



SWAMI DAYANANDA  
COLLEGE OF ARTS & SCIENCE,  
MANJAKKUDI-612610

---

**DEPARTMENT OF MATHEMATICS**

Mathematical Foundation for Computer

Science(P16CS11)

Study Material

Class : I-M.Sc Computer Science

Prepared by

**M.Gunanithi,**

Assistant Professor,

Department of Mathematics.

## **CORE COURSE I**

### **MATHEMATICAL FOUNDATION FOR COMPUTER SCIENCE**

#### **Objective :**

To learn the basis of the mathematical applications for developing the program.

#### **Unit I**

Propositions - evaluation - precedence rules -tautologies - reasoning using equivalence transformation - laws of equivalence - substitution rules - a natural deduction system. Deductive proofs - inference rules - proofs - sub proofs.

#### **Unit II**

Introduction - Cryptography – Ceaser Cyphor Coding - Matrix encoding – scrambled codes - Hamming metric - Hamming distance - Error detecting capability of an encoding.

#### **Unit III**

Assignment problem and its solution by Hungarian method. Project Scheduling by PERT -CPM: Phases of project scheduling - Arrow diagram - Critical path method – Probability and Cost Considerations in project scheduling - Crahing of Networks.

#### **Unit IV**

Testing of hypothesis : Tests based on normal population - Applications of chi-square, Student's-t, F-distributions - chi-square Test - goodness of fit - Test based on mean, means, variance, correlation and regression of coefficients.

#### **Unit V**

Graph - Directed and undirected graphs - Subgraphs - Chains, Circuits, Paths, Cycles -Connectivity - Relations to partial ordering - adjacency and incidence matrices – Minimal paths - Elements of transport network - Trees - Applications.

#### **Text Books**

1. "The Science of Programming", David Gries. Narosa Publishing House, New Delhi, 1993.
2. "Application Oriented Algebra", James L. Fisher, Dun Donnelly Publisher, 1977.
3. "Operation Research - An Introduction", Hamdy A.Taha, Macmillan Publishing Co., 4th Edn., 1987.
4. "Fundamentals of Mathematical Statistics", Gupta, S.C. and V.K.Kapoor, Sultan Chand & Sons, New Delhi, 8th Edn., 1983.
5. "Fundamentals of Applied Statistics", Gupta, S.C. and V.K.Kapoor, Sultan Chand & Sons, New Delhi, 2nd Edn., 1978.

#### **References**

1. "Discrete Mathematics", Seymour Lipschutz and Marc Laris Lipson, Second edition, Schuam's Outlines by Tata McGraw- Hill publishing Company Limited, New Delhi 1999.
2. "Operations Research", Kanti Swarup, P.K.Gupta and Man Mohan, Sultan Chand & Sons, New Delhi, 1994.
3. "Introductory Mathematical Statistics", Erwin Kryszig, John Wiley & Sons, New York, 1990.
4. "Probability and Statistics Engineering and Computer Science", Milton, J.S. and J.C.Arnold, McGraw Hill, New Delhi, 1986.

# Mathematical foundation for Computer

Science

## Unit - I

Propositions - evaluation - precedence rule -  
tautologies - Reasoning using equivalence transformation -  
laws of equivalence - Substitution rules - a natural  
deduction system. Deductive proofs - inference rules.  
proofs - sub proofs.

## Unit - II

Introduction - Cryptography - Caesar Cypher Coding -  
Matrix encoding - Scrambled codes - Hamming metric -  
Hamming distance - Error detecting Capability of an  
encoding.

## Unit - III

Assignment problem and its solution by Hungarian  
method. Project Scheduling by PERT - CPM: Phases of  
project scheduling - Arrow diagram - Critical path  
method - Probability and cost considerations in project  
scheduling - Cracking of networks.

## Unit - IV

Testing of hypothesis: Tests based on normal

population - Applications of Chi-Square, Student's-t,

F-distributions - Chi-Square Test - goodness of fit.

Test based on mean, means, Variance, Correlation  
and Regression of Co-efficient.

## Unit - V

Graph - Directed and undirected graphs -

Subgraphs - Chains, Circuits, Paths, Cycles - Connectivity

Relations to partial Ordering - adjacency and incidence

matrices - minimal paths - Elements of transport

networks - Trees - Applications.

Contingency  $\rightarrow \frac{F}{T}$

# Boolean Expressions

T	F
True	False
Truth	Falsity

Proposition:

Kind of boolean or logical expression

Propositions are similar to arithmetic expression.

These are operands, which represents the values

T & F (instead of integers) and operators (AND,

OR, instead of  $*$ ,  $+$ )

And parentheses are used to determining the order of evaluation.

Propositions are formed according to the following

Rules: As can be seen, parenthesis are required around each proposition that includes an operation

T & F are propositions

An identifier is a proposition (An identifier is a sequence of one or more digits and letters the first of which is a letter.)

If  $b$  is a proposition, then  $\neg b$  is  $(\neg b)$

If  $b$  and  $c$  are proposition then  $(b \wedge c)$ ,  $(b \vee c)$ ,  $(b \Rightarrow c)$  &  $(b = c)$

Examples:

$F$ ,  $(\neg T)$ ,  $(b \vee xyz)$ ,  $((\neg b) \wedge (c \Rightarrow d))$

$(c \wedge ab (F = id) \wedge (nd))$

the following are not proposition

$FF$ ,  $(b \vee c)$ ,  $(b) \wedge$ ,  $a + b$ ,  $(1abc = id)$

Five Operation:

$\neg b$	$\text{not } b$	negation
$(b \wedge c)$	$b \text{ and } c$	conjunction
$(b \vee c)$	$b \text{ or } c$	disjunction
$(b \Rightarrow c)$	$b \text{ implies } c$	implication
$(b = c)$	$b \text{ equals } c$	equality

Evaluation of constant propositions

Constant propositions - propositions that contain

only constants as operands and we do this in

3 cases based on the structure of a proposition:

Case (i):  $e$  with no operators

The value of proposition  $T$  is  $T$

The value of  $F$  is  $F$ .

Case (ii):  $e$  with one operators

$(\sim b)$ ,  $(b \wedge c)$ ,  $(b \vee c)$ ,  $(b \Rightarrow c)$ ;  $(b = c)$  where

$b$  and  $c$  are each one of the constants  $T$  and  $F$

Ex: Let  $f$  be the function

$b$	$c$	$b \wedge c$	$b \vee c$	$b \Rightarrow c$	$b = c$	$\sim b$
$T$	$T$	$T$	$T$	$T$	$T$	$F$
$T$	$F$	$F$	$T$	$F$	$F$	$F$
$F$	$T$	$F$	$T$	$T$	$F$	$T$
$F$	$F$	$F$	$F$	$T$	$T$	$T$

Case (iii)

$e$  with more than one operators

It is evaluated repeatedly by applying the single evaluation to a sub proposition and replacing the subproposition by its value, until the proposition is reduced to  $T$  or  $F$ .

Ex:

$$(\sim (T \wedge T)) \Rightarrow (F)$$

$$(\sim (T \Rightarrow F)) = F$$

Evaluation  $(b \Rightarrow c) = (\sim b \vee c)$

$b$	$c$	$\sim b$	$b \Rightarrow c$	$(\sim b \vee c)$	$(b \Rightarrow c) = (\sim b \vee c)$
$T$	$T$	$F$	$T$	$T$	$T$
$T$	$F$	$F$	$F$	$F$	$F$
$F$	$T$	$T$	$T$	$T$	$T$
$F$	$F$	$T$	$T$	$T$	$T$

State:

A state  $s$  is a function from a set of identifiers to the set of values  $T$  and  $F$ .

Ex: Let state  $s$  be the function defined by a

Set  $s = \{(a, T), (bc, F), (ye, T)\}$  then

$s(a) = T$	$s(bc) = F$	$s(ye) = T$
$s(a) = T$	$s(bc) = F$	$s(ye) = T$
$s(a) = T$	$s(bc) = F$	$s(ye) = T$
$s(a) = T$	$s(bc) = F$	$s(ye) = T$

Proposition  $e$  is well defined in state  $s$  if each identifier in  $e$  is associated with  $T$  or  $F$  in a state  $s$ .

Let proposition  $e$  is well defined in a state  $s$  then  $s(e)$  is the value obtained by replacing all occurrences of identifiers  $b$  in  $e$  by their values  $s(b)$  and evaluating the resulting constant proposition according to the rules.

$s((\neg b) \vee c)$  is evaluated in state  $s$

$= \{ (b, T), (c, F) \}$

$s((\neg b) \vee c) = ((\neg T) \vee F) = (F \vee F) = F$

# Precedence rules for Operators!

Sequence of the Same operators are evaluate from the left to right.

Ex:  $b \wedge c \wedge d$  is equivalent to  $((b \wedge c) \wedge d)$

The order of evaluation of different, adjacent operators is given by the list NOT, AND, OR,

Ex:  $\neg b = b \wedge c$  is equivalent to  $(\neg) = (b \wedge c)$

$b \vee \neg c = d$  is equivalent to  $(b \vee (\neg c)) = d$

$b \Rightarrow c = d \wedge e$  is equivalent to  $(b \Rightarrow c) = (d \wedge e)$

## Tautology!

A Tautology is a proposition that is true in every state in which it is well defined.

for EX!

proposition T is a Tautology

proposition F is not

b	$\neg b$	$b \vee \neg b$
T	F	T
F	T	T

for a proposition with n distinct identifiers there are  $2^n$  case.

prove that  $(b \wedge c) \wedge d \Rightarrow (d \Rightarrow b)$  is a tautology

b	c	d	$(b \wedge c)$	$((b \wedge c) \wedge d)$	$d \Rightarrow b$	$((b \wedge c) \wedge d) \Rightarrow (d \Rightarrow b)$
T	T	T	T	T	T	T
T	T	F	T	F	T	T
T	F	T	F	F	T	T
T	F	F	F	F	T	T
F	T	T	F	F	F	T
F	T	F	F	F	T	T
F	F	T	F	F	F	T
F	F	F	F	F	T	T

Disproving a Conjecture:

To prove a Conjecture, it is necessary to prove it is true in all cases.

To disprove a Conjecture, it is sufficient to find a single cases, where it is false.

Sometimes we conjecture that a proposition is a tautology, but are unable to develop a proof of it, so we decide to try to disprove it.

It is possible to prove the converse

(ie)  $r \wedge c$  is a tautology.

for a proposition with a distinct variables there are 8 cases

## Proposition:

It represents or describes the set of states in which it is true. Conversely, for any set of states containing only identifiers associated with T or F.

We can define a proposition that represent that state set. Thus, the empty set, the set containing no states, is represented by F because F is true in no state.

The set of all state is represented by proposition T because T is true in all state.

Ex: the set of two states  $\{(b, T), (c, T), (d, T)\}$

$\neq \{(b, F), (c, T), (d, T)\}$  is represented by the proposition  $\{b \wedge (c \vee d) \vee (\neg b \wedge (c \vee d))\}$

proposition b is weaker than c if  $c \Rightarrow b$ .

Correspondence c is said to be strong than b

A stronger proposition makes up more req on the combinations of value its identifiers can be associated with & or  $\vee$  weaker proposition makes fewer.

$c \Rightarrow b$  less restrictive.

the weakest proposition is T (or any tautology) because it represents the set of all states. the strongest is F, because it represents the set of no states.

### Transforming English to propositional form

It rains

$x$

picnic is cancelled

$pc$

Stay at home

$s$

If it rains but I stay at home, I won't

be wet

$$(x \wedge \neg s) \Rightarrow \neg wet$$

I will be wet if it rains  $x \Rightarrow wet$

If it rains and the picnic is not cancelled.

I don't stay home, I will be wet

$$(x \wedge \neg pc) \vee \neg s \Rightarrow wet$$

$$(x \wedge \neg pc \vee \neg s) \Rightarrow wet$$

whether or not the picnic is cancelled, I am staying at home it is rains.

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

this reduces  $r \rightarrow s$

(either) it does not rain or I am staying home

### Equivalent in proposition:

propositions  $E_1$  &  $E_2$  are equivalent.

if  $E_1 = E_2$  is a tautology. In this case

$E_1 = E_2$  is an equivalent.

Thus  $\therefore$  an equivalence is an equality that is a tautology.

Below, we give a list of equivalence these are the basic equivalence from which all others will be derived. So we call them the laws of equivalence.

Actually they are schemas.

### Commutative Laws.

$$(E_1 \wedge E_2) = (E_2 \wedge E_1)$$

$$(E_1 \vee E_2) = (E_2 \vee E_1)$$

$$(E_1 = E_2) = (E_2 = E_1)$$

2) Associative Laws:

$$E_1 \wedge (E_2 \wedge E_3) = (E_1 \wedge E_2) \wedge E_3$$

$$E_1 \vee (E_2 \vee E_3) = (E_1 \vee E_2) \vee E_3$$

3) Distributive Laws:

$$E_1 \vee (E_2 \wedge E_3) = (E_1 \vee E_2) \wedge (E_1 \vee E_3)$$

$$E_1 \wedge (E_2 \vee E_3) = (E_1 \wedge E_2) \vee (E_1 \wedge E_3)$$

4) De - Morgan's Laws

$$\neg (E_1 \wedge E_2) = (\neg E_1) \vee (\neg E_2)$$

$$\neg (E_1 \vee E_2) = (\neg E_1) \wedge (\neg E_2)$$

5) Laws of Negation:

$$\neg (\neg E_1) = E_1$$

6) Law of the Excluded middle:

$$E_1 \vee \neg E_1 = T$$

7) Law of Contradiction

$$E_1 \wedge \neg E_1 = F$$

8) Law of Implication

$$E_1 \Rightarrow E_2 = \neg E_1 \vee E_2$$

9) Law of equality

$$(E_1 = E_2) = (E_1 \Rightarrow E_2) \wedge (E_2 \Rightarrow E_1)$$

10) Laws of simplification

$$E_1 \vee E_1 = E_1$$

$$E_1 \vee T = T$$

$$E_1 \vee F = E_1$$

$$E_1 \vee (E_1 \wedge E_2) = E_1$$

11) Laws of And simplification

$$E_1 \wedge E_1 = E_1$$

$$E_1 \wedge T = E_1$$

$$E_1 \wedge F = F$$

$$E_1 \wedge (E_1 \vee E_2) = E_1$$

12) Laws of identities

$$E_1 = E_1$$

Proving that the logical laws are equivalences:

We have stated, without proof that laws, 1-12 are equivalences. One way to prove this is to build truth tables. Note that the laws are true in all states.

For Ex:

the truth law of De Morgan's law

$$\sim (E_1 \wedge E_2) = \sim E_1 \vee \sim E_2$$

$E_1$	$E_2$	$\sim E_1$	$\sim E_2$	$\sim (E_1 \wedge E_2)$	$\sim E_1 \vee \sim E_2$
T	T	F	F	F	F
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

Clearly, the laws is true in all state, so that is a tautology.

The rules of subtraction & transitivity.

$$a + (c - a) = c$$

$$(a + (c - a)) * d = c * d$$

Rule of Substitution:

Let  $e_1 = e_2$  be an equivalence &  $E(p)$  be a proposition, written as a function of one of its identifiers  $p$ .

Then  $E(e_1) = E(e_2)$  &  $E(e_2) = E(e_1)$  are also equivalence.

Ex:  $(b \Rightarrow c) = (\neg b \vee c)$  is an equivalence

$$E(p) = \neg b \vee c$$

$$E(e_1) = \neg b \vee c$$

$$E(e_2) = \neg b \vee c$$

So that  $\neg b \vee c = \neg b \vee c$  is an equivalence.

Rule of Transitivity:

If  $e_1 = e_2$ ,  $e_2 = e_3$  are equivalences

then, so is  $e_1 = e_3$  (hence  $e_1$  is equivalent to  $e_3$ ).

Ex 1

$(b \Rightarrow c) = (\neg c \Rightarrow \neg b)$  is an equivalence.

b -

$$= \neg b \vee c \text{ (Simplification)}$$

$$= c \vee \neg b \text{ (Commutativity)}$$

$$= \neg(\neg c) \vee \neg b \text{ (Negation)}$$

$$= \neg c \Rightarrow \neg b \text{ (Implication)}$$

$$(b \wedge (b \Rightarrow c) \Rightarrow c)$$

$$= (b \wedge (\neg b \vee c)) \Rightarrow c \text{ (Simplification)}$$

$$= \neg(b \wedge (\neg b \vee c)) \vee c \text{ (Implication)}$$

$$= \neg b \vee \neg(\neg b \vee c) \vee c \text{ (DeMorgan)}$$

$= \top$

### Transforming an Implication:

Suppose we want to prove that,

$E_1 \wedge E_2 \wedge E_3 \Rightarrow E$  is an equivalence. This proposition is transformed as follows ( $E$  denotes  $*$ )

$$(E_1 \wedge E_2 \wedge E_3) \Rightarrow E$$

$$= \neg(E_1 \wedge E_2 \wedge E_3) \vee E \text{ (Implication)}$$

$$= \neg E_1 \vee \neg E_2 \vee \neg E_3 \vee E \text{ (DeMorgan)}$$

The final proposition is true in any state in which atleast one of  $\neg E_1, \neg E_2, \neg E_3, E$  is true

Hence to prove \* is a tautology, we need only prove that in any state in which three of them are false, the fourth is true.

And we can choose which three to assume false based on other form.

$$E_1 \wedge E_2 \wedge E_3 \Rightarrow E$$

$$E_1 \wedge E_2 \wedge \sim E \Rightarrow \sim E_3$$

$$E_1 \wedge \sim E_2 \wedge E_3 \Rightarrow \sim E_1$$

$$\sim E_1 \wedge E_2 \wedge E_3 \Rightarrow \sim E_1$$

$$\sim E_1 \vee \sim E_2 \vee \sim E_3 \vee E$$

prove that  $(\sim(b \Rightarrow c) \wedge \sim(\sim b \Rightarrow (c \wedge d))) \Rightarrow (\sim c \Rightarrow d)$  is a tautology.

$$(\sim(b \Rightarrow c) \wedge \sim(\sim b \Rightarrow (c \wedge d))) \Rightarrow$$

$$(\sim c \Rightarrow d)$$

Eliminate the main implication & use De Morgan law,

law,

$$(\sim \sim(b \Rightarrow c) \vee \sim \sim(\sim b \Rightarrow (c \wedge d))) \Rightarrow (\sim c \Rightarrow d)$$

$$(\sim \sim(b \Rightarrow c) \vee \sim \sim(\sim b \Rightarrow (c \wedge d))) \vee (\sim c \Rightarrow d)$$

$$= (b \Rightarrow c) \vee (\sim b \Rightarrow (c \wedge d)) \vee (\sim c \Rightarrow d)$$

$$= (\sim b \vee c) \vee (b \vee c \vee d) \vee (c \vee d)$$

use the laws of Associativity, Commutativity, and  $\alpha$ -Simplification to arrive at

$$b \vee b \vee c \vee d$$

which is true because of excluded middle  $b \vee \neg b = T$  &  $\alpha$ -Simplification T.

A formal System of Axioms & <sup>inference</sup> ~~Inference~~ rules.

Define the propositions that arise direct from laws 1-12 to be theorems.

These are called axioms (and the laws 1-12 are axiom schemas)

Axioms:

Any proposition that arises, by substituting propositions for  $E_1, E_2$  &  $E_3$  in one of the laws 1-12 is called theorem.

Inference rule:

Define the propositions that arise by using the rules of substitution & transitivity and an already derived theorem to be a theorem.

In this context, the rules are often called inference rules, for they can be used to infer that proposition is a theorem.

The inference rule is often written in the form

$$\frac{E_1 \dots E_n}{E} \text{ and } \frac{E_1, E_2 \dots E_n}{E, E_0}$$

where the  $E_i$  &  $E$

stands for arbitrary propositions

The inference rule has the following meaning.

If propositions  $E_1, E_2 \dots E_n$  are theorems, then is proposition  $E$ . (Or  $E_0$  in the second case)

written in this form, the rules of substitution & transitivity are

$$\text{Rule of substitution} = \frac{e_1 = e_2}{E(e_1) = E(e_2), E(e_2) = E(e_1)}$$

$$\text{Rule of transitivity} = \frac{e_1 = e_2, e_2 = e_3}{e_1 = e_3}$$

A theorem of the formal system, then is either an axiom or a proposition that is derived from one of the inference rules (2.3.2) & (2.3.3)

Natural Deduction System:

Introduction to deductive proofs.

Considers the problem of proving that a conclusion follows from certain premises.

For, example, we might want to prove that  $P \wedge (x \vee q)$  follows from  $P \wedge q$

(i.e)  $P \wedge (x \vee q)$  is true in every state in which  $P \wedge q$  is true. This problem can be written as follows

Premise :  $P \wedge q$

Conclusion:  $P \wedge (x \vee q)$

Since  $P \wedge q$  is true (in state  $s$ ). So is  $P$  and so is  $q$ . One property of  $\vee$  is that, for any  $x$ ,  $x \vee q$  is true if  $q$  is, so  $x \vee q$  is true. finally since  $P \wedge x \vee q$  are both true.

The properties of  $\wedge$  and  $\vee$  allows us to conclude that  $P \wedge (x \vee q)$  is true in  $s$  also

From	$P \wedge q$	Infer, $P \wedge (x \vee q)$
1	$P \wedge q$	premise
2	$P$	property of $\wedge$ , 1
3	$q$	property of $\wedge$ , 1
4	$x \vee q$	property of $\vee$ , 3
5	$P \wedge (x \vee q)$	property of $\wedge$ , 2, 4.

I - A formula is true in a state  $s$  if and only if...

II - A formula is true in a state  $s$  if and only if...

Show that  $\sim (p \wedge q) \wedge (\sim q \vee x) \wedge \sim x \Rightarrow \sim p$

From	$\sim (p \wedge q) \wedge (\sim q \vee x) \wedge \sim x \Rightarrow \sim p$
1	$\sim (p \wedge q) \wedge (\sim q \vee x) \wedge \sim x$ premise
2	$\sim (p \wedge q)$ property of And, 1
3	$\sim q \vee x$ property of And, 1
4	$\sim x \vee$ property of and, 1
5	$\sim p \vee q$ property by demorgans law
6	$q \Rightarrow x$ Implication law, 3
7	$p \Rightarrow q$ Implication law, 5
8	$p \Rightarrow x$ Rule of transitivity 6, 7
9	$\sim x \Rightarrow \sim p$ Negation law, 8
10	$\sim p$ from 4

Inference rules:

not - 2

and - 2

or - 2

imp - 2

equals - 2

10 inference rules in the natural deduction system.

The rule for introducing and is called  $\wedge - I$

The rule for eliminating and is called  $\wedge - E$

# Inference Rules:

$\wedge$ -I,  $\wedge$ -E and  $\vee$ -I

$$\wedge$$
-I : 
$$\frac{E_1, E_2, \dots, E_n}{E_1 \wedge E_2 \wedge \dots \wedge E_n}$$

$$\wedge$$
-E : 
$$\frac{E_1 \wedge E_2 \wedge E_3 \dots \wedge E_n}{E_i}$$

$$\vee$$
-I : 
$$\frac{E_i}{E_i \vee \dots \vee E_n}$$

for example, since  $p \vee q$  and  $\neg x$  are propositions, the following is an instance of  $\wedge$ -I

$$\wedge$$
-I : 
$$\frac{E_1, E_2}{E_1 \wedge E_2}$$

$$\frac{p \vee q, \neg x}{(p \vee q) \wedge (\neg x)}$$

From	$p \vee q$	infer $p \wedge (\neg x \vee q)$
1	$p \vee q$	$\neg x$
2	$p$	$\wedge$ -E, 1
3	$q$	$\wedge$ -E, 1
4	$\neg x \vee q$	$\vee$ -I, 3
5	$p \wedge (\neg x \vee q)$	$\wedge$ -I, 2, 4

## Inference rule

$\vee$ -E

$$\vee$$
-E : 
$$E_1 \vee \dots \vee E_n, E_1 \Rightarrow E, \dots, E_n \Rightarrow E \Rightarrow E$$

$E$

From  $\forall v (q \wedge r)$ ;  $p \Rightarrow s$ ,  $(q \wedge r) \Rightarrow s$  infer  $\forall v p$

- 1  $\forall v (q \wedge r)$   $\forall x 1$
- 2  $p \Rightarrow s$   $\forall x 2$
- 3  $(q \wedge r) \Rightarrow s$   $\forall x 3$
- 4  $s$   $\forall - E, 1, 2, 3$
- 5  $\forall v p$   $\forall - I, 4$

Inference rule  $\Rightarrow - E$

$$\frac{\begin{array}{l} \Rightarrow - E \\ E_1 \Rightarrow E a, E_1 \\ E a \end{array}}{\Rightarrow - E}$$

From  $\forall v p, p \Rightarrow r$  infer  $\forall v (q \Rightarrow r)$

- 1  $\forall v p$   $\forall x 1$
- 2  $p \Rightarrow r$   $\forall x 2$
- 3  $p$   $\forall - E, 1$
- 4  $r$   $\Rightarrow E, 2, 3$
- 5  $\forall v (q \Rightarrow r)$   $\forall - I, 4$

Inference rule:

$$\frac{\begin{array}{l} = - I, = - E \\ = - I : E_1 \Rightarrow E a, E a \Rightarrow E_1 \\ E_1 = E a \end{array}}{= - I, = - E}$$

$$\frac{\begin{array}{l} = - I : E_1 \Rightarrow E a, E a \Rightarrow E_1 \\ E_1 \Rightarrow E a, E a \Rightarrow E_1 \end{array}}{= - I, = - E}$$

From	$p, p = (q \Rightarrow x)$	$x \Rightarrow q$	infer	$x = q$
1	$p$		$Px1$	
2	$p = (q \Rightarrow x)$		$Px2$	
3	$x \Rightarrow q$		$Px3$	
4	$p \Rightarrow (q \Rightarrow x)$		$= -E, Px2$	
5	$q \Rightarrow x$		$\Rightarrow -E, Px1$	
6	$x = q$		$= -I, Px3, 5$	

### Proofs and Subproofs:

proofs:

A theorem of the form

"From  $e_1, \dots, e_n$  infer  $e$ " is interpreted as

if  $e_1, e_2, \dots, e_n$  are true in a state then so is  $e$

If  $e_1, e_2, \dots, e_n$  appear on lines of a proof which is interpreted to mean that they are assumed or proven true, then we should be able to write  $e$  on a line also.

Rule  $\Rightarrow -I$  gives us permission to do so

$$\Rightarrow -I \frac{\text{From } E_1, \dots, E_n \text{ infer } E}{(E_1 \wedge E_2 \wedge \dots \wedge E_n) \Rightarrow E}$$

$$(E_1 \wedge E_2 \wedge \dots \wedge E_n) \Rightarrow E$$

Infer  $(p \supset q) = (q \supset p)$

- 1  $(p \supset q) \supset (q \supset p)$   $\Rightarrow$  -I
- 2  $(q \supset p) \supset (p \supset q)$   $\Rightarrow$  -I, 1
- 3  $(p \supset q) = (q \supset p)$   $=$  -I, 1, 2

Rule  $\Rightarrow$  -I allows us to conclude  $p \supset q$  if we have a proof of  $q$  given premise  $p$  on the other hand, if we take  $p \supset q$  as a premise, then rule  $\Rightarrow$  -E allows us to conclude that  $q$  holds when  $p$  is given

### Deduction Theorem:

"Infer  $p \supset q$ ", is a theorem of the natural deduction system, which can be interpreted to mean that  $p \supset q$  is a tautology, iff "from  $p$  infer  $q$ " is a theorem.

### Subproofs:

Infer  $(p \supset q) = (q \supset p)$

1	From	$(p \supset q) \supset (q \supset p)$
	1.1	$p$ <span style="margin-left: 100px;">A-E, PK1</span>
	1.2	$q$ <span style="margin-left: 100px;">A-E, PK1</span>
	1.3	$q \supset p$ <span style="margin-left: 100px;">A-I, 1.1, 1.2</span>

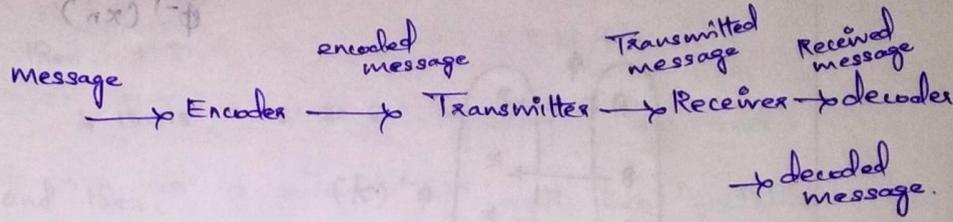
2  $(p \supset q) \supset (q \supset p)$   $\Rightarrow$  -I, 1

3  $(q, p) \Rightarrow (p, q) \Rightarrow \mathbb{I}$

4  $(p, q) = (q, p) = -\mathbb{I}, a, 3.$

Unit - II

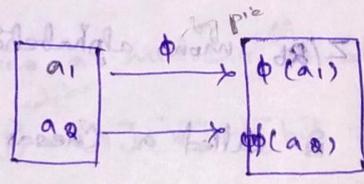
Cryptography:



the study of encoding & decoding to ensure secrecy is called cryptography.

Definition:

An encoding  $\phi$  of a set  $A$  (called the base set) into set  $X$  is a one-to-one function  $\phi$  from  $A$  into  $X$ .



Caesar Cypher Coding:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
R	S	T	U	V	W	X	Y	Z								
↓	↓	↓	↓	↓	↓	↓	↓	↓								
U	V	W	X	Y	Z	A	B	C								

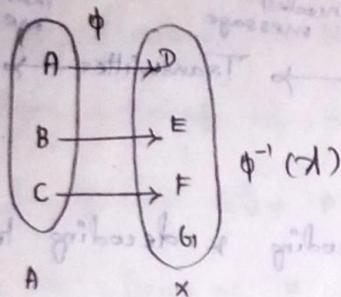
the encoding  $\phi$  is extended to the set of all sequences  $a_1, a_2, \dots, a_n$  where  $a_i$  is contained in  $A$ , by

$$a_1, a_2, \dots, a_n \rightarrow \phi(a_1), \phi(a_2), \dots, \phi(a_n)$$

the encoding of  $\phi$  is defined to be the function  $\phi^{-1}$  from  $\phi(x)$  to  $x$ .

Decoding of sequences  $x_1, x_2, \dots, x_n$  where  $x_i$  is in

$\phi(x) = x$  by  $x_1, x_2, \dots, x_n \rightarrow \phi^{-1}(x_1), \phi^{-1}(x_2), \dots, \phi^{-1}(x_n)$



letter of the english alphabet,  $n$  tuples of letters of

the english alphabet with  $n$  a small positive  $Z/(K)$

with  $k = 26, 27, 28, \dots$

$Z/26$  mono alphabetic

this encoding is called a Caesar cypher and  $\phi$

(letter) is the letter three letters after a given letter

the Caesar encoding has a very simple mathematical

explanation. If we associate with each letter of the alphabet one of integers from 0 to 25 take modulo 26

$\phi([x]) = [x] + [3]$  where the addition takes place in  $Z/26$

A	B	C	D	E	F	G	H	I	J	K	L
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]

M N O P Q R S T U V W X Y Z  
 [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26]

then the encoding the message

ALL ARE GOOD

can proceed as

1 12 12 1 18 5 7 15 15 14 1 M I

then, + 3

4 15 15 4 21 8 10 18 18 7

and then

DOO DUH JRRG

A mathematical formulation however indicates an easy generalization of the above example, which is more difficult to decode.

If above integers with  $\gcd\{a, 26\} = 1$

then define a modular encoding

$$\phi([x]) = [a][x] + [b]$$

the caesar cypher is defined to be a modular encoding with  $a=1$ .

the  $\gcd\{a, 26\}$  must equal 1, otherwise the modular encoding will not be one-one.

In fact  $\phi(0) = [b]$  and  $\phi(26 / \gcd\{a, 26\}) = [b]$

thus, if the letter corresponding to  $[b]$  were received it would be ambiguous as to whether this should be decoded as to letter corresponding to  $[0]$  or  $[26 / \gcd\{a, 26\}]$

However if  $\gcd(a, 26) \neq 1$ , then  $a^{-1}$  exists and  
 there is decoding  $\phi^{-1}(y) = [a^{-1}]y - [a]^{-1}[b]$

the element  $[a]^{-1}$  can be determined by the

Euclidean Algorithm

MILITARY  
 XTWTELCJ is decoded as

Hence we suppose that XTWTELCJ is decoded as 'military' and then the encoding is an example of a Caesar Cypher in which the displacement is 11 letters.

$\phi^{-1}(y) = [y] + [15]$ , and the remainder of the message can be decoded.

Matrix encoding:

Mono alphabetic encoding is only one possibility among numerous methods of encoding. This section deals with a type of block encoding called matrix encoding

the alphabetic is again represented by the integers modulo 26.

the base set of this encoding is the vector

Space of  $m$  tuples with elements in the integers modulo 26.

(ie) A can be thought of as blocks of  $m$  letters

let  $m$  be an invertible  $m \times m$  matrix with entries in  $\mathbb{Z}/26$ .

The encoding thus takes a block of  $m$  letters, realizes this as a vector in  $[Z/26]^m$ , multiplies this vector by  $M$ , and then produces the corresponding blocks of letters.

For example, if we encode block of two letters by multiplication by the matrix

$$M = \begin{bmatrix} 1 & 15 \\ 13 & 12 \end{bmatrix}$$

then "to" becomes

$$\begin{bmatrix} 20 & 15 \end{bmatrix} \times \begin{bmatrix} 1 & 15 \\ 13 & 12 \end{bmatrix} = \begin{bmatrix} 20 \times 1 + 15 \times 13 & 20 \times 1 + 15 \times 12 \end{bmatrix} = \begin{bmatrix} 205 & 205 \end{bmatrix} = \begin{bmatrix} 7 & 18 \end{bmatrix} \text{ or "GR"}$$

the word "do" becomes

$$\begin{bmatrix} 4 & 15 \end{bmatrix} \begin{bmatrix} 1 & 15 \\ 13 & 12 \end{bmatrix} = \begin{bmatrix} 17 & 12 \end{bmatrix}$$

$$M^{-1} = \left( \begin{bmatrix} 1 & 15 \\ 13 & 12 \end{bmatrix} \right)^{-1}$$

$$\frac{1}{|M|} \text{adj } M$$

$$|M| = 12 - 13 = -1$$

$$\text{adj } M = \begin{bmatrix} 12 & -1 \\ -13 & 1 \end{bmatrix}$$

$$M^{-1} = \frac{1}{(-1)} \begin{bmatrix} 12 & -1 \\ -13 & 1 \end{bmatrix} = \begin{bmatrix} -12 & 1 \\ 13 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 14 & 1 \\ 13 & 25 \end{bmatrix}$$

$M^{-1} (GJR)$

$$\begin{bmatrix} 7 & 18 \\ 13 & 25 \end{bmatrix} \begin{bmatrix} 14 & 1 \\ 13 & 25 \end{bmatrix} = \begin{bmatrix} 20 & 15 \\ 16 & 1 \end{bmatrix}$$

This encoding is clearly not monoalphabetic, since in the first case the letter O was replaced by 'R' in the same second case O was replaced by 'B'.

If the matrix  $M^{-1}$  is calculated, then the decoding is simply multiplication by  $M^{-1}$ .

$$(VM)M^{-1} = V \text{ for each vector}$$

multiplication by  $M^{-1}$  transforms GJR back to "to" and OB back to "do".

LMR SX CCHDV SHBUS "NBGTU RDRDY  
 WLUR [M] KYK YHWSA KYURG SPRYV  
 WQPT UYM  
 OXTRM FURYK AGDVS [H] BUPH OBKYH  
 WBAKY SBUUS FRVQT MEOTV M

The first message contains 58 characters, hence the block length is 2, 29, 58.

The second message contains 46 characters, hence the block length is 2, 23, 46.

Hence, the code is a matrix encoding then

the block size is  $\begin{bmatrix} 2 & 1 & 46 \\ & 23 & 81 \end{bmatrix}$

Indo China

In the first message the sequence KYHWSAKY occurs and furthermore, this sequence occurs in the second message.

$$\text{Hence Assume } \phi^{-1}(KY) = IN \quad \phi^{-1}(HW) = DO$$

this we have

$$\begin{bmatrix} 11 & 25 \\ 8 & 23 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} 9 & 14 \\ 4 & 15 \end{bmatrix}$$

$$\begin{bmatrix} 11 & 25 \\ 8 & 23 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} 9 & 14 \\ 4 & 15 \end{bmatrix}$$

where  $\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}^{\phi^{-1}}$  is the inverse of the encoding

matrix. This yields the equations in  $\mathbb{Z}_{26}$ .

$$11x_1 + 25x_2 = 9, \quad 11x_2 + 25x_4 = 14$$

$$8x_1 + 23x_3 = 4, \quad 8x_2 + 23x_4 = 15$$

which have the unique solutions

$$x_1 = 3, \quad x_2 = 25, \quad x_3 = 24, \quad x_4 = 1$$

To see if the code is actually a matrix encoding and

$$\text{the matrix } \begin{bmatrix} 3 & 25 \\ 24 & 1 \end{bmatrix}$$

$$\phi^{-1}(IM) = \phi^{-1}([12, 13]) = [12, 13] \begin{bmatrix} 3 & 25 \\ 24 & 1 \end{bmatrix}$$

$$= [10, 1] = JA$$

$$\phi^{-1}(RS) = \phi^{-1}([18, 19]) = [18, 19] \begin{bmatrix} 3 & 25 \\ 24 & 1 \end{bmatrix}$$

$$= [16, 1] = PA$$

$$\phi^{-1}(XC) = \phi^{-1} \begin{bmatrix} 24 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 & 25 \\ 24 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 3 \\ 25 \end{bmatrix} = \begin{bmatrix} 14 \\ 15 \end{bmatrix} = NE$$

$$\phi^{-1}(CH) = \phi^{-1} \begin{bmatrix} 3 \\ 8 \end{bmatrix} = \begin{bmatrix} 3 & 25 \\ 24 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 3 \\ 8 \end{bmatrix} = \begin{bmatrix} 19 \\ 5 \end{bmatrix} = SE$$

So that  $\phi^{-1}(IMRS \times CCH) = \text{"Japanese"}$ .

Decoding the remainders of the encoded text gives the following messages:

Japanese troops currently stationed in Indochina will be withdrawn.

Withdrawal of troops from Indochina is a smokescreen.

Decrypting an encoded message encoded by matrix multiplication or vector of large block size is extremely difficult for block size 2 or 3 or 4 or 5 or 6 or 7 or 8 or 9 or 10 or 11 or 12 or 13 or 14 or 15 or 16 or 17 or 18 or 19 or 20 or 21 or 22 or 23 or 24 or 25 or 26 or 27 or 28 or 29 or 30 or 31 or 32 or 33 or 34 or 35 or 36 or 37 or 38 or 39 or 40 or 41 or 42 or 43 or 44 or 45 or 46 or 47 or 48 or 49 or 50 or 51 or 52 or 53 or 54 or 55 or 56 or 57 or 58 or 59 or 60 or 61 or 62 or 63 or 64 or 65 or 66 or 67 or 68 or 69 or 70 or 71 or 72 or 73 or 74 or 75 or 76 or 77 or 78 or 79 or 80 or 81 or 82 or 83 or 84 or 85 or 86 or 87 or 88 or 89 or 90 or 91 or 92 or 93 or 94 or 95 or 96 or 97 or 98 or 99 or 100 or 101 or 102 or 103 or 104 or 105 or 106 or 107 or 108 or 109 or 110 or 111 or 112 or 113 or 114 or 115 or 116 or 117 or 118 or 119 or 120 or 121 or 122 or 123 or 124 or 125 or 126 or 127 or 128 or 129 or 130 or 131 or 132 or 133 or 134 or 135 or 136 or 137 or 138 or 139 or 140 or 141 or 142 or 143 or 144 or 145 or 146 or 147 or 148 or 149 or 150 or 151 or 152 or 153 or 154 or 155 or 156 or 157 or 158 or 159 or 160 or 161 or 162 or 163 or 164 or 165 or 166 or 167 or 168 or 169 or 170 or 171 or 172 or 173 or 174 or 175 or 176 or 177 or 178 or 179 or 180 or 181 or 182 or 183 or 184 or 185 or 186 or 187 or 188 or 189 or 190 or 191 or 192 or 193 or 194 or 195 or 196 or 197 or 198 or 199 or 200 or 201 or 202 or 203 or 204 or 205 or 206 or 207 or 208 or 209 or 210 or 211 or 212 or 213 or 214 or 215 or 216 or 217 or 218 or 219 or 220 or 221 or 222 or 223 or 224 or 225 or 226 or 227 or 228 or 229 or 230 or 231 or 232 or 233 or 234 or 235 or 236 or 237 or 238 or 239 or 240 or 241 or 242 or 243 or 244 or 245 or 246 or 247 or 248 or 249 or 250 or 251 or 252 or 253 or 254 or 255 or 256 or 257 or 258 or 259 or 260 or 261 or 262 or 263 or 264 or 265 or 266 or 267 or 268 or 269 or 270 or 271 or 272 or 273 or 274 or 275 or 276 or 277 or 278 or 279 or 280 or 281 or 282 or 283 or 284 or 285 or 286 or 287 or 288 or 289 or 290 or 291 or 292 or 293 or 294 or 295 or 296 or 297 or 298 or 299 or 300 or 301 or 302 or 303 or 304 or 305 or 306 or 307 or 308 or 309 or 310 or 311 or 312 or 313 or 314 or 315 or 316 or 317 or 318 or 319 or 320 or 321 or 322 or 323 or 324 or 325 or 326 or 327 or 328 or 329 or 330 or 331 or 332 or 333 or 334 or 335 or 336 or 337 or 338 or 339 or 340 or 341 or 342 or 343 or 344 or 345 or 346 or 347 or 348 or 349 or 350 or 351 or 352 or 353 or 354 or 355 or 356 or 357 or 358 or 359 or 360 or 361 or 362 or 363 or 364 or 365 or 366 or 367 or 368 or 369 or 370 or 371 or 372 or 373 or 374 or 375 or 376 or 377 or 378 or 379 or 380 or 381 or 382 or 383 or 384 or 385 or 386 or 387 or 388 or 389 or 390 or 391 or 392 or 393 or 394 or 395 or 396 or 397 or 398 or 399 or 400 or 401 or 402 or 403 or 404 or 405 or 406 or 407 or 408 or 409 or 410 or 411 or 412 or 413 or 414 or 415 or 416 or 417 or 418 or 419 or 420 or 421 or 422 or 423 or 424 or 425 or 426 or 427 or 428 or 429 or 430 or 431 or 432 or 433 or 434 or 435 or 436 or 437 or 438 or 439 or 440 or 441 or 442 or 443 or 444 or 445 or 446 or 447 or 448 or 449 or 450 or 451 or 452 or 453 or 454 or 455 or 456 or 457 or 458 or 459 or 460 or 461 or 462 or 463 or 464 or 465 or 466 or 467 or 468 or 469 or 470 or 471 or 472 or 473 or 474 or 475 or 476 or 477 or 478 or 479 or 480 or 481 or 482 or 483 or 484 or 485 or 486 or 487 or 488 or 489 or 490 or 491 or 492 or 493 or 494 or 495 or 496 or 497 or 498 or 499 or 500 or 501 or 502 or 503 or 504 or 505 or 506 or 507 or 508 or 509 or 510 or 511 or 512 or 513 or 514 or 515 or 516 or 517 or 518 or 519 or 520 or 521 or 522 or 523 or 524 or 525 or 526 or 527 or 528 or 529 or 530 or 531 or 532 or 533 or 534 or 535 or 536 or 537 or 538 or 539 or 540 or 541 or 542 or 543 or 544 or 545 or 546 or 547 or 548 or 549 or 550 or 551 or 552 or 553 or 554 or 555 or 556 or 557 or 558 or 559 or 560 or 561 or 562 or 563 or 564 or 565 or 566 or 567 or 568 or 569 or 570 or 571 or 572 or 573 or 574 or 575 or 576 or 577 or 578 or 579 or 580 or 581 or 582 or 583 or 584 or 585 or 586 or 587 or 588 or 589 or 590 or 591 or 592 or 593 or 594 or 595 or 596 or 597 or 598 or 599 or 600 or 601 or 602 or 603 or 604 or 605 or 606 or 607 or 608 or 609 or 610 or 611 or 612 or 613 or 614 or 615 or 616 or 617 or 618 or 619 or 620 or 621 or 622 or 623 or 624 or 625 or 626 or 627 or 628 or 629 or 630 or 631 or 632 or 633 or 634 or 635 or 636 or 637 or 638 or 639 or 640 or 641 or 642 or 643 or 644 or 645 or 646 or 647 or 648 or 649 or 650 or 651 or 652 or 653 or 654 or 655 or 656 or 657 or 658 or 659 or 660 or 661 or 662 or 663 or 664 or 665 or 666 or 667 or 668 or 669 or 670 or 671 or 672 or 673 or 674 or 675 or 676 or 677 or 678 or 679 or 680 or 681 or 682 or 683 or 684 or 685 or 686 or 687 or 688 or 689 or 690 or 691 or 692 or 693 or 694 or 695 or 696 or 697 or 698 or 699 or 700 or 701 or 702 or 703 or 704 or 705 or 706 or 707 or 708 or 709 or 710 or 711 or 712 or 713 or 714 or 715 or 716 or 717 or 718 or 719 or 720 or 721 or 722 or 723 or 724 or 725 or 726 or 727 or 728 or 729 or 730 or 731 or 732 or 733 or 734 or 735 or 736 or 737 or 738 or 739 or 740 or 741 or 742 or 743 or 744 or 745 or 746 or 747 or 748 or 749 or 750 or 751 or 752 or 753 or 754 or 755 or 756 or 757 or 758 or 759 or 760 or 761 or 762 or 763 or 764 or 765 or 766 or 767 or 768 or 769 or 770 or 771 or 772 or 773 or 774 or 775 or 776 or 777 or 778 or 779 or 780 or 781 or 782 or 783 or 784 or 785 or 786 or 787 or 788 or 789 or 790 or 791 or 792 or 793 or 794 or 795 or 796 or 797 or 798 or 799 or 800 or 801 or 802 or 803 or 804 or 805 or 806 or 807 or 808 or 809 or 810 or 811 or 812 or 813 or 814 or 815 or 816 or 817 or 818 or 819 or 820 or 821 or 822 or 823 or 824 or 825 or 826 or 827 or 828 or 829 or 830 or 831 or 832 or 833 or 834 or 835 or 836 or 837 or 838 or 839 or 840 or 841 or 842 or 843 or 844 or 845 or 846 or 847 or 848 or 849 or 850 or 851 or 852 or 853 or 854 or 855 or 856 or 857 or 858 or 859 or 860 or 861 or 862 or 863 or 864 or 865 or 866 or 867 or 868 or 869 or 870 or 871 or 872 or 873 or 874 or 875 or 876 or 877 or 878 or 879 or 880 or 881 or 882 or 883 or 884 or 885 or 886 or 887 or 888 or 889 or 890 or 891 or 892 or 893 or 894 or 895 or 896 or 897 or 898 or 899 or 900 or 901 or 902 or 903 or 904 or 905 or 906 or 907 or 908 or 909 or 910 or 911 or 912 or 913 or 914 or 915 or 916 or 917 or 918 or 919 or 920 or 921 or 922 or 923 or 924 or 925 or 926 or 927 or 928 or 929 or 930 or 931 or 932 or 933 or 934 or 935 or 936 or 937 or 938 or 939 or 940 or 941 or 942 or 943 or 944 or 945 or 946 or 947 or 948 or 949 or 950 or 951 or 952 or 953 or 954 or 955 or 956 or 957 or 958 or 959 or 960 or 961 or 962 or 963 or 964 or 965 or 966 or 967 or 968 or 969 or 970 or 971 or 972 or 973 or 974 or 975 or 976 or 977 or 978 or 979 or 980 or 981 or 982 or 983 or 984 or 985 or 986 or 987 or 988 or 989 or 990 or 991 or 992 or 993 or 994 or 995 or 996 or 997 or 998 or 999 or 1000

the problem is tractable

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 280 & 0 \\ 0 & 0 & 0 & 1 & 480 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

then the word 'prize' will be encoded as

$$\phi(PRIZE) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 280 & 0 \\ 0 & 0 & 0 & 1 & 480 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 16 \\ 8 \\ 25 \\ 16 \\ 21 \end{bmatrix} = \begin{bmatrix} 16 \\ 8 \\ 25 \\ 16 \\ 21 \end{bmatrix} = \text{PHYPU}$$

$$M^{-1} = \begin{bmatrix} 1 & 25 & 25 & 25 & 25 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

encode message PHYPV is changed to QHYPU. Then the encoding of QHYPU will be

$$(17, 8, 25, 16, 21) M^{-1} = (17, 17, 8, 25, 4) \\ = QQHYD$$

Scrambled Codes:

permutations are the basis for a type of cryptographic code called a scrambled code.

If  $\pi$  is a permutation on  $\{1, 2, \dots, n\}$  then we define the encoding function  $\pi$  to be the map from  $(a_1, a_2, \dots, a_n)$  to  $(a_{\pi(1)}, a_{\pi(2)}, \dots, a_{\pi(n)})$

this is actually a very special type of matrix encoding, since the mapping  $\pi \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$   
 $(3, 5, 2, 1, 4)$

for example, suppose  $\pi = (1 \ 3 \ 2 \ 5 \ 4)$  and wish to use the encoding induced by this permutation to encode the message "the trial begins tomorrow". this message is divided into blocks of 5, and to encode a block the  $\pi(1)$  letter is placed in the 1st position, the  $\pi(2)$  letter in the 2nd position, the  $\pi(3)$  letter in the 3rd position

$\pi(4)$  in the 4<sup>th</sup> position and  $\pi(5)$  5<sup>th</sup> letter in the 5<sup>th</sup> position.

The blocked message is

THETR DALTA BLEBE GDNST OMORR  
<sup>35214</sup> THETR TALBE GDNST OMORR OWXXX  
<sub>12345</sub>

which encoded as

ERHTT LEADB NPIGTS ORMOR ZXWXX

Since  $\pi(1) = 3, \pi(2) = 5, \pi(3) = 2, \pi(4) = 1$   
 $\pi(5) = 4$

To decode a permutation encoding, first make sure that the encoding is indeed a permutation encoding. Second determine the block size and third determine the permutation.

Block size is determined in the same manner as the block size of matrix encoding.

If a sequence of letters is repeated then it can be assumed that the same word or phrase was repeated in the original message, hence the block size is a divisor of the number of letters separating the successive occurrences of the repeated sequence. Once the block size is determined, construct a table whose

$i$ th row is  $j$ th block  
 permute the columns of the table to obtain a reasonable fit of pairs and continue until the

message can be read from the <sup>table</sup> Suppose the following  
encoded message interpreted.

SARKL BIEINR EELOA MHDSE  
YNAAA Ssysa IRIFE IREOC  
WLSIP LUBC LATMK OTAIL  
ASPSX

Since the frequency of occurrence of letters in  
the message so closely matches the statements standard  
count, we assume that the code is a permutation  
code, the block size must now be determined.

The sequence of 28 letters from the start of  
the first to the second occurrence

thus the block size of the encoding is a  
divisor of 28, hence must be 2, 4, 7, 28.

Since the only permutations of two elements are the  
identity permutations and a permutation interchanging  
the two elements, a quick check shows that the  
block length is not 2. Suppose now that the block  
length is 4. If we write the message in a table with  
4 columns, where row  $i$  is simply blocks of the  
message, then by permutating the columns we will  
eventually, if the block size is 4, obtain the  
message,

continue.

SAIR  
LGED  
NREE  
LOAM  
HDBE  
YNAA  
ASSY  
SAIR

LFEE  
RFOC  
WLSI  
POLLU  
BCIA  
TMKO  
TARL  
ASPS  
Z

and we can attempt to permute the columns to determine the message. Since column 1, column 2,

do not seem to belong together, we can try col 1, col 3 but in this case we obtain the unusual combinations.

It's from row 5 and PK from row 14. If we try col 1 adjacent to col 4 these will be fewer, unusual two letters combinations, so we may adjacent. This gives

If column 2 or column 3 is placed before column 1, column 3 will yield slightly better, 3 letter sequences putting column 2 before the already determined position yields are nonsense, but putting it after the determine position yields

SR  
LD  
NE  
LM  
HE  
YA  
AY  
BR  
LD  
RC  
WM  
DU  
BA  
TO  
TL  
AS

Israeli, general Moshe Dayan says

Israeli force will pull back to mitla pass

Unit - III.

Assignment problem, Hungarian method.

Assignment problem:

The assignment problem is a special case of the transportation problem in which the objective is to assign a no. of origins to the equal number of destinations at a minimum cost (or) maximum profit.

Mathematical formulation of the Assignment problem.

$$\text{Minimize } z = \sum_{i=1}^n \sum_{j=1}^n c_{ij} x_{ij}$$

Subject to the constraints

$$\sum_{j=1}^n x_{ij} = 1 \quad \& \quad \sum_{i=1}^n x_{ij} = 1$$

$$x_{ij} = 0 \text{ or } 1$$

for all  $i = 1, 2, \dots, n$

$j = 1, 2, \dots, n$

	$J_1$	$J_2$	$J_3$	...	$J_n$
$M_1$	$C_{11}$	$C_{12}$	$C_{13}$	...	$C_{1n}$
$M_2$	$C_{21}$	$C_{22}$	$C_{23}$	...	$C_{2n}$
$M_3$	$C_{31}$	$C_{32}$	$C_{33}$	...	$C_{3n}$
$\vdots$					
$M_n$	$C_{n1}$	$C_{n2}$	$C_{n3}$	...	$C_{nn}$

## Balanced Assignment Problem.

Assignment problem is said to be balanced if total no. of rows is equal to total no. of columns.

Ex: 1

	D	E	F
A	1	2	3
B	4	5	6
C	7	8	9

## Unbalanced assignment problem:

Total number of rows  $\neq$  total number of columns. In this case, we add dummy row or dummy column to balance the problem.

Ex: 1

	B <sub>1</sub>	B <sub>2</sub>	B <sub>3</sub>	B <sub>4</sub>
A <sub>1</sub>	1	2	3	4
A <sub>2</sub>	5	6	7	8

	B <sub>1</sub>	B <sub>2</sub>
A <sub>1</sub>	9	10
A <sub>2</sub>	11	12
A <sub>3</sub>	13	14

	B <sub>1</sub>	B <sub>2</sub>	B <sub>3</sub>	B <sub>4</sub>
A <sub>1</sub>	1	2	3	4
A <sub>2</sub>	5	6	7	8
A <sub>3</sub>	0	0	0	0
A <sub>4</sub>	0	0	0	0

	B <sub>1</sub>	B <sub>2</sub>	B <sub>3</sub>
A <sub>1</sub>	9	10	0
A <sub>2</sub>	11	12	0
A <sub>3</sub>	13	14	0

① Solve the assignment problem to minimize the total working hours.

	E	F	G	H
A	18	26	17	11
B	13	28	14	26
C	38	19	18	15
D	19	26	24	10

Total number rows = total number of columns

∴ the given Assignment problem is balanced.

Step 1

7	15	6	0
0	15	1	13
23	4	3	0
9	16	14	0

→ Subtract minimum value with other value.

(row - min)

Row reduction

Step 2

7	11	5	0
0	11	0	13
23	0	2	0
9	12	3	0

Column reduction.

Step 3

Row scanning

7	11	5	0
0	11	0	13
23	0	2	0
9	12	3	0

Step 4

Column scanning

7	11	5	0
0	11	0	13
23	0	2	0
9	12	3	0

□ - optimal assignment

Step 5:  $\sum_{i=1}^m u_i + \sum_{j=1}^n v_j = \sum_{i,j} c_{ij} x_{ij}$

7	11	5	0	$\sqrt{3}$
0	11	0	13	
23	0	2	0	
9	12	13	$\times$	$\sqrt{2}$

add minimum value with the interested

- 1) unassigned row
- 2) zero column
- 3) assigned row

Unmarked rows, marked column.

Step 6:

Smallest element

	E	F	G	H
A	2	6	0	$\times$
B	0	11	$\times$	18
C	23	0	2	5
D	4	7	8	0

Optimum solution is

- A  $\rightarrow$  G 17
- B  $\rightarrow$  E 13
- C  $\rightarrow$  F 19
- D  $\rightarrow$  H 10

Total = 17 + 13 + 19 + 10 = 59 //

Find an optimum assignment schedule & maximum profit to the given assignment problems.

		Zones			
		A	B	C	D
Sales engineers	P	120	112	98	154
	Q	90	72	63	99
	R	110	88	77	121
	S	80	64	56	88

Step 1:

↳ we have to convert our given maximization problem into minimization problem.

↳ largest element = ~~120~~ 154

↳ Subtract all the elements from 154

↳ we get the following resultant matrix which is a minimization problem.

		A	B	C	D
P		14	42	56	0
Q		64	82	91	55
R		44	66	77	33
S		74	90	98	66

Number of rows = number of columns.

∴ the problem is balanced

Step 2:

(Row reduction)

14	42	56	0
9	27	36	0
11	33	44	0
8	24	32	0

Step 3:

Column reduction

6	18	24	0
1	3	4	0
3	9	12	0
0	0	0	0

Step 4:

row scanning

6	18	24	0
1	3	4	0
3	9	12	0
0	0	0	0

Step 5:

Column Scanning

6	18	24	0
1	3	4	0
3	9	12	0
0	0	0	0

Step 6:

Drawing minimum number of lines.

5	17	23	0
0	2	3	0
2	8	11	0
0	0	0	0

5	17	23	0
0	2	3	0
2	8	11	0
0	0	0	0

unassigned row  
 ↓  
 zero column  
 ↓  
 assigned row  
 ↓  
 unmarked row & marked column.

least element subtract with unmarked row & marked column.

3	15		0
0	2	3	2
2	6	9	X
2	0	0	3

15	2	0	3
2	3	2	
6	9	X	0
0	0	3	0
0	0	8	0
8	5	8	0

	A	B	C	D
P	3	13	19	0
Q	X	0	1	2
R	0	4	7	0
S	2	X	0	5

Zones Profit  
 $P \rightarrow D = 154$   
 $Q \rightarrow B = 72$   
 $R \rightarrow A = 110$   
 $S \rightarrow C = 56$

392

7	2	8	0
7	0	11	0
P	0	0	0
0	7	0	0

	A	B	C	D
1	10	25	15	20
2	15	30	5	15
3	35	20	12	24
4	17	25	24	20

No. of rows = 4  
 No. of columns = 4.

Therefore no. of rows = no. of columns  
 the given assignment problem is balanced.

Step 1: Row reduction

0	15	5	10
10	25	0	10
13	8	0	12
0	8	7	3

Step 2: Column reduction

0	7	5	7
10	17	0	7
13	0	0	9
0	0	7	0

Step 3: Row reduction & column reduction

	A	B	C	D
1	$\boxed{0}$	7	5	7
2	10	17	$\boxed{0}$	7
3	13	$\boxed{0}$	<del>x</del>	9
4	<del>x</del>	<del>x</del>	7	$\boxed{0}$

Optimum solution is

$$1 \rightarrow A$$

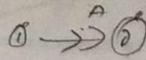
$$2 \rightarrow C$$

$$3 \rightarrow B$$

$$4 \rightarrow D$$

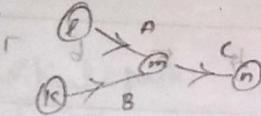
$$10 + 5 + 20 + 20 = 55 //$$

# Critical path method



Immediate predecessor

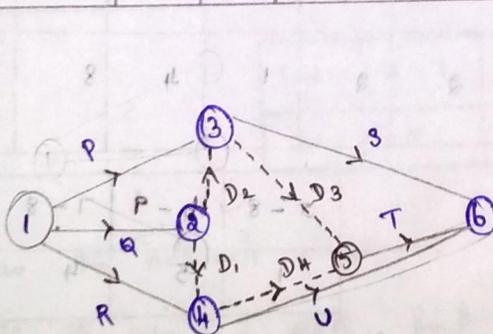
" Successor.



"A is a predecessor of C"

- ① Draw the network for the project whose activities and their precedence relationships are given below.

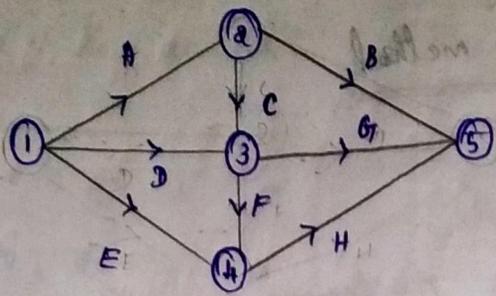
Activity	P	Q	R	S	T	U
Predecessor	-	-	-	P, Q	P, R	Q, R



- 2) Construct the network for the project whose activities and their relationships are given below.

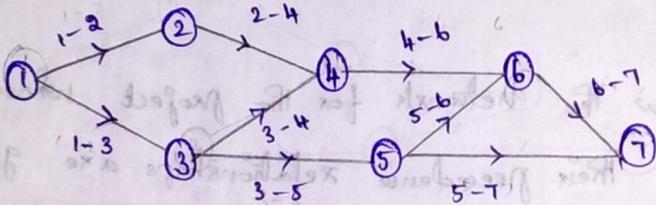
Activities A, D, E can start simultaneously

Activities B, C > A; G, F > D, C; H > E, F



3) Draw the network.

Event no	1	2	3	4	5	6	7
Immediate predecessors	-	1	1	2,3	3	4,5	5,6

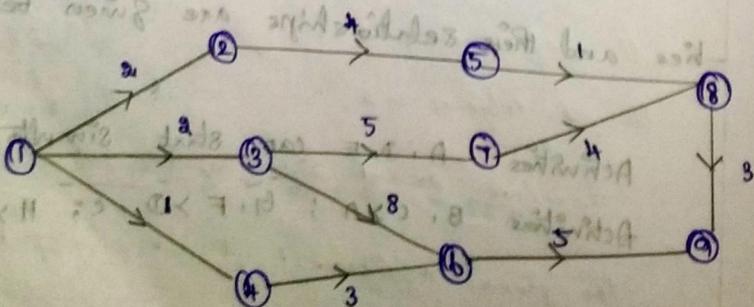


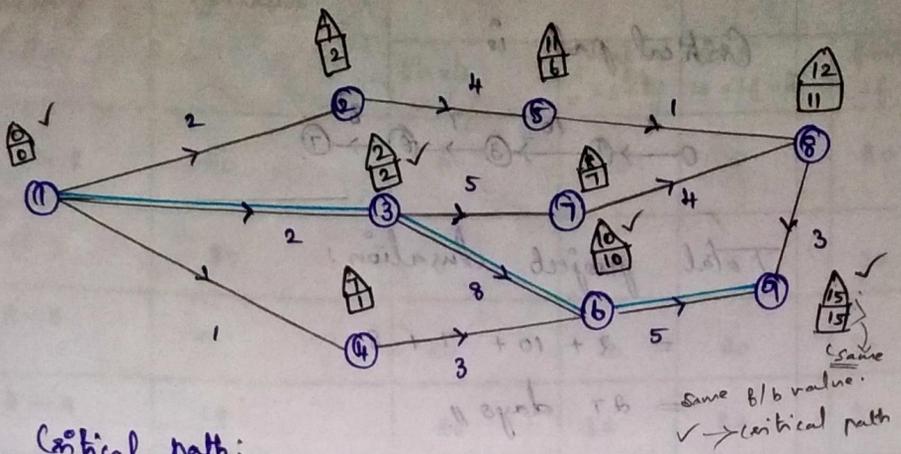
Activity	1-2	1-3	1-4	2-5	3-6	3-7	4-6
Time (duration)	2	2	1	4	8	5	3

5-8	6-9	7-8	8-9
1	5	4	3

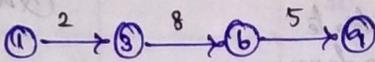
i, Draw network diagram

ii, find the critical path & total project duration.





Critical path:



for maximum (+)  
 for minimum value (-)

Total project duration

$$2 + 8 + 5 = 15 \text{ Weeks.}$$

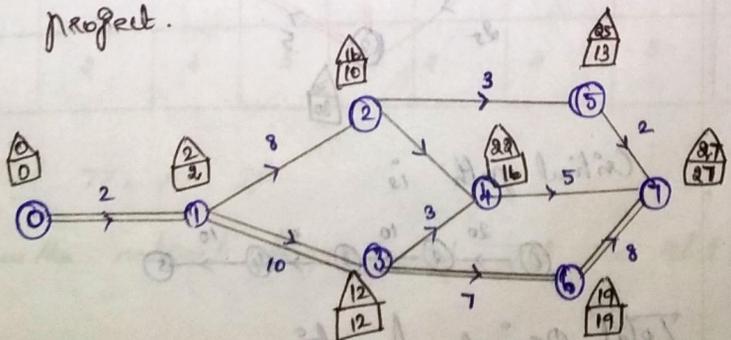
①

Activity	0-1	1-2	1-3	2-4	2-5	3-4
duration	2	8	10	6	3	3

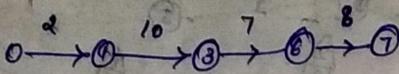
3-6	4-7	5-7	6-7
7	5	2	8

Draw the network diagram.

Identify the critical path, find the total duration of the project.



Critical path is

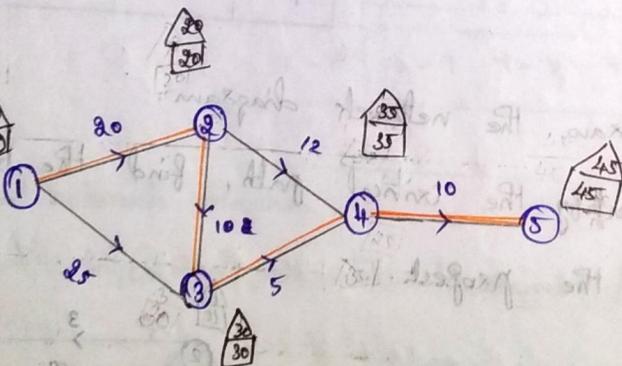


Total project duration:

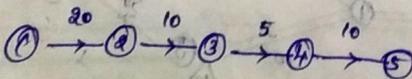
$$= 2 + 10 + 7 + 8$$

$$= 27 \text{ days} //$$

Activity	Immediate Predecessors	Duration (Days)
1-2	-	20
1-3	-	25
2-3	1-2	10
2-4	1-2	12
3-4	1-3 & 2-3	5
4-5	2-4 & 3-4	10



Critical path is



Total project duration:

$$20 + 10 + 5 + 10 = 45 \text{ days} //$$

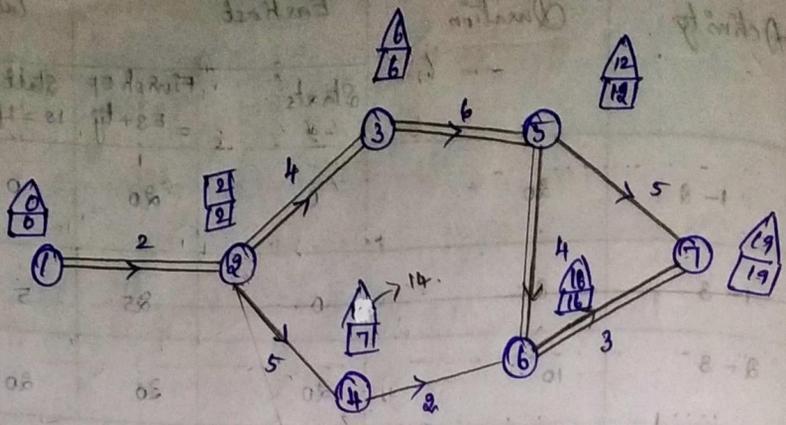
Activity	Duration	Earliest		Latest	
		Starts Start ES	Finish EF End EF = ES + tj	Start LS = LF - tj	Finish LF
1-2	20	0	20	0	20
1-3	25	0	25	5	30
2-3	10	20	30	20	30
2-4	12	20	32	23	35
3-4	5	30	35	30	35
4-5	10	35	45	35	45

total float = latest end - earliest end. slack - difference  
SHE STE hand event  $\frac{14}{12} = 2$

Total float (LF - EF)	Free float (total float - SHE)	Independent float (free float - STE)
0	0 - 0 = 0	0 - 0 = 0
5	5 - 0 = 5	5 - 10 = 5
0	0 - 0 = 0	0 - 0 = 0
3	3 - 0 = 3	3 - 0 = 3
0	0 - 0 = 0	0 - 0 = 0
0	0 - 0 = 0	0 - 0 = 0

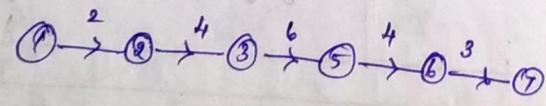
Activity	1-2	2-3	2-4	3-5	4-6	5-6	5-7	6-7
Duration	2	4	5	6	2	4	5	3

- i, find TF, FF, IF
- ii, Draw the network diagram and find the total project time.



Activity	Duration	Earliest time		Latest time		TF (LF - EF)	FF TF - SFE	IF FF -
		Start ES	End EF	LS	LF			
1-2	2	0	2	0	2	0	0-0=0	0-0=0
2-3	4	2	6	2	6	0	0-0=0	0-0=0
2-4	5	2	7	9	14	7	7-7=0	0-0=0
3-5	6	6	12	6	12	0	0-0=0	0-0=0
4-6	2	7	9	14	16	7	7-0=7	7-7=0
5-6	4	12	16	12	16	0	0-0=0	0-0=0
5-7	5	12	17	14	19	0	2-0=2	2-0=2
6-7	3	16	19	16	19	0	6-0=6	0-0=0

Critical path :



Total project time = 19 hours,

Activity	Immediate Predecessors	$t_o$	$t_m$	$t_p$
A	-	1	1	7
B	-	1	4	7
C	-	2	2	8
D	A	1	1	1
E	B	2	5	14
F	C	2	5	8
G	D, E	3	6	15
H	F, G	1	2	3

$t_e$  - expected time.  
to opposite time.

i) Draw the PERT Network, find out the expected project completion time.

ii) What is the probability of completing the project in 14 days.

$$t_e = \frac{t_o + 4t_m + t_p}{6}$$

$$\sigma^2 = \left( \frac{t_p - t_o}{6} \right)^2$$

Variance  $SD = \sqrt{\text{Variance}} = \sqrt{\sigma^2} = \sigma$

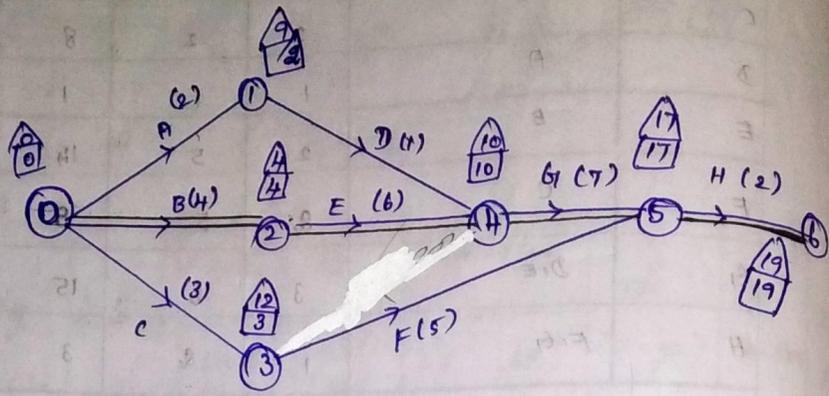
Activity	Immediate Predecessors	$t_o$	$t_m$	$t_p$	$t_e = \frac{t_o + 4t_m + t_p}{6}$	$\sigma^2 = \left( \frac{t_p - t_o}{6} \right)^2$
A	-	1	1	7	$\frac{1+4+7}{6} = \frac{12}{6} = 2$	$\left( \frac{7-1}{6} \right)^2 = 1$
B	-	1	4	7	$\frac{1+16+7}{6} = \frac{24}{6} = 4$	$\left( \frac{7-1}{6} \right)^2 = 1$
C	-	2	2	8	$\frac{2+8+8}{6} = \frac{18}{6} = 3$	$\left( \frac{8-2}{6} \right)^2 = 1$
D	A	1	1	1	$\frac{1+4+1}{6} = \frac{6}{6} = 1$	0
E	B	2	5	14	$\frac{2+20+14}{6} = \frac{36}{6} = 6$	4
F	C	2	5	8	$\frac{2+4(5)+8}{6} = 5$	1

G1 DIE 3 6 15

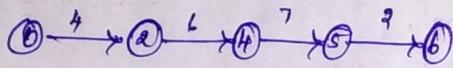
$$\frac{3 + 4(6) + 15}{6} = 7 \quad \left(\frac{15-3}{6}\right)^2 = 4$$

H FIG 1 2 3

$$2 \quad \frac{1}{9}$$



Critical path



Total project time = 19 days.

Variance

$$\sigma^2 = \left(\frac{t_p - t_o}{6}\right)^2$$

$$\sigma^2_e = 1 + 4 + 4 + \frac{1}{9}$$

$$\sigma e^2 = \frac{9 + 36 + 36 + 1}{9} = \frac{82}{9} = 9.1 \quad \sqrt{9.1}$$

S.D =  $\sigma e = 3.02$

Variance  $\sigma^2$   
 SD  $\sigma$   
 ↓  
 Standard deviation

In standard normal distribution

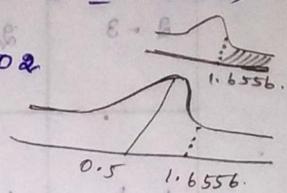
$$z = \frac{x - \mu}{\sigma}$$

let the project completing in 14 days

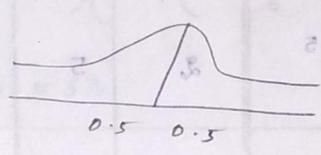
$$x = 14, \quad \mu = 19, \quad \sigma = 3.02$$

$$z = \frac{14 - 19}{3.02} = -1.6556$$

$$\begin{aligned}
 P(x=14) &= P(Z \leq z) = P(Z \leq -1.6556) \\
 &= P(Z \geq 1.6556) \\
 &= 1 - P(Z \leq 1.6556) \\
 &= 0.5 - P(0 \leq Z \leq 1.6556) \\
 &= 0.5 - 0.4502 \\
 &= 0.0498
 \end{aligned}$$



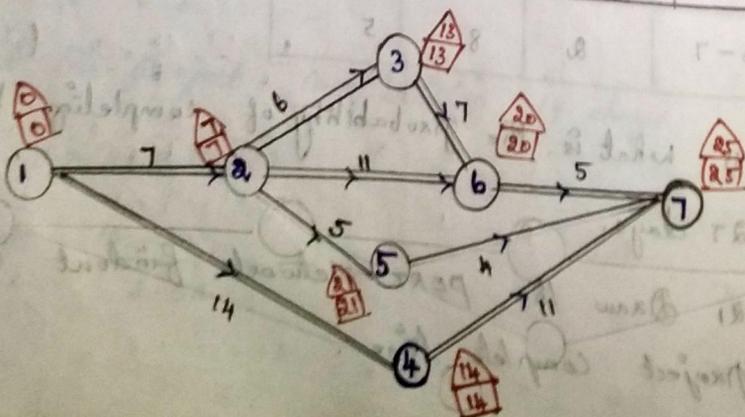
thus the probability of completing the project in 14 days is 4.98%.

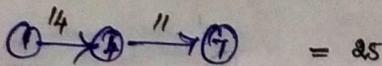
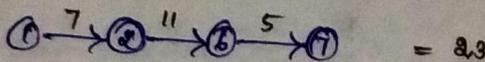
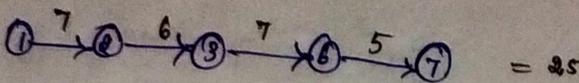


Task	$t_o$	$t_p$	$t_m$
1-2	3	15	6
2-3	2	14	5
1-4	6	30	12
2-5	2	8	5
2-6	5	17	11
3-6	3	15	6
4-7	3	27	9
5-7	1	7	4
6-7	2	8	5

- what is the probability of completing the project in 27 days.
- Draw the PERT Network, find out the expected project complete time.

task	$t_0$	$t_m$	$t_p$	$t_e = \frac{t_0 + 4t_m + t_p}{6}$	$\sigma^2 = \left(\frac{t_p - t_0}{6}\right)^2$
1-2	3	6	15	$\frac{3 + 4(6) + 15}{6} = \frac{37}{6} = 6.17$	$\left(\frac{15-3}{6}\right)^2 = 4$
2-3	2	5	14	$\frac{2 + 4(5) + 14}{6} = \frac{36}{6} = 6$	$\left(\frac{14-2}{6}\right)^2 = 4$
1-4	6	12	30	$\frac{6 + 4(12) + 30}{6} = \frac{84}{6} = 14$	$\left(\frac{30-6}{6}\right)^2 = 16$
2-5	2	5	8	$\frac{2 + 4(5) + 8}{6} = \frac{30}{6} = 5$	$\left(\frac{8-2}{6}\right)^2 = 1$
2-6	5	11	17	$\frac{5 + 4(11) + 17}{6} = \frac{66}{6} = 11$	$\left(\frac{17-5}{6}\right)^2 = 4$
3-6	3	6	15	$\frac{3 + 4(6) + 15}{6} = 7$	$\left(\frac{15-3}{6}\right)^2 = 4$
4-7	3	9	27	$\frac{3 + 4(9) + 27}{6} = \frac{66}{6} = 11$	$\left(\frac{27-3}{6}\right)^2 = 16$
5-7	1	4	7	$\frac{1 + 4(4) + 7}{6} = \frac{24}{6} = 4$	$\left(\frac{7-1}{6}\right)^2 = 1$
6-7	2	5	8	$\frac{2 + 4(5) + 8}{6} = \frac{30}{6} = 5$	$\left(\frac{8-2}{6}\right)^2 = 1$





Total project time = 25 days.

Variance,

$\sigma^2 e = \left( \frac{16+16}{6} \right)^2 = \left( \frac{32}{6} \right)^2 = \left( \frac{30-27}{6} \right)^2$

$\sigma^2 e = 16 + 16 = 32$

$\sigma e = 5.6568$

In standard normal distribution

$z = \frac{x - \mu}{\sigma} = \frac{27 - 25}{5.6568} = \frac{2}{5.6568} = 0.3535$

$z = 0.3535$

$P(x = 27) = P(z \leq z)$

$P(z \leq 0.3535)$

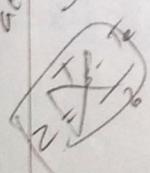
$1 - P(0 \leq z \leq 0.3535)$

$= 0.5 -$

preempt:

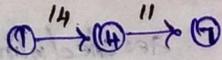
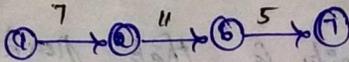
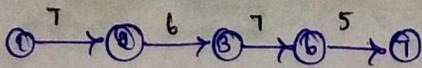
(FF)

FF of an activity is that activity which can be used for scheduling the activity without affecting the activity



FF = TF - (lag) (if) Slack of the head event

$FF = \frac{TF - SFE - SE}{FF - STE}$   
 $FF \leq FF \leq TF$



Total project time = 25 days.

Variance,

$$\sigma^2 = \left( \frac{t_p - t_o}{6} \right)^2$$

$$= 16 + 16 = 32$$

$$\sigma = \sqrt{32} = 5.6569$$

In standard normal distribution

$$z = \frac{x - \mu}{\sigma}$$

$$z = \frac{27 - 25}{5.6569}$$

$$= 0.3536$$

$$P(x = 27) = P(z \leq z)$$

$$= P(z \leq 0.3536)$$

$$= 0.5 + 0.1368 = 0.6368$$

$$\therefore P(x = 27) = 0.6368$$

Thus the probability of completing the project in 27 days is 63.68%.

## Free float:

FF of an activity is that portion of the which can be used for rescheduling that activity without affecting the succeeding activity.

$$FF = TF - \text{Slack of the head event}$$

(i, j)      (i, j)

$$I.F \leq F.F \leq T.F$$

## Independent float:

IF of an activity is the amount of time by which the activity can be rescheduled without affecting the preceding or succeeding activities or that activity.

$$IF = FF - \overset{STE}{(STE)}$$

of an activity (i, j)      Slack Tail Event

$$IF \leq FF \leq TF$$

# Graph theory:

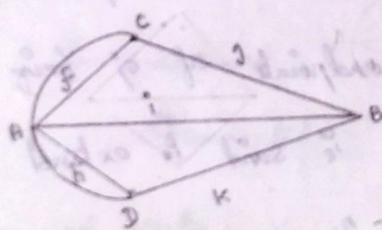
## Graph:

A graph  $G$  consists of a non empty set  $V$  of elements called vertices.

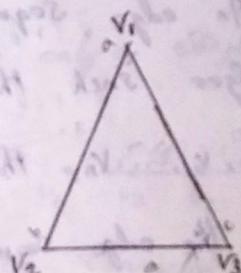
Set  $E$  elements called edges, and a function  $\epsilon$  from  $E$  to the set of unordered pairs of elements.

the two vertices in  $\epsilon(e)$  for an edge are called endpoints of  $e$

$$G = \{V, E, \epsilon\}$$



$$\epsilon(e) = \{A, C\}$$



$$\{a, b, c\}$$

$$\{v_1, v_2, v_2, v_3, v_3, v_1\}$$

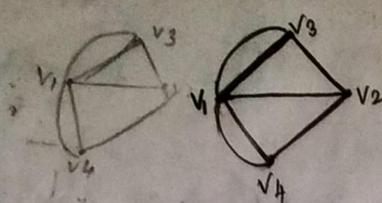
## Adjacency Matrix:

Another method is to represent the graph as a matrix.

Label the vertices of the graph  $1, 2, \dots, n$ . the matrix  $A = (a_{ij})_{n \times n}$  where  $i, j$  entry equal to the number of edges with end points  $i, j$ .

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

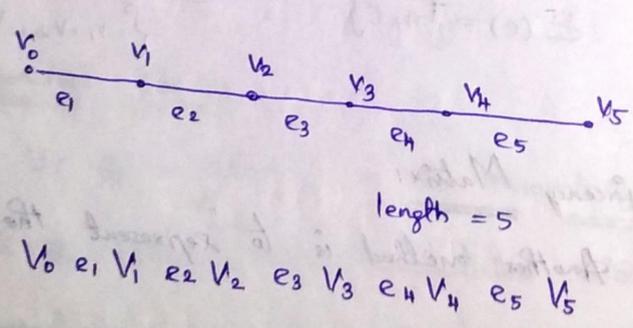
adjacent matrix



$$A = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{pmatrix} 0 & 1 & 2 & 2 \\ 1 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix} \end{matrix}$$

Edge Sequence: Edge Sequence!

An edge sequence is a sequence  $e_1, e_2, \dots, e_n$  of edges such that there is a sequence of vertices  $v_0, v_1, \dots, v_n$ , the endpoints of  $e_j$  being  $v_{j-1}$  &  $v_j$ . The edge sequence is said to extend from  $v_0$  to  $v_n$  and to have length  $n$ .



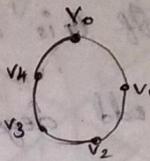
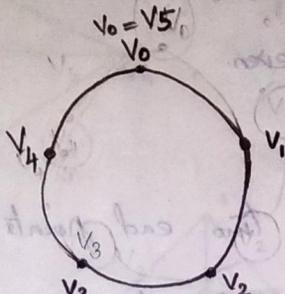
Chain Sequence!

A chain sequence is an edge sequence in which there is no repetition of edges.

A cycle sequence is a chain sequence that extends from  $v_0$  to  $v_n$ .  $v_0 = v_n$

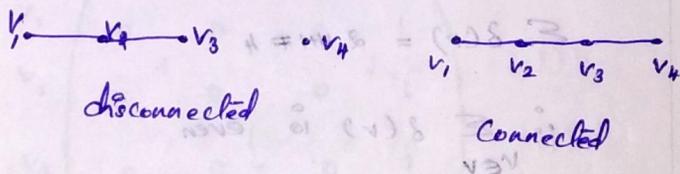
whether it extends from  $v_0$  to  $v_n$  or  $v_n$  to  $v_0$

then the chain (cycle), sequence is called a chain (cycle).



### Connected graph:

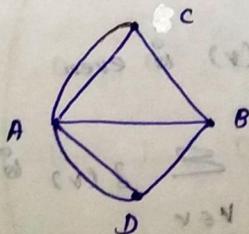
A graph is said to be connected if there exists a chain between any two vertices of the graph or else if the graph contains only a single vertex.



### Degree of vertex:

The degree  $\delta(v)$  of a vertex  $v$  of a graph  $G$  is the number of edges with endpoints  $v$ , with the convention that a loop with endpoints  $v$  and  $v$  contributes two to the degree of  $v$ .

4 vertices  
7 edges



- $\delta(A) = 5$
- $\delta(B) = 3$
- $\delta(C) = 3$
- $\delta(D) = 3$

### Theorem:

If  $G$  is a finite graph, the number of vertices of odd degree is even.

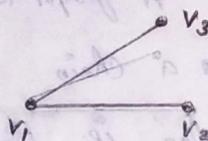
Proof:

Each edge has two end points and thus contributes two end points to the sum of degrees of the vertices.

$$\delta(v_1) = 2$$

$$\delta(v_2) = 1$$

$$\delta(v_3) = 1$$



$$\sum \delta(v) = 2 + 1 + 1 = 4$$

$$\therefore \sum_{v \in V} \delta(v) \text{ is even}$$

Let  $V_0$  be the set of vertices with even degrees,

$V_1$  be the set of vertices with odd degree.

$$\text{thus } \sum_{v \in V} \delta(v) = \sum_{v \in V_0} \delta(v) + \sum_{v \in V_1} \delta(v)$$

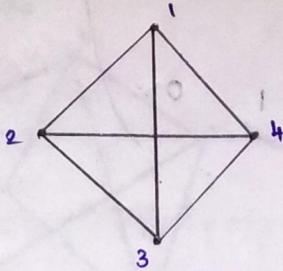
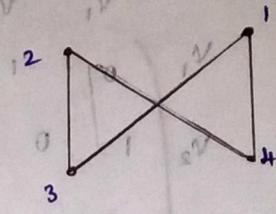
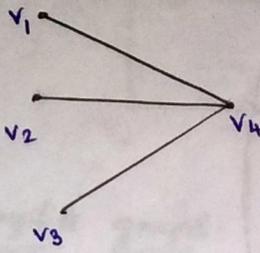
Since  $\delta(v)$  is even for each  $v \in V_0$

$$\Rightarrow \sum_{v \in V_0} \delta(v) \text{ is even}$$

If we know that  $\sum_{v \in V} \delta(v)$  is even

$$\text{even} = \text{ev} + \text{ev}$$

write adjacency matrix of

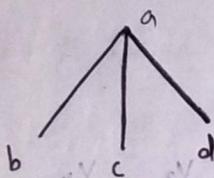


$$A = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \end{matrix}$$

$$\begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \end{matrix}$$

if vertices are the joining two vertices are allowed, the resulting object is called a multigraph.

	$V_1$	$V_2$	$V_3$	$V_4$
$V_1$	0	1	1	1
$V_2$	1	0	1	1
$V_3$	1	1	0	1
$V_4$	1	1	1	0



$$V(G_1) = \{a, b, c, d\} = 4$$

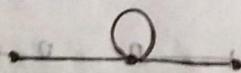
$$E(G_1) = \{ab, ac, ad\} = 3$$

$$G_1 = (4, 3) \text{ graph}$$

A graph  $G_1$  with  $p$  vertices,  $q$  edges can be written as  $G_1 = (p, q)$  graph.

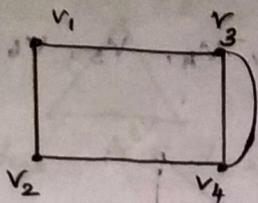
**loop:**

A line joining a point to itself is called a loop.

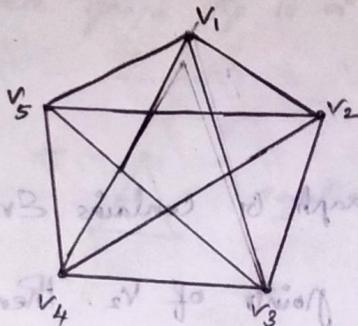


Multigraph:

If more than one line joining two vertices are allowed, the resulting object is called a multigraph. (multiple lines)



Complete graph:



A graph in which any two distinct points are adjacent is called a complete graph.

Totally disconnected graph:

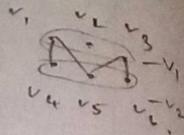
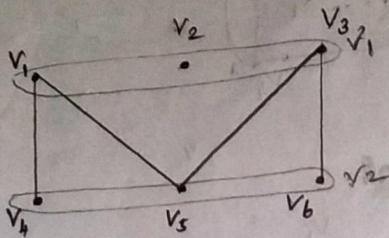


A graph whose edge set is empty is called a null graph or a totally disconnected graph.

Bipartite graph: or bigraph.

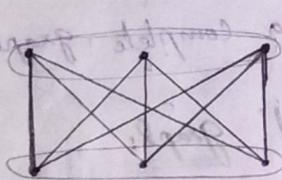
A Graph  $G$  is called a bipartite graph if  $V$  can be partitioned into two disjoint subsets  $V_1, V_2$  such that every line of  $G$  joins a point of  $V_1$  to a point of  $V_2$ .  $(V_1, V_2)$  is called a bipartition of  $G$ .

$$V(G) = \{v_1, v_2, v_3, v_4, v_5, v_6\}$$

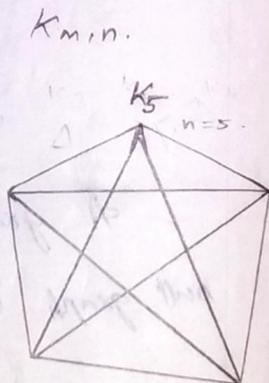
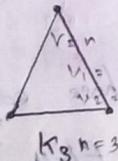
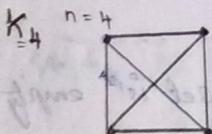


Complete bipartite graph:

If a bipartite graph  $G$  contains every line joining the points of  $v_1$  to the points of  $v_2$ . Then  $G$  is called a complete bipartite graph.

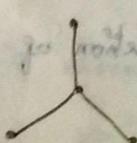


Complete graph with n vertices



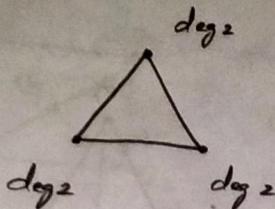
Regular graph:

If all the points of  $G$  have the same degree  $x$  then  $G$  is called a regular graph of degree  $x$ .



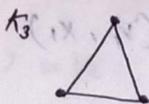
Regular graph of degree 3 = Cubic graph

$\deg(v) = 3 \quad \forall v \in V$  Regular graph of degree 3



$\deg(v) = 2$   
 for all  $v \in V$   
 regular of degree 2.

Complete graph  $K_p$  is a regular graph of degree  $p-1$



regular graph of deg 2

$K_4$



regular graph of deg 3

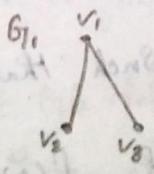
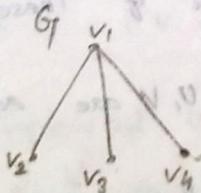
Subgraphs:

$G = (V, E)$  vertices edges

$G_1 = (V_1, E_1)$

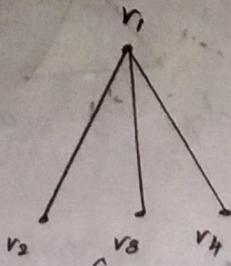
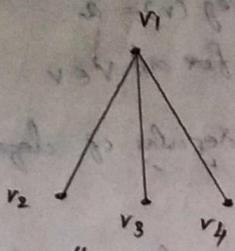
$G_1 = (V_1, E_1)$  is said to be a subgraph of  $G$  if

$(V_1, E_1) \subseteq (V, E)$  subset  
 $V_1 \subseteq V$  &  $E_1 \subseteq E$



If  $G_1$  is a subgraph of  $G$ , then we say  
 that  $G$  is a supergraph of  $G_1$ .

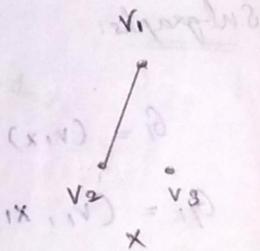
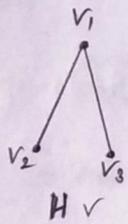
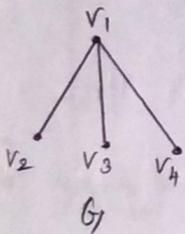
## Spanning Subgraph:



A subset is called a spanning subgraph of  $G = (V, X)$  if  $V_1 = V$ .  $H = (V_1, X_1)$

## Induced Subgraph:

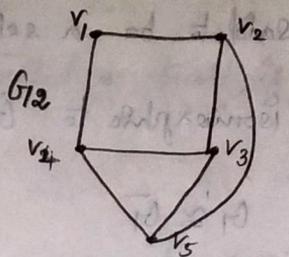
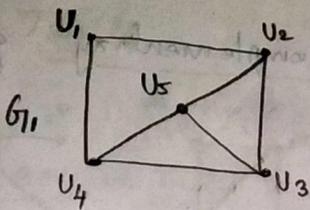
$H$  is called an induced subgraph of  $G$  if, two points are adjacent in  $H$  if and only if they are adjacent in  $G$ .



## Isomorphism:

Two graphs  $G_1 = (V_1, X_1)$  and  $G_2 = (V_2, X_2)$  are said to be isomorphic if there exists a bijection  $f: V_1 \rightarrow V_2$  such that  $u, v$  are adjacent in  $G_1$  if and only if  $f(u), f(v)$  are adjacent in  $G_2$ .

$G_1 \cong G_2$  The map  $f$  is called an isomorphism from  $G_1$  to  $G_2$ .



$$f: v_i \rightarrow v_i$$

$$f(u_i) = v_i$$

$$f(u_1) = v_1$$

$$f(u_2) = v_2$$

$$f(u_3) = v_3$$

$$f(u_4) = v_4$$

$$f(u_5) = v_5$$

### Automorphism:

An isomorphism of a graph  $G$  onto itself is called an automorphism of  $G$ .

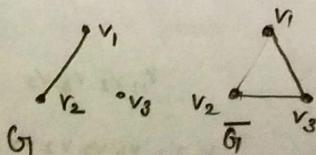
$\Gamma(G)$  denote the set of all automorphisms of  $G$ .

$$f(v_i) = v_i \quad \text{identity map} \quad f: v \rightarrow v \quad \text{automorphism of } G$$

### Complement:

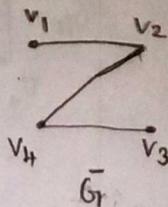
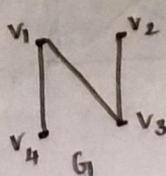
Let  $G = (V, E)$  be a graph

The complement  $\bar{G}$  of  $G$  is defined to be the graph which has  $\overset{V}{V}$  vertices and two points are adjacent in  $\bar{G}$  iff they are not adjacent in  $G$ .

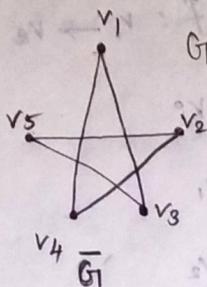
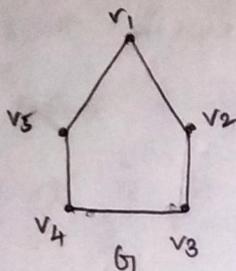


$G$  is said to be a self complementary graph if  $G$  is isomorphic to  $\bar{G}$

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



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



$$f(v_i) = v_{i+1}$$

$$f(v_1) = v_2$$

$$f(v_2) = v_3$$

$$f(v_3) = v_4$$

$$f(v_4) = v_5$$

Connectedness:

\* walk

\* path ~~trail~~

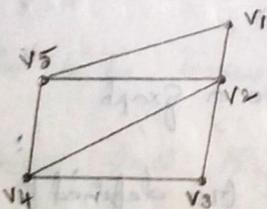
*points are distinct.*

i) Walk:

A walk of a graph  $G$  is an alternating sequence of points & lines  $v_0 x_1 v_1 x_2 v_2 x_3 v_3 x_4 v_4 \dots$

If  $v_0 = v_n$  (Initial point = terminal point) (Starting point = End point)

then the walk is said to be closed.



$v_1, v_2, v_3, v_4, v_2, v_1, v_2, v_5$

ii) Path:

A walk is called a path if all its points are distinct.

$v_1, v_2, v_4, v_5$

$v_1, v_2, v_4, v_3, v_2, v_5$  - not a path

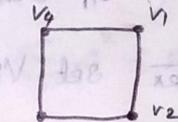
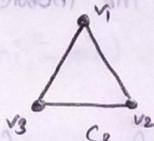
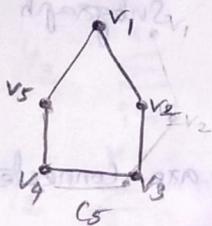
but its trail.

(ii) Trajectory:

A walk is called a trail if all its lines are distinct.

A  $v_0 - v_n$  walk is called closed if  $v_0 = v_n$ .

A closed walk  $v_0, v_1, v_2, \dots, v_n = v_0$  in which  $n \geq 3$  and  $v_0, v_1, \dots, v_{n-1}$  are distinct is called a cycle of length  $n$  (denoted by  $C_n$ )



A graph  $G$  is said to be connected, if there exists a  $u-v$  path between every pair of vertices  $u$  and  $v$  in  $G$ .

A graph which is not connected is said to be disconnected



Connected



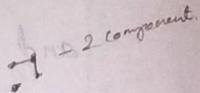
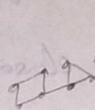
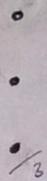
Disconnected

component.



Components:

$V$  is partitioned into non empty subsets  $V_1, V_2, \dots, V_k$  such that two vertices  $u$  and  $v$  are connected iff both  $u, v$  belong to the same set  $V_i$ .

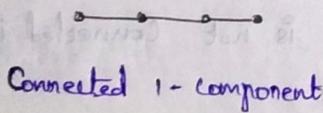


Let  $G_i$  denote the induced subgraph of  $G$  with vertex set  $V_i$

Clearly  $G_1, G_2, \dots, G_k$  are connected and are called the components of  $G$ .

$G$  is connected iff it has only one component.

$G$  is said to be disconnected if it has more than one components.



Connected 1-component



disconnected 2 components.

Theorem:

A simple graph  $G$  with  $n$  vertices,  $k$  components

can have at most  $\frac{(n-k)(n-k+1)}{2}$  edges

$$G = G_1 \cup G_2 \cup G_3 \dots \cup G_k$$

$$\begin{matrix} n_1 & n_2 & n_k \\ G_1 & G_2 & G_k \end{matrix}$$

$$n = n_1 + n_2 + \dots + n_k \quad (E_{ii})$$

Let the number of vertices in each of the component of a graph be  $n_1, n_2, \dots, n_k$

$$n_1 + n_2 + n_3 + \dots + n_k = n \quad n_i \geq 1$$

Maximum number of edges in  $i^{\text{th}}$  component of a graph is  $\frac{1}{2} n_i (n_i - 1)$

the maximum number edges in the graph  $G$  is

$$= \frac{1}{2} \sum_{i=1}^k n_i (n_i - 1)$$

$$= \frac{1}{2} \sum_{i=1}^k (n_i^2 - n_i) \quad \sum n_i^2 \leq n^2 - (k-1) \quad (2n-k)$$

$$= \frac{1}{2} \sum_{i=1}^k n_i^2 - \frac{1}{2} \sum_{i=1}^k n_i$$

$$= \frac{1}{2} \sum_{i=1}^k n_i^2 - \frac{n}{2}$$

$$\leq \frac{1}{2} [n^2 - (k-1)(2n-k)] - \frac{n}{2}$$

$$\leq \frac{1}{2} [n^2 - (2nk - k^2 - 2n + k)] - \frac{n}{2}$$

$$\leq \frac{1}{2} [n^2 - 2nk + k^2 + 2n - k] - \frac{n}{2}$$

$$\leq \frac{1}{2} [(n-k)^2 + (n-k)]$$

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

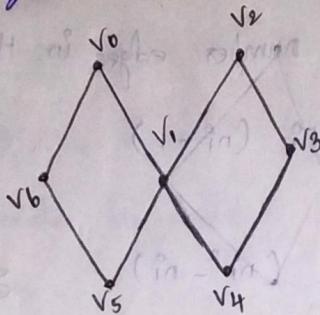
$$\leq \frac{(n-k)(n-k+1)}{2}$$

Hence Proved.

## Eulerian Trail:

A closed trail containing all the points & lines is called an Eulerian trail.

A graph having an Eulerian trail is called an Eulerian graph.



## Eulerian trail

$v_0 v_1 v_2 v_3 v_4 v_1 v_5 v_6 v_0$

## Euler graph: Theorem:

\* A connected graph  $G$  is Euler graph iff all the vertices of  $G$  are of even degree.

Proof:

Direct part:

Let  $G$  be a connected graph assume that  $G$  is an Euler graph to prove  $\deg(v)$  is even  $\forall v \in V$

$G$  is an Euler graph

$G$  contains an Eulerian 'trail'

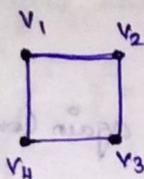
( $G$  contains a closed walk containing all edges)

In a closed walk every time a walk meets a vertex

It goes through two new edges incident with  $v$  (one we entered and the other exited)

This is true for all vertices in a closed walk.

$\therefore$  degree of every vertex is even



$v_1, v_2, v_3, v_4$

Converse part:

Assume that  $\deg(v)$  is even  $\forall v \in V$ .

to prove  $G$  is an Euler Graph.

i.e. to prove  $G$  contains at least one Eulerian trail (closed walk contains all the edges)

Construct a closed walk starting at  $v$  and going through the edges of  $G$  (such that no edge is repeated)

Name the closed walk as  $h$

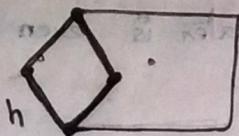
Case (i): If  $h$  covers all the edges. Then  $h$  becomes an Eulerian trail.

and hence  $G$  is an Eulerian graph.

Case (ii): If  $h$  doesn't cover all the edges of  $G$  then remove all the edges of  $h$  from  $G$  and obtain the graph  $G'$ .

Every vertex of  $G_1$  is also of an even degree.

Since  $G_1$  is connected,  $h$  will touch  $G_1$  at least one vertex  $v$ .



Starting from  $v$ , we can again construct a new walk  $h'$  in  $G_1$ .

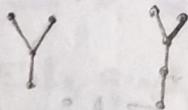
Now this walk  $h'$  combined with  $h$  forms a closed walk. Starts and ends at  $v$  and  $h$  as more edges than  $h$ . This process is repeated until we get a closed walk covering all the edges of  $G_1$ .

thus  $G_1$  is an Euler Graph.

Tree:

A connected graph with no cycles is called a tree.

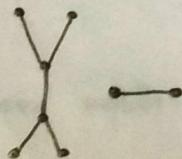
A connected acyclic graph.



forest:

Any graph without cycles is also called a forest.

So the components of a forest are trees.



If  $G_1$  is a tree

then

1) Every points of  $G_1$  are joined by a unique path.

2)  $G_1$  is connected and  $p = q + 1$

3)  $G_1$  is acyclic and  $p = q + 1$



$$p = 6 \text{ - vertices}$$
$$q = 5 \text{ - edges}$$

① Every connected graph has a spanning tree:

Proof:

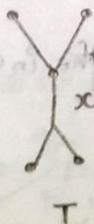
↳ Let  $G_1$  be a connected graph.

↳ Let  $T$  be a minimal connected spanning subgraph of  $G_1$ . Then for any line  $x$  of  $T$ .

↳  $T - x$  is disconnected and hence  $x$  is a bridge of  $T$ .

Hence  $T$  is acyclic

↳ Since  $T$  is connected  $\therefore T$  is a spanning tree.



$T-x$

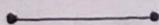
(2) Sum of the degree of the vertices in a finite graph

$G$  is even.

Proof: Let  $G$  be a finite graph with  $n$  vertices

Every line of  $G$  is incident with two points.

Hence Every line contributes 2 to the sum of the degrees of the points



Hence Sum of the degrees of the vertices in  $G$  
$$= \sum_{i=1}^n \text{deg}(v_i) = 2q = \text{even}$$

Incidence.

Incidence Matrix:

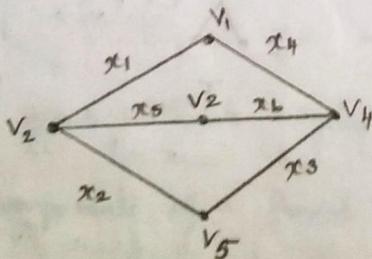
Let  $G = (V, X)$  be a  $(p, q)$  graph

Let  $V = \{v_1, v_2, \dots, v_p\}$   $X = \{x_1, x_2, \dots, x_q\}$

the  $p \times q$  matrix  $B = (b_{ij})$  where

$$b_{ij} = \begin{cases} 1 & \text{if } v_i \text{ is incident with } x_j \\ 0 & \text{otherwise} \end{cases}$$

$B$  is called the incidence matrix.



$$B = \begin{matrix} & \begin{matrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

(5x6) matrix.

① Show that the maximum number of edges in a simple graph is  $\frac{n(n-1)}{2}$

Proof:

Let  $G_1$  be a simple graph with  $n$  vertices.  
(no loop or multiple lines are allowed)

Let  $v_1$  be a vertex in  $G_1$ .

$v_1$  can be adjacent with at most  $n-1$  edges

Maximum

$$\text{Value of } \deg(v_1) = n-1$$



Maximum no. of edges in  $G_1$  is

$$\text{Sum of the degree} = \sum_{i=1}^n \deg(v_i) = \frac{(n-1) + (n-1) + \dots + (n-1)}{n \text{ times}}$$

$$= n(n-1)$$

$$2E = n(n-1) \quad (\text{where } E = \text{number of edges})$$

$$E = \frac{n(n-1)}{2}$$

$\therefore$  Maximum no. of edges in a simple graph is  $\frac{n(n-1)}{2}$

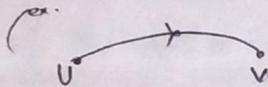
## Directed graph (digraph)

A directed graph  $D$  is a pair  $(V, A)$  where  $V$  is a vertex set &  $A$  is a arc set.

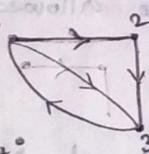
In particular  $A$  is a subset of  $V \times V - \{(x, x) \mid x \in V\}$

If  $(u, v) \in A$  then the arc  $(u, v)$  is said to have  $u$  as its initial vertex (tail) & Terminal vertex  $v$  (head)

Also the arc  $(u, v)$  is said to join  $u$  to  $v$ .



$$(u, v) \in A \subseteq V \times V - \{(x, x) \mid x \in V\}$$



$$V = \{1, 2, 3, 4\} \quad A = \{(1, 2), (2, 3), (1, 3), (3, 1), (3, 4), (4, 1)\}$$

$$D = \{V, A\}$$

### Indegree:

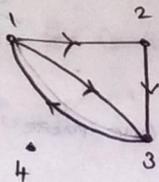
the indegree  $d^-(v)$  of a vertex  $v$  in a digraph  $D$  is the number of arcs having  $v$  as its terminal vertex.

Out degree  $d^+(v)$

$d^+(v)$  of  $v$  is the number of arcs having  $v$  as its initial vertex.

Degree pairs:

The ordered pair  $(d^+(v), d^-(v))$  is called the degree pair of  $v$



Degree pairs:

$$(d^+(1), d^-(1)) = (2, 1)$$

$$(d^+(2), d^-(2)) = (1, 1)$$

$$(d^+(3), d^-(3)) = (1, 2)$$

$$(d^+(4), d^-(4)) = (0, 0)$$

Theorem

If  $G$  has more than 2 vertices of odd degree then there can be no Euler path.

If  $G$  has exactly two vertices of odd degree then there can be Euler path.

Proof: Let  $G$  be a finite graph with exactly two vertices of odd degree call them  $u$  &  $v$ .

If  $G$  is connected, then the proof is trivial.

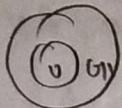
Thus we can assume that  $G$  is disconnected

Let  $G_1$  be the connected component of  $G$  such that

$$u \in G_1$$

Since  $G_1$  is a graph  $\rightarrow G_1$  must contain an even number of odd vertices.

Since  $\sum_{w \in V(G_1)} \deg(w) = 2 \cdot E(G_1)$   
 $\hookrightarrow$  edges in  $G_1$



$G_1$  thus there is atleast one more vertex of odd degree, we must have  $v \in G_1$

$\rightarrow$  this implies that there is a path from  $u$  to  $v$

$\rightarrow$  there is an Euler path in  $G_1$ .

Hence proved.

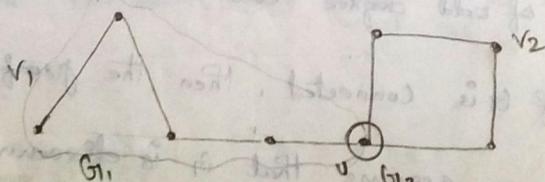
2) If  $G_1, G_2$  are connected subgraphs of  $G$  with atleast one vertex in common then  $G_1 \cup G_2$  is connected.

Proof:

Let  $G$  be a graph &  $G_1, G_2$  are connected subgraphs of  $G$  to prove  $G_1 \cup G_2$  is connected.

$$G_1 \cup G_2 = \{(v_1, v_2), (x_1, x_2)\}$$

where  $G_1 = (v_1, x_1)$   $G_2 = (v_2, x_2)$



Let  $v_1$  be a point in  $G_1$

$$v_1 \in V_1$$

$$\& v_2 \in V_2$$

$U$  be the common point between  $G_1$  &  $G_2$ .

Since  $G_1$  is connected, therefore we can find a  $V_1 - U$  path in  $G_1$ .

Since  $G_2$  is connected, therefore we can find a  $U - V_2$  path in  $G_2$ .

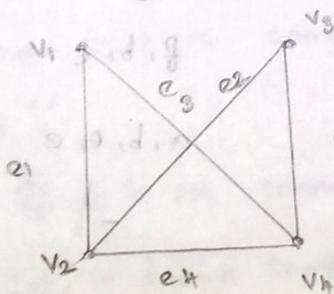
We can find a path from  $V_1 - V_2$  along  $U$  by joining  $V_1 - U$  &  $U - V_2$  path.

(Since  $V_1 \in V_1, V_2 \in V_2$ )

$\therefore G_1 \cup G_2$  is connected.

(because we can find a path between every pair of vertices in  $G_1 \cup G_2$ ).

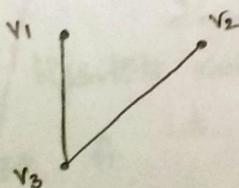
Let  $G_1$  be the following graph.



$G_1$  is a  $(5, 5)$  graph

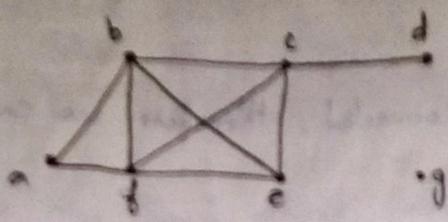
$G_1$  has 2 components

$G_1$  is disconnected



$v_5$

total no. the degree or neighbours hands of the vertices in the graph is:

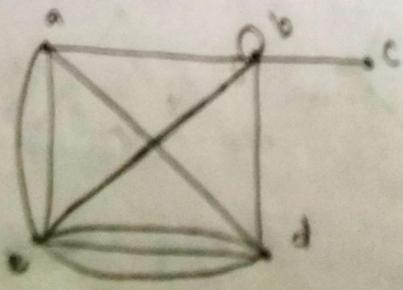


$$V = \{a, b, c, d, e, f, g\}$$

$$E = \{(a,b), (b,c), (c,d), (a,f), (b,f), (b,e), (c,e), (e,f), (e,g)\}$$

degrees & neighbours of vertices.

Vertex	degree	neighbours.
a	2	b, f
b	4	a, f, e, c
c	4	b, f, e, d
d	1	c
e	3	f, b, c
f	4	a, b, e, c
g	1	e



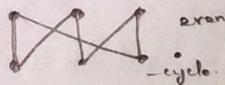
$$V = \{a, b, c, d, e\}$$

$$E = \{(a,b), (b,c), (c,d), (d,e), (e,b), (e,d), (b,d), (c,b), (d,e), (e,a)\}$$

Vertex	degree	neighbourhoods.
a	4	e, b
b	6	a, d, c
c	1	b
d	4	e, a, b
e	5	a, b, d.

Every component in a graph is bipartite then the graph is bipartite.

If  $G$  is connected, then it has <sup>only</sup> one component  
 we know that the component is bipartite  $\Rightarrow G$  is bipartite.



If  $G$  is not connected

Let  $G$  has  $n$  components  $\Leftarrow$  all are bipartite

$G_1, G_2, \dots, G_n$  are bipartite graphs.

which is bipartite. The proof is trivial.  
 ~~$G_1$  is bipartite  $\Leftarrow G_1$~~  has no odd cycles.

~~proof~~ A

Let  $G_1, G_2, \dots, G_n$  are bipartite  
 we need to show that  $G = G_1 \cup G_2 \dots G_n$  is bipartite

Let  $G_1, G_2, \dots, G_n$  are bipartite

We need to show that  $G = G_1 \cup G_2 \dots \cup G_n$  is bipartite

Since  $G_i$  is bipartite  $\Rightarrow G_i$  has no odd cycles.

$\forall i \in \{1, 2, \dots, n\}$

$\Rightarrow G = G_1 \cup G_2 \dots \cup G_n$  has no odd cycles

(because  $G_1 \cap G_2 = \emptyset$ )

$\Rightarrow G$  has no odd cycle

(Since we know that graph is bipartite iff it has no odd cycles).

$\Rightarrow G$  is bipartite



Clearly  $V_1 \cap V_2 = \emptyset \wedge V_1 \cup V_2 = V$

We have to prove  $V_1, V_2$  be a bipartition of  $V$ .

to prove every line joins a point of  $V_1$  to a point of  $V_2$

Suppose two points in  $V_1$  are adjacent,

Suppose  $U, V \in V_1$  are adjacent

let  $P$  be the shortest  $V_1 - U$  path of length  $m$

$Q$  be the shortest  $V_1 - V$  path of length  $n$ .

Since  $U, V \in V_1$ , both  $m, n$  are even.

Now, let  $U_i$  be the last common point between  $P \wedge Q$

then the  $V_1 - U_i$  path along  $P \wedge V_1 - U_i$  path along  $Q$  and both shortest paths  $\wedge$  have same length  $i$

Now  $U_i - U$  path along  $P$ , then line  $UV$  followed by the  $V - U_i$  path along  $Q$  form a cycle of length

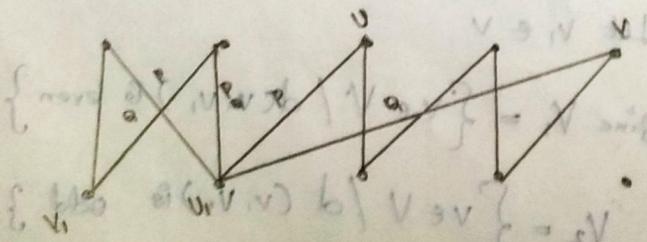
$$(m-i) + 1 + (n-i) = m+n - 2i + 1$$

which is odd  $\wedge$  this is a contradiction.

thus <sup>no</sup> two points of  $V_1$  are adjacent

$\rightarrow$  every line joins a point of  $V_1$  to a point of  $V_2$ .

$\Rightarrow$   $G$  is bipartite.



$V_1 - U$  path  $P$

$V_1 - V$  path  $Q$

$U_1$  is a last common point b/w  $P-Q$

$U_1 - V$  path along  $P$ ,  $UV$ ,  $V - U_1$  along  $Q$



$P = (x, y)$   
 $Q = (x, z)$   
 $U = (x, y)$

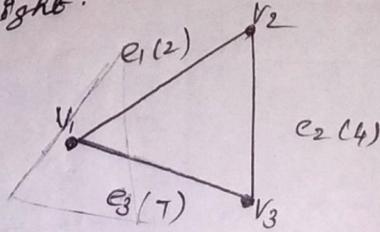
Weighted graph:

A graph  $G$  is called a weighted graph if there is a real number associated with each edge of  $G$ . The real number associated with each edge is called its weight.

$$w(e_1) = 2$$

$$w(e_2) = 4$$

$$w(e_3) = 7$$



Hypothesis:

Find mean, median, mode for the following data

40, 50, 55, 78, 58, 60, 73, 35, 43, 58

To find

mean, median, mode

$$\text{Mean} = \bar{x} = \frac{\sum_{i=1}^n x_i}{n}$$

where  $n$  = number of observations

$$\text{Median } M = \text{Size of } \left(\frac{n+1}{2}\right)^{\text{th}} \text{ item}$$

mode:  $Z$  = highest value

Here we have  $n = 10$

i, mean

$$= \frac{\sum_{i=1}^n x_i}{n} = \frac{40 + 50 + 55 + 78 + 58 + 60 + 73 + 35 + 43 + 58}{10}$$

$$= \frac{550}{10}$$

$$\bar{x} = 55 //$$

ii, Median:

$$M = \text{Size of } \left(\frac{n+1}{2}\right)^{\text{th}} \text{ item}$$

$$= \left(\frac{10+1}{2}\right)^{\text{th}} \text{ item}$$

Values	1	2	3	4	5	6	7	8	9	10
observed item	35	40	43	50	55	58	58	60	73	78

$$= \frac{11}{2} = 5.5$$

$$= \frac{5^{\text{th}} \text{ item} + 6^{\text{th}} \text{ item}}{2} = \frac{55 + 58}{2}$$

$$= 56.5$$

$$\text{Median} = 56.5$$

iii, Mode.

$$\text{Mode} = \text{highest value} = 78.$$

2) Find mean, median, mode

$x$	75	100	120	150	100
$f(x)=y$	5	12	20	14	9

$$\text{Mean} = \bar{x} = \frac{\sum_{i=1}^n f_i x_i}{N}$$

$$\text{where, } N = \sum_{i=1}^n f_i$$

$x_i$	$f_i$	$f_i x_i$
75	5	375
100	12	1200
120	20	2400
150	14	2100
100	9	900

$$N = \sum_{i=1}^n f_i = 60 \quad \sum_{i=1}^n f_i x_i = 6975$$

$$\text{Mean} = \bar{x} = \frac{6975}{60}$$

$$= 116.25$$

ii, Median

$$M = \text{Size of } \left( \frac{N+1}{2} \right)^{\text{th}} \text{ item}$$

$$\text{where } N = \sum_{i=1}^n f_i$$

$x_i$	$f_i$	C.f
75	5	5
100	12	17
120	20	37
150	14	51
100	9	60

Cumulative frequency.

$$\sum f_i = 60$$

$$\text{Median } M = \left( \frac{N+1}{2} \right)^{\text{th}} \text{ item}$$

$$= \left( \frac{60+1}{2} \right)^{\text{th}} \text{ item}$$

$$= 30.5$$

$$\text{Median } M = 120.$$

iii, Mode:

$x_i$	$f_i$
75	5
100	12
120	20
150	14
100	9

Highest value in frequency = 20

Corresponding x value = 120

∴ Mode = 120

$\sum_{i=1}^n f_i = N$

$x_i$	$f_i$	$f_i$
100	4	4
120	11	15
130	20	35
140	12	47
150	2	49

Median  $M = \left( \frac{N+1}{2} \right)^{th}$  value

$\left( \frac{49+1}{2} \right)^{th} = 25^{th}$

$\therefore 25 =$

Median  $M = 120$

(iii) Mode

$x_i$	$f_i$
100	4
120	11
130	20
140	12
150	2

# Standard Deviation.

$$S.D = \sigma = \sqrt{\frac{\sum (x - \bar{x})^2}{n}}$$

$$\text{Variance} = \frac{\sum (x - \bar{x})^2}{n}$$

$$S.D = \sqrt{\text{Variance}}$$

where  $\sum (x - \bar{x})^2$  is the sum of the square of deviations from Arithmetic mean.

Coefficient of Standard deviation

$$= \frac{\sigma}{\bar{x}}$$

Coefficient of Variation (or) Coefficient of Variability

$$C.V = \frac{\sigma}{\bar{x}} \times 100$$

Calculate the range & standard deviation, coefficient of variation for the following observations.

50 55 57 49 54 61 64 59 59 56

Range = Highest value - lowest value

$$= 64 - 49$$

$$= 15$$

$$\text{Mean} = \bar{x} = \frac{\sum x_i}{n} = \frac{50 + 55 + 49 + 57 + 54 + 61 + 64 + 59 + 59 + 56}{10}$$

$$= \frac{550}{10} = 55$$

# Calculation of standard deviation.

$x$	$x - \bar{x}$ $x - 55$	$(x - \bar{x})^2$ $(x - 55)^2$
50	-5	25
55	0	0
57	2	4
49	-6	36
54	-1	1
61	6	36
64	9	81
59	4	16
59	4	16
64	9	81

$$\begin{aligned} \Sigma(x - \bar{x}) &= \Sigma(x - \bar{x})^2 \\ &= 4 &= 216 \end{aligned}$$

$$\begin{aligned} \text{Variance} &= \frac{\Sigma(x - \bar{x})^2}{n} \\ &= \frac{\Sigma(x - 55)^2}{10} = \frac{216}{10} = 21.6 \end{aligned}$$

$$\text{Standard Deviation} = \sqrt{\text{Variance}}$$

$$= \sqrt{\frac{\Sigma(x - \bar{x})^2}{n}} = \sqrt{\frac{216}{10}} = \sqrt{21.6}$$

$$\text{Standard deviation} = s = \sqrt{\frac{\sum (x - \bar{x})^2}{n} - \left(\frac{\sum (x - \bar{x})}{n}\right)^2}$$

$$= \sqrt{\frac{216}{10} - \left(\frac{14}{10}\right)^2}$$

$$= \sqrt{21.6 - (1.4)^2}$$

$$= \sqrt{21.6 - 1.96}$$

$$= \sqrt{19.64}$$

$$= 4.43$$

$$\begin{aligned} \bar{x} &= \bar{x} + \frac{\sum (x - \bar{x})}{n} \\ \text{C.P.S.} \quad &= 55 + \frac{14}{10} = 55 + 1.4 = 56.4 \end{aligned}$$

$$\text{C.V} = \frac{s}{\bar{x}} \times 100 = \frac{4.43}{56.4} \times 100$$

$$= 7.85\%$$

Find the S.D for the following data

45, 36, 40, 37, 39, 42, 45, 35, 40, 39

$$n = 10$$

$$\text{Arithmetic mean } \bar{x} = \frac{\sum (x_i)}{n} = \frac{45 + 36 + 40 + 37 + 39 + 42 + 45 + 35 + 40 + 39}{10}$$

$$= \frac{398}{10} = 39.8 \approx 40$$

$$\bar{x} = 40.$$

$x$	$d = (x - \bar{x})$ $= (x - 40)$	$d^2 = (x - \bar{x})^2$ $= (x - 40)^2$
45	5	25
36	-4	16
40	0	0
37	-3	9
39	-1	1
42	2	4
45	5	25
35	-5	25
40	0	0
39	-1	1

$$\sum (x - \bar{x}) = -2$$

$$\sum (x - \bar{x})^2 = 106$$

$$\text{Standard deviation} = s = \sqrt{\frac{\sum (x - \bar{x})^2}{n} - \left(\frac{\sum (x - \bar{x})}{n}\right)^2}$$

$$= \sqrt{\frac{\sum d^2}{n} - \left(\frac{\sum d}{n}\right)^2}$$

$$= \sqrt{\frac{106}{10} - \left(\frac{-2}{10}\right)^2}$$

$$\frac{-14}{10} + \frac{12}{10} = \frac{-2}{10}$$

$$= \sqrt{10.6 - 0.04} = \sqrt{10.56}$$

$$= 3.24961$$

$$= 3.25$$

$$\bar{x} = \bar{x} + \frac{\sum d}{n} = \bar{x} + \frac{\sum (x - \bar{x})}{n}$$

$$= 40 + \left( \frac{-2}{10} \right)$$

$$= 40 - \frac{1}{5} = \frac{200 - 1}{5} = \frac{199}{5}$$

$$= 39.8 \approx 40$$

$$\bar{x} = 40$$

$$C.R = \frac{r}{x} \times 100$$

$$= \frac{3.25}{39.8} \times 100$$

$$= 8.16582\%$$

Correlation Coefficient =

$$r = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2} \sqrt{\sum (y - \bar{y})^2}}$$

$$= \frac{\sum xy}{\sqrt{\sum x^2} \sqrt{\sum y^2}}$$

$$= \frac{\sum xy}{\sqrt{\sum x^2} \sqrt{\sum y^2}}$$

Calculate the coefficient of correlation b/w x and y from the following table

x	1	3	5	8	9	10
y	3	4	8	10	12	14

$$n = 6$$

$$\bar{x} = \frac{\sum x}{n} = \frac{1+3+5+8+9+10}{6}$$

$$= \frac{36}{6} = 6$$

$$\bar{x} = 6$$

$$\bar{y} = \frac{\sum y}{n} = \frac{3+4+8+10+12+11}{6}$$

$$= \frac{48}{6} = 8$$

$$\bar{y} = 8$$

$x$	$y$	$(x - \bar{x})$ $= (x - 6)$	$(y - \bar{y})$ $= (y - 8)$	$(x - \bar{x})^2$	$(y - \bar{y})^2$	$(x - \bar{x})(y - \bar{y})$
1	3	-5	-5	25	25	25
3	4	-3	-4	9	16	12
5	8	-1	0	1	0	0
8	10	2	2	4	4	4
9	12	3	4	9	16	12
10	11	4	3	16	9	12
$\sum x = 36$	$\sum y = 48$	$\sum (x - \bar{x}) = 0$	$\sum (y - \bar{y}) = 0$	$\sum (x - \bar{x})^2 = 64$	$\sum (y - \bar{y})^2 = 70$	$\sum (x - \bar{x})(y - \bar{y}) = 65$

Correlation  
Coefficient

$$r = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2} \sqrt{\sum (y - \bar{y})^2}} = \frac{65}{\sqrt{64} \sqrt{70}} = 0.97$$

Calculate the coefficient of correlation  $r$  and  $x$  and  $y$  from the following table:

x	1	2	3	4	5	6	7
y	2	4	5	3	8	6	7

Correlation

Coefficient

$$= \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2} \sqrt{\sum (y - \bar{y})^2}}$$

$$n = 7$$

$$\bar{x} = \frac{\sum x}{n} = \frac{1 + 2 + 3 + 4 + 5 + 6 + 7}{7} = \frac{28}{7} = 4$$

$$\bar{x} = 4$$

$$\bar{y} = \frac{\sum y}{n} = \frac{2 + 4 + 5 + 3 + 8 + 6 + 7}{7} = \frac{35}{7} = 5$$

$$\bar{y} = 5$$

x	y	$(x - \bar{x})$ $= x - 4$	$(y - \bar{y})$ $= (y - 5)$	$(x - \bar{x})^2$	$(y - \bar{y})^2$
1	2	-3	-3	9	9
2	4	-2	-1	4	1
3	5	-1	0	1	0
4	3	0	-2	0	4
5	8	1	3	1	9
6	6	2	1	4	1
7	7	3	2	9	4

$\Sigma x$	$\Sigma y$	$\Sigma(x-\bar{x})$	$\Sigma(y-\bar{y})$	$\Sigma(x-\bar{x})^2$	$\Sigma(y-\bar{y})^2$	$\Sigma(x-\bar{x})(y-\bar{y})$
$= 28$	$= 35$	$= 0$	$= 0$	$= 28$	$= 28$	$= 22$

Correlation coefficient  $r = \frac{\Sigma(x-\bar{x})(y-\bar{y})}{\sqrt{\Sigma(x-\bar{x})^2} \sqrt{\Sigma(y-\bar{y})^2}}$

$$= \frac{22}{\sqrt{28} \sqrt{28}}$$

$$= 0.79$$

(1) Calculate the coefficient of correlation b/w x and y from the following table.

x	5	10	5	11	12	4	3	2	7	1
y	1	6	2	8	5	1	4	6	5	2

$$r = \frac{\Sigma xy - \Sigma x \cdot \Sigma y}{\sqrt{\Sigma x^2 - \left(\frac{\Sigma x}{N}\right)^2} \sqrt{\Sigma y^2 - \left(\frac{\Sigma y}{N}\right)^2}}$$

$n = 10$

$$= \frac{288 - (60 \times 40)/10}{\sqrt{494 - \frac{(60)^2}{10}} \sqrt{212 - \frac{(40)^2}{10}}}$$

$$= \frac{288 - 240}{\sqrt{494 - 360} \sqrt{212 - 160}}$$

$$= \frac{48}{\sqrt{134} \times \sqrt{52}}$$

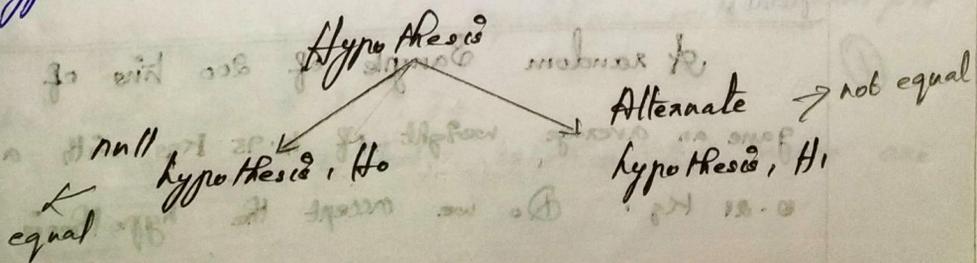
$$= 0.58$$

83.475

$x$	$y$	$xy$	$x^2$	$y^2$
5	1	5	25	1
10	6	60	100	36
5	2	10	25	4
11	8	88	121	64
12	5	60	144	25
4	1	4	16	1
3	4	12	9	16
2	6	12	4	36
7	5	35	49	25
1	2	2	1	4
$\Sigma x$ = 60	$\Sigma y$ = 40	$\Sigma xy$ = 258	$\Sigma x^2$ = 494	$\Sigma y^2$ = 212

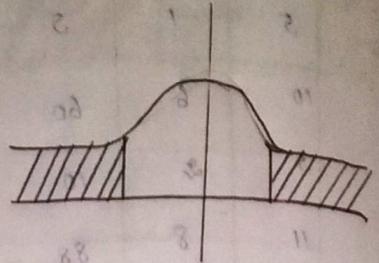
## Hypothesis Testing:

A test of hypothesis is a two action decision problem after the experimental sample values have been obtained, the two actions being the acceptance or rejection of the hypothesis under consideration.



## Critical Region

### Rejection region



one tail test

two tail test

Errors

$$H_0: \mu = \mu_0$$

Type I,  $H_0$  true,  $H_1$  false

$$H_1: \mu \neq \mu_0$$

Type II

$H_0$  false,  $H_1$  true

$$H_0: \mu = \mu_0$$

$$H_1: \mu \leq \mu_0$$

less than

## level of significance ( $\alpha$ )

the probability of type I error is known as the level of significance ( $\alpha$ ) size of critical region.

power of the test:

$1 - \beta$  is called the power functions of the test hypothesis  $H_0$  against the alternate hypothesis  $H_1$ .

the value of the power function at a parameter point is called the power of the test at that point.

① A random sample of 200 bins of coconuts gave an average weight of 4.95 kgs with a S.D of 0.21 kg. Do we accept the hypothesis of net

weight 5 kgs per tin at 1% level?

Sample Size = 200

Sample mean = 4.95 kg

Sample S.D = 0.21 kg

Population mean  $\mu = 5$  kg

$$Z = \frac{\bar{x} - \mu}{S/\sqrt{n}}$$

We apply Z test

the test statistic is  $Z = \frac{\bar{x} - \mu}{S/\sqrt{n}}$

$$Z = \frac{4.95 - 5}{0.21/\sqrt{200}} = \frac{-0.05 \times \sqrt{200}}{0.21}$$

$$= -3.37$$

$$|Z| = 3.37$$

At 1% level of significance the tabulated value of Z is 2.58

Our calculated value of  $|Z|$  is greater than the tabulated value of Z.

Conclusion:

$H_0$  is rejected at 1% level. ~~the~~ therefore the next net weight of a tin is not equal to 5 kg.

---

Test for equality of two means:

Suppose two independent large samples of sizes  $n_1, n_2$  drawn from two populations with means  $\mu_1, \mu_2$  and S.D  $\sigma_1, \sigma_2$ .

We want to test whether the means are equal.

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 \neq \mu_2 \quad (\text{Two tailed test})$$

$$Z = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

(1)

	place A	place B
mean height	68.50	68.58
SD of heights	2.5	3.0
Sample size	1200	1500

Test at 5% level that the mean height is the same for adults in 2 places (table values of  $Z$  at 5% level for two tailed test is 1.96)

mean of 1<sup>st</sup> sample  $\bar{x}_1 = 68.50$

S.D of 1<sup>st</sup> sample  $s_1 = 2.5$

Sample size of 1<sup>st</sup> sample }  $n_1 = 1200$

mean of 2<sup>nd</sup> sample  $\bar{x}_2 = 68.58$

S.D of 2<sup>nd</sup> sample  $s_2 = 3.0$

Sample size of 2<sup>nd</sup> sample }  $n_2 = 1500$

$H_0: \mu_1 = \mu_2$  (mean height is the same in the two places)

$H_1: \mu_1 \neq \mu_2$

the test statistic  $Z = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$

$$= \frac{68.5 - 68.56}{\sqrt{\frac{(2.5)^2}{1200} + \frac{(3.0)^2}{1500}}}$$

$$= \frac{-0.06}{\sqrt{0.00052 + 0.006}} = \frac{-0.06}{0.1058} = -0.76$$

$$\therefore |z| = 0.76$$

Conclusion:

$H_0$  is accepted at <sup>5%</sup>5% level since the calculated value for  $z$  is less than the table value of  $z$ . Hence the mean height is same.

① Electric bulbs manufactured by x.y. Companies gave the following results.

	x y company	y Company.
No. of bulbs used	100	100 (using steel envy of the diff. thro)
Mean life in hrs	1300	1248 (1% level sig. makes)
S.D in hrs	82	93 (Question)

$$n_1 = 100$$

$$n_2 = 100$$

$$\bar{x}_1 = 1300$$

$$\bar{x}_2 = 1248$$

$$s_1 = 82$$

$$s_2 = 93$$

$H_0: \mu_1 = \mu_2$  (There is no significant difference between mean life of the two makes.)

$$H_1: \mu_1 \neq \mu_2$$

$$\text{Test statistic is } z = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

54.1.96  
 1.1.2.53

$$= \frac{1300 - 1248}{\sqrt{\frac{82^2}{100} + \frac{93^2}{100}}}$$

$$= 52$$

$$67.24 + 86.49$$

Table value of  $z$  at 1% level = 2.58

$H_0$  is rejected at 1% level of significance  
 Since the calculated value of  $z$  is greater than the table value of  $z$ .

Therefore there is significant difference in the mean life of two makes.

### Test for equality of two S.D

$S_1, S_2$  - SD of the samples of size  $n_1, n_2$  respectively from two populations with SD  $\sigma_1, \sigma_2$  respectively.

$$H_0: \sigma_1 = \sigma_2$$

$$H_1: \sigma_1 \neq \sigma_2$$

The test statistic is  $z =$

$$z = \frac{S_1 - S_2}{\sqrt{\frac{S_1^2}{2n_1} + \frac{S_2^2}{2n_2}}}$$

① In two random samples of sizes 150, 250 the S.D are calculated as 15.8, 18.8. Can we conclude that the samples are drawn from the populations with same S.D?

Soln:

$$n_1 = 150 \quad n_2 = 250$$

$$s_1 = 15.3 \quad s_2 = 13.8$$

$H_0: \sigma_1 = \sigma_2$  (The samples belong to the populations with same S.D.)

$H_1: \sigma_1 \neq \sigma_2$  (The samples belong to populations with diff S.D.)

$$\text{Test statistic } z = \frac{s_1 - s_2}{\sqrt{\frac{s_1^2}{2n_1} + \frac{s_2^2}{2n_2}}}$$

$$= \frac{15.3 - 13.8}{\sqrt{\frac{(15.3)^2}{300} + \frac{(13.8)^2}{500}}}$$

$$= \frac{1.5}{1.0770} = 1.34$$

Since  $|z| < 1.96$ ,  $H_0$  is accepted at 5% level of significance. Hence, the samples belong to the populations with the same S.D.

# Hypothesis testing

Large Sample

Z test

Z, F

$n > 30$

Small Samples

t-test

t-distributions

$n < 30$

Small Sample:

Sample mean  $\bar{x}$

Sample SD  $s$

Sample Var  $s^2 = \frac{\sum (x - \bar{x})^2}{n-1}$

Population mean  $\mu$

Population SD  $= \sigma$

Population Var  $= \sigma^2$

t statistic  $t = \frac{\bar{x} - \mu}{SE(\bar{x})}$

$SE(\bar{x}) = \frac{s}{\sqrt{n-1}}$  (if sample SD is given)

$SE(\bar{x}) = \frac{\sigma}{\sqrt{n}}$  (if population SD is given)

degrees of freedom  $= v = n-1$

Type I:

Test of hypothesis of a single mean

$H_0: \mu = \text{a specified value}$

or

$\mu > a$

$\mu < a$

test statistic  $t = \frac{\bar{x} - \mu}{\frac{s}{\sqrt{n-1}}}$  (or)  $t = \frac{\bar{x} - \mu}{\frac{\sigma}{\sqrt{n}}}$

① A Soap manufacturing company was distributing a particular brand through a large number of retail shops. Before heavy advertisement campaign, the mean sales per shop was 140 dozens. After the campaign, a sample of 26 shops was taken, and the mean sales was found to be 147 dozens. with SD 16. Can you consider the advertisements effective at a 5% level of significance.

$$H_0: \mu = 140$$

$$H_1: \mu > 140 \quad (\text{one tailed test})$$

$$n = 26, \quad \bar{x} = 147, \quad s = 16$$

$$\text{test statistic } t = \frac{\bar{x} - \mu}{\frac{s}{\sqrt{n-1}}}$$

$$= \frac{147 - 140}{\frac{16}{\sqrt{26-1}}} = \frac{7}{\frac{16}{\sqrt{25}}} = \frac{7 \times 5}{16}$$

$$= \frac{7 \times 5}{16} = 2.19$$

level of significance  $\alpha = 0.05$

Critical value of  $t$  at 0.05,  $v = 25$  is 1.708

$$t_{\alpha, 25} = 1.708$$

It is  $t > t_{0.05, 25}$ ,  $H_0$  is rejected.

$H_1$  is accepted.

Hence the advertisement is effective

( $\mu > 140$  is accepted)

Type II:

Difference of two means (Small samples)

two independent samples of sizes  $n_1, n_2$  with mean  $\bar{x}_1, \bar{x}_2$  & the sample variance  $S_1^2$  &  $S_2^2$  Test

the diff. b/w the means of two samples is

significant or not

$$t = \frac{\bar{x}_1 - \bar{x}_2}{S \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}}$$

Caps

where,  $S = \frac{\sum (x_1 - \bar{x}_1)^2 + \sum (x_2 - \bar{x}_2)^2}{n_1 + n_2 - 2}$

$$n_1 + n_2 - 2 = 11 + 11 - 2 = 20$$

deg of freedom  $v = n_1 + n_2 - 2$

① Two independent samples of 8 & 7 items respectively had the following values.

Sample I	9	13	11	11	15	9	12	14
Sample II	10	12	10	14	9	8	10	

Is the diff b/w the mean of the samples significant?

let  $H_0: \mu_1 = \mu_2$

(Two sample means are equal)

$H_1: \mu_1 \neq \mu_2$  (Two sample means are not equal)

test statistic  $t = \frac{\bar{x}_1 - \bar{x}_2}{S \sqrt{\frac{1}{n_1} + \frac{1}{n_2}}}$

$x_1$	$x_1 - \bar{x}$ $x_1 - 11$	$(x_1 - \bar{x}_1)^2$	$\bar{x}_2$	$(x_2 - \bar{x}_2)$ $x_2 - 10$	$(x_2 - \bar{x}_2)^2$
9	-2	4	10	0	0
13	2	4	12	2	4
11	0	0	10	0	0
11	0	0	14	4	16
15	4	16	9	-1	1
9	-2	4	8	-2	4
12	1	1	10	0	0
14	3	9			
	$\Sigma d_1$ or $\Sigma x_1 - \bar{x}$ = 6	$\Sigma d_1^2$ or $\Sigma (x_1 - \bar{x}_1)^2$ = 38		$\Sigma d_2$ or $\Sigma x_2 - \bar{x}_2$ = 3	$\Sigma d_2^2$ or $\Sigma (x_2 - \bar{x}_2)^2$ = 25

$$\bar{x}_1 = A + \frac{\Sigma d_1}{n} \quad \text{or} \quad A + \frac{\Sigma x_1 - \bar{x}_1}{n}$$

$$\bar{x}_1 = 11 + \frac{6}{8} = \frac{88+6}{8} = \frac{94}{8} = 11.75$$

$$\bar{x}_1 = 11.75$$

$$\bar{x}_2 = 10 + \frac{\Sigma x_2 - \bar{x}_2}{n} = 10 + \frac{3}{7} = \frac{70+3}{7} = \frac{73}{7}$$

$$\bar{x}_2 = 10.42$$

$$\begin{aligned} \Sigma (x_1 - \bar{x}_1)^2 &= \Sigma (x_1 - \bar{x})^2 - \frac{(\Sigma d_1)^2}{n_1} \\ &= \frac{38}{7} - \frac{36}{8} \\ &= \frac{304-36}{8} = \frac{268}{8} = 33.5 \end{aligned}$$

$$\begin{aligned} \Sigma (x_2 - \bar{x}_2)^2 &= \Sigma (x_2 - \bar{x}_2)^2 - \frac{(\Sigma d_2)^2}{n_2} \\ &= 25 - \frac{9}{7} = \frac{175-9}{7} = \frac{166}{7} = 23.71 \end{aligned}$$

$$\Sigma (x_2 - \bar{x}_2)^2 = 23.71$$

Two random samples of size 8 and 11, drawn from two normal populations, are characterised as follows.

	Sample size	Sample of observations	Sum of squares of observations
Sample I	8	9.6	61.52
Sample II	11	16.5	73.26

You are to decide if two populations can be taken to have the same variance.

Let  $x, y$  be the observation for two samples.

$$H_0: \sigma_1^2 = \sigma_2^2 \quad / \quad H_1: \mu_1 = \mu_2$$

$$H_1: \mu_1 \neq \mu_2$$

$$S_1^2 = \frac{\sum x^2}{n} - \left(\frac{\sum x}{n}\right)^2$$

$$= \frac{61.52}{8} - \left(\frac{9.6}{8}\right)^2$$

$$= 7.69 - (1.2)^2 = 6.285$$

$$S_1^2 = 6.285$$

$$S_2^2 = \frac{\sum y^2}{n} - \left(\frac{\sum y}{n}\right)^2$$

$$= \frac{73.26}{11} - \left(\frac{16.5}{11}\right)^2$$

$$= 6.66 - 2.25$$

$$= 4.41$$

$$\hat{\sigma}_1^2 \mu_1 = \frac{n_1 S_1^2}{n_1 - 1} = \frac{8(6.285)}{8-1} = \frac{50}{7} = 7.143$$

$$= \frac{12.82^2}{12-1} = \frac{11(A.41)}{10} = \frac{48.57}{10} = 4.851$$

$$= \frac{\frac{11(A.41)}{12}}{\frac{48.57}{12-1}} = \frac{7.143}{4.851} = 1.472$$

the table value of  $F$  at 5% level for degree of freedom (7, 10) is 3.14

Conclusion: Since computed value of  $F <$  table value of  $F$ ,  $H_0$  is accepted at 5% level.

$\therefore$  Variance of two populations may be same.

Random samples are drawn from two populations and the following results are obtained.

Sample x:	16	17	18	19	20	21	22	24	26	27		
Sample y:	19	22	23	25	26	28	29	30	31	32	35	36

find the variance of two populations and test whether the two samples have same variance.

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 \neq \mu_2$$

$x$	$(x - \bar{x})$ $= x - 21$	$(x - \bar{x})^2$ $= (x - 21)^2$	$y$	$(y - \bar{y})$ $= y - 28$	$(y - \bar{y})^2$ $= (y - 28)^2$
16	-5	25	19	-9	81
17	-4	16	22	-6	36
18	-3	9	23	-5	25
19	-2	4	25	-3	9
20	-1	1	26	-2	4
21	0	0	28	0	0
22	1	1	29	1	1
24	3	9	30	2	4
26	5	25	31	3	9
27	6	36	35	7	49
			36	8	64
$\Sigma x = 210$		$\Sigma (x - \bar{x})^2$ $= 126$	$\Sigma y =$ 336		$\Sigma (y - \bar{y})^2$ $= 278$

$$\bar{x} = \frac{\Sigma x}{n} = \frac{210}{10} = 21$$

$$\bar{y} = \frac{\Sigma y}{n} = \frac{336}{12} = 28$$

$$s_1^2 = \frac{\Sigma (x_i - \bar{x})^2}{n_1 - 1} = \frac{126}{9} = 14$$

$$s_2^2 = \frac{\Sigma (y_i - \bar{y})^2}{n_2 - 1} = \frac{278}{11} = 25.27$$

$$\text{test statistic } F = \frac{s_1^2}{s_2^2} = \frac{27.09}{14} = 1.94$$

The tabled value of  $F$  at 5% level for degrees of freedom (14, 9) is 2.6458.

Conclusion:

The computed value of  $F$  < table value of  $F$ ,  $H_0$  is accepted. Since, the two samples have same variance.

Chi Square Test ( $\chi^2$  test) goodness of fit

$O_i$  = observed frequency of  $i^{\text{th}}$  event

$E_i$  = Expected frequency of  $i^{\text{th}}$  event

$$\text{test statistic } \chi^2 = \sum_{i=1}^n \left( \frac{O_i - E_i}{E_i} \right)^2$$

Degrees of freedom

$V = n - 1$  where  $n$  is a number of items in the series.

for binomial distribution  $V = n - 1$

poisson distribution  $V = n - 2$

normal  $V = n - 3$

① A die is thrown 264 times with the following results.

No. appeared on the die	1	2	3	4	5	6
frequency	40	32	28	58	54	60

Show that die is biased.

$H_0$ : the die is <sup>not</sup> biased

$H_1$ : the die is <sup>not</sup> biased

$$\text{test statistic } \chi^2 = \sum_{i=1}^n \frac{(O_i - E_i)^2}{E_i}$$

$$\text{Expected (E) frequency} = \frac{264}{6} = 44.$$

No. of the die	1	2	3	4	5	6
Observed frequency $O_i$	40	32	28	58	54	60
Expected freq $E_i$	44	44	44	44	44	44

$$\text{test statistic} = \frac{(40-44)^2}{44} + \frac{(32-44)^2}{44} + \frac{(28-44)^2}{44} + \frac{(58-44)^2}{44} + \frac{(54-44)^2}{44} + \frac{(60-44)^2}{44}$$

$$= \frac{1}{44} [16 + 144 + 256 + 196 + 100 + 250]$$

$$\text{Level of significance } \alpha = 0.05$$

Critical value of  $\chi^2$  at 0.05 for degree of freedom 5 = 11.07

Conclusion: Calculated value is greater than the table

value of  $\chi^2$

$\therefore H_0$  is rejected

$H_1$  is accepted

$\therefore$  Hence, the die is biased.

Regression Equation

(1) The following table gives the no. of aircraft accidents that occurred during the various days of the week.

Test whether the accidents are uniformly distributed over the week.

Days	Mon	Tues	Wed	Thurs	Fri	Sat	Total
no. of accidents	14	18	12	11	15	14	84

Let  $H_0$ : the accidents are uniformly distributed over the week.

$H_1$ : the accidents are not uniformly distributed over the week.

$$\chi^2 = \sum_{i=1}^n \frac{(O_i - E_i)^2}{E_i}$$

expected frequency accidents on each day.

Days

No. of accidents

$$\chi^2 = \frac{(14-14)^2}{14} + \frac{(18-14)^2}{14} + \frac{(12-14)^2}{14} + \frac{(11-14)^2}{14}$$

$$= \frac{(14-14)^2}{14} + \dots$$

$$= 2.14$$

$$P = 0.05$$

Critical value of  $\chi^2$  at 0.05 for the  
degree of freedom  $n-1$

$$6-1 = 5$$

$$11.071$$

$$\chi^2 = 0.65, 6$$

Conclusion:

So,  $H_0$  is rejected so calculated value greater than the  $\chi^2$

~~Chi 2 test~~  
~~Correlation~~  
~~Linear regression~~  
Case Sample - 10  
Exam #