 0 & 1 & 0 & 0 \\ b & 0 & 1 & 0 & 1 & 0 \\ c & 1 & 0 & 1 & 0 & 0 \\ d & 0 & 1 & 0 & 1 & 0 \\ e & 0 & 1 & 0 & 1 & 0 \end{array} \quad , \quad \begin{array}{c} W_5 = \\ (= W_4) \end{array} \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

∴ the required transitive closure for R is

$R_{t.c} = \{(a,a), (a,c), (b,b), (b,d), (c,a),$
$(c,c), (d,b), (d,d), (e,b), (e,$

Equivalence Relation

$(a \sim b)$

Two elements a & b ~~a~~ that are related by an equivalence relation are said to be equivalent

Q Let R be the relation on the set of $\{a, b\}$ such that $a R b$ iff $a = b$ or $a = -b$. Is R an equivalence relation?
Yes

Q Let R be the relation on the set of real numbers such that $a R b$ iff $a - b$ is an integer. Is R an equivalence relation?

- $a - a$ is an integer, hence reflexive.
- $a - b \in Z$ and $b - a \in Z$ (with negative sign) hence symmetric.
- $a - b \in Z$ and $b - c \in Z$ $\therefore$ $a - c \in Z$.

Hence yes it is an equivalence relation.

Q Prove that the congruence modulo 'm' is an equivalence relation.

$$R = \{(a, b) \mid a \equiv b \pmod m\}, \quad m > 1$$

- $a \equiv a \pmod m$
  $\because m / (a - a)$ or $m / 0$.
  Hence $(a, a) \in R \Rightarrow R$ is reflexive.
- If $a \equiv b \pmod m$
  $\Rightarrow m / (a - b)$
  $\Rightarrow a - b = mk, \; k \in Z$
  $\therefore b - a = -mk = m(-k) \Rightarrow m / (b - a)$
  $\Rightarrow b \equiv a \pmod m$
  Hence $(b, a) \in R \Rightarrow R$ is symmetric
- If $a \equiv b \pmod m$
  $\Rightarrow m / (a - b) \Rightarrow a - b = mk_1, \; k_1 \in Z$

Also if $b \equiv c \pmod{m}$

$\Rightarrow b - c = m k_2 \quad , \quad k_2 \in Z$

Adding, $a - c = m(k_1 + k_2)$

$\Rightarrow a - c = mk \quad , \quad k \in Z$ as $k = k_1 + k_2$

$\Rightarrow a \equiv b \pmod{m}$.

Hence R is transitive

$\therefore$ congruence modulo m is an equivalence relation

Q $R = \{(a,b) \mid a \text{ divides } b\}$

Reflexive, asymmetric, anti-symmetric

Q Let R be the relation on the set of real numbers such that $x R y$ iff x & $y \in$ real no.s that differ by 1. Is R an equivalence relation?

Given, $x R y$ iff $|x - y| < 1$.

- $|x - x| < 1$, reflexive
- $|x - y| < 1$ then $|y - x| < 1$. Symmetric
- If $x = 5.5, \quad y = 5, \quad z = 4.5$

  $|x - y| = 0.5, \quad |y - z| = 0.5$

  $\therefore |x - z| = 1$.

Hence, it is not transitive.

OR, $x = 5.5, \quad y = 5, \quad z = 4.3$

$|x - y| = 0.5, \quad |y - z| = 0.7$

& $|x - z| = 1.2 > 1$

Hence, it is not transitive.

Equivalence class:

Let R be an equivalence relation on set A. The set of all elements that are related to element 'a' is called the equivalence class of A. It is denoted as $[a]_R$.

Teacher's Signature..................

Equivalence Classes

Q What ~~is~~ re the equivalence classes ~~for~~ of 0 and 1 for congruence modulo 5.

$a \equiv b \pmod 5$

$[0]$ $a \equiv 0 \pmod 5$

$\therefore [0] = \{\ldots -10, -5, 0, 5, 10, \ldots\}$

$[1]$ $a \equiv 1 \pmod 5 \Rightarrow 5 / (a-1)$.

$\therefore [1] = \{\ldots -9, -4, 1, 6, 16 \ldots\}$

For 5, we can have 5 disjoint equivalence classes i.e. $[0], [1], [2], [3], [4]$.
Taking the union of all these disjoint equivalence classes will give us the set of all integers.

Here, $[2] = \{\ldots -8, -3, 2, 7, 12 \ldots\}$

$[3] = \{\ldots -7, -2, 3, 8, 13 \ldots\}$

$[4] = \{\ldots -6, -1, 4, 9, 14 \ldots\}$

So, $[0] \cup [1] \cup [2] \cup [3] \cup [4] \in Z$

Q For $R : \{(a,b) \mid a = b \text{ or } a = -b\}$, $a, b \in Z$

$[3] = \{3, -3\}$

$[-3] = \{3, -3\}$

Since $R = \{(1,1), (1,-1), (2,2), (2,-2), (3,3), (3,-3), (-3,3), (-3,-3) \ldots\}$

Q What are the sets in the partition of the integers arising from congruence modulo 5?

$[0] = \{5k\}$, $[1] = \{5k+1\}$, $[2] = \{5k+2\}$,

$[3] = \{5k+3\}$, $[4] = \{5k+4\}$

Now, $[5] = [0] \ldots$

Teacher's Signature........................

→ Partition of a set S means collection of disjoint subsets of S, the union of which gives the entire set S of domain which is the set of integers here.

How many possible partitions for a set of integers
Infinitely many

. Partition P1 is called a refinement of partition P2 if every set in P1 is a subset of one of the sets in P2

Q Congruence modulo 3 and congruence modulo 6.
Which one is a refinement of the other?

$[0]_3 = \{ \dots -9, -6, -3, 0, 3, 6, 9 \dots \}$
$[1]_3 =$
$[2]_3 =$

$[0]_6 = \{ \dots -12, -6, 0, 6, 12, 18, \dots \}$
$[1]_6 = 6k+1$ $\quad [4]_6 =$
$[2]_6 = 6k+2$ $\quad [5]_6 =$
$[3]_6 = 6k+3$
Here 6 is the refinement of 3.

PROVE Show that the partition form from congruence classes modulo 6 is a refinement of the partition form from congruence classes modulo 3.
$P_1 = \{ [0]_3, [1]_3, [2]_3 \}$
$P_2 = \{ [0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \}$
Hence P2 is a refinement of P1.

V. Imp. The partition with more number of classes is a refinement of the other.

Teacher's Signature..........

ii) $ad = bc$

Q Let R be the relation on the set of ordered pairs of positive integers such that $((a,b),(c,d)) \in R$ iff

i) $a+d = b+c$. Show that R is an equivalence relation

Reflexive : $((a,b),(a,b))$: $a+b = b+a$ is T.

Hence $((a,b),(a,b)) \in R$.

Symmetric : $((a,b),(c,d))$: $a+d = b+c$.

$((c,d),(a,b))$: $c+b = d+a$ ~~is~~ T.

$\Rightarrow$ $b+c = a+d$ is T.

$\therefore$ $((c,d),(a,b)) \in R$.

Transitive : $((a,b),(c,d))$: $a+d = b+c$

$((c,d),(e,f))$: $c+f = d+e$.

$\therefore$ $((a,b),(e,f))$: $a+f = b+e$

$\Rightarrow$ $a+\underline{d}+\underline{c}+f = b+\underline{c}+\underline{d}+e$

Hence, $((a,b),(e,d)) \in R$. is T

Partially Ordered Sets

Posets

- A totally ordered set is also called as chain.

Poset: A non-empty set S together with a ~~partiallytotally~~ partially-ordered relation ($\preceq$)
NOTATION (S, R) where R is a partially ordered
or ($S, \preceq$).

- Two elements 'a' & 'b' of a poset ($S, \preceq$) are called comparable if either $a \preceq b$ or $b \preceq a$ when 'a' & 'b' are elements of S when neither $a \preceq b$ nor $b \preceq a$, then they are said to be comparable.
- When every two elements in the set are comparable a set is called a total ordering or linear ordering

Lexicographic Ordering

Lexicographic ordering $\preceq$ on $A_1 \times A_2$ is defined by specifying that one pair is less than a second pair if the first entry of the first pair is less than the first entry of the second pair, or if the first entries are equal, but the second element of the ~~second~~ first pair is less than the second element of the second pair.

ex discreet $\prec$ discrete

Q Find the lexicographic ordering of the bit strings 0, 01, 11, 001, 010, 011, 0001, 0101.

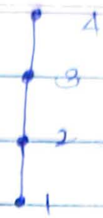
0 $\prec$ 0001 $\prec$ 001 $\prec$ 01 $\prec$ 010 $\prec$ 0101 $\prec$ 011 $\prec$ 11

Hasse Diagram

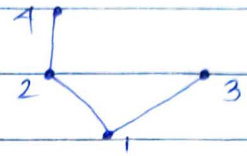
It is used only for posets.

Hasse Diagrams

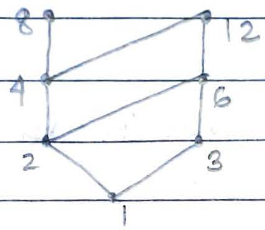
ex $(\{1,2,3,4\}, \leq)$



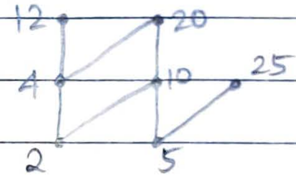
$(\{1,2,3,4\}, /)$



Q i> Draw the hasse diagram for $(\{1,2,3,4,6,8,12\}, /)$



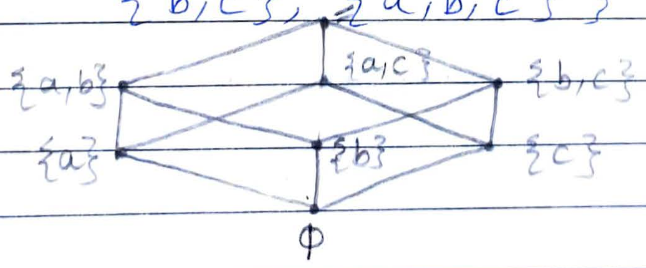
ii> $(\{2,4,5,10,12,20,25\}, /)$



iii> $A = \{a,b,c\}$, $(P(A), \subseteq)$

~~$P(A) = \{\{a,a\}, \{a,b\}, \{a,c$~~

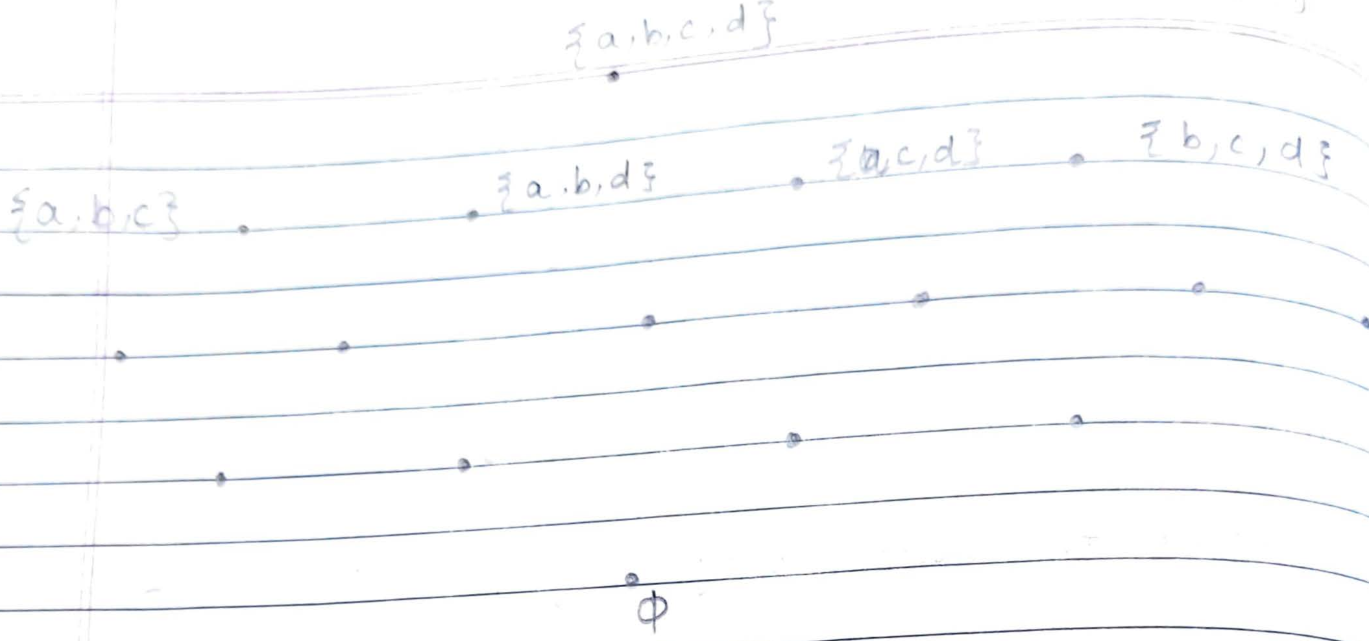
$P(A) = \{ \phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\},$
$\{b,c\}, \{a,b,c\}\}$



iv> $A = \{a,b,c,d\}$, $(P(A), \subseteq)$

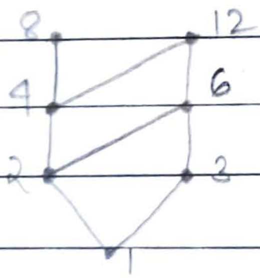
$P(A) = \{ \phi, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{b,c\},$
$\{a,d\}, \{a,c\}, \{a,b,c\}, \{a,b,d\}, \{a,c,d\},$
$\{b,c,d\}, \{b,d\}, \{c,d\}, \{a,b,c,d\}\}$

Teacher's Signature.........................

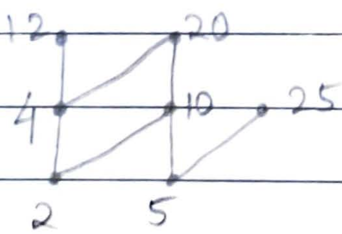


Maximal and Minimal Elements

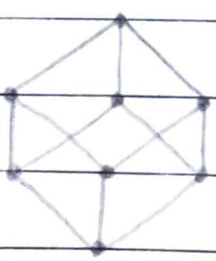
Let $(S, \subseteq)$ be a poset, an element $a \in S$ is called maximal element or is maximal if there is no $b \in$ (belonging to S) such that $a < b$.



Maximal : 8, 12
Minimal : 1



Maximal : 12, 20, 25
Minimal : 2, 5

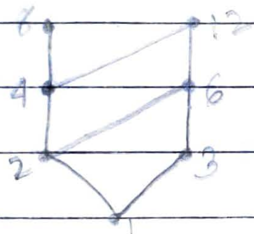


Greatest and Least Elements

Let $(S, \leq)$ be a poset, an element 'a' $\in S$ is called the greatest element if $b \leq a \ \forall\ b \in S$.

An element 'a' $\in S$ is said to be the least element if $a \leq b \ \forall\ b \in S$.

Greatest and least elements are unique – can not be more than one. Hence from the hasse diagram, if there are more than one maximal or minimal elements, then there is no greatest or least element respectively.



No greatest element

Upper bounds and Lower bounds

lub : ~~Lowest~~ least upper bound

glb : Greatest ~~upper~~ lower bound

Let $(S, \leq)$ be a poset and $A \subseteq S$, an element $u \in S$ is called an upper bound if $a \leq u \ \forall a \in A$

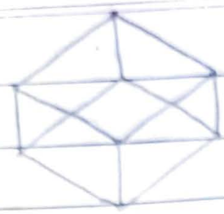
Let $(S, \leq)$ be a poset and $A \subseteq S$, an element $l \in S$ is called a lower bound if $l \leq a \ \forall\ a \in A$.

The greatest of all ~~upper~~ lower bounds is called glb.
The least of all upper bounds is called lub.

lub and glb are unique always.

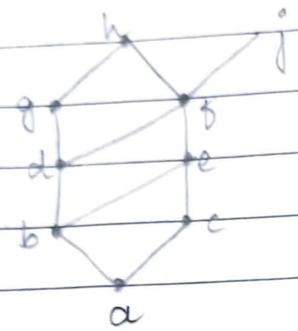
$A = \{\{a\}, \{b\}\}$

i)



upper bounds $= \{a, b\}, \{a, b, c\}$
Lower bounds $= \phi$
glb $= \phi$, lub $= \{a, b\}$

Q Find the upper and lower bounds for the following



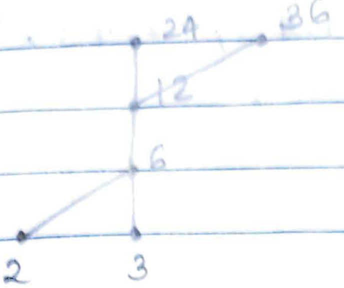
i) $A = \{a, b, c\}$
u.b. $= \{e, f, h, j\}$
l.b. $= \{a\}$ = glb
lub $= \{e\}$

ii) $A = \{j, h\}$ u.b. = no ub, no lub
l.b. $= \{f, e, c, a, d, b\}$
glb $= \{f\}$

iii) $A = \{a, c, d, f\}$ u.b. $= \{f, j, h\}$
lub $= f$
l.b. $= a$ = glb

iv) $A = \{b, d, g\}$ u.b. $= \{g, h\}$
lub $= g$
l.b. $= \{a, b\}$, glb =

Q i) Draw the Hasse diagram for $(\{2, 3, 6, 12, 24$
Find the greatest, least, maximal and mini
elements. Find the upper bounds, lower bounds
lub and glb for the following sets.
a) $A = \{2, 3, 6\}$
b) $B = \{2, 3\}$
c) $C = \{6, 12\}$



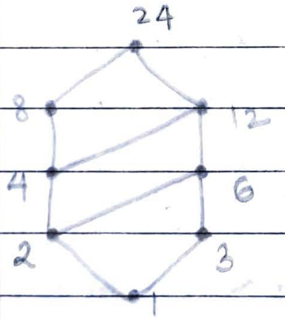
Maximal : 24, 36
Minimal : 2, 3
No greatest or least element

a) u.b. = {6, 12, 24, 36} , lub = 6
l.b. = no lower bounds , no glb.

b) u.b. = {6, 12, 24, 36} , lub = 6
l.b. = no lower bounds , no glb.

c) ~~u.b.~~ A = {6, 12}.
u.b. = {24, 36, 12} , lub = 12
l.b. = {2, 3} . , glb = 3.

ii) ({1, 2, 3, 4, 6, 8, 12, 24}, /)



Maximal = 24 = greatest
Minimal = 1 = lowest

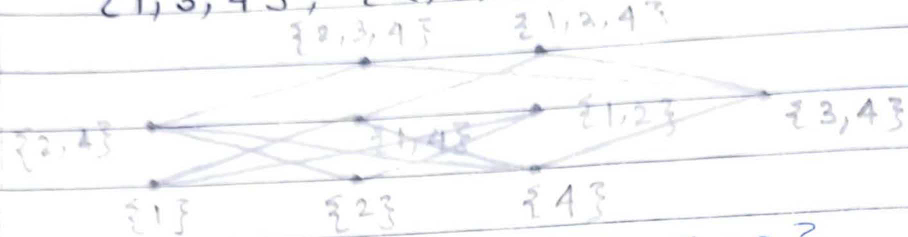
a) {8, 12} u.b. = {24} l.b. = {1, 2, 4}
lub = 24 glb = 4

b) {3, 4} u.b. = {12, 24} l.b. = {1}
lub = 12 glb = 1

c) {6, 8, 12} u.b. = {24} l.b. = {1, 2}
lub = 24 glb = 2

Teacher's Signature......................

iii> $(\{\{1\},\{2\},\{4\},\{1,2\},\{1,4\},\{2,4\},\{3,4\},$
$\{1,3,4\},\{2,3,4\}\}, \subseteq)$



Minimal = $\{\{1\},\{2\},\{4\}\}$
Maximal = $\{\{1,3,4\},\{2,3,4\}\}$

a> ~~u.b.~~ $\{\{2\},\{4\}\}$ u.b. = $\{\{2,4\},\{2,3,4\}\}$
lub = $\{2,4\}$ ~~l.b. = $\{\{2\},\{4\}\}$~~ No lb, glb
why?

b> $\{\{1,3,4\},\{2,3,4\}\}$ No ub, lub
l.b. = $\{\{4\},\{3,4\}\}$, glb = $\{3,4\}$

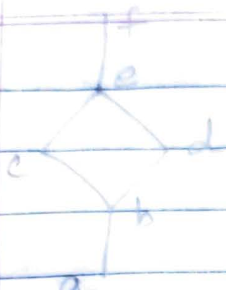
Q Find lub and glb of $\{3,9,12\}$ and $\{1,2,4,5,$
if they exist in the poset $(Z^+, /)$.
lub is LCM and glb is GCD.
Here, lub = LCM(3,9,12) = 36
glb = GCD(1,2,4,5,10) = 3
glb is GCD and lub is ~~multiple~~ LCM for (
lub = LCM(1,2,4,5,10) = 20
glb = GCD(1,2,4,5,10) = 1

For subset $\subseteq$ in power set, lub = $A \cup B$
glb = $A \cap B$

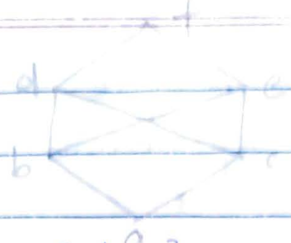
Lattices

It is a poset where every pair of element h
and glb.

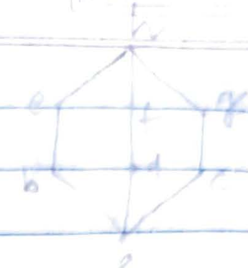
Lattices



Lattice



For $\{d, e\}$, no glb
For $\{b, c\}$, no lub

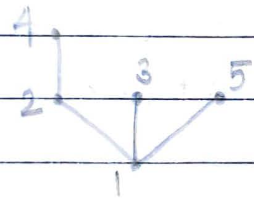


Lattice

$(Z^+, \div)$ is a lattice.
$(P(A), \subseteq)$ is a lattice where $P(A)$ = Power set of A

Q Determine whether the posets are lattices or not.
i> $(\{1, 2, 3, 4, 5\}, /)$
ii> $(\{1, 2, 4, 8, 16\}, /)$

i>



Not a lattice as $\{2, 3\}$ does not have any lub.

ii>

Lattice

Q Let R be a ~~symmetric~~ reflexive and transitive relation on a set A. Show that if $\forall a \in A$, there is $b \in A$ such that $(a, b) \in R$, then R is an equivalence relation.

Given R is reflexive and transitive.
$(a, a) \in R \Rightarrow (a, a) \in T$ (Reflexive)
If $(a, b) \in T \Rightarrow (a, b)$ & $(b, a) \in R$
$\Rightarrow (b, a)$ & $(a, b) \in R \Rightarrow (b, a) \in T$ (Symmetric)
If (a, b) & $(b, c) \in T$
$\Rightarrow (a, b), (b, a)$ & $(b, c), (c, b) \in R$
$\Rightarrow (a, c) \in R$ & $(c, a) \in R$ ($\because$ R is transitive)
$\Rightarrow (a, c) \in T$ (Transitive)

Teacher's Signature...............

Algebraic System

Groups, Semi groups & Monoids

[Lia]

Page No.
Date: / /

Any non-empty set A (i.e. $A \neq \phi$) together with one or more binary operations is called an algebraic system.

A binary operation on a set A is a mapping from $A \times A \to A$. Let 'a' & 'b' be two elements in A, then $a * b \in A$.

1 Closure Property: Let $(A, *)$ be an algebraic system. 'A' is said to be closed if $\forall (a,b) \in A$, $(a*b) \in A$.

2 Associative Property: Let A be a non-empty set and $*$ is a binary operation, then set A is said to be associative if $\forall a,b,c \in A$ then $a*(b*c) = (a*b)*c$.

3 Commutative Property: $a*b = b*a \quad \forall a,b \in A$.

4 Existence of Identity: Let $(A, *)$ be an algebraic system, an element $e \in A$ is called an identity element if $a*e = e*a = a \quad \forall a \in A$.

Left identity

★ 0 is the additive identity and 1 is multiplicative ide (but not always).

5 Existence of Inverse: Let $(A, *)$ be an algebraic system, $\forall a \in A$, $\exists a^{-1} \in A$ such that $a * a^{-1} = e$.

Imp.

Semi-groups

A non-empty set S together with a binary operation $*$ is said to be a semi-group if it satisfies the closure property and associative property.

ex $(N, +)$

Teacher's Signature.........

Page No.
Date: / /

Imp. Monoids : Any non-empty set M together with a binary operation $*$ is said to be monoid if it satisfies the closure property, associative property and the existence of identity element.

ex $(W, +)$

Imp. Groups (G): Any non-empty set G together with a binary operation $*$ is said to be a group if it satisfies the closure property, associative property, existence of identity and inverse.

ex $(Z, +)$, $e = 0$
$\longrightarrow a, (-a)$ where $(-a)$ is a^{-1}.

V. Imp. Abelian Group : A group is said to be abelian if it satisfies the commutative property also.

ex $(Z^+, +)$

Order of a group : Number of elements in the group

ex Set of integers : Infinite abelian group

$(Z, \times) \rightarrow$ not a group because inverse property is not satisfied as $a^{-1} \notin Z$ always. For 2, $1/2 \notin Z$.

$(Q, \times) \rightarrow$ not a group though it satisfies all properties as inverse for 0 doesn't exist

$(Q - \{0\}, \times) \rightarrow$ a group

$(R - \{0\}, \times) \rightarrow$ Group

Teacher's Signature..................

Page No.
Date: / /

Trivial Groups: Taking identity elements with binary operation.
ex $(\{0\}, +)$, $(\{1\}, \times)$

Q Is $(\{1, \omega, \omega^2\}, \times)$ a group?
$e = 1$, inverse of $1 = 1$
inverse of $\omega = \omega^2$ $\left(\because \frac{1}{\omega} = \frac{\omega^2}{\omega^3} = \frac{\omega^2}{1}\right)$
inverse of $\omega^2 = \omega$

Cayley's Table

$\times$	1	ω	ω^2
1	$\boxed{1}$	ω	ω^2
ω	ω	ω^2	$\boxed{1}$
ω^2	ω^2	$\boxed{1}$	ω

Search for the identity element, the column in which it is present for a particular row, is its identity.

Q Is $(\{1, -1, i, -i\}, \times)$ a group?

$\times$	1	-1	i	$-i$
1	$\boxed{1}$	-1	i	$-i$
-1	-1	$\boxed{1}$	$-i$	i
i	i	$-i$	$\boxed{-1}$	$\boxed{1}$
$-i$	$-i$	i	$\boxed{1}$	-1

Closure, associative,
$e = 1$
$1^{-1} = 1$, $-1^{-1} = -1$,
$i^{-1} = -i$, $-i^{-1} = i$

★ All entries of table $\in$ elements of set, hence closure
★ $i(-1 \cdot -i) = (i \cdot -1)(-i)$, hence associative
★ Abelian group with order 4.

Q The set of all 2×2 matrices with real entries under matrix addition will form a group?

$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in R \right.$

Closure $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix} \in R \Rightarrow \in G$

induction, $n = 0$, $P(0)$ if true

Teacher's Signature.........

- Matrix addition is associative.
- $e = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ or the null matrix as

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- Inverse $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + i = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow i = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$

$\therefore \forall$ matrix A, inverse $= -A$.

- Matrix addition is commutative as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\therefore$ this is an infinite abelian group.

Q The collection of all non-singular 2×2 matrices with real entries under matrix multiplication. Is this a group?

given $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in R \;\&\; ad - bc \neq 0 \right.$

Closure $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + c_1d_2 \end{pmatrix}$

$\in R$

$\in G$

Associative Since matrix multiplication is associative.

- $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ = identity matrix as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}_{2 \times 2}$$

Inverse. For any set $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $A^{-1} = \frac{1}{|A|} \operatorname{adj} A$

as A is not singular. For non-singular matrices inverse exists.

Teacher's Signature..........................

Matrix multiplication is not commutative.
Hence, this is an infinite non-abelian group.

Q $G = R - \{0\}$ $\forall a, b \in G$, $a * b = \frac{ab}{2}$. will this be a group?

1. CLOSURE $\forall a, b \in R - \{0\}$, $a * b = \frac{ab}{2} \in R - \{0\}$

$\Rightarrow a * b \in G$.

Hence, closure is satisfied.

2. ASSOCIATIVE $\forall a, b, c \in R - \{0\}$,

$(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4}$

$a * (b * c) = a * \frac{bc}{2} = \frac{abc}{4}$

Hence, association is satisfied.

3. IDENTITY

$\forall a \in R - \{0\}$, $a * e = e * a = a$,

$\Rightarrow ae/2 = ea/2 = a$

$\Rightarrow e = 2$.

4. INVERSE

$\forall a \in R - \{0\}$, $a * a^{-1} = e = 2$

$\Rightarrow \frac{aa^{-1}}{2} = 2 \Rightarrow a^{-1} = \frac{4}{a}$.

Abelian group

Q $G = R - \{1\}$ $\forall a, b \in G$, $a * b = a + b - ab$.

1. CLOSURE

$\forall a, b \in R - \{1\}$, $a * b = a + b - ab \neq 1$.

$\in R - \{1\}$

2. ASSOCIATIVE

$\forall a, b, c \in R - \{1\}$, $(a * b) * c = (a + b - ab) * c$

Teacher's Signature..............

$= a+b-ab+c-ac-bc+abc \in R-\{1\}$

~~∴ associative~~

$a*(b*c) = a*(b+c-\cancel{ab}\,bc)$

$= a+b+c-bc-ab-ac+abc$

hence associative property holds good.

3. IDENTITY

$\forall a \in R-\{1\}, \quad a*e = a+e-ae = a.$

$\Rightarrow \cancel{a}+e(1-a) = \cancel{a}$

$\Rightarrow e = \cancel{\frac{1}{1-a}}\ 0 \quad (\because 1-a \neq 0$ as $a \neq 1)$

4. INVERSE

$\forall a \in R-\{1\}, \quad a*a^{-1} = a+a^{-1}-aa^{-1} = e$

$\Rightarrow a+a^{-1}-aa^{-1} = \cancel{\frac{1}{1-a}}\ 0$

$\Rightarrow a+a^{-1}(1-a) = \cancel{\frac{1}{1-a}}\ 0$

$\Rightarrow \boxed{a^{-1} = \frac{a}{a-1}}$

5. COMMUTATIVE

$\forall a,b \in R-\{1\}, \quad a*b = a+b-ab,$

$b*a = b+a-ba$

Hence, this is an abelian group.

Q Will $(Z_5, \oplus_5)$ be a group? → modulo addition

$Z_5 = \{[0],[1],[2],[3],[4]\}$

CLOSURE ✓ (from Table)

$\oplus_5$	[0]	[1]	[2]	[3]	[4]
[0]	$\boxed{[0]}$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	$\boxed{[0]}$
[2]	[2]	[3]	[4]	$\boxed{[0]}$	[1]
[3]	[3]	[4]	$\boxed{[0]}$	[1]	[2]
[4]	[4]	$\boxed{[0]}$	[1]	[2]	[3]

Page No.
Date: / /

2. ASSOCIATIVE

ex $[2] \oplus_5 ([3] \oplus_5 [4])$

$= [2] \oplus_5 [2] = [4]$.

$([2] \oplus_5 [3]) \oplus_5 [4] = [0] \oplus_5 [4] = [4]$.

3. IDENTITY

$e = [0]$

4. INVERSE

Inverses of $[0]^{-1} = [0]$, $[1]^{-1} = [4]$, $[2]^{-1} = [3]$,
$[3]^{-1} = [2]$, $[4]^{-1} = [1]$.

This is an abelian group.

~~Q (Z_6,~~ $\boxed{Z_n, \oplus_n}$ is a group always

Q Is $(Z_6, \otimes_6)$ a group?

$\otimes_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

1. CLOSURE

As all the elements of the Cayley's table $\in G$ hence it is closure property.

2. ASSOCIATIVE

$[2]([3]\cdot[4]) = ([2]\cdot[3])[4] = [0]$

3. IDENTITY

$e = [1]$

4. INVERSE

Inverse does not exist for every element. Hence Z_6 is not a group.

Teacher's Signature................

Scanned by CamScanner

Page No.
Date: / /

Imp.

Q. Check if $(Z_5 - [0], \otimes_5)$ is a group?

$\otimes_5$	[1]	[2]	[3]	[4]
[1]	$\boxed{[1]}$	[2]	[3]	[4]
[2]	[2]	[4]	$\boxed{[1]}$	[3]
[3]	[3]	$\boxed{[1]}$	[4]	[2]
[4]	[4]	[3]	[2]	$\boxed{[1]}$

1. CLOSURE

As all the elements in the table $\in G$.

2. ASSOCIATIVE

$[2]([3].[4]) = [2].[2] = [4]$.

$([2].[3])[4] = [1].[4] = [4]$.

Hence, associative property holds good.

3. IDENTITY

$e = [1]$

4. INVERSE

Inverse of $[1] = [1]$, Inverse of $[2] = [3]$,

" " $[3] = [2]$, " " $[4] = [4]$.

5. COMMUTATIVE

$[2].[4] = [3]$ & $[4][2] = [3]$

Hence, commutative property holds good too.

Therefore, $(Z_5 - [0], \otimes_5)$ is an finite abelian group.

Q Is $(Z_6 - [0], \otimes_6)$ a group?

$\otimes_6$	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[2]	[0]	[4]	[3]
[5]	[5]	[4]	[3]	[2]	[1]

As $[0] \notin G$, the given ~~group~~ set is not closure, hence not a group.

Teacher's Signature..................

Q Is $(Z_7 - [0], \otimes_7)$ a group?

$\otimes_7$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[8]				
[5]						
[6]						

This is a finite group.

$\boxed{(Z_p - [0], \otimes_n) \text{ where } p: \text{prime number is ALWAYS a group.}}$

Q Prove that the identity element of a group is unique.

Let us assume that the group $(G, *)$ has two identity elements e_1 and e_2.

$e_1 = e_1 * e_2$ ($\because e_2$ is identity)

$\Rightarrow e_1 = e_2$ ($\because e_1$ is identity)

Q Let $(G, *)$ be a group. Prove that every element has a unique inverse.

Let $a \in G$. Assume that a has two inverses x & y.

$a * x = x * a = e$.

$a * y = y * a = e$ ($\because y$ is also inverse)

Now, $x = x * e$

$= x * (a * y)$

$= (x * a) * y$ (Associative law)

$= e * y$

$\Rightarrow x = y$

Cancellation Laws

Page No.
Date: / /

Right Cancellation Law

If $x * a = y * a \Rightarrow x = y$.

Left Cancellation Law

If $a * x = a * y \Rightarrow x = y$

PROOF

$a^{-1} * a * x = a^{-1} * a * y \Rightarrow e * x = e * y \Rightarrow x = y$

Q Let $(G, *)$ be a group, let $a \in G$, prove that $(a^{-1})^{-1} = a$.

$\forall a \in G$, $\exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

It can be concluded that the inverse of a^{-1} is a.

Hence, mathematically $(a^{-1})^{-1} = a$.

Q Let $(G, *)$ be a group, $\forall a, b \in G$. Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$.

CLAIM The inverse of $a * b$ is $b^{-1} * a^{-1}$.

PROOF $(a * b) * (b^{-1} * a^{-1})$

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

$= (a * e) * a^{-1}$ $(\because b * b^{-1} = e)$

$= a * a^{-1}$ $(\because a * e = a)$

$= e$

Similarly, $(b^{-1} * a^{-1}) * (a * b)$

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

$= (b^{-1} * e) * b$

$= b^{-1} * b = e$.

$\therefore (a * b)$ is the inverse of $(b^{-1} * a^{-1})$.

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

Q Let $(G, *)$ be a group and $a^2 = e$ where $a \neq e$ then prove that G is abelian where $a^2 = a * a$.

Teacher's Signature.......................

Page No.
Date: / /

CLAIM $a * b = b * a$

PROOF $a^2 = e \Rightarrow a * a = e$

$\Rightarrow a^{-1} = a \quad (\because a * a^{-1} = e)$

Every element (which is not the identity element) is the inverse of itself.

Now, $a * b = a^{-1} * b^{-1}$

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

OR If every element of a group $(G, *)$ is its own inverse prove that G is abelian.

Q Let $(G, *)$ be a group so that the group is abelian iff $a^2 * b^2 = (a * b)^2$.

Let us assume that $(G, *)$ is an abelian group.

$\Rightarrow a * b = b * a \quad \forall a, b \in G$

$a^2 * b^2$

$= (a * a) * (b * b)$

$= a * (a * b) * b = a * (b * a) * b \quad (\because a * b = b * a)$

$= (a * b) * (a * b)$

$= (a * b)^2$

Now, given that $(a * b)^2 = a^2 * b^2$

Claim $(G, *)$ is abelian.

$a^2 * b^2 = (a * b)^2$

$\Rightarrow (a * a) * (b * b) = (a * b) * (a * b)$

$\Rightarrow a * (a * b) * b = (a * (b * a) * b)$

$\Rightarrow a * b = b * a$ (using right & left cancellation laws)

As $(G, *)$ is commutative, hence it is an abelian group as well.

Q Let $(A, *)$ be a semi-group. Furthermore, $\forall a, b \in A$

Teacher's Signature.................

Page No.
Date: / /

if $a \neq b$, then $a * b \neq b * a$

i> Show that $\forall a \in A$, $a * a = a$

ii> $\forall a, b \in A$, $a * b * a = a$

iii> $\forall a, b, c \in A$, $a * b * c = a * c$

Page No.
Date: / /

Q Let $(A, *)$ be a monoid such that $\forall x$ in A, $x * x = e$ where e is the identity element. Prove that it is an abelian group.

Order of an element

Let $(G, *)$ be a group. Let $'a' \in G$. The order of an element is the least positive integer 'm' such that $a^m = e$.

If such an 'm' does not exist, then order of element is ∞.

ex $\{1, -1, i, -i\}$

$1^1 = 1$, $o(1) = 1$

$(-1)^2 = 1$, $o(-1) = 2$

$i^4 = 1$, $o(i) = 4$, $(-i)^4 = 1$, $o(-i) = 4$.

Subgroups

Sub-semigroup: Let $(S, *)$ be a semigroup where $S_1 \subseteq S$, $(S_1, *)$ is said to be a subsemigroup if it is a semigroup in itself.

ex $(2N, +)$ is a subsemigroup for $(N, +)$.

Sub-monoid: Let $(M, *)$ be a monoid where $M_1 \subseteq M$, $(M_1, *)$ is said to be a sub-monoid if it is a monoid in itself.

ex $(2W, +)$ is a submonoid of $(W, +)$.

Subgroups: Let $(G, *)$ be a group where $H \subseteq G$, $(H, *)$ is said to be a subgroup of G if H is a group in itself.

ex $(2Z, +)$ is a subgroup of $(Z, +)$.

Q $\{(1, \omega, \omega^2), \times\}$, $o(1) = 1$, $o(\omega^2) = 3$

$o(\omega) = 3$

Teacher's Signature..............

THEOREM 1 Let $(H,*)$ be a subgroup of $(G,*)$. Prove that the identity element of H and G are the same.

Let $a \in H$

$\Rightarrow \quad a \in G \qquad (\because H \subseteq G)$

Let e and e_1 be the identity elements of G & H.

$e \in G$

$e_1 \in H$

$a * e = e * a = a$

$a * e_1 = e_1 * a = a$

$\therefore \quad a * e = a * e_1 \quad \Rightarrow e = e_1$

THEOREM 2 A non-empty sub set H of a group $(G,*)$ is a subgroup of $(G,*)$ iff

1. $\forall a, b \in H, \quad a * b \in H$
2. $\forall a \in H, \quad a^{-1} \in H$

PROOF:

Given: Given that $(H,*)$ is a subgroup of $(G,*)$.

To prove: 1 & 2.

Since $(H,*)$ is a subgroup of $(G,*)$, $(H,*)$ is a group in itself. Hence it satisfies the closure and inverse properties i.e. properties 1 & 2.

CLOSURE

INVERSE

ASSOCIATIVE Since $H \subseteq G$ ~~and~~ under the same binary operation and in $(G,*)$, $*$ is associative.

Hence $*$ is associative in $(H,*)$ also.

IDENTITY Let $a \in H \Rightarrow a^{-1} \in H$ (from (ii))

$\therefore \quad a * a^{-1} \in H$ (from (i))

$\Rightarrow \quad e \in H$

Hence, $(H,*)$ is a subgroup of $(G,*)$.

THEOREM 3 A non-empty subset H of a group $(G,*)$ is a subgroup of $(G,*)$ iff $\forall a, b \in H, \ a * b^{-1} \in H$.

given $(H, *)$ is a subgroup of $(G, *)$ ~~and a*b⁻¹∈H~~

PROOF $\forall a, b \in H$

$b^{-1} \in H$ (existence of inverse)

$a * b^{-1} \in H$ (existence of closure).

Converse Proof

ASSOCIATIVE $\because (G, *)$ is a group and $*$ is associative on G, hence $*$ is associative in H.

IDENTITY $a \in H$.

$a \in H$

$\therefore a * a^{-1} \in H$ (given condition)

$\Rightarrow e \in H$ $(\because a * a^{-1} = e)$

INVERSE $e \in H$

$a \in H$

$\therefore e * a^{-1} \in H \Rightarrow a^{-1} \in H$

CLOSURE $a \in H$, $b^{-1} \in H$

$\therefore a * (b^{-1})^{-1} \in H \Rightarrow a * b \in H$

THEOREM 4 Let $(G, *)$ be a group and H is a finite subset of G, then $(H, *)$ will be a subgroup of $(G, *)$ if $*$ is closed on $(H, *)$ i.e. $\forall a, b \in H$, $a * b \in H$.

PROOF As $(G, *)$ is a group and $*$ is associative on G, and as $H \subseteq G$, hence $*$ is associative on H.

IDENTITY Let $a \in H$

$a^2 \in H$ $(\because a^2 = a * a)$

$a^3, a^4, \ldots \in H$

At some point $a^i = a^j$

Now, $a^i = a^i * a^{j-i}$, $j > i$

$\Rightarrow a^{j-i} = e$

INVERSE $a^i * a^{(j-2i)} = e = a^{j-i}$

$\Rightarrow a * a^{(j-i-1)} = a^{j-i}$

Teacher's Signature....................

group $(G, *)$. Prove that $H \cap K$ is a subgroup of G.

PROOF Since H and K are subgroups of G, therefore the identity element of $(H, *)$, $(K, *)$ and $(G, *)$ are same.

$\therefore$ $e \in G$, $e \in H$, $e \in K$.

$\Rightarrow$ $e \in H \cap K$

Hence, $H \cap K$ is non-empty.

Let $a, b \in H \cap K$

$\Rightarrow$ $a, b \in H$ & $a, b \in K$

$\Rightarrow$ $a * b^{-1} \in H$ & $a * b^{-1} \in K$ ($\because$ H & K are subgroups of G)

$\Rightarrow$ $a * b^{-1} \in H \cap K$

$\Rightarrow$ $H \cap K$ is a subgroup.

Cosets and Lagrange's Theorem

~~[illegible]~~ Let $(G, *)$ be a group and $(H, *)$ be a subgroup of $(H, *)$, then the left coset of $(H, *)$ and $(G, *)$ is defined as $a * H = \{a * h \mid h \in H\}$ and the right coset as $H * a = \{h * a \mid h \in H\}$ where 'a' is an element in $(G, *)$.

Ex $G = (\{1, -1, i, -i\}, \times)$, $H = (\{1, -1\}, \times)$

$a * H$ for $a = 1$: $1 \times H = \{1(1), 1(-1)\} = \{1, -1\} = H$

$a = -1$: $(-1)H = \{1(-1), (-1)(-1)\} = \{1, -1\}$

$a = i$: $iH = \{i(1), i(-1)\} = \{i, -i\}$

$a = -i$: $-iH = \{(-i)1, (-i)(-1)\} = \{i, -i\}$

$H * a$ for $a = 1$: $H \times 1 = \{1(1), (-1)1\} = \{1, -1\} = H$

$a = -1$: $H(-1) = \{1(-1), (-1)(-1)\} = \{1, -1\}$

$a = i$: $H \times i = \{1(i), (-1)i\}$

$a = -i$:

Scanned by CamScanner

Page No.
Date: / /

1. The no. of left/right cosets is same as the order of the group.
2. The number of elements in each left/right coset is equal to the order of the subgroup.
3. The group $(G,*)$ can be partitioned into k no. of disjoint left or right cosets.
4. $(H,*)$ itself is a left as well as right coset.
5. If $a \in H$ then then $a * H \neq H$.
6. Any two left or right cosets are either disjoint or identical.

Imp. Prove the sixth conclusion.

PROOF Let us assume that $a*H$ and $b*H$ are two left cosets of H and G, and are not disjoint.

$\Rightarrow a*H \cap b*H \neq \phi$

$\Rightarrow c \in (a*H) \cap (b*H)$

$\Rightarrow c \in a*H$ and $c \in b*H$

$\Rightarrow c = a*h_1$ and $c = b*h_2$

$\Rightarrow a*h_1 = b*h_2$ ($\because$ c is equal for both)

$\Rightarrow a*h_1*h_1^{-1} = b*h_2*h_1^{-1}$

$\Rightarrow a = b*h_2*h_1^{-1}$ ——— (1)

Let $x \in a*H$

$\Leftrightarrow x = a*h_3$

$\Leftrightarrow x = b*(h_2*h_1^{-1}*h_3)$ (from (1))

$\Leftrightarrow x = b*h_4$ $(h_4 \in H)$

$\Leftrightarrow x \in b*H$

Clearly, an element in $a*H$ is in $b*H$. Hence they are identical.

Q $G = (\{[0],[1],[2],[3]\}, \oplus_4)$

$H = (\{[0],[2]\}, \oplus_4)$

Teacher's Signature..................

How many cosets are there?

$[0] \oplus_4 H = \{[0], [2]\} = H$

$[1] \oplus_4 H = \{[1], [3]\} \neq H$

$[2] \oplus_4 H = \{[2], [0]\} = H$

$[3] \oplus_4 H = \{[1], [3]\} \neq H$.

G can be partitioned into two groups $([0], [1])$ and $([2], [3])$ as they make the group $(G, \oplus_4)$ together.

Lagrange's Theorem

The order of any subgroup of a finite group G divides the order of the group.

PROOF Let the order of G be m and the order of H be n where $m \leq n$.

CLAIM m divides n

PROOF G can be partitioned into 'k' distinct left cosets of H in G.

$\therefore \quad G = H \cup a_1 H \cup a_2 H \ldots \cup a_{k-1} H$

$|G| = |H| + |a_1 H| + |a_2 H| \ldots |a_{k-1} H|$

$\Rightarrow \quad n = m + m + m + \ldots + m \quad$ (k times)

$\Rightarrow \quad n = mk$

$\therefore$ m divides k $\Rightarrow O(M) / O(G)$.

Converse of this is not true.

Q A group of prime order has no non-trivial subgrp.

Let the order of G be 'p' which is a prime number.

From Lagrange's theorem we know that $O(H)/O(G)$.

i.e, $O(H) / O(P)$

Hence $O(H)$ = either 1 or 'p'

If $O(H) = 1 \Rightarrow (\{e\}, *) = H$

or if $O(H) = p$

$\Rightarrow H = G$.

Teacher's Signature..................

Homomorphism,

Isomorphism / Automorphism

$\phi : (G, *) \longrightarrow (G', \Delta)$

Let $x, y \in G$ — HOMOMORPHISM

$\phi(x * y) = \phi(x) \Delta \phi(y)$

Let ϕ be a mapping from $(G, *)$ to (G', Δ) then ϕ is said to be homomorphism when

$$\phi(x * y) = \phi(x) \Delta \phi(y).$$

Homomorphism + one-one + onto = isomorphism

Automorphism is an isomorphism from a group to itself.

Q $\phi : (R, +) \longrightarrow (R, +)$, $\phi(x) = 2x$

Let $x, y \in R$

- $\phi(x+y) = 2(x+y) = 2x + 2y$
  $= \phi(x) + \phi(y)$

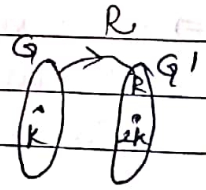
Hence it is a homomorphism.

- If $\phi(x) = \phi(y)$

$\Rightarrow$ $2x = 2y \Rightarrow x = y$

$\therefore$ the function is one-one.

- Let $z \in R - G'$



$z = 2k = \phi(k)$

$\Rightarrow k \in R - G$

Hence it is onto, and hence a ~~homo~~ isomorphism.

Q $\phi : (R^+, \times) \longrightarrow (R, +)$, $\phi(x) = \ln x$

Check for all types of morphisms.

$\phi(xy) = \ln(xy) = \ln x + \ln y = \phi(x) + \phi(y)$

Hence it is a homomorphism.

Q $\phi : (R, +) \rightarrow (R, +)$, $\phi(x) = x + 1$

$$\phi(x+y) = (x+y)+1$$
$$= (x+1)+(y+1)-1$$
$$= \phi(x)+\phi(y)-1$$

Hence it is not a homomorphism.

Q $\phi : (R,+) \longrightarrow (R,\times)$, $\phi(x) = 2^x$.

- $\phi(x+y) = 2^{(x+y)} = 2^x \cdot 2^y = \phi(x)\cdot\phi(y)$

$\therefore$ ϕ is a homomorphism

- If $\phi(x) = \phi(y) \Rightarrow 2^x = 2^y$

$\cancel{\Rightarrow 2^x - 2^y = 0 \Rightarrow 2^x(1-2^y) = 0}$

$\Rightarrow x = y$

Hence this is one-one.

- This is an isomorphism and not automorphism.

Q Let H_1 & H_2 be the subgroups of group G, neither of which contain the other so that $\exists$ an element in G belonging neither to H_1 and H_2.

Let $x \in H_1$ and $x \notin H_2$ and $y \in H_2$ and $y \notin H_1$.

$\Rightarrow x \in G$ and $y \in G$.

$\Rightarrow x * y \in G$

If $x * y \in H_1$, let $x * y = h_1$

$\Rightarrow y = x^{-1} * h_1 \in H_1$

$\Rightarrow y \in H_1$ which is not possible

If $x * y \in H_2$, let $x * y = h_2$

$\Rightarrow x = h_2 * y^{-1} \in H_2$

$\Rightarrow x \in H_2$ which is not possible.

as we have assumed that $x \notin H_2$ & $y \notin H_1$.

Hence, proved.

Teacher's Signature.....................

Normal Subgroups (N)

Page No.
Date: / /

Let $(G, *)$ be a group and $(N, *)$ be a subgroup of $(G, *)$, then $(N, *)$ is said to be normal in $(G, *)$ if $a * N = N * a \quad \forall\, a \in G$.

ex $N = (\{1, -1\}, \times)$ for $G = (\{1, -1, i, -i\}, \times)$.

ii)

Let $(N, *)$ be a subgroup of the group $(G, *)$ then N is said to be normal in G if $gng^{-1} \in N \;\forall\, g \in G \;\&\; n \in N$.

$$g * N * g^{-1} = \{g * n * g^{-1} \mid g \in G \;\&\; n \in N\}$$
$$= gNg^{-1} \in N$$

$$gNg^{-1} = N$$
$$gN = Ng$$

PROOF For any two normal subgroups H and K of a group G,

i) prove that $H \cap K$ is also a normal subgroup of G.

ii) If H is normal in G, then $H \cap K$ is normal in K.

STEP 1 Since H and K are subgroups of G, hence the identity element for H, K and G would be same.

$\therefore\; e \in G,\; e \in H$ and $e \in K$ also. $\Rightarrow e \in H \cap K$

Hence, $H \cap K$ is non-empty.

STEP 2 Let $a, b \in H \cap K$

$\Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow a * b^{-1} \in H$ and $a * b^{-1} \in K$

$\Rightarrow a * b^{-1} \in H \cap K$

$\Rightarrow H \cap K$ is a subgroup in G.

STEP 3 Let $a \in H \cap K$ and $g \in G$

$\Rightarrow a \in H$ and $a \in K$, $g \in G$

$\Rightarrow gag^{-1} \in H$ and $gag^{-1} \in K$

$\Rightarrow gag^{-1} \in H \cap K$

$\Rightarrow H \cap K$ is normal in G.

(i) Proved)

Teacher's Signature..................

e

Page No.
Date: / /

ii) ~~Given that H is normal in G $\Rightarrow gag^{-1} \in H \; \forall a \in H$~~
~~Also given that K is normal in G $\Rightarrow gbg^{-1} \in K \; \forall b \in H$.~~
~~$\therefore gag^{-1} \in H$ and $gbg^{-1} \in K$~~
~~$\Rightarrow gag^{-1} \in H \cap K$~~
~~$\Rightarrow H \cap K$ is normal to H and is normal to K.~~

EN. Let $a \in H \cap K$ and $k \in K \Rightarrow k \in G$ ($\because K \in G$)
$\Rightarrow a \in H$, $a \in K$ & $k \in K$
$\Rightarrow kak^{-1} \in H$ & $kak^{-1} \in K$ ($\because$ H is normal in G)
$\Rightarrow kak^{-1} \in H \cap K$
$\Rightarrow H \cap K$ is normal in K.

Group Codes

$B = \{0, 1\}$
$B^m = B \times B \times B \times \dots \times B$ (m times)

Word : A sequence of letters from binary alphabets.
ex 010, 000110, 110011

Code : Collection of words that are used to represent distinct messages.

Codeword : A word in a code.

Block Code : A code consisting of words of same length.

~~Def~~ Let A be the set on binary sequences of length 'n'. Let $\oplus$ be the binary operation such that $x \oplus y$ is a sequence of length 'n' that has '1's in those positions where x & y differ and '0's in those positions where x & y are same.

Teacher's Signature........

$A = \{0000, 0011, 1101, 1110\}$.

ex $0011 \oplus 1101 = 1110$

$\oplus$	0000	0011	1101	1110
0000	0000	0011	1101	1110
0011	0011	0000	1110	1101
1101	1101	1110	0000	0011
1110	1110	1101	0011	0000

Hence closure property is satisfied.
Here $e = 0000$ and the inverse of every element is the element itself.
$\therefore$ this is an abelian group.

Q $A = \{00000, 01110, 00111, 11111\}$

	00000	01110	00111	11111
00000	00000	01110	00111	11111
01110	01110	00000	01001 $\notin A$	
00111				
11111				

hence this is not closure

Weight of a word: Let x be a word, then weight of x $(= W(x))$ is the no. of ~~no~~ 1s in it.

The distance between two words x & y is defined as weight of $x \oplus y$ or $W(x \oplus y)$.

OR

The distance between two words x & y is the number of places where x and y differ.

$$d(x,y) \leq d(x,z) + d(z,y)$$

Teacher's Signature..................

Page No.
Date: / /

Let G be a block code. We define the distance of G to be the minimum distance between any pair of distinct code words in G.

Maximum Likelihood Ratio

Original word x $\longrightarrow$ y Received word after transmission

$\Rightarrow$ $\{x_1, x_2, x_3, \dots x_n\} \longrightarrow y$

$P(x_1/y), P(x_2/y), \dots\dots P(x_n/y) \equiv P(x_i/y)$

The probability with highest value will be the original word.

$\Longrightarrow$ Let $\{x_1, x_2 \dots x_n\}$ denote the code words in G. If $P(x_k/y)$ where x is the transmitted word and y is the received word, is the largest of all conditional probabilities computed, we shall conclude that x_k was the transmitted word. Such a criterion for determining the transmitted word is known as maximum likelihood decoding criterion.

Minimum Distance Decoding Criterion

We compute $d(x_i, y)$ $\forall$ $i = 1, 2, \dots n$ and if $d(x_i, y)$ is minimum then x_i is the transmitted word. This is known as the minimum distance decoding (MDDC) criterion.

Q A code of distance $2t+1$ can correct 't' or fewer transmission errors when the MDDC is followed. If no more than 't' errors have occured in the transmission where $x \rightarrow y$

$x_1 \rightarrow$ code word

$d(x_1, x) \geq 2t+1$

$\Rightarrow d(x_1, x) \leq d(x_1, y) + d(y, x)$

Teacher's Signature..................

$\Rightarrow d(x_1, x) \leq d(x_1, y) + t$

$\Rightarrow 2t + 1 \leq d(x_1, x) \leq d(x_1, y) + t$

$\Rightarrow 2t + 1 \leq d(x_1, y) + t$

$\Rightarrow d(x_1, y) \geq t + 1$.

As $d(x, y) \leq t$ & $d(x_1, y) \geq t + 1$, hence x is the original transmitted word.

Group Code: A subset G of A ($G \subseteq A$) is called a group code if $(G, \oplus)$ is a subgroup of $(A, \oplus)$.

Q $G = \{0000, 0011, 1101, 1110\}$

Here $A = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$

Using Cayley's table we already proved that G is a group. As elements of $G \in$ elements of A, hence $(G, \oplus)$ is a subset of $(A, \oplus)$.

Q Let x be the transmitted word and y be the received word with $(G, \oplus)$ be a group code where G is a subset of A. Let e be the word of smallest weight in $G \oplus y$. Let $e = x_j \oplus y$ and $e \oplus y = x_j$ where $G = \{x_1, x_2 \ldots x_n\}$

$G = \{0000, 0011, 1101, 1110\}$

Already proved that G is a group using Cayley's table

$\oplus$	0000	0011	1101	1110
0000	0000	0011	1101	1110
0001	0001	0010	1100	$\boxed{1111}$
0010	0010	0001	$\boxed{1111}$	1100
0100	0100	$\boxed{0111}$	0101	1010
1000	1000	0100	0101	1001

□ : Received word.

○ : Transmitted word chosen

Leaders (Smallest weights)

The encoding function $e: B^m \to B^n$ is a one to one function. The minimum distance of an encoding function is the minimum of the distance between all distinct pair of code words, for $n > m$.

An (m, n) encoding function can detect 'k' or fewer errors if the minimum distance is at least $k+1$.

Q Consider the $(2,6)$ encoding function $(B^2 \to B^6)$ given by $e(00) = 000000$, $e(01) = 011110$, $e(10) = 101010$, $e(11) = 111000$. Find the minimum distance in B and how many errors it can detect?

$d(e(00), e(11)) = d(000000, 111000) = 3$

$d(e(00), e(10)) = 3$ $\quad$ $d(e(00), e(01)) = 4$

$d(e(11), e(10)) = 2$ $\quad$ $d(e(11), e(01)) = 3$

$d(e(10), e(01)) = 3$

As distance $= 2$, it can detect 1 or no errors.

Q $e: B^2 \to B^5$, $e(00) = 00000$, $e(01) = 01110$, $e(10) = 00111$, $e(11) = 11111$.

$d(e(00), e(01)) = 3$, $\quad$ $d(e(00), e(10)) = 3$

$d(e(00), e(11)) = 5$, $\quad$ $d(e(01), e(10)) = 2$

$d(e(01), e(11)) = 2$, $\quad$ $d(e(10), e(11)) = 2$.

As distance $= 2$, it can detect one or no errors.

Q Let the following be a group be $\{00000000, 0011111000, 1100000111, 1111111111\}$. Check if it is a group code and find the number of errors.

$d(0000000000, 0011111000) = 5$,

$d(0000000000, 1100000111) = 5$.

$d(0000000000, 1111111111) = 10$

Teacher's Signature........................

Page No.
Date: / /

Here distance $d = 5$.
So $2t+1 = 5 \Rightarrow t = 2$.
Hence it can detect two or fewer errors.

Q Let $(G, \circledast)$ be a group such that G has even number of elements. Show that there's an element $a \in G$ such that $a * a = e$ where e is the identity element.

$|G|$ = even and as $(G, *)$ is a group hence $\forall x \in G$, $x^{-1} \in G$ with 'e' being the only element without an inverse. This makes $|G| = 2k+1$, ~~$k = n(x)$~~.
But given that $|G|$ is even. Hence $\exists$ an element which is the inverse of itself i.e. $a = a^{-1}$.

$$\therefore \quad a * a^{-1} = e$$
$$\Rightarrow a * a = e$$

Rings

We have a group $(R, +, \cdot)$. ~~whose order is even~~

1. $(R, +)$ is an abelian groups.
2. $(R, \cdot)$ is a semigroup.
3. $\cdot$ is distributive over $+$.

ex $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

$(R, +, \cdot)$ is said to be ring with unity if $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a \ \forall a \in R$

ex For equivalence classes, $e = [1]$.
$(Z_n, \oplus_n, \odot_n)$

Let R be a ring so $(R, +, \cdot)$ is said to be a commutative ring if $a \cdot b = b \cdot a \ \forall a, b \in R$.

Teacher's Signature.........

Ring with zero divisors

Let R be a commutative with unity ring, then it is said to be a ring with zero divisors if $\exists\, a \neq 0,\ b \neq 0$ such that $ab = 0$.

ex $\mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_{10}$

Integral Domain: Let R be a commutative ring, then it is said to be an integral domain if R has zero divisors.

ex $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_p, \oplus_p, \otimes_p)$

Division Ring: It is a ring with unity where every non-zero element has a multiplicative inverse.

ex $\cancel{(\mathbb{Z}, +, \cdot)}$, $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Z}_p, \oplus_p, \otimes_p)$

Field: It is a commutative division ring.

Q Prove that ~~$\mathbb{Z}_5$ under~~ $(\mathbb{Z}_5, \oplus_5, \otimes_5)$ is a field. [11 props.]

Q Prove that every field is an integral domain.

Let F be a field, let a & b be two elements in F,

$a, b \in F$, $a \neq 0$ and $ab = 0$

$\because a \in F$, $\exists\, a^{-1} \in F$ such that $aa^{-1} = F$

Hence, $a^{-1}(ab) = a^{-1} \cdot 0$

$\Rightarrow (a^{-1}a)\, b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$

$\therefore F$ is an integral domain.

The converse is not necessarily true. $(\mathbb{Z}, +, \times)$

Every integral domain is a field but every finite integral domain is a field

ex $(\mathbb{Z}, +, \cdot)$

Teacher's Signature.............

Scanned by CamScanner

Page No.
Date: / /

Subring: A non-empty subset of R and it is also a ring in itself.

Ring Homomorphism

$f : (R, +, \cdot) \longrightarrow (R', \oplus, \otimes)$

f is an onto function from $(R, +, \cdot)$ ring to $(R', \oplus, \otimes)$ ring is said to be a homomorphism

if $f(x+y) = f(x) \oplus f(y)$

$f(xy) = f(x) \oplus Fy$

Q. Let N be the set of natural numbers. Verify ~~and~~ $*$ is an associative operation.

i> $a * b = \max(a, b)$

Let $a > b > c \ \forall \ a, b, c \in N$

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

~~Identity~~

ii> $a * b = a + b + 3$

$a * (b * c) = a * (b + c + 3) = a + b + c + 6$

$(a * b) * c = (a + b + 3) * c = a + b + c + 6$

iii> $a * b = \min(a, b+2)$

Date
Page

Graph Theory

Graph :-

Graph is the order pair (V, E) where V is non-empty sets of vertices or nodes and E is the set of edges or arcs

Infinite and finite graph

A graph with infinite no. of vertices and edges are known as infinite graphs.

A graph with ~~infinite~~ finite no. of vertices and edges are known as ~~infinite~~ finite graphs

Undirected Graph :-

Degree of the vertex :

Number of edges incident with that vertex.

Isolated vertex :-

A vertex with degree 0.

Pendent vertex.

A vertex with degree 1

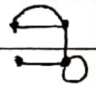
Simple graph

A graph in which each edge connects two diff vertices and where no two edges connect to the same pair of vertices.

Multigraph.

Graphs with multiple edges

Pseudograph



Graphs that may include loops and possibly multiple edges.

The handshaking theorem

Let $G = (V, E)$ be a undirected graph e edges

$$2e = \sum_{v \in V} \deg(v)$$

How many edges are there in a graph with 10 vertices each of degree 6?

$2e = 10(6) \Rightarrow e = 30$ edge.

Theorem - 2

An undirected have even no. of vertices of odd degree.

Lets us ~~be~~ partition $(V = V_1 \cup V_2)$

From handshaking threoem

$$2e = \sum_{v_1 \in V_1} degree(v_1) + \quad [even]$$

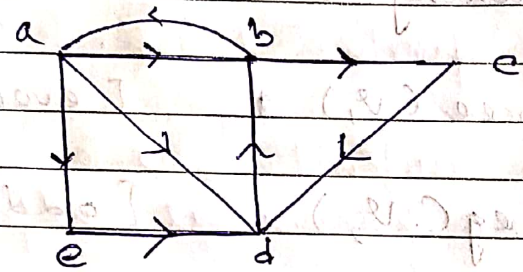
$$\cancel{2} \cdot 2e = \sum_{v_2 \in V_2} deg(v_2) \quad [odd]$$

2e is even

Indegree and Outdegree

In a graph with directed edges the indegree of vertices denoted by $deg^-(v)$ is the no. of edges with ~~with~~ as there terminal vertex

The outdegree is denoted by $deg^+(v)$



	In degree
$deg^+(a) = 3$	$deg^-(a) = 1$
$deg^+(b) = 2$	$deg^-(b) = 2$
$deg^+(c) = 1$	$deg^-(c) = 1$
$deg^+(d) = 1$	$deg^{-1}(d) = 3$
$deg^+(e) = 1$	$deg^{-1}(e) = 1$
deg^+ : 8	8

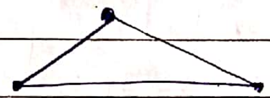
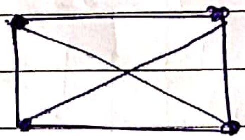
sum of indegree and outdegree is no. of edges.

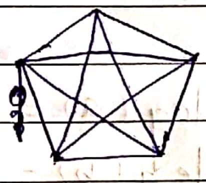
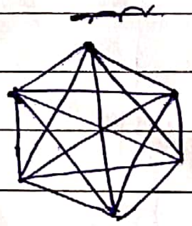
Some Simple Graphs

① Complete Graph :- (K_n)

A complete graph on n vertices (K_n) is the simple graph that contains exactly one edge bet^n each pair of distinct vertices.

K_1 K_2 

K_3  K_4 

K_5  K_6 

edges $^nC_2$

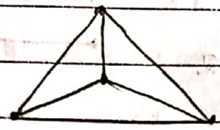
Cycle:

The cycle C_n, $n \geq 3$ consist of n vertices ($1, 2, 3 \ldots n-1, n$) and edges $\{1,2\}$, $\{2,3\}$, $\{3,4\}$, $\ldots$ $\{(n-1), n\}$, $\{n,1\}$.

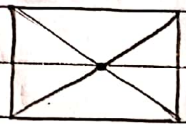
Wheel (W_n):-

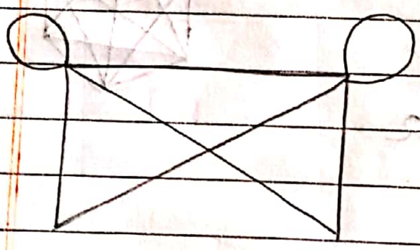
Wheel (W_n) is obtained when we have a additional vertex to the cycle C_n where $n \geq 3$, and connect this new vertex to each of the n vertices in C_n by new edges.

W_3

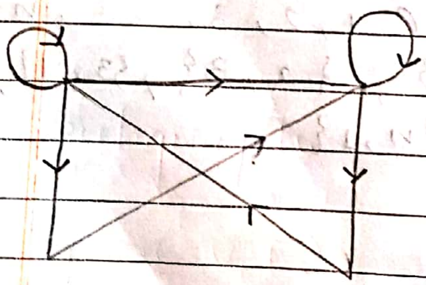


W_4





deg (a) = 5
deg (b) = 5
deg (c) = 2
deg (d) = 2

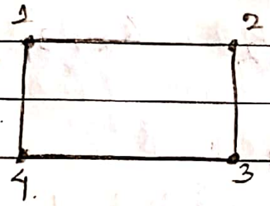


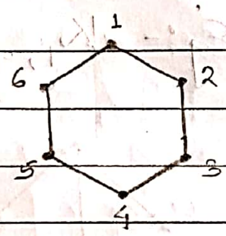
$deg^-(a) = 2$ $deg^+(a) = 3$
$deg^-(b) = 3$ $deg^+(b) = 2$
$deg^-(c) = 1$ $deg^+(c) = 1$
$deg^-(d) = 1$ $deg^+(d) = 1$

Bipartite Graph

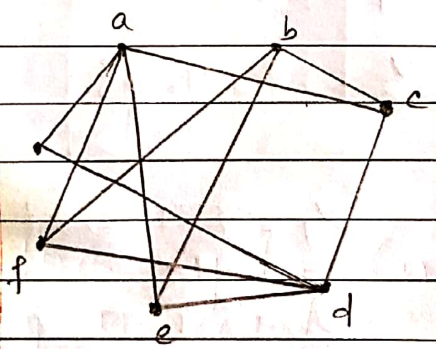
A simple graph G is called bipartite if it's vertex ~~band~~ set V can be partition into: into 2 disjoint sets V_1 and V_2 such that every edge in the graph connects the vertex in V_1 and vertex in V_2 [so, that no edge in G connects either two vertices in V_1 or two vertices in V_2]

(V_1, V_2) is called bipartition of the vertex $V(G)$

C_4 

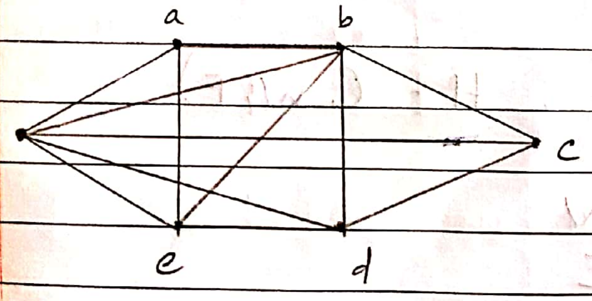
C_6 

$V_1 = \{1, 3\}$
$V_2 = \{2, 4\}$

Q 

$V_1 = \{a, b, d\}$

$V_2 = \{g, f, c, e\}$



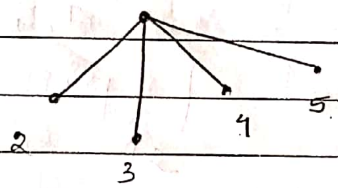
Not a bipartite graph

Complete bipartite graph :-

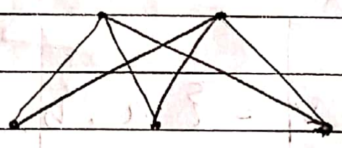
It is denoted as $K_{m,n}$ is the graph that has it's vertex at partition into two subsets into m and n vertices respectively. There is an edge betn two vertices if and only if ~~one~~ 1st vertices ~~in~~ 1st ~~vert~~ and to the 2nd vertex in second set

[total no. of edges mn]

Eg:- $K_{1,4}$, $K_{2,2}$, $K_{2,3}$.

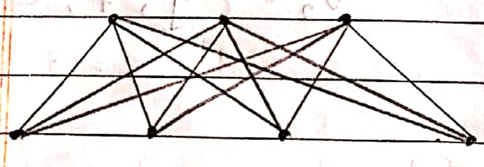


$V_1 = \{1\}$
$V_2 = \{2, 3, 4, 5\}$



$V_1 = \{1, 2\}$

$V_2 = \{3, 4, 5\}$



$V_1 = \{1, 2, 3\}$

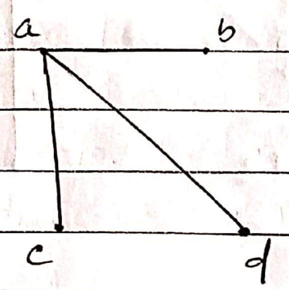
$V_2 = \{4, 5, 6, 7\}$

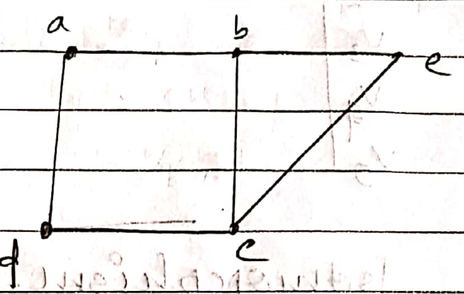
Subgraph

$G = (V, E)$, $H = (W, F)$

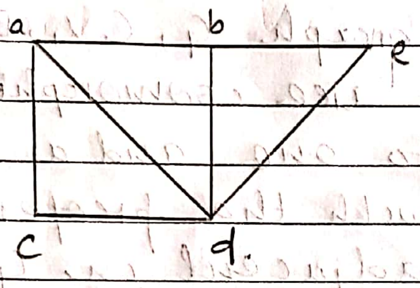
$W \subseteq V$
$F \subseteq E$

Union of graphs.



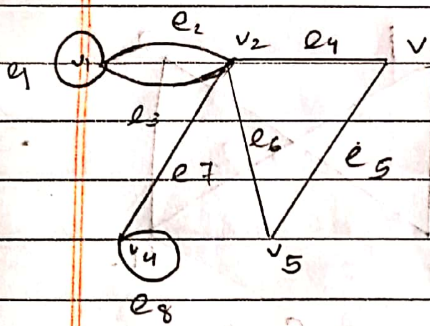


G_1 $\qquad\qquad$ G_2



$G_1 \cup G_2$

Adjacency and Incidence Matrix.



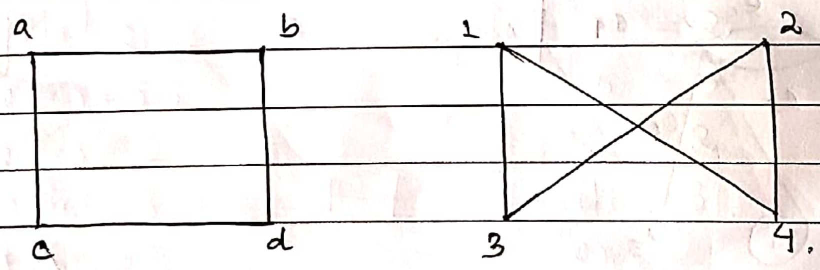
$$\begin{array}{c|ccccc|} & v_1 & v_2 & v_3 & v_4 & v_5 \\ \hline v_1 & 1 & 1 & 0 & 0 & 0 \\ v_2 & 1 & 0 & 1 & 1 & 1 \\ v_3 & 0 & 1 & 0 & 0 & 1 \\ v_4 & 0 & 1 & 0 & 1 & 0 \\ v_5 & 0 & 1 & 1 & 0 & 0 \\ \hline \end{array}$$

[Adjacent matrix]

$$\begin{array}{c|cccccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\ \hline v_1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ v_2 & & & & & & & & \\ v_3 & & & & & & & & \\ v_4 & & & & & & & & \\ v_5 & & & & & & & & \end{array}$$

Isomorphism

The simple graph $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ are isomorphic if there is a one to one and a onto funcⁿ $f : V_1 \to V_2$ with the property that a, b are adjacent in G_1 if and only if $f(a), f(b)$ are adjacent to G_2

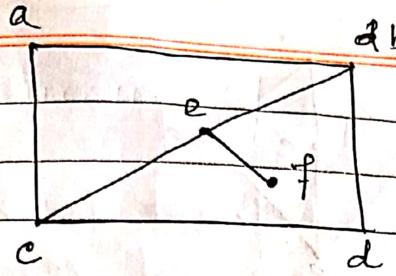


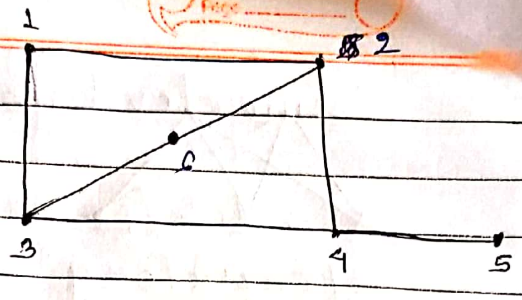
G_1 G_2

$V_1 = \{a, b, c, d\}$. $V_2 = \{1, 2, 3, 4\}$

$f : V_1 \to V_2$, $f(a) = 1$ $f(c) = 3$
$f(b) = 4$ $f(d) = 2$.

~~No~~ isomorphism possible.





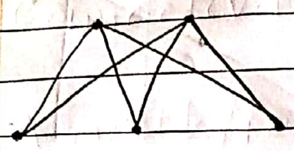
deg (a) = 2
deg (b) = 3
deg (c) = 3
deg (d) = 2
deg (e) = 3
deg (f) = 1

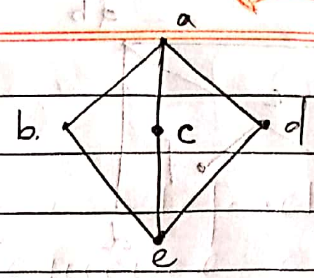
deg (1) = 2
(2) = 3
(3) = 3
(4) = 3
(5) = 1
(6) = 2

f (f) = 5 f (a) = 1 f (b) = 2
f (d) = 6 f (e) = 4 f (c) = 3

	a	b	c	d	e	f
a	0	1	1	0	0	0
b	1	0	0	1	0	0
c	1	0	0	1	1	0
d	0	1	1	0	0	0
e	0	1	1	0	0	1
f	0	0	0	0	1	0

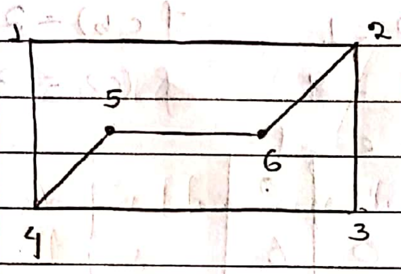
	1	2	3	4	5
1					
2					
3					
4					
5					

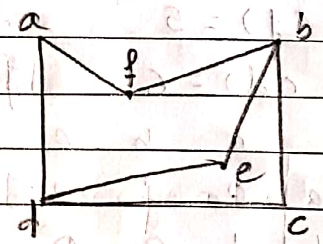




G_1 G_2

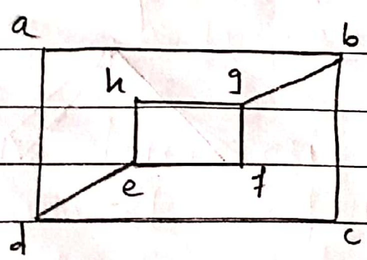
$f(1) = a$
$f(2) = e$
$f(3) = b$
$f(4) = c$
$f(5) = d.$

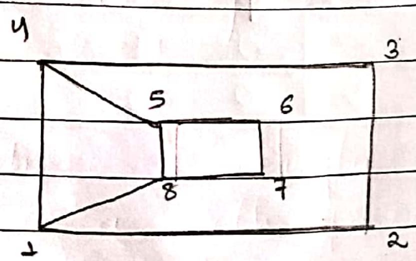




$\deg(1) = 2$	$\deg(a) = 2$
$(2) = 3$	$(b) = 3$
$(3) = 2$	$(c) = 2$
$(4) = 3$	$(d) = 3$
$(5) = 2$	$(e) = 2$
$(6) = 2$	$(f) = 2$

$f(2) = b$ $f(5) = a$ $f(1) = e$
$f(3) = c$ $f(4) = d.$ $f(6) = f.$





deg (a) = 2

(b) = 3

(c) = 2

(d) = 3

(e) = 3

(f) = 2

(g) = 3

(h) = 2

deg (1) = 3

(2) = 2

(3) = 2

(4) = 3

(5) = 3

(6) = 2

(7) = 2

(8) = 3

~~f,=~~ f (1) = d   f (2) = c

f (3) = a   f (4) = b   f (5) = g

f (6) = h   f (7) = f   f (8) = e

Connectivity :-

A walk/path is defined to be an alternating sequence of vertices and edge.

Cycle / Circuit :-

A closed walk is called a ~~trail~~ cycle / circuit [initial are terminal are same]

Simple path / Trail :-

A path without reepeatation of edges

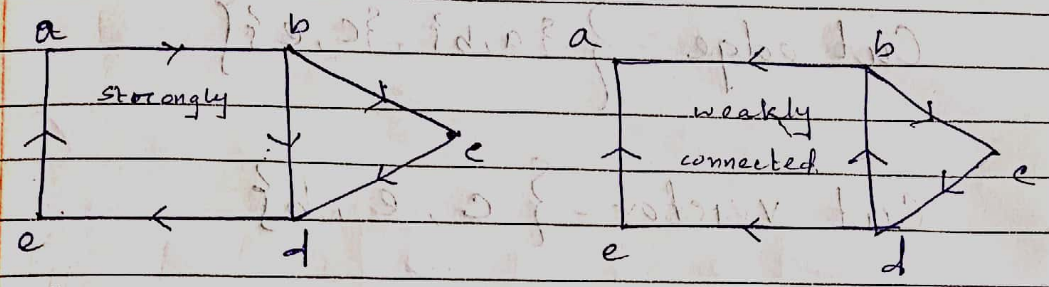
~~An~~

~~An undirected graph path is~~

An undirected graph is called connected if there is a path betⁿ every pair of vertices of the graph.

→ A directed graph is strongly connected if there is a path from A to B and from B to A whenever A and B are vertices in the graph

A directed graph is weakly connected if there is a path betn every two vertices in an underline undirected graph.



Q There is a simple path betn every pair of distint vertices of an connected undirected graph

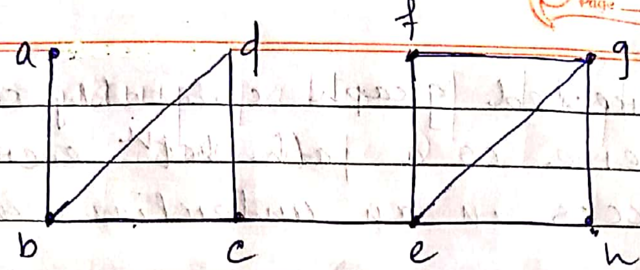
Connected Components:

A connected component graph G is a maximal connected subgroup of G

Cut vertex / cut edge :-

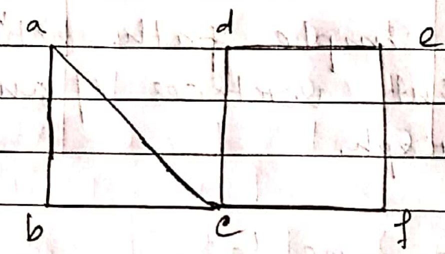
Removal of a vertex that makes a connected graph disconnected is called a cut vertex.

Removal of a edge that makes a connected graph disconnected is called a edge vertex



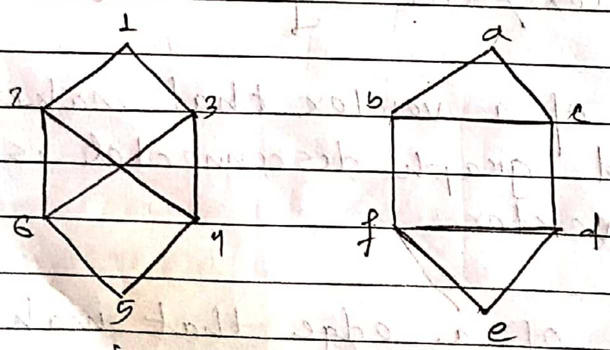
Cut edge = { {a,b}, {c,e} }

Cut veretex = { c, e, b }

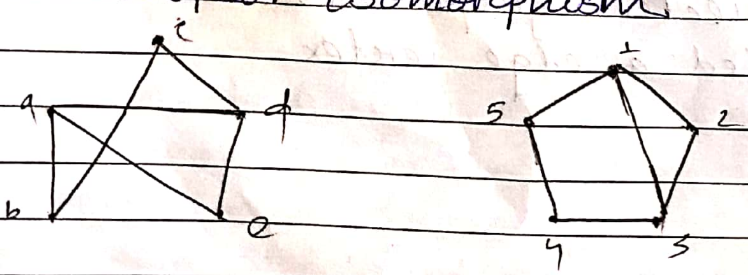


Cut Veretex = { c }

Path and Isomorephism.



No ~~isophor~~ isomorephism.

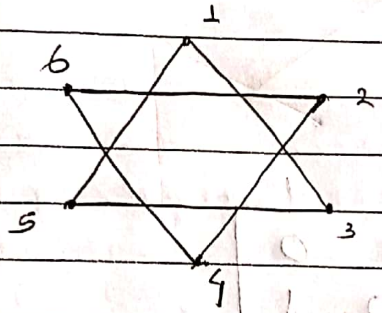


Isomorephism

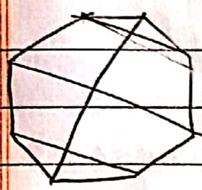
$f(e) = 2$ $f(c) = 5$

$f(a) = 3$ $f(d) = 1$

$f(b) = 4$



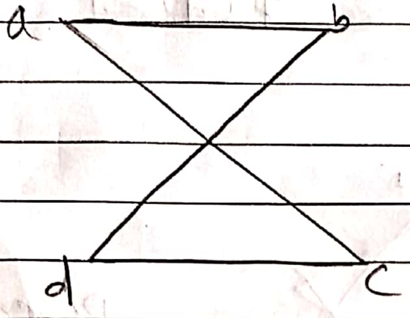
Disconnected



Counting path betⁿ vertices

Let G be a graph with adjacency matrix A with ordering 1, 2, 3 … … n (with directed or undirected edges with multiple edges, loops allowed) the no. of different paths of length r from "i" to "j" where r is a +ve integer equals $a(i,j)^{th}$ entry of A^r.

How many paths of length 4 are there from A to D

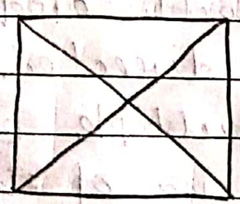


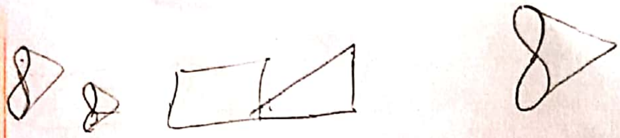
$$A = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$$A^4 = \begin{bmatrix} 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \\ 8 & 0 & 0 & 8 \\ 0 & 8 & 8 & 0 \end{bmatrix}$$

length = 8

Find the no. of paths of length 2, 3, 4 betn 2 diff. vertices in K_4

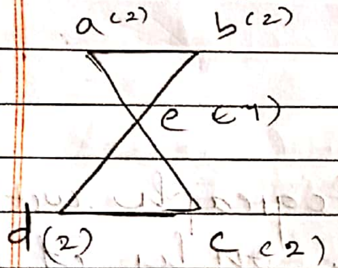




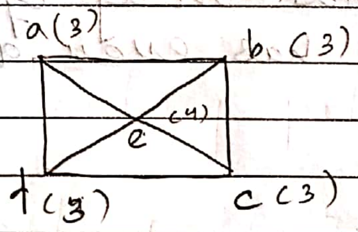
Euler path and Euler Circuit.

A circuit in a graph G is a simple circuit containing every edge of G.

A Euler path in G is a simple path containing every edge of G.

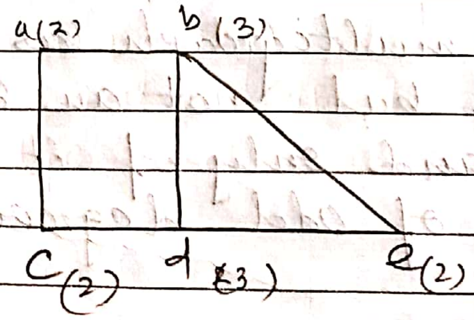


Euler Circuit
Path
(even degree)

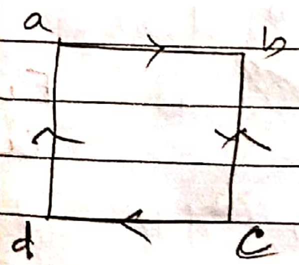


No

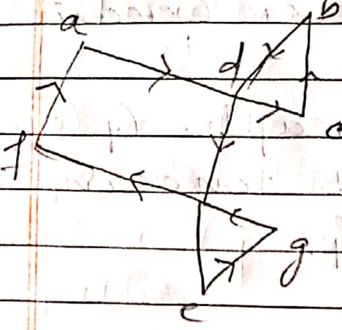
More than two vertices are odd degree so,



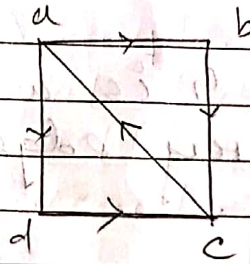
Euler Path
(Two vertices are odd degree)



~~Euler circuit~~
No.



Euler path
circuit



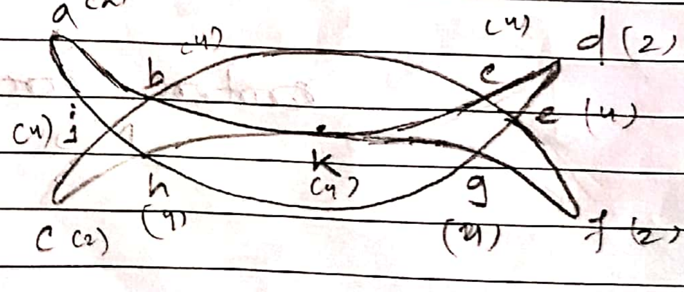
Euler path

Theorem - I

A connected multigraph with only two vertices if and only if each of the vertices has even degree

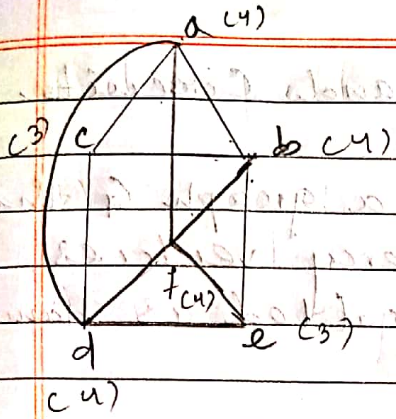
Theorem - II

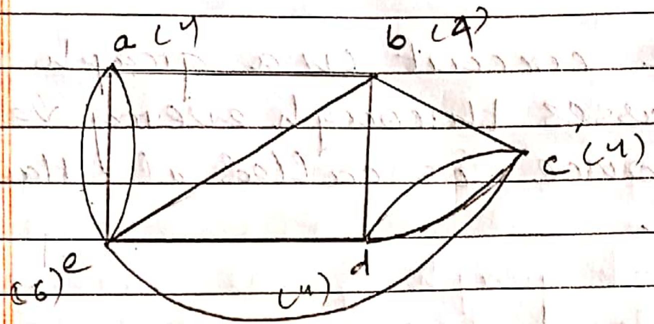
A connected multigraph has an Euler path but not an Euler circuit if and only if it has two vertices of odd degree.

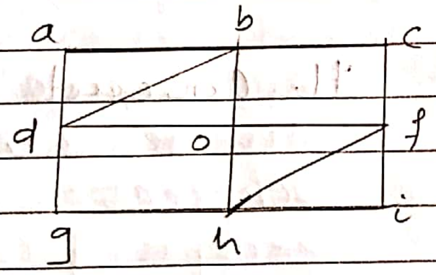


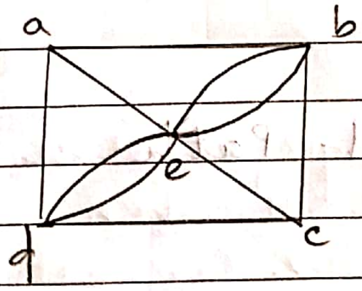
Euler circuit

Path





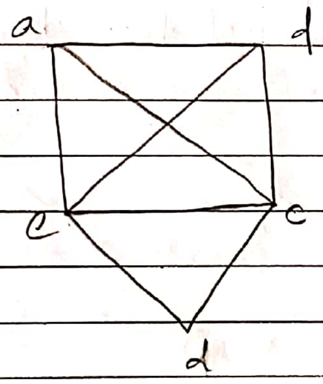




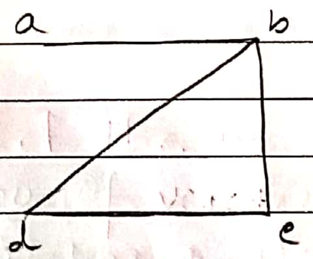
Hamilton paths and Circuits.

A simple path in a graph G That passes through every vertices exactly once is called as Hamilton path.

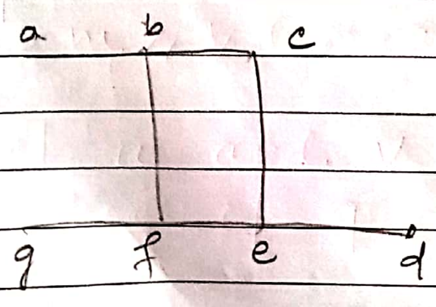
A simple circuit in a graph G that passes through every vertex exactly once is called as Hamilton circuit.



H. Circuit



H. Path



No.

Theorem :-

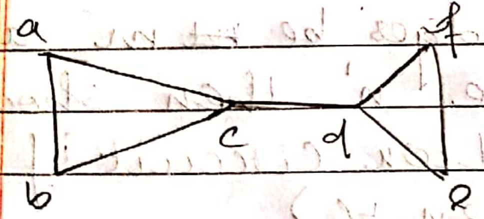
If G is a simple graph with n vertices such that the degree of every vertex in G is atleast $n/2$ then G has a Hamilton circuit

- The converse of the statement is not true.

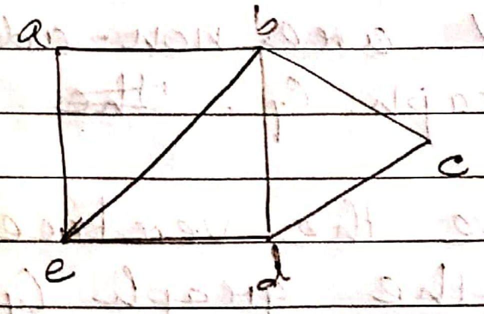
Ore's Theorem :-

If G is a simple graph with n vertices when $n \geq 3$, such that degree (u) + degree $(v) \geq n$ for every pair of non-adjacent vertices u, v ~~then~~ in G then G has a Hamilton circuit

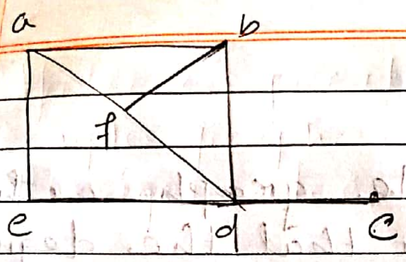
Eg :- travelling - salesman prob.

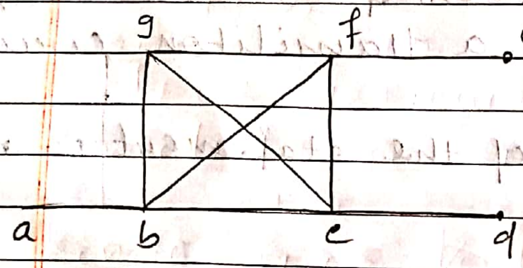


path

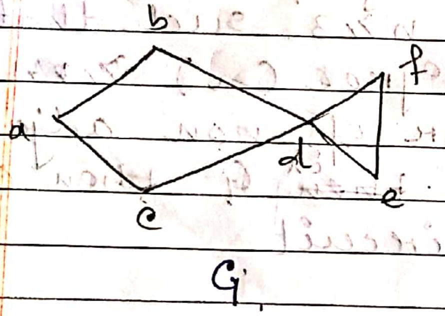


circuit





Prove that graph G has Euler circuit, but not hamilton circuit



~~All degree are~~
All degree of the vertices is 2 except d (4).

Let the no. of edges be ~~m~~ 'm' and no. of vertices be 'n' then show that G has a Hamilton circuit if m. is $m \geq \frac{1}{2}(n^2 - 3n + 6)$

Let u and v are non-adjacent vertices of graph G. ~~The~~

Let us remove the vertices u and v from the graph G.

No. of vertices = $n-2$

No. of edges = $m - \deg(u) - \deg(v)$

The max no. of edges from $n-2$ vertices is ${}^{n-2}C_2$

Thus:

$${}^{n-2}C_2 \geq m - \deg(u) - \deg(v)$$

$$\frac{(n-2)(n-3)}{3} \geq m - \deg(u) - \deg v.$$

$$\deg u + \deg v \geq m - \frac{(n-2)(m-3)}{2}$$

$$\geq \frac{1}{2}\left(n^2 - 3n + 6\right) - \frac{(n-2)(n-3)}{2}$$

$$\geq \frac{n^2 - 3n + 6 - (n^2 - 5n + 6)}{2}$$

$$= \frac{n^2 - 3n + 6 - n^2 + 5n - 6}{2}$$

$$= \frac{2n}{2} = n$$

*. If G is a simple graph with n vertices and K-components then G can have atmost $\frac{(n-K)(n-K+1)}{2}$ edges.

If e is greater than. then a simple graph with n vertices and e edges are connected.

$$e > \frac{1}{2}(n-1)(n-2)$$

Let us assume that G is disconnected.

since G is ~~di~~ disconnected ∴ it will definitely have 2 or more connected components.

K = 2

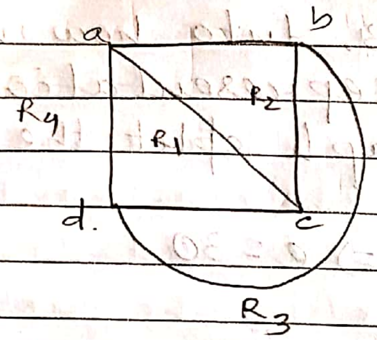
n vertices

$$\text{Max edges } \frac{(n-2)(n-2+1)}{2}$$

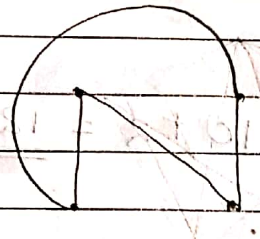
$$= \frac{(n-2)(n-2)}{2}$$

Planar Graph

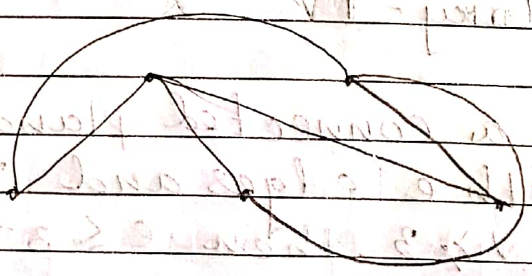
A graph is called planar if it can be drawn in the plane without any edges crossing, where a crossing of edges is the intersection of lines or arcs representing them at a point other than their common end point.
Such a drawing is called planar representation of a graph.



K_4



$K_{2,2}$



$K_{2,3}$

Euler's Formula :-

Theorem - I

Let G be a connected ~~graph~~ simple planar graph with edges ~~ve~~ and vertices. Let R be a region on a planar representation of G, then
$R = e - v + 2$

Suppose that a connected planar simple graph has 20 vertices each of degree 3. Into how much region does the representation of the planar graph split the plane.

$2e = 60 \Rightarrow e = 30.$

Now $r = e - v + 2$

$= 30 - 20 + 2 = 10 + 2 = \underline{\underline{12}}$

Corollary - I

If G is a connected planar simple graph with e edges and v vertices where $v \geq 3$ then $e \leq 3v - 6$.

Degree of the region :-

It is define to be the no. of edges on the boundary of the region when an edge occurs twice on the boundary (so, that it is stretched out twice), it contributes two to the degree.

$2e = \sum \deg r.$

$2e \geq 3r$

$r \leq \frac{2}{3} e$

$\Rightarrow e - v + 2 \leq \frac{2}{3} e$

$e - \frac{2}{3} e \leq v - 2$

$\Rightarrow \frac{e}{3} \leq v - 2$

$\Rightarrow e \leq 3v - 6$

Corollary - II

If G is a connected planar simple graph, then G has a degree of not exceeding 5.

$2e \geq 6v$

$\Rightarrow e \geq 3v.$

$\Rightarrow v \leq e/3.$

$r + v \leq 2/3 e + e/3.$

$v + e + 2 \leq e$

$2 \leq e.$

∴ our assumption is wrong.

G has a degree not exceeding 5.

Corollary - III

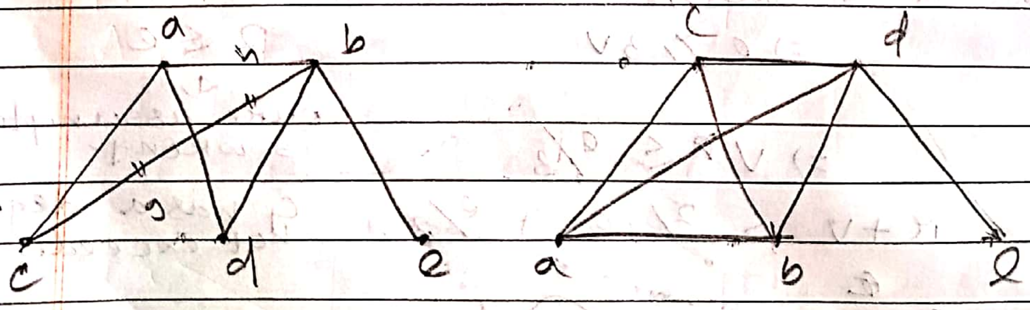
If a connected planar simple graph with v vertices and e edges, with $v \geq 3$ and no circuits of length 3, then $e \leq 2v - 4$

e E/R
Prove

K.

Elementary

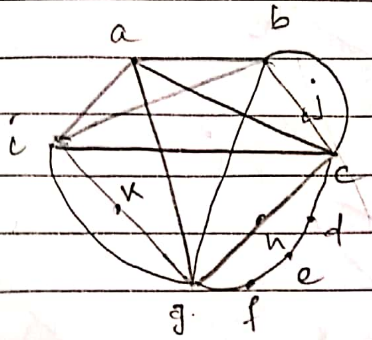
If a graph is planar, so will be any graph obtain by removing an edge uv and adding a new vertex with the edges ow and wv.



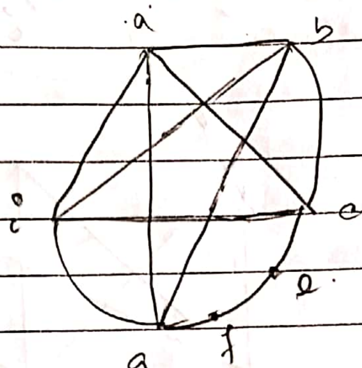
The Graph G_1 and G_2 are called homeomorphic if they can be obtain from the same graph by a sequence elementary subdivisions.

Kuratoski's Theorem

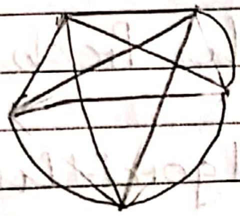
A graph is non planar if and only it contains a sub-graph homeomorphic to $K_{3,3}$ or K_5.



G

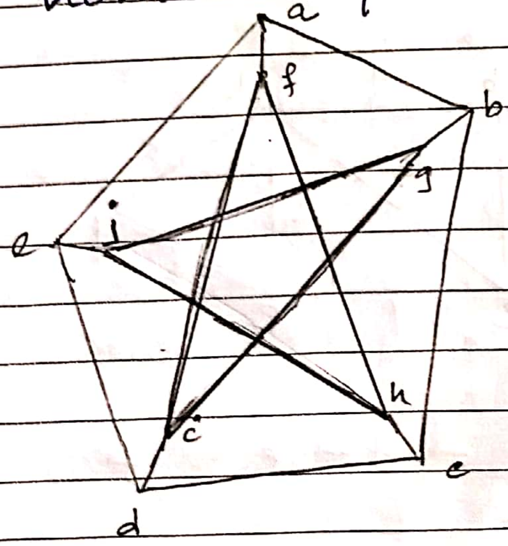


H.

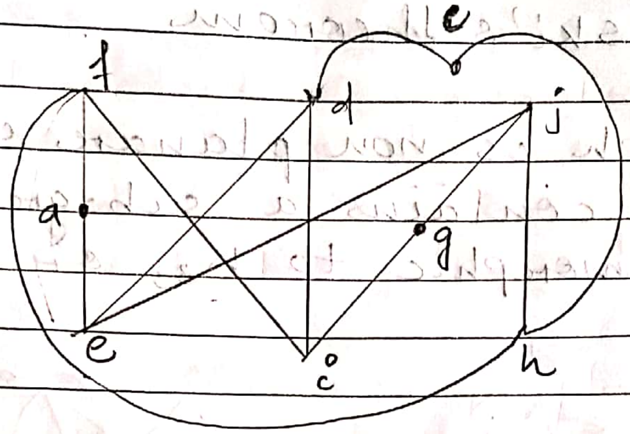


K_5

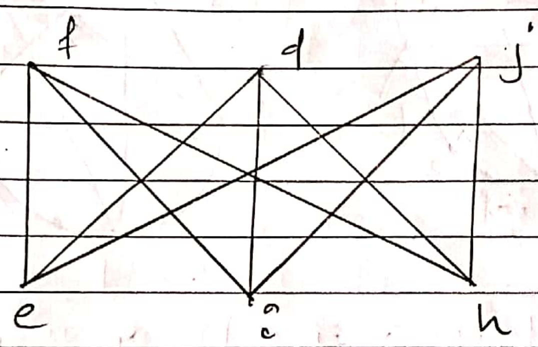
H is the subgraph to G.
H is homeomorphic to K_5.



perderson graph



H

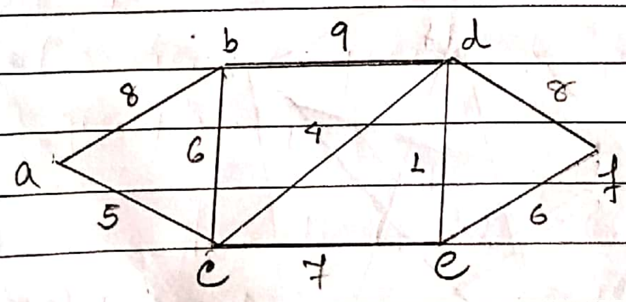


$K_{3,3}$

Imp **Shortest Path Problem.**

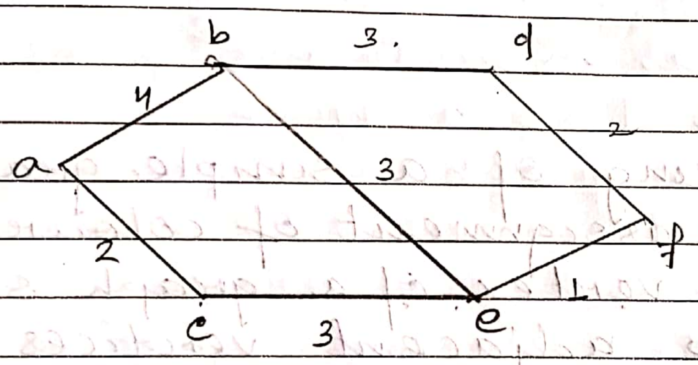
Dijkstra's Algorithm.

Find the shortest path from A to F



a → c → d → e → f.

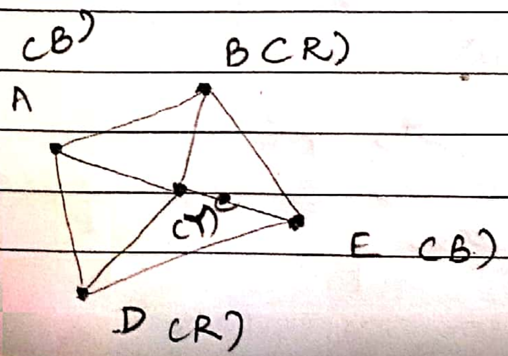
S	L(a)	L(b)	L(c)	L(d)	L(e)	L(f)
ϕ	$\boxed{0}$	∞	∞	∞	∞	∞
{a}	—	8	$\boxed{5}$	∞	∞	∞
{a, c}	—	$\boxed{8}$	—	9	12	∞
{a, c, b}	—	—	—	$\boxed{9}$	12	∞
{a, c, b, d}	—	—	—	—	$\boxed{10}$	17
{a, c, b, d, e}	—	—	—	—	—	$\boxed{16}$

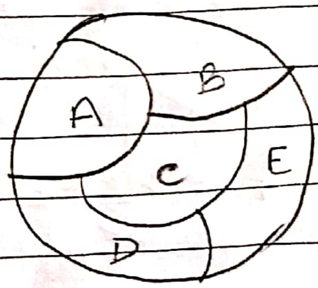


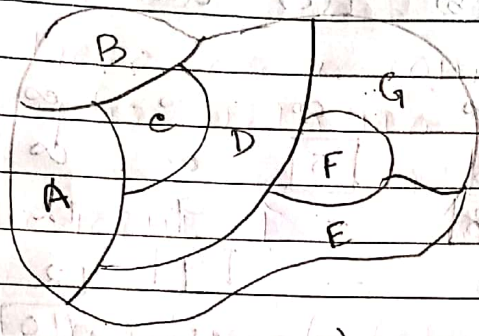
a → c → e → f

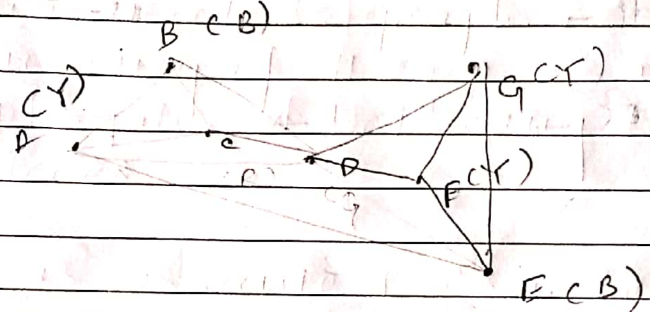
S	L(a)	L(b)	L(c)	L(d)	L(e)	L(f)
ϕ	$\boxed{0}$	∞	∞	∞	∞	∞
{a}	—	4	$\boxed{2}$	∞	∞	∞
{a, c}	—	$\boxed{4}$	—	∞	5	∞
{a, c, b}	—	—	—	7	$\boxed{5}$	∞
{a, c, b, e}	—	—	—	7	—	$\boxed{6}$

Graph Coloring:







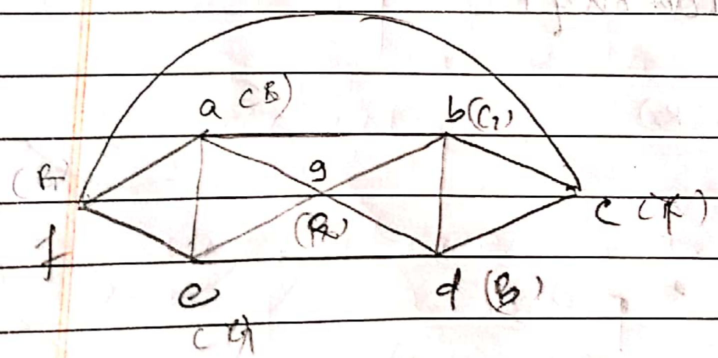


coloring of a simple graph is the assignment of colour to each vertex of a graph so that no to adjacent vertices are assigned to same colour

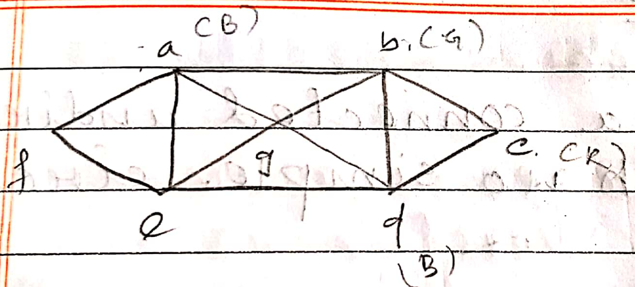
Chromatic Number

Ch It is the least of no. of colour required for colouring of graph.

It is denoted as $\chi(G)$



4


a (B)
b (G)
c (R)
d (B)
e
f
g

TREES

A tree is a connected undirected graph with no simple circuit.

Theorem - I

An undirected graph is a tree if an only if there is a unique simple path ~~a~~ betn any two of it's vertices.

Let us assume T is a tree. Since T is a tree is a connected simple graph with no simple circuit.

Let x, y be two vertices of T. Since T is connected there is a simple path from x to y.

Moreover this path must be unique, for if there was a second such path, this path form by combining the first path from x to y followed by the path from y to x obtained by reversing the order of the second path from x to y would form a circuit.

Hence there is a unique simple path from x to y.

Let us assume that there is a unique simple path betn any two vertices of graph T.

Then T is connected because there is a path betn any two of its vertices. Furthermore we can have no simple circuits.

To prove that

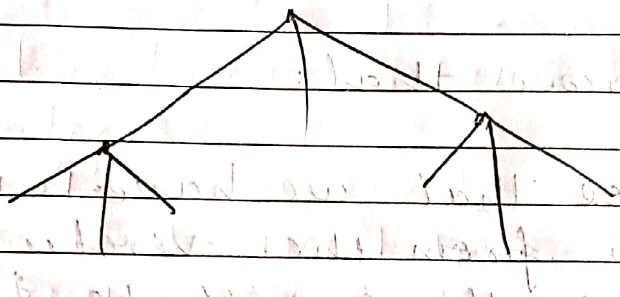
suppose that we have a simple circuit from the vertices x and y. Then there will be two simple path from x to y,

which is not possible because there is a unique path.

Then there would be 2 simple because the simple circuit is made of a simple path from x to y which is not possible because there is a unique simple path. (Because the simple circuit is made up of a simple path from x to y and a second simple path from y to x).

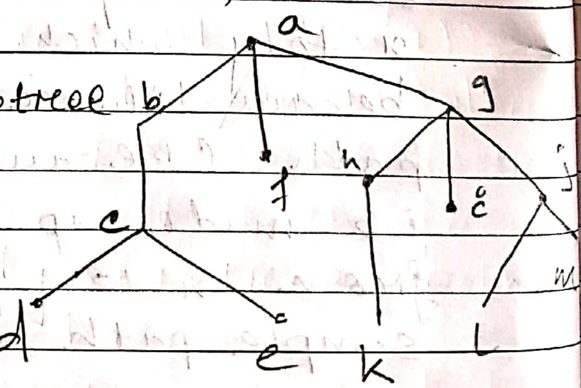
Rooted Tree.

A rooted tree is a tree in which one vertex as been designated as the root and every edge is directed away from the root.



In the rooted tree T, then find the parent of c.

(ii) The child of G.
(iii) The siblings of H.
(iv) All ancestores of E
(v) All decendents of D
(vi) All internal vertecces
(vii) All leaves
(viii) What is the subtree rooted at G



(i) b
(ii) h, i, j
(iii) i, j

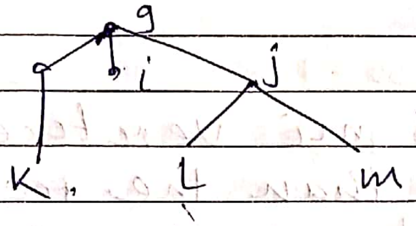
(iv) c, b, a

(v) c, d, e

(vi) b, c, h, g, j

(vii) d, e, f, k, i, l, m

(viii)



m - ary :-

A rooted tree is called a m-ary tree if every interenal vertex has no more than m children

Full m-ary

~~A Exa~~.

A tree is called a full m-ary if exactly it has m-ary. It's also called regular.

Theorem - II

A tree with n vertices has n-1 edges.

Theorem - III

A full m-ary tree with i interenal vertices contains $n = mi + 1$ vertices.

Every vertex except the root is the child of the internal vertex because each of the i internal vertices has the m children.

There are mi vertices in the tree other than the root.

$\therefore$ The tree contains $n = mi+1$ vertices.

Theorem 4:-

A full m-ary tree or regular m-ary tree with

(i) n - vertices has $i = (n-1)/m$ internal vertices and $l = [(m-1)n + 1]/m$ leaves.

(ii) 'i' internal vertices has $n = mi+1$ vertices and $l = (m-1)i + 1$ leaves

(iii) 'l' leaves has $n = (ml-1)/(m-1)$ vertices and $i = (l-1)/(m-1)$ internal vertices

How many edges a tree with 10,000 vertices has.

9999

How many veretices does a full 5-ary tree with 100 interenal veretices

501

How many edges does a full binary tree ~~does a~~ with 1000 interenal verticles have?

2001

How leaves does a full 3-ary tree with 100 Veretices have

67

Suppose that someone starets a chain letter. Each person receives the lettere is asked to send it to 4 othere people. Some do this, other donot send any letters. How many people have seen ~~that~~ lettere ~~induo~~ including the 1st person, if no one receives more than 1 letter and if chain lettere ends aftere that hade been 100 people who read it but don't send it out.

How many people send out the lettere.

11. $L = 100 \quad m = 4$

$$n = \frac{(mL - 1)}{m-1}$$

$$= \frac{(4 \times 100 - 1)}{4-1}$$

$$= \frac{399}{3} = 133.$$

$$i = \frac{L-1}{m-1} = \frac{100-1}{4-1} = \frac{99}{3} = 33.$$

- The level of a veretex in a rooted tree is the length of the unique path from the root to the veretex.

- The height of a rooted tree is the max of the levels of vertices.

- The ht of a rooted tree is the length of the longest path from root to any vertex.

- A rooted m-ary tree of ht 'h' is balanced if all leaves are at level 'h' or (h-1)

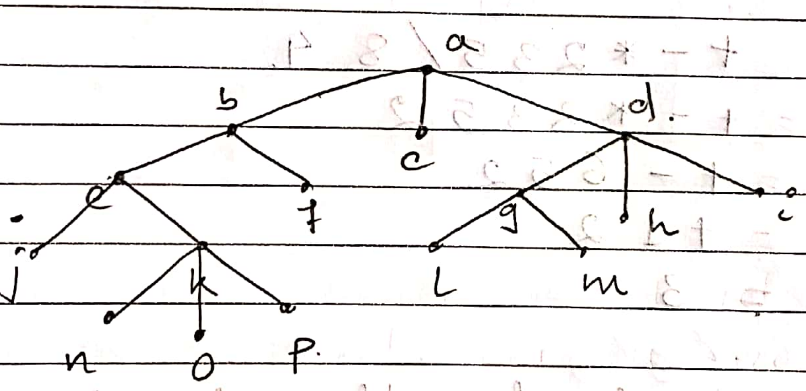
Theorem - 5 :-

There are atmost m^h ~~tree~~ leaves in an m-ary tree of ht. 'h'

Let P(n) : An n-ary tree with ht 'h' has m^h leaves.

TREE TRAVERSAL :-

In-order, Pre-order, post-order.

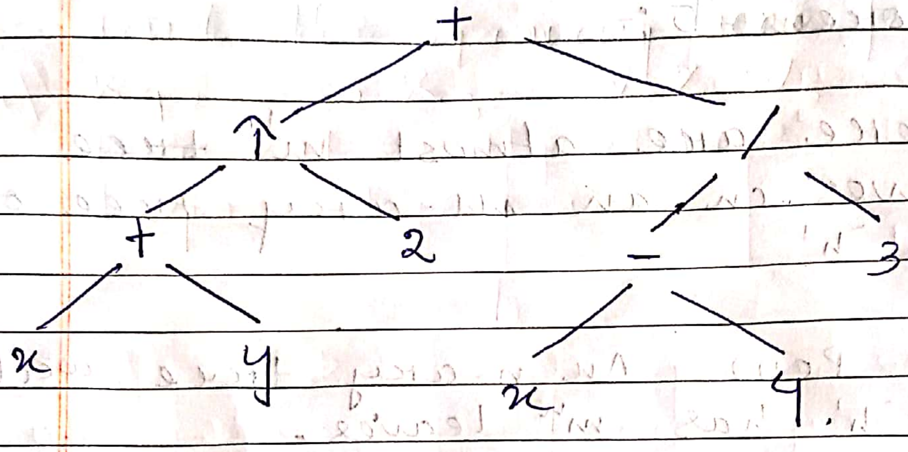


Pre-order :- a b e j k n o p f c d g l m h i

Inorder : j e ~~k~~ n k o p b f a c l g m d h i

Post order : j n o p k ~~b~~ e f b c l ~~m~~ m g h i d a

Order rooted tree :- that represents the expression $((x+y)\uparrow 2)+((x-4)/3)$



what is the value of the prefix expression + − * 2 3 5 / ↑ 2 3 4.

+ − * 2 3 5 / 8 4.
= + − * 2 3 5 2
= + − 6 5 2
= + 1 2
= 3

Evaluate the postfix expression of 7 2 3 * − 4 ↑ 9 3 / +

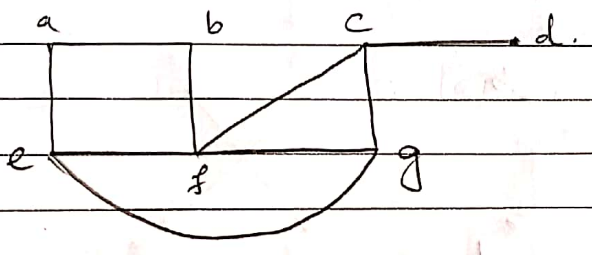
7 2 3 * − 4 ↑ 9 3 / +

= 7 6 − 4 ↑ 9 3 / +
= 1 4 ↑ 9 3 / +
= 1 9 3 / +
= 1 3 + = 4

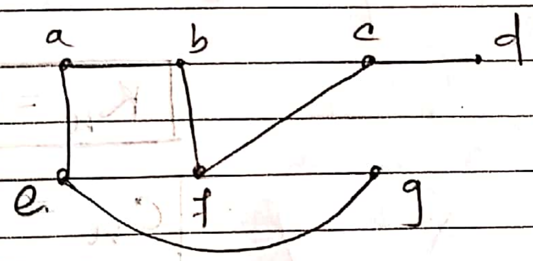
Spanning Tree :

Let G be a simple graph. A spanning tree of G is a subgraph of G i.e a tree containing ~~ver~~ every vertex of G.

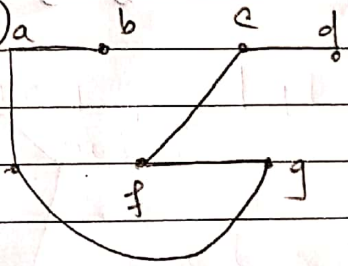
Form a spanning tree for the given graph.



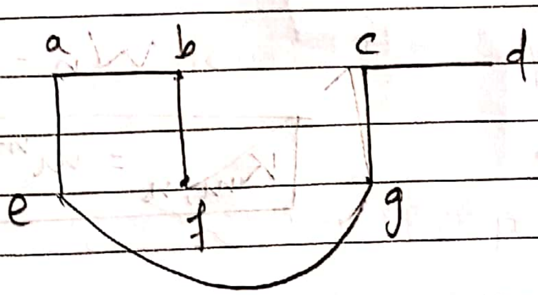
①



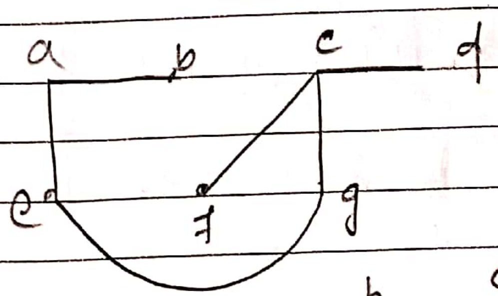
②

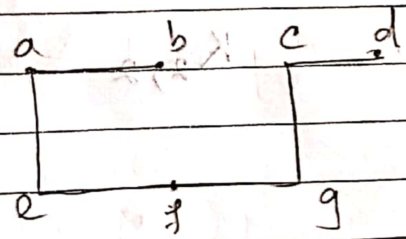


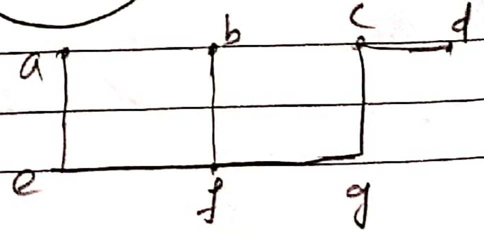
④

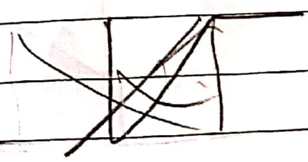


③



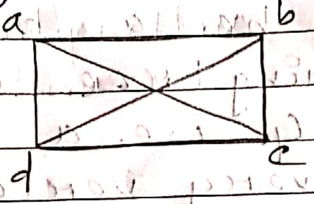




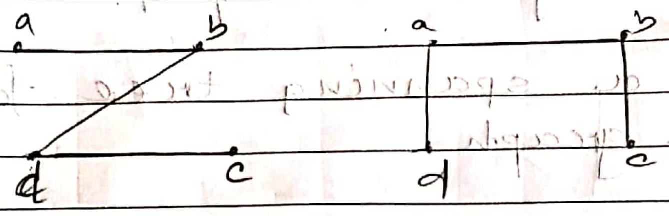


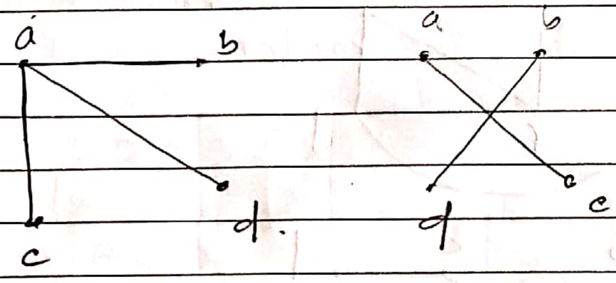
Find the spanning tree for K_3, K_4, K_5, $K_{2,2}$, ~~W_3~~, W_5, C_5.

K_4



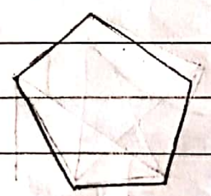
n^2





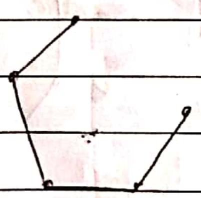
$\boxed{K_n = n^{n-2}}$

K_5 C_5



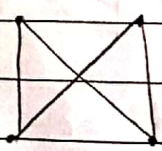
$\boxed{C_n = n}$

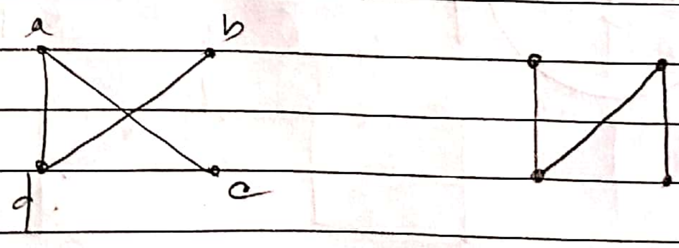
$W_n =$



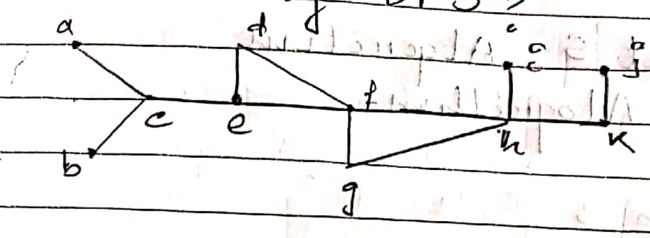
$\boxed{K_{m,n} = m^{n-1} \cdot n^{n-1}}$

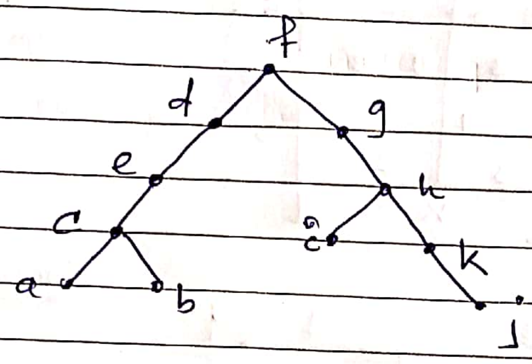
$K_{2,2}$



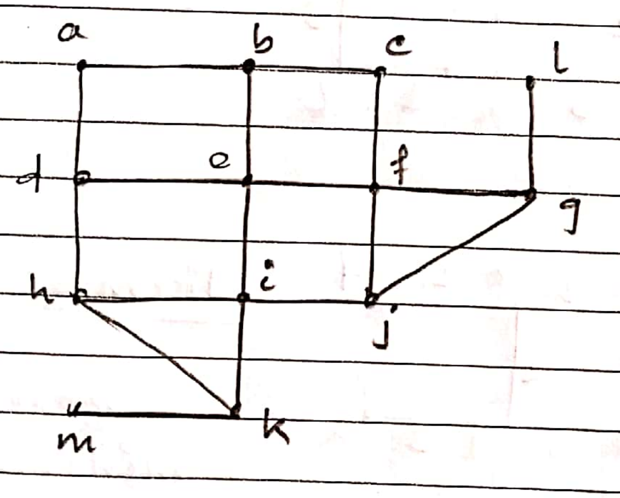


Q.8 Find out the minimum spanning trees using DFS?

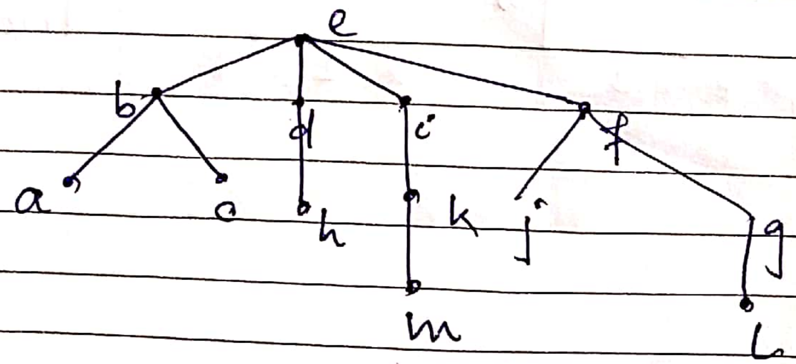




Use BFS

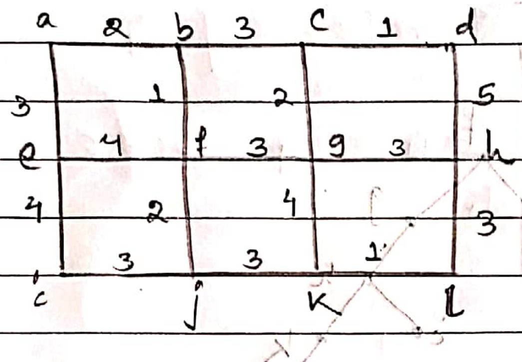


highest degree

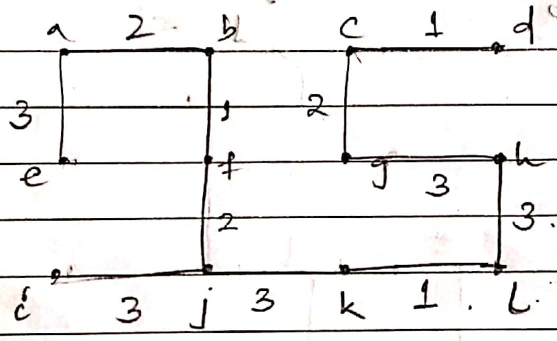


Minimum Spanning Tree :

Imp
→ Kruskal's Algorithm
→ Prim's Alogrithm



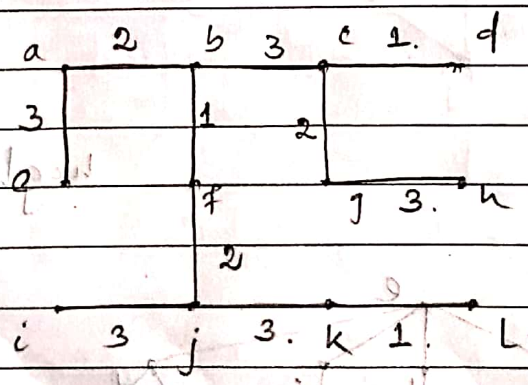
Kruskal's



n-1 edges

24

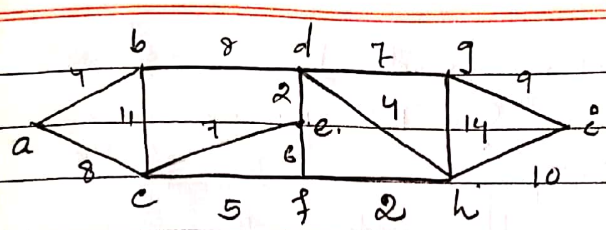
Prim's



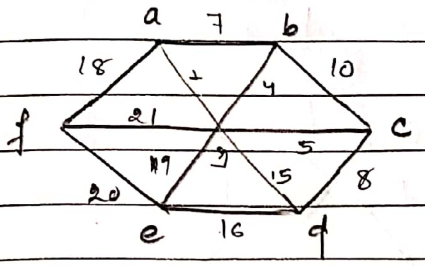
move in minimum wt. dirn.

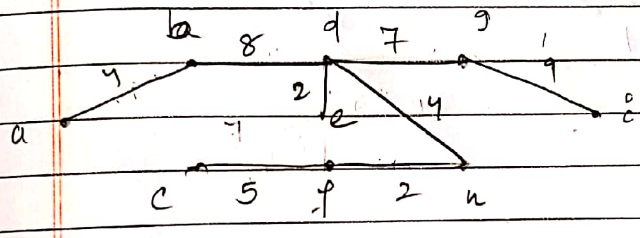
24

1

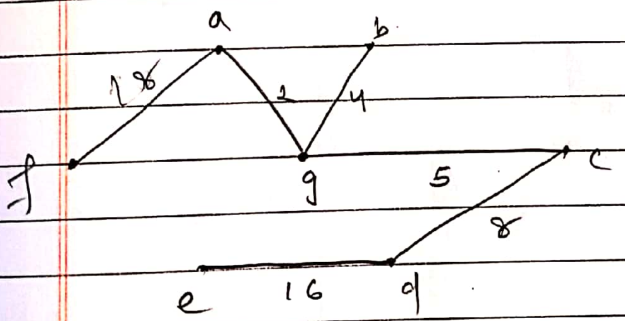

a b c d e f g h i
4 8 7 9 11 7 2 4 14 6 8 5 2 10

2


a b c d e f
7 18 10 21 5 20 8 16 15 4


a b d g i e c f h
4 8 7 9 2 14 5 2

41


a b f g c e d
18 4 5 8 16

6

Sig

A Note on Discrete Fourier Transform and Fast Fourier Transform

Contents

Signals, Sampling and Quantization

Fourier Transforms play an important part in the theory of many branches of science and engineering. A waveform – optical, electrical, or acoustical – and its spectrum are appreciated equally as physical picturable and measurable entities: an oscilloscope enables us to see an electrical waveform, and a spectroscope or spectrum analyzer enables us to see optical or electrical spectra. Waveforms and spectra are Fourier transforms of each other. The Fourier transformation is thus an eminently physical relationship.

Introduction of the Fast Fourier Transform (FFT) algorithms has greatly broadened the scope of application of the Fourier transform to data handling and to the digital formulation in general and has brought prominence to the Discrete Fourier Transform (DFT). These are indispensable to any professional who handles masses of data, not only engineers but experts in many subfields of medicine, biology, and remote sensing.

A student of computer science will find it immensely useful in data transfer and data processing for images or audio signals. We will start with a very brief introduction to signals and digital signals before coming to the mathematics of Discrete Fourier Transform and the Fast Fourier Transform algorithm.

A signal is a function defined over a domain with independent variables like time, space or any other variables. It refers to a physical quantity that varies with time, space or any other independent variables. The most common signals occurring in nature are the audio signals and video signals which are received by our ears and eyes. The ECG signal from the heart and the EEG signal from the brain are also natural signals which can be received / processed by appropriate receivers which are sophisticated machines. Similarly we have other natural signals like seismic signals which are received and processed by sophisticated machines.

The signals, whether natural or processed, are classified into four broad categories.

- Continuous-Time &Continuous-Valued
- Continuous-Time &Discrete-Valued
- Discrete-Time& Continuous-Valued
- Discrete-Time &Discrete-Valued

The last one is called as Digital Signals and shall be in the focus of our study.

Almost all signals available in nature are of the first type, that is, Continuous-Time Continuous-Valued and are called as Analog Signals. These signals can be received and processed as analog signals by using analog hard wares. However the analog signals are converted to digital signals by the process of sampling and quantization. Sampling makes the time discrete while quantization make the value discrete.

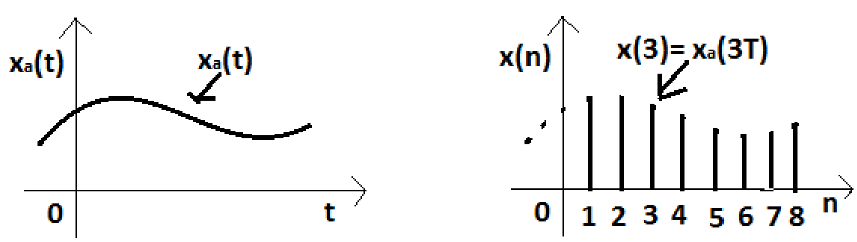
There are advantages of Digital Signal processing over Analog Signal processing. Digital signal processing is cheap and fast without compromising the accuracy and quality.

Sampling: Sampling converts a continuous-time signal to a discrete-time signal by taking samples of the continuous-time signal at discrete-time instants. Let $x_a(t)$ be the input from the analog signal then the sampler provides an output $x_a(nT) \equiv x(n)$, where T is called the sampling interval.

There are many ways to sample an analog signal. We shall discuss only on periodic sampling or uniform sampling. This is because of its frequent use. Periodic sampling is described by the relation

$$x(n) = x_a(nT), \qquad -\infty < n < \infty$$

where $x(n)$ is the discrete-time signal obtained by taking samples of the analog signal $x_a(t)$ every T seconds. The time interval T between successive samples is called the sampling period or sample interval and its reciprocal $1/T = F_s$ is called the sampling rate (samples per second) or the sampling frequency (hertz).



Periodic Sampling of an Analog Signal

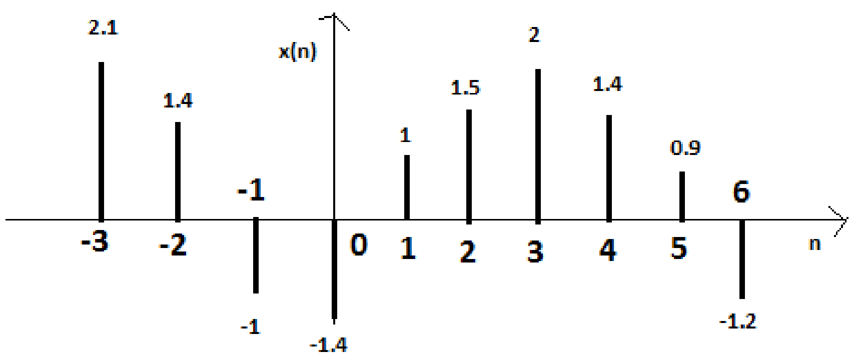
Periodic sampling establishes a relationship between the time variable t and n of continuous-time and discrete-time signals, respectively. These variables are linearly related through the sampling rate $1/T = F_s$ as $t = nT = \frac{n}{F_s}$.

The sampling period T or, equivalently, the sampling rate F_s is selected using the sampling theorem and the value of F_{max}, the maximum frequency which our signal under study will not exceed. The **sampling theorem** says "If the highest frequency contained in an analog signal $x_a(t)$ is $F_{max} = B$ and the signal is sampled at a rate $F_s > 2F_{max} \equiv 2B$, then, $x_a(t)$ can be exactly recovered from its sample value using the interpolation function $g(t) = \frac{\sin 2\pi Bt}{2\pi Bt}$.

Quantization: The process of converting a discrete-time continuous-amplitude signal into a digital signal by expressing each sample value as a finite (instead of an infinite) number of digits, is called quantization. The error introduced in representing the continuous valued signal by a finite set of discrete values is called quantization error or quantization noise.

Discrete-Time Signals, Classifications and Simple Manipulations

As discussed earlier a discrete-time signal *x(n)* is a function of an independent variable that is an integer. A graphical example of such a signal is given below:



Graphical Representation of a discrete-time signal

There are other ways of expressing a discrete-time signal. Some of them are given below.

a) **Functional Representation**

$$x(n) = \begin{cases} 3, & for\ \ n = 1,3 \\ 1, & for\ \ n = 2 \\ 0, & elsewhere \end{cases}$$

b) **Tabular Representation**

n	……. ……	–2	–1	0	1	2	3	4	5	6
x(n)	…….. ----	0	0	0	3	1	3	0	0	0

c) **Sequence Representation**

An infinite-duration signal or sequence with the time origin (n = 0) indicated by the symbol ↑ is represented as follows

$$x(n) = \{\ldots\ldots,\ 0,\ 0,\ \underset{\uparrow}{3},\ 1,\ 3,\ 0,\ 0,\ \ldots\ldots\ldots\}$$

A sequence *x(n)* which is zero for *n < 0* can be represented as

$$x(n) = \{\underset{\uparrow}{0},\ 3,\ 1,\ 3,\ 0,\ 0,\ \ldots\ldots\ldots\}$$

Some more examples are as follows.

A finite-duration Discrete-Time Signal:

$$x(n) = \{-3,\ 2,\ 0,\ \ \underset{\uparrow}{0},\ 3,\ 1,\ 3,\ 0,\ 0,\}$$

A finite duration duration Discrete-Time Signal with *x(n) = 0* for *n < 0*

$$x(n) = \{\underset{\uparrow}{0},\ 3,\ 1,\ 3,\ 0,\ 0,\}$$

Some Elementary Discrete-Time Signals

The Unit Impulse Sequence (Unit Sample Sequence)

$$\delta(n) = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases}$$

The Unit Step Signal

$$u(n) = \begin{cases} 1, & n \geq 0 \\ 0, & n < 0 \end{cases}$$

The Unit Ramp Signal

$$u_r(n) = \begin{cases} n, & n \geq 0 \\ 0, & n < 0 \end{cases}$$

Periodic and Aperiodic signals

A signal is periodic with period N *(N > 0)* if and only if $x(n+N) = x(n), \ \forall n$

The smallest value of N for which the above holds is called the fundamental period of the signal. If there is no such N for which the above relation holds then the signal is called non-periodic or aperiodic.

Symmetric (even) and anti-symmetric (odd) signals

A real valued signal is called symmetric (even) if $x(-n) = x(n)$. On the other hand, a signal is called anti-symmetric if $x(-n) = -x(n)$.

Simple Manipulations of Discrete-Time signals

Transformation of the independent variable (time): A signal $x(n)$ may be shifted in time by replacing the independent variable n by $n - k$, where k is an integer. If k is a positive integer, the time shift results in a delay of the signal by k units of time. If k is a negative integer, the time shift results in an advance of the signal by $|k|$ units in time. It is denoted as

$$TD_k[x(n)] = x(n-k) \quad k > 0$$

A signal $x(n)$ and its delayed version $x(n-2)$ and an advance version $x(n+3)$ are represented below.

$$x(n) = \{. . . \ 0, \ 0, \ 1, \ 2, \ \underset{\uparrow}{3}, \ 3, \ 3, \ 3, \ 3, \ 0, \ 0, \ ...\}$$

$$TD_2[x(n)] = x(n-2) = \{. . . \ 0, \ 0, \ \underset{\uparrow}{1}, \ 2, \ 3, \ 3, \ 3, \ 3, \ 3, \ 0, \ 0, \ ...\}$$

$$z(n) = x(n+3) = \{. . . \ 0, \ 0, \ 1, \ 2, \ 3, \ 3, \ 3, \ \underset{\uparrow}{3}, \ 3, \ 0, \ 0, \ ...\}$$

The folding operation is denoted by $FD[x(n)] = x(-n)$

Now $\qquad TD_k\{FD[x(n)]\} = TD_k x(-n) = x(-n+k)$

whereas $\qquad FD\{TD_k[x(n)]\} = FDx(n-k) = x(-n-k)$

Another modification of the independent variable involves replacing n by μn, where μ is an integer. This time-base modification is referred as time-scaling or down-sampling. From the signal $x(n)$ as given above we get $x(2n)$ as

$$w(n) = x(2n) = \{. . . \ 0, \ 0, \ 0, \ 1, \ \underset{\uparrow}{3}, \ 3, \ 3, \ 0, 0, \ 0, \ 0, \ ...\}$$

Amplitude Scaling of a signal: The amplitude scaling of a signal by a constant A is accomplished by multiplying the value of every signal sample by A. So we have

$$y(n) = Ax(n), \qquad -\infty < n < \infty$$

For the $x(n)$ as above we have $y(n)=3x(n)$ as given below.

$$y(n)=3x(n)=\{...\ 0,\ 0,\ 3,\ 6,\ \underset{\uparrow}{9},\ 9,\ 9,\ 9,\ 9,\ 0,\ 0,\ ...\}$$

Sum of two signals: The sum of two signals $x_1(n)$ and $x_2(n)$ is a signal $y(n)=x_1(n)+x_2(n)$ where the value of $y(n)$ at any instant is the sum of the value of the two signals $x_1(n)$ and $x_2(n)$ at the same instant.

Product of two signals: The product of two signals is defined on a sample-to-sample basis as

$$y(n)=x_1(n)x_2(n)$$

Example: Let us have two signals as follows.

$$x_1(n)=\{........,\ 0,\ 0,\ \frac{1}{3},\ \frac{1}{2},\ \underset{\uparrow}{1},\ 1,\ 1,\ 1,\ 0,\ 0,\ ....\}\ \&\ x_2(n)=\{.......,\ 0,\ 0,\ 0,\ -1,\ \underset{\uparrow}{1},\ 3,\ 5,\ 7,\ 0,\ 0,\ .....\}$$

We have

$$FD[x_1(n)]=x_1(-n)=\{........,\ 0,\ 0,\ 1,\ 1,\ 1,\ \underset{\uparrow}{1},\ \frac{1}{2},\ \frac{1}{3},\ 0,\ 0,\ ....\}$$

and

$$TD_3\{FD[x_1(n)\}]=TD_3\{x_1(-n)\}=\{........,\ 0,\ 0,\ \underset{\uparrow}{1},\ 1,\ 1,\ 1,\ \frac{1}{2},\ \frac{1}{3},\ 0,\ 0,\ ....\}$$

Further

$$TD_3[x_1(n)]=x_1(n-3)=\{........,\ 0,\ \underset{\uparrow}{0},\ \frac{1}{3},\ \frac{1}{2},\ 1,\ 1,1,\ 1,\ 0,\ 0,\ ....\}$$

and

$$FD\{TD_3[x_1(n)]\}=x_1(-n-3)=\{........,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,\ \frac{1}{2},\ \frac{1}{3},\ \underset{\uparrow}{0},\ 0,\ ....\}$$

Adding the two signals we get

$$x_1(n)\ +\ x_2(n)=\{........,\ 0,\ 0,\ \frac{1}{3},\ -\frac{1}{2},\ \underset{\uparrow}{2},\ 4,\ 6,\ 8,\ 0,\ 0,\ ....\}$$

Multiplying the two signals we get

$$x_1(n)\,x_2(n)=\{........,\ 0,\ 0,\ 0,\ -\frac{1}{2},\ \underset{\uparrow}{1},\ 3,\ 5,\ 7,\ 0,\ 0,\ ....\}$$

Exercise:

1. A discrete-time signal $x(n)$ is defined as

$$x(n) = \begin{cases} 1+\frac{n}{3}, & -3 \le n \le -1 \\ 1, & 0 \le n \le 3 \\ 0, & Elsewhere \end{cases}$$

   a. Express the signal in sequence form and sketch it.
   b. Find $TD_4\{FD[x(n)]\}$ & $FD\{TD_4[x(n)]\}$ and compare the outcomes.
   c. Can you express the signal $x(n)$ in terms of $\delta(n)$ & $u(n)$?

2. Show that
   a. $\delta(n) = u(n) - u(n-1)$
   b. $u(n) = \sum_{k=-\infty}^{n} \delta(k) = \sum_{k=0}^{\infty} \delta(n-k)$

3. Show that any signal can be decomposed into an even and odd component. Is the decomposition unique? Illustrate your argument using the signal

n	-2	-1	0	1	2
x(n)	2	3	4	5	6

4. For the signal in question number 1 find out the following signals and express them in any suitable form.
   a) $x(n)u(2-n)$
   b) $x(n-1)\delta(n-3)$
   c) $x(n^2)$

The Discrete Fourier Transform (DFT)

Let $x(n)$ be a periodic sequence with period *N*, that is $x(n+N) = x(n),\ \forall n$. This periodic sequence when expressed as a series of *N* exponential functions

$$e^{j2\pi kn/N}, \quad k = 0, 1, \ldots.., N-1$$

Takes the form of the **Fourier series** as

$$x(n) = \sum_{k=0}^{N-1} c_k e^{j2\pi kn/N} \qquad \text{(A)}$$

Where the $\{c_k\}$ are the coefficients in the series representation.

The expressions for the Fourier coefficients c_k can be obtained by multiplying both sides of the above equation by the exponential $e^{-j2\pi kn/N}$ and then summing the product from *n = 0* to *n = N* – 1. So we have

$$\sum_{n=0}^{N-1} x(n)e^{-j2\pi kn/N} = \sum_{n=0}^{N-1}\sum_{k=0}^{N-1} c_k e^{j2\pi(k-l)n/N} \qquad \text{(B)}$$

By performing the summation over *n* first on the right hand side we get

$$\sum_{n=0}^{N-1} e^{j2\pi(k-l)n/N} = \begin{cases} N, & k-l = 0, \pm N, \pm 2N, \ldots \\ 0, & Otherwise \end{cases}$$

Therefore the right hand side of the equation (B) reduces to Nc_l and hence we get

$$c_l = \frac{1}{N}\sum_{n=0}^{N-1} x(n)e^{-j2\pi nl/N}, \; l = 0, 1, \ldots, N-1 \qquad \text{(C)}$$

The relationship between $x(n)$ and c_k as given by (A) and (C), which looks somehow similar, motivates us to define the Fourier Transform of a finite duration Discrete-Time signal with length $L \leq N$ as follows.

Given a sequence $x(n)$ of finite duration $L \leq N$, we define a periodic sequence $x_p(n)$ with period N as follows

$$x_p(n) = \begin{cases} x(n), & 0 \leq n \leq L-1 \\ 0, & L \leq n \leq N-1 \end{cases}$$

It may be noted that the zero padding for $L \leq n \leq N-1$ does not provide any additional information but, we will see it soon, it will help us to adjust our length of the sequence with a particular radix to compute the Fourier transform fast. Using the expression of the periodic sequence and its Fourier coefficient in (A) and (C) which can be obtained for our constructed periodic sequence $x_p(n)$ with period N we define the Discrete Fourier Transform (DFT) and the Inverse Discrete Fourier Transform of $x(n)$ as follows.

DFT $\quad X(k) = \sum_{n=0}^{N-1} x(n)e^{-j2\pi kn/N}, \; k = 0, 1, \ldots, N-1$

IDFT $\quad x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X(k)e^{j2\pi kn/N}, \; n = 0, 1, \ldots, N-1$

Here the sequence $x(n)$ is the original sequence or called as the input sequence and the sequence $X(k)$ is the computed DFT sequence or the output sequence.

The above expressions of DFT and IDFT can be made simpler by introducing a notation W_N which stands for $e^{-j2\pi/N}$. This is one of the Nth root of 1. With this improvisation we get

$$W_N = e^{-2j\pi/N}$$
$$W_N^{kn} = e^{-2j\pi kn/N}$$

And the DFT and IDFT as

DFT $$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn}, \; k = 0, 1, \ldots., N-1$$

IDFT $$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) W_N^{-kn}, \; n = 0, 1, \ldots.., N-1$$

We will apply this formula to compute the DFT and IDFT in matrix notation as that will be easier to implement. The expressions of DFT and IDFT in matrix form are presented in the next section.

The DFT as a Linear Transformation and Its Other Properties

The formulas of DFT and IDFT given in the previous article may be expressed as

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn}, \; k = 0, 1, \ldots., N-1$$

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) W_N^{-kn}, \; n = 0, 1, \ldots.., N-1$$

where, by definition $W_N = e^{-j2\pi/N}$, which is an Nth root of 1.

The computation of each point of the DFT can be accomplished by N complex multiplications and $(N – 1)$ complex additions. So the N-point DFT values can be computed using N^2 complex multiplications and $N(N – 1)$ complex additions.

To see that the DFT and IDFT are linear transformations on sequences $\{x(n)\}$ & $\{X(k)\}$ respectively let us express the N-point vector $\mathbf{x}_N$ of the signal sequence $x(n), \; n = 0, 1, \ldots, \; N-1$, and the N-point vector $\mathbf{X}_N$ of the transformed sequence $X(k)$ and an N×N matrix $\mathbf{W}_N$ as

$$\mathbf{x}_N = \begin{bmatrix} x(0) \\ x(1) \\ \vdots \\ x(N-1) \end{bmatrix}, \; \mathbf{X}_N = \begin{bmatrix} X(0) \\ X(1) \\ \vdots \\ X(N-1) \end{bmatrix}, \; \mathbf{W}_N = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W_N & W_N^2 & \cdots & W_N^{N-1} \\ 1 & W_N^2 & W_N^4 & \cdots & W_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & W_N^{N-1} & W_N^{2(N-1)} & \cdots & W_N^{(N-1)(N-1)} \end{bmatrix}$$

With these notations and definitions the N-point DFT can be expressed in matrix form as

$$\mathbf{X}_N = \mathbf{W}_N \mathbf{x}_N$$

Where $\mathbf{W}_N$ is the matrix of the linear transformation. It can be observed that $\mathbf{W}_N$ is a symmetric matrix. In fact, it is also a scalar multiple of a unitary matrix where the scalar is $\sqrt{N}$. So the IDFT is obtained by multiplying the inverse of the matrix both side and it gives us

$$\mathbf{x}_N = \mathbf{W}_N^{-1}\,\mathbf{X}_N = (1/N)\,\mathbf{W}_N^{*}\,\mathbf{X}_N$$

where $\mathbf{W}_N^{*}$ denotes the complex conjugate of the matrix $\mathbf{W}_N$. The elements of the matrix $\mathbf{W}_N$ are referred as **phase factors**.

Example: Compute the DFT of $x(n) = (0\ \ 1\ \ 4\ \ 9)$.
Solution: The first step is to construct $\mathbf{W}_4$. Here $W_4 = e^{-j\pi/2} = -j$. So the matrix $\mathbf{W}_4$ is constructed as follows.

$$\mathbf{W}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & -j \end{bmatrix}$$

So

$$\mathbf{X}_4 = \mathbf{W}_4\,\mathbf{x}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -j & -1 & j \\ 1 & -1 & 1 & -1 \\ 1 & j & -1 & -j \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 4 \\ 9 \end{bmatrix} = \begin{bmatrix} 14 \\ -4+8j \\ -6 \\ -4-8j \end{bmatrix}$$

Similarly the matrix for IDFT can be constructed and applied.

Example: Find the DFT of $x(n) = (1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1)$.

Solution: Here $N = 8$ and $W_8 = \frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}}$. We construct the $\mathbf{W}_8$ as follows.

$$\mathbf{W}_8 = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} & -j & -\frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} & -1 & -\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} & j & \frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} \\
1 & -j & -1 & j & 1 & -j & -1 & j \\
1 & -\frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} & j & \frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} & -1 & \frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} & -j & -\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} & -j & \frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} & -1 & \frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} & j & -\frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} \\
1 & j & -1 & -j & 1 & j & -1 & -j \\
1 & \frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} & j & -\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}} & -1 & -\frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}} & -j & \frac{1}{\sqrt{2}} - \frac{j}{\sqrt{2}}
\end{bmatrix}$$

Hence we get $\mathbf{X}_8 = \mathbf{W}_8\,\mathbf{x}_8 = (8\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0)$

Linearity: As DFT is implemented using a matrix and a matrix transforms vectors following the linear property, so the DFT is a linear transform. That is, if $x_1(n) \underset{N}{\overset{DFT}{\leftrightarrow}} X_1(k)$ and $x_2(n) \underset{N}{\overset{DFT}{\leftrightarrow}} X_2(k)$ then for any real valued or complex valued constants a_1 & a_2 we have

$$a_1 x_1(n) + a_2 x_2(n) \underset{N}{\overset{DFT}{\leftrightarrow}} a_1 X_1(k) + a_2 X_2(k)$$

Periodicity: If $x(n)$ & $X(k)$ are the N-point DFT pair then

$x(n+N) = x(n) \ \forall n \quad \& \quad X(k+N) = X(k) \ \forall k$

So the DFT preserves the periodic property of the signal

Exercise: Find the DFT of the following finite duration signals.

a) $x(n) = \left(\frac{1}{2}\right)^n, \ 0 \le n \le 3$
b) $x(n) = (-1)^n, \ 0 \le n \le 7$
c) $x(n) = \{2, 1, 3, 1, 4, 1\}$
d) $x(n) = \{0, 1, 2, 3, 4\}$

Divide-and-Conquer Approach to Computation of DFT

We have seen that to compute a N-point DFT we have to perform N^2 complex multiplication and $N(N-1)$ complex additions. This finally becomes $4N^2$ real multiplications and $2N(N-1)$ real additions. In practice N is large; hence the number of multiplication becomes very large. To reduce the number of operations there are efficient algorithms to compute the DFT. One of them is the Divide-and-Conquer method.

Direct computation of the DFT is basically inefficient primarily because it does not exploit the symmetry and periodicity properties of the phase factor W_N. In particular, these two properties are:

Symmetry property: $W_N^{k+N/2} = -W_N^k$

Periodicity property: $W_N^{k+N} = W_N^k$

The computationally efficient algorithms described in this section, known collectively as fast Fourier transform (FFT) Algorithms; exploit these two basic properties of the phase factor.

Let us consider the computation of an N-point DFT where $N = LM$. To have a composite N is not a restriction as we can pad zeros to make N composite. Now the sequence $x(n)$, $0 \le n \le N-1$, can be stored in a one dimensional array indexed by n or in a two dimensional array indexed by l & m where $0 \le l \le L-1$ & $0 \le m \le M-1$ as illustrated in the following tables.

n	0	1	2	………	$N-1$
$x(n)$	$x(0)$	$x(1)$	$x(2)$	………	$x(N-1)$

$l\downarrow$ $m\rightarrow$	0	1	……..	M – 1
0	$x(0,\ 0)$	$x(0,\ 1)$		
1	$x(1,\ 0)$	$x(1,\ 1)$		
2	$x(2,\ 0)$	$x(2,\ 1)$		
$L-1$				

Here l is the row index and m is the column index. So the sequence $x(n)$, $0 \le n \le N-1$ can be stored in a rectangular array in a variety of ways, each of which depends on the mapping of index n to the indexes (l, m).

For example, if we select the mapping $n = Ml + m$ then this leads to an arrangement in which the first row consist of the first M elements of $x(n)$, the second row consists of the next M elements of $x(n)$, and so on. On the other hand if the mapping $n = l + Lm$ is selected then the first L elements of $x(n)$ will be in the first column, the next L elements will be in the second column and so on.

A similar arrangement can be made to store the computed DFT values using a mapping $k = Mp + q$ or using a mapping $k = p + Lq$ where the index k of $X(k)$ is mapped to the indexes (p, q).

Once $x(n)$ is mapped to the rectangular array $x(l, m)$ and $X(k)$ is mapped into a corresponding rectangular array $X(p, q)$ the DFT can be expressed as a double sum over the elements of the rectangular array multiplied by the corresponding phase factors.

To make it specific let us adopt a column-wise mapping for $x(n)$ given by $n = l + Lm$ and row wise mapping of the computed DFT given by $k = Mp + q$. In such a case we have

$$X(p,q) = \sum_{m=0}^{M-1}\sum_{l=0}^{L-1} x(l,m) W_N^{(Mp+q)(mL+l)} \qquad (*)$$

However

$$W_N^{(Mp+q)(mL+l)} = W_N^{MLmp} W_N^{mLq} W_N^{Mpl} W_N^{lq}$$

where $W_N^{MLmp} = W_N^{Nmp} = 1$; $W_N^{mqL} = W_{N/L}^{mq} = W_M^{mq}$ and $W_N^{Mpl} = W_{N/M}^{pl} = W_L^{pl}$

With this simplifications (*) can be written as

$$X(p,q) = \sum_{l=0}^{L-1} \left\{ W_N^{lq} \sum_{m=0}^{M-1} x(l,m) W_M^{mq} \right\} W_L^{lp} \qquad (**)$$

The expression in (**) involves the computation of DFTs of length M and length L. To make it more elaborate let us subdivide the computation into three steps.

1. First the M-point DFT is computed using
   $F(l,q) \equiv \sum_{m=0}^{M-1} x(l,m) W_M^{mq}$, $0 \le q \le M-1$ for each of the rows $l = 0, 1, \ldots.., L-1$
2. Second, a new rectangular array $G(l,q)$ is defined as
   $G(l,q) = W_N^{lq} F(l,q), \quad 0 \le l \le L-1, \ 0 \le q \le M-1$
3. Finally, the L-point DFTs are computed using
   $X(p,q) = \sum_{l=0}^{L-1} G(l,q) W_L^{lp}$ for each column $q = 0, 1, \ldots.., M-1$ of the array $G(l,q)$.

Let us evaluate the computational complexity of (**). The first step involves the computations of L DFTs, each of M points. Hence this step requires LM^2 complex multiplications and $LM(M-1)$ complex additions. The second step requires LM complex multiplications. Finally the third step requires ML^2 complex multiplications and $ML(L-1)$ complex additions. Therefore, the computational complexity is

Complex Multiplications:	$N(M + L + 1)$
Complex Additions:	$N(M + L - 2)$

Where $N = ML$. Thus the number of multiplications has been reduced from N^2 to $N(M + L + 1)$ and the number of additions has been reduced from $N(N-1)$ to $N(M + L - 2)$.

For example, if $N = 1000$ and we select $L = 2$ and $M = 500$, then instead of performing 10^6 complex multiplications via direct computation of the DFT, this approach leads to 503000 complex multiplication. This is a 50% reduction. The number of additions is also similarly reduced by 50%.

When N is highly composite number, that is, N can be factored in to product of prime numbers of the form $N = r_1 r_2 \ldots\ldots r_\nu$ then the decomposition above can be repeated $\nu - 1$ times. This procedure results in smaller DFTs, which, in turn, leads to a more efficient computational algorithm.

The above algorithm can be summarized as follows

Algorithm 1

1. Store the signal column-wise
2. Compute the *M*-point DFT of each row
3. Multiply the resulting array by the phase factors W_N^{lq}
4. Compute the *L*-point DFT of each column
5. Read the resulting array row-wise

An additional algorithm with a similar computational structure can be obtained if the input signal is stored row-wise and the resulting transformation is column-wise. In this case the mappings selected are $n = Ml + m$ and $k = p + Lq$. This choice of indices leads to the formula for the DFT in the form

$$X(p,q) = \sum_{m=0}^{M-1}\sum_{l=0}^{L-1} x(l,m) W_N^{pm} W_L^{pl} W_M^{qm} = \sum_{m=0}^{M-1} W_M^{mq} \left\{ \sum_{l=0}^{L-1} x(l,m) W_L^{lp} \right\} W_N^{mp}$$

Thus we obtain the second algorithm

Algorithm 2

1. Store the signal row-wise
2. Compute the *L*-point DFT of each column
3. Multiply the resulting array by the phase factors W_N^{pm}
4. Compute the *M*-point DFT of each row
5. Read the resulting array column-wise

The two Algorithms given above have same complexity. However they differ in the arrangement of the computation. These special Algorithms are called as FFT, Fast Fourier Transform.

When $N = r_1 r_2 \ldots\ldots r_\nu$ where $r_1 = r_2 = \ldots\ldots = r_\nu = r$ so that $N = r^\nu$ the case becomes very special. In such a case the DFTs are of same size *r*, so that the computation of the *N*-point DFT has a regular pattern. The number *r* is called the radix of the FFT.

Now we will study the Radix-2 FFT Algorithm.

Radix-2 FFT Algorithm

Let us consider the computation of the $N = 2^\nu$ point DFT by the divide-and-conquer approach with $M = N/2$ and $L = 2$. This selection results in a split of the *N*-point data sequence into two *N*/2 point data sequences $f_1(n)$ & $f_2(n)$, corresponding to the even-numbered and odd numbered samples of $x(n)$, respectively, that is

$$f_1(n) = x(2n) \text{ \& } f_2(n) = x(2n+1),\ n = 0, 1, \ldots.., \frac{N}{2} - 1$$

Thus $f_1(n)$ & $f_2(n)$ are obtained by decimating $x(n)$ by a factor of 2, and hence the resulting FFT Algorithm is called a decimating-in-time Algorithm.

Now the N-point DFT can be expressed in terms of the DFTs of the decimated sequences as follows:

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn}, \;\; k = 0, 1, ..., \; N-1$$

$$= \sum_{n\ even} x(n) W_N^{kn} + \sum_{n\ odd} x(n) W_N^{kn}$$

$$= \sum_{m=0}^{(N/2)-1} x(2m) W_N^{2mk} + \sum_{m=0}^{(N/2)-1} x(2m+1) W_N^{k(2m+1)}$$

But $W_N^2 = W_{N/2}$. With this substitution the above can be expressed as

$$X(k) = \sum_{m=0}^{(N/2)-1} f_1(m) W_{N/2}^{km} + W_N^k \sum_{m=0}^{(N/2)-1} f_2(m) W_{N/2}^{km}$$

$$= F_1(k) + W_N^k F_2(k) \qquad k = 0, 1, ..., \; N-1$$

where $F_1(k)$ & $F_2(k)$ are the N/2-point DFTs of the sequences $f_1(m)$ & $f_2(m)$, respectively.

As $F_1(k)$ & $F_2(k)$ are periodic, with period $N/2$, we get $F_1(k+N/2) = F_1(k)$ and $F_2(k+N/2) = F_2(k)$. In addition to this we have the factor $W_N^{k+N/2} = -W_N^k$. Hence we get

$$X(k) = F_1(k) + W_N^k F_2(k) \qquad k = 0, 1, ..., \; \frac{N}{2} - 1$$

$$X(k + \frac{N}{2}) = F_1(k) - W_N^k F_2(k) \qquad k = 0, 1, ..., \; \frac{N}{2} - 1$$

We observe that the direct computation of $F_1(k)$ requires $(N/2)^2$ complex multiplications. The same applies to the computation of $F_2(k)$. Furthermore, there are $N/2$ additional complex multiplications required to compute $W_N^k F_2(k)$. Hence the computation of $X(k)$ requires $2(N/2)^2 + N/2 = N^2/2 + N/2$ complex multiplications. This first step results in a reduction of the number of multiplications from N^2 to $N^2/2 + N/2$ which is close to 50% for large N.

To be consistent with our previous notation, we may define

$$G_1(k) = F_1(k), \qquad k = 0, 1, ..., \; \frac{N}{2} - 1$$

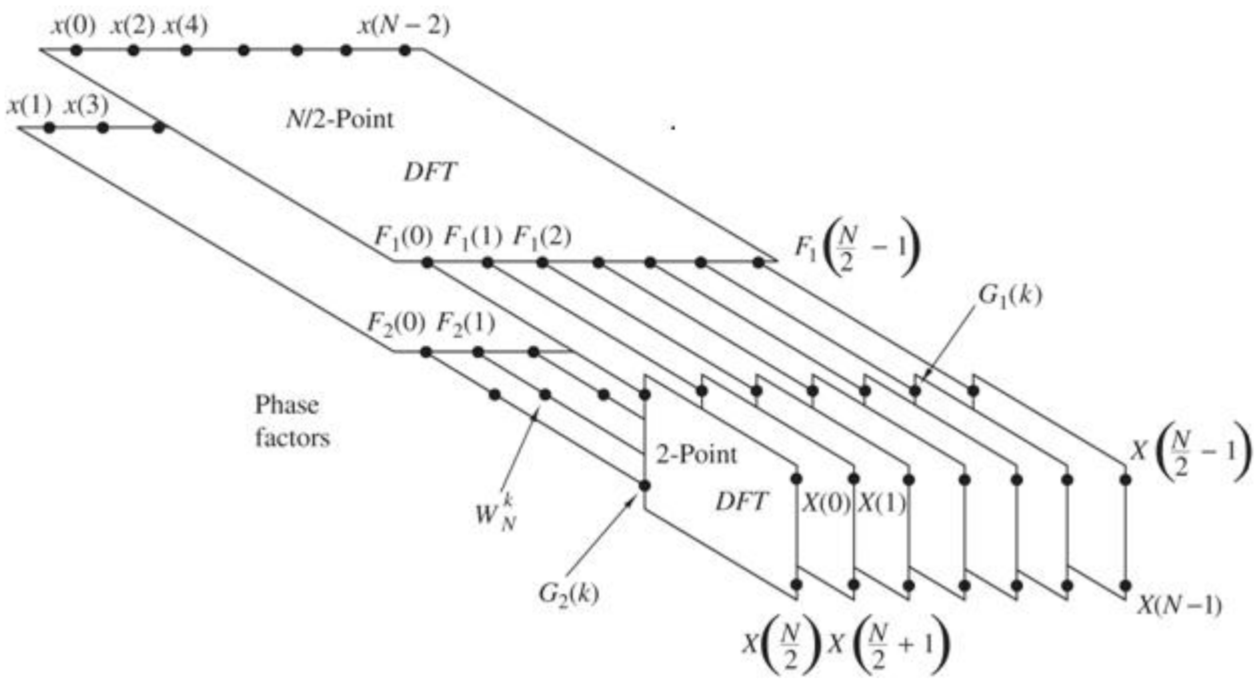
$$G_2(k) = W_N^k F_2(k), \; k = 0, 1, ..., \; \frac{N}{2} - 1$$

Then the DFT $X(k)$ may be expressed as

$$X(k) = G_1(k) + G_2(k), \qquad k = 0, 1, ..., \; \frac{N}{2} - 1$$

$$X(k + \frac{N}{2}) = G_1(k) - G_2(k), \; k = 0, 1, ..., \; \frac{N}{2} - 1$$

The above computation is illustrated in the figure below



Having performed the decimation-in-time once, we can repeat the process for each of the sequences $f_1(n)$ & $f_2(n)$. Thus $f_1(n)$ would result in the two N/4 point sequences

$$v_{11}(n) = f_1(2n) \qquad n = 0, 1, ..., \frac{N}{4} - 1$$

$$v_{12}(n) = f_1(2n+1) \quad n = 0, 1, ..., \frac{N}{4} - 1$$

And $f_2(n)$ would yield

$$v_{21}(n) = f_2(2n) \qquad n = 0, 1, ..., \frac{N}{4} - 1$$

$$v_{22}(n) = f_2(2n+1) \quad n = 0, 1, ..., \frac{N}{4} - 1$$

By computing N/4-point DFTs we would obtain the N/2-point DFTs $F_1(k)$ and $F_2(k)$ from the relations

$$F_1(k) = V_{11}(k) + W_{N/2}^{k} V_{12}(k) \qquad k = 0, 1, ..., \frac{N}{4} - 1$$

$$F_1(k + \frac{N}{4}) = V_{11}(k) - W_{N/2}^{k} V_{12}(k) \qquad k = 0, 1, ..., \frac{N}{4} - 1$$

$$F_2(k) = V_{21}(k) + W_{N/2}^{k} V_{22}(k) \qquad k = 0, 1, ..., \frac{N}{4} - 1$$

$$F_2(k + \frac{N}{4}) = V_{21}(k) - W_{N/2}^{k} V_{22}(k) \qquad k = 0, 1, ..., \frac{N}{4} - 1$$

Where the $\{V_{ij}(k)\}$ are the N/4-point DFTs of the sequences $\{v_{ij}(n)\}$.

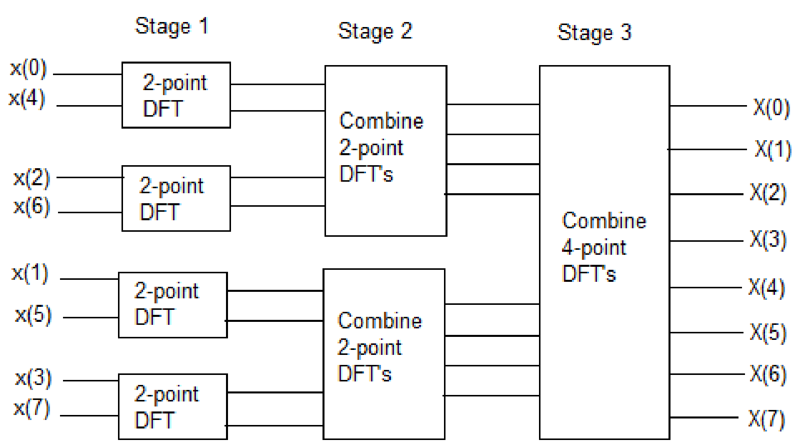
It can be observed that the computation of $\{V_{ij}(k)\}$ requires $4(N/4)^2$ multiplications and hence the computation of $F_1(k)$ and $F_2(k)$ can be accomplished with $N^2/4 + N/2$ complex multiplications. An additional $N/2$ complex multiplications are required to compute $X(k)$ from $F_1(k)$ and $F_2(k)$. Consequently, the total number of multiplications is reduced approximately by a factor of 2 again to $N^2/4 + N$.

The decimation of the data sequence can be repeated again and again until the resulting sequences are reduced to one-point sequences. For $N = 2^\nu$, this decimation can be performed $\nu = \log_2 N$ times. Thus the total number of complex multiplications is reduced to $(N/2)\log_2 N$. The number of complex addition is $N \log_2 N$. The table below presents a comparison of the number of complex multiplications in the FFT and in direct computation of the DFT.

Number of points: N	Complex Multiplications in Direct Computations: N^2	Complex Multiplications in FFT Algorithm: $(N/2)\log_2 N$	Speed Improvement Factor
4	16	4	4.0
8	64	12	5.3
16	256	32	8.0
32	1024	80	12.8
64	4096	192	21.3
128	16384	448	36.6
256	65536	1024	64.0
512	262144	2304	113.8
1024	1048576	5120	204.8

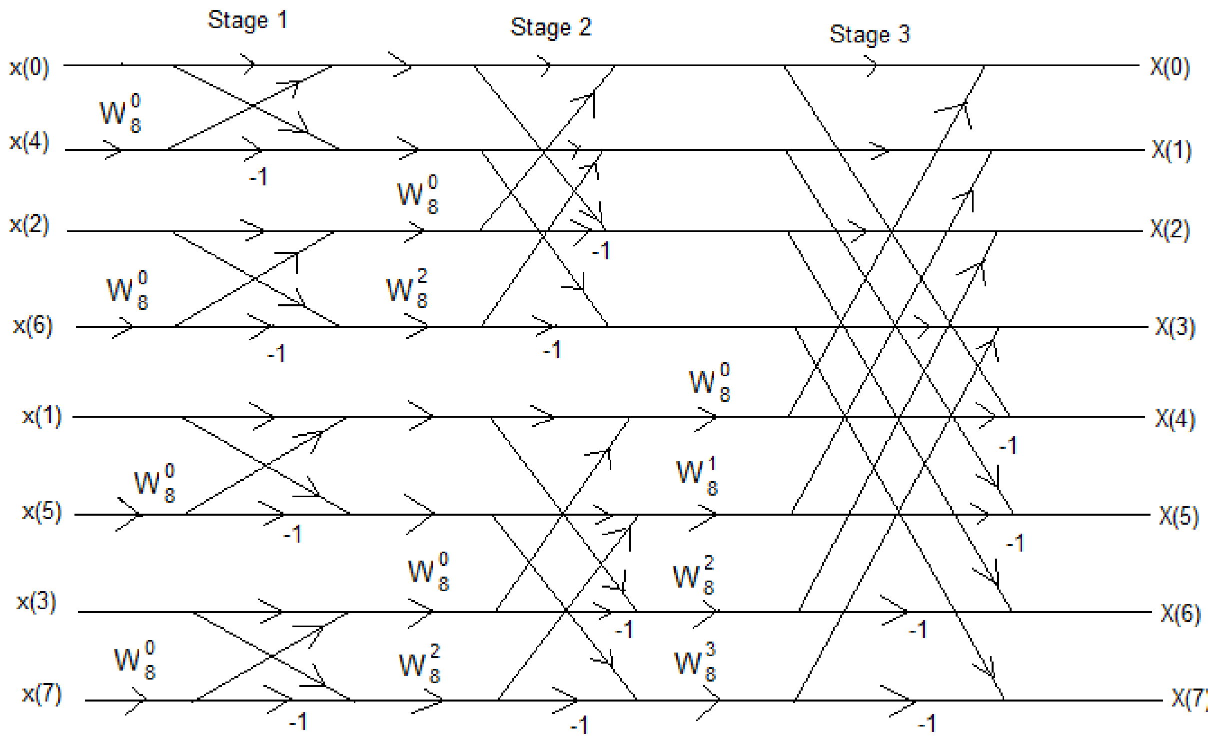
The development process of FFT started around 1965 by Cooley and Tukey who showed a procedure to substantially reduce the amount of computations involved in DFT. The next two decades saw a tremendous improvement in the computation complexity of FFT. In 1969 the 2048-point analysis of a seismic trace took 13.5 hours. Using the FFT, the same task in the same machine took 2.4 seconds!

An illustrative diagram given below depicts the computation of an N = 8-point DFT.



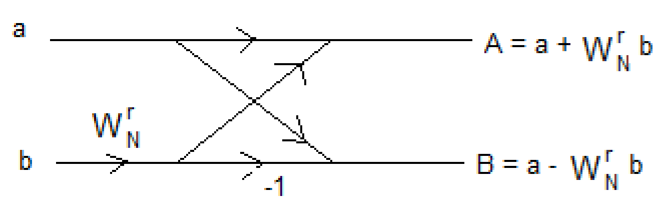
Three stages in the computation of an N=8-point DFT

We observe that the computation is performed in three stages, beginning with the computations of four two-point DFTs, then two four-point DFTs and finally, one eight-point DFT. The combination of smaller DFTs to form the larger DFT is illustrated in the figure below for $N = 8$.



Eight-point decimination-in-time FFT Algorithm

Observe that the basic computation performed at every stage, as illustrated above is to take two complex numbers, say the pair (a, b), multiply 'b' by W_N^r, and then add and subtract the product from 'a' to form two new complex numbers (A, B). This basic computation shown in the figure below is called a butterfly because the flow graph resembles a butterfly.



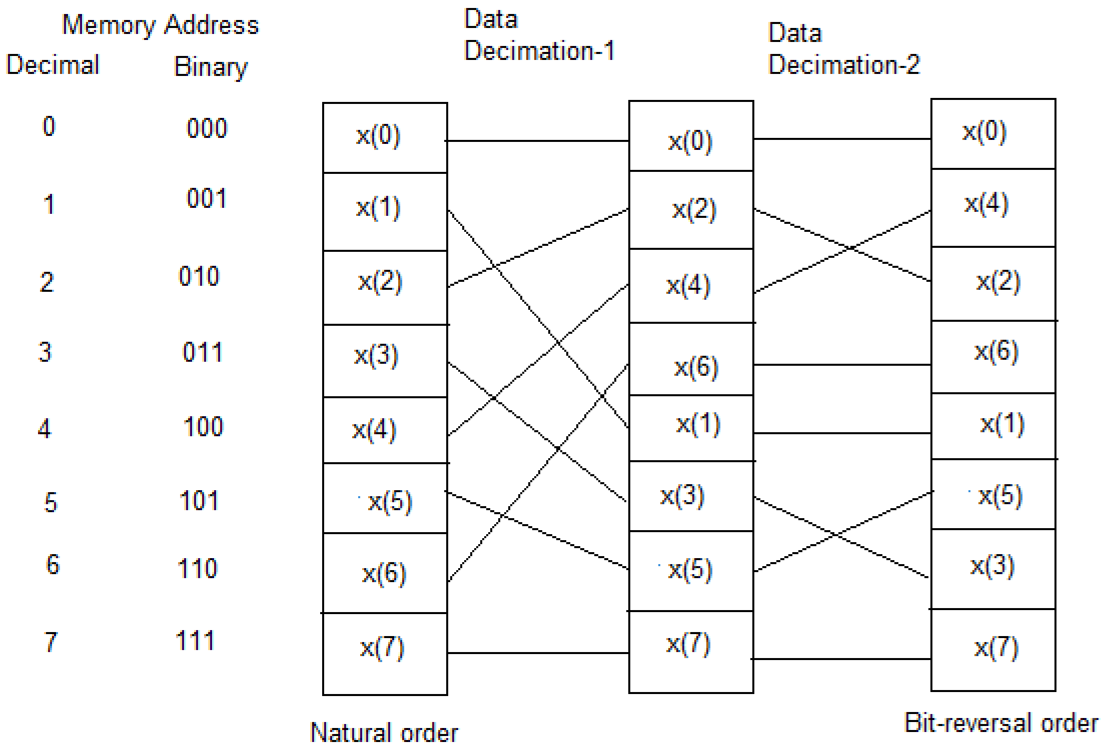
The Basic Butterfly Computation

In general, each butterfly involves one complex multiplication and two complex additions. For $N = 2^{\nu}$, there are $N/2$ butterflies per stage of the computation process and $\log_2 N$ stages. Therefore, as previously indicated the total number of complex multiplications is $(N/2)\log_2 N$ and complex additions is $N \log_2 N$.

Once a butterfly operation is performed on a pair of complex numbers (a, b) to produce (A, B), there is no need to save the input pair (a, b). Hence we can store the result (A, B) in the same location as (a, b). Consequently, we require a fixed amount of storage, namely, $2N$ storage registers, in order to store the results (N complex numbers) of the computations at each stage.

Since the same 2N storage locations are used throughout the computation of the N-point DFT, we say that the computations are done in place.

A second important observation is concerned with the order of the input data sequence after it is decimated (ν - 1) times. For example, if we consider the case where N = 8, we know that the first decimation yields the sequence $x(0), x(2), x(4), x(6), x(1), x(3), x(5), x(7)$ and the second decimation results in the sequence $x(0), x(4), x(2), x(6), x(1), x(5), x(3), x(7)$. The shuffling of the input data sequence has a well-defined order as can be ascertained from observing the following figure which illustrates the 8-point sequence. By expressing the index n, in the sequence $x(n)$, in binary form, we note that the order of the decimated data sequence is easily obtained by reading the binary representation of the index n in reverse order. Thus the data point $x(3) = x(011)$ is placed in position m = 110 or m = 6 in the decimated array. Thus we say that the data $x(n)$ after decimation is stored in bit-reversed order.

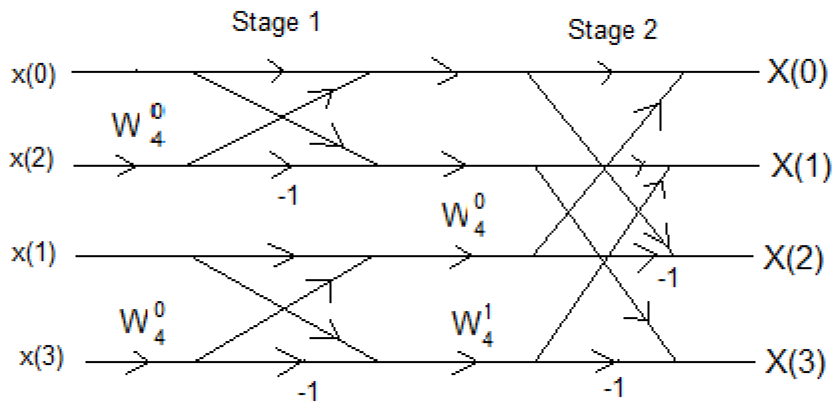


Shuffling of the data and bit reversal

For computing an 8-point DFT manually by applying the radix-2 FFT one can use the diagram of the Eight-point decimation-in-time Algorithm as a template with values for the phase factors as

$$W_8^0 = 1,\ W_8^1 = \frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}},\ W_8^2 = -j\ \&\ W_8^3 = -\frac{1}{\sqrt{2}} - j\frac{1}{\sqrt{2}}$$

For computing a 4-point DFT manually by applying the radix-2 FFT one can use the template given below.

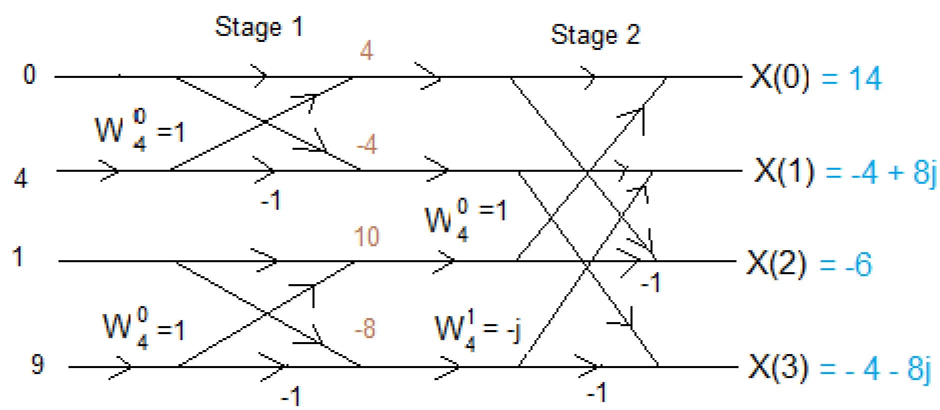


Four-point butterfly template

Here the values of the phase factors are given as $W_4^0 = 1$ & $W_4^1 = -j$

Example: Compute the DFT of $x(n)$ = (0 1 4 9) using radix-2 FFT Algorithm

Solution: The solution is presented in the following diagram by using the butterfly for a 4-point FFT.



In the above the output after the stage 1 are given in red and the output after the stage 2 are given in blue. It can be compared with the solution obtained earlier for the same signal using direct matrix multiplication.

Another important radix-2 FFT algorithm, called the decimation-in-frequency algorithm, is obtained by using the divide-and-conquer approach described in the previous section with the choice of $L = N/2$ and $M = 2$. This choice of parameters implies a column-wise storage in the input data sequence. The computational complexity here is exactly same as the decimation-in-time algorithm but the process and the diagrams looks reversed. The details of this process are omitted in this note.

Exercise: Find the DFT of the given finite duration signals using redix-2 FFT.

a) $x(n) = \left(\frac{1}{2}\right)^n,\ 0 \le n \le 3$

b) $x(n)=\left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right\}$

c) $x(n)=\{1, 2, 3, 4\}$

d) $x(n)=1,\ 0 \le n \le 7$

e) $x(n)=(-1)^n,\ 0 \le n \le 7$

f) $x(n)=\left\{\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 0, 0, 0, 0\right\}$

Appendix: On complex number and complex exponential

A complex number z is defined as $z = x + j\,y$ where x and y are real numbers and $j = \sqrt{(-1)}$. The quantity j is called as the imaginary quantity and the numbers x and y are called the real part and the imaginary part of z respectively.

For two complex numbers $z_1 = x_1 + j\,y_1$ and $z_2 = x_2 + j\,y_2$ the sum and product are defined as follows.

$$z_1 + z_2 = (x_1 + j\,y_1) + (x_2 + j\,y_2) = (x_1 + x_2) + j\,(y_1 + y_2)$$

The real part is added to the real part and the imaginary part is added to the imaginary part.

$$z_1 \times z_2 = (x_1 + j\,y_1) \times (x_2 + j\,y_2) = (x_1x_2 - y_1y_2) + j\,(x_1y_2 + x_2y_1)$$

The modulus of a complex number z is defined as $|z| = \sqrt{(x^2 + y^2)} = r$ and the argument of a complex number is defined as $\arg z = \tan^{-1}(y/x) = \theta$.

When a complex number $z = x + j\,y$ is represented by a point (x, y) on the Cartesian plane then the modulus is the distance of the point from the origin and the argument is the angle (in radian) the position vector of the point makes with the positive side of the x-axis. Using the modulus and argument the complex number can be expressed by its polar form as follows

$$z = x + j\,y = r(\cos\theta + j\sin\theta) = re^{j\theta}$$

The complex number $x - j\,y$ is called as the conjugate of z and is denoted by $\bar{z}$. This represents the point which is the mirror reflection of the point of z with respect to the x-axis. We have $z \times \bar{z} = |z|^2$.

The complex number $\cos\theta + j\sin\theta$ which is equal to $e^{j\theta}$ has modulus equal to 1 and argument equal to θ. All such numbers are on the unit circle. The unit circle is the circle with radius equal to 1 and with the centre at the origin.

When we find the nth roots of 1 we get n roots which are expressed as

$$1,\ e^{2\pi/n},\ e^{4\pi/n},\ \ldots\ldots.,\ e^{2\pi k/n},\ \ldots\ldots.,\ e^{2(n-1)\pi/n}$$

These n roots are placed on the unit circle with equal angular gap of $2\pi/n$ between them. In short we can express the nth root of 1 as

$$e^{2\pi k/n},\ k = 0,\ 1,\ ....,\ n-1.$$

The sum of these roots is zero and the product of these roots is 1. When n = 2 the roots are 1 and –1, when n = 3 the roots are 1, $\omega = -\frac{1}{2} + j\frac{\sqrt{3}}{2}$ and $\omega^2 = -\frac{1}{2} - j\frac{\sqrt{3}}{2}$. For n = 4 there roots are 1, j, –1 and $-j$.

For N^{th} roots we denote $e^{-j2\pi/N}$ by W_N and all the N roots are obtained as

$$W_N^k,\ k = 0,\ 1,\ ......,\ N-1$$

We also have the following formulas, which is used during the derivations of some of the expressions in this note.

$$\sum_{n=0}^{N-1} e^{-j2\pi kn/N} = \begin{cases} N, & k = 0, \pm N, \pm 2N, ... \\ 0, & Otherwise \end{cases}$$

$$\sum_{n=0}^{N-1} W_N^{kn} = \begin{cases} N, & k = 0, \pm N, \pm 2N, ... \\ 0, & Otherwise \end{cases}$$

References:

1. Digital Signal Processing Principles, Algorithms and Applications by John. G. Proakis and Dimitris G. Manolakis
2. The Fourier Transform and Its Applications by Ronald N. Bracewell

Disclaimer

This is a note prepared by the Faculty Members of Mathematics of the Department of Basic Science and Humanities of Silicon Institute of Technology, Bhubaneswar. This is to facilitate the teaching of the Module-6 of the course "Mathematics III for Computer Science" of 3rd semester B. Tech. for the branches of CSE, CST and CEN.

DISCLAIMER