Date : 18-5-22

Z mod 2

↳ set of Integers

$35 \equiv 1 \text{ Mod } 2$

$36 \equiv 0 \text{ Mod } 2$

$37 \equiv 1 \text{ Mod } 2$

$\boxed{Z_n = \{0, \ldots n-1\}}$ Z_n ~~mod~~ $Z \bmod n$

$Z_2 = \{0, 1\}$

$Z_3 = \{0, 1, 2\}$

Modular addition

$3 \text{Mod} 5 + 4 \text{Mod} 5 = (3+4) \text{Mod} 5 = 7 \text{Mod} 5 = 2 \text{Mod} 5$

- Addition is closed under modular
- Closer property

→ Modular subtraction

$3 \text{Mod} 7 - 6 \text{Mod} 7 = -3 \text{Mod} 7 = 4 \text{Mod} 7$

$7 \overline{)-3}$ (1) $\quad 7$ (4)

→ Modular Multiplication

$4 \text{Mod} 7 \times 5 \text{Mod} 7 = 20 \text{Mod} 7 = 6 \text{Mod} 7$

$5 \text{Mod} 7 \times 6 \text{Mod} 7 = 2 \text{Mod} 7$

$7 \overline{)20}$ (2) $\quad 14$ (6)

Encryption

CAT

$Z_{26} = \{0, \ldots 25\}$

$C = 2, A, 0, T = 19, \quad k = 9$

$y_1 = x_1 + k \text{ Mod } 26 = 2 + 9 \text{Mod} 26 = 11 \text{Mod} 26$

$y_2 = x_2 + k \text{Mod } 26 = 0 + 9 \text{Mod} 26 = 9 \text{Mod} 26$

$y_3 = x_3 + k \text{Mod } 26 = 19 + 9 \text{Mod} 26 = 28 \text{Mod} 26 = 2 \text{Mod} 26$

CAT → LJC

Decryption

$L = 11$, $J = 9$, $C = 2$

$x_1 = y_1 - k \bmod 26 = 11 - 9 \bmod 26 = 2 \bmod 26 = C$

$x_2 = y_2 - k \bmod 26 = 9 - 9 \bmod 26 = 0 \bmod 26 = A$

$x_3 = y_3 - k \bmod 26 = 2 - 9 \bmod 26 = -7 \bmod 26 = 19 \bmod 26 = T$

LJC → CAT

→ Modular division

2 Aditive 2 Mod 7

$(2+5) \bmod 7 = 7 \bmod 7 = 0 \bmod 7$

- Find additive inverse of 3

$(3+4) \bmod 7 = 7 \bmod 7 = 0 \bmod 7$

- Modular multiplicative Inverse

$8 = a \Rightarrow 8 \times \frac{1}{8} \Rightarrow 8 \times 8^{-1} = 1$, where $8^{-1} = a^{-1}$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$a \in Z_6$

$a^{-1} \bmod$ exists iff $GCD(a, 6) = 1$

- $2^{-1} \bmod$ does not exist
- $5^{-1} \bmod 6$ exists

GCD

- Greatest Common divisor

12, 6

$1 \times 2 \times (2 \times 3)$, $1 \times (2 \times 3)$

GCD = 3

9, 14

$(1 \times) 3 \times 3$, $(1 \times) 7 \times 2$

GCD = 1

If GCD is 1 then it exists

If n is prime number then its exist

1, 2

1, 2, 3, 6

Date: 19-5-22

Invertable = Inverse exist

Non-invertable = Inverse does not exist

Relatively Prime:

Two integers are relatively Prime iff $GCD(a, b) = 1$

Example:

GCD (9, 14) = 1 , GCD (9, 25) = 1

Eucleden Algorithm

(85, 34)

① 85 = 34 (2) + 17

② 34 = (2) 17 + 0 Algorith is terminated

③ GCD of (85, 34) = 17

(1331, 1001)

1331 = 1001 (1) + 330

1001 = 330 (3) + 11

330 = 11 (30) + 0

GCD = 11

$1331x + 1001y = 11$

$11 = 1001 - 330(3)$

$11 = 1001 - [1331 - 1001]3$

$11 = 1001 - 1331(3) + 1001(3)$

$11 = 1001(4) + 1331(-3)$

(9888, 6060)

9888 = 6060 (1) + 3828

6060 = 3828 (1) + 2232

3828 = 2232 (1) + 1596

2232 = 1596 (1) + 636

1596 = 636 (2) + 324

636 = 324 (1) + 312

324 = 312 (1) + 12

312 = 12 (26) + 0

5^{-1} Mod 26 $\Rightarrow$ $26 = 5(5)+1 \Rightarrow 1 = 26 - 5(5) \Rightarrow 1 = 26 + 5(-5)$

-5 Mod 26

$26 = 5(5) + 1$

$(213, 117)$

$213 = 117 + 96$

$117 = 96(1) + 21$

$96 = 21(4) + 12$

$21 = 9(1) + 3$

$9 = 3(3) + 0$

GCD $= 3$

$213x + 117y = 3$

$3 = 12 - 9$

$= 12 - [21 - 12]$

$= 12 - 21 + 12$

$3 = 12(2) - 21$

$= [96 - 21(4)](2) - 21$

$= 96(2) - 21(8) - 21$

$= 96(2) - 21(9)$

$= 96(2) - [117 - 96](9)$

$= 96(11) - 117(9)$

$= [213 - 117](11) - 117(9)$

$3 = 213(11) - 117(11) - 117(9)$

$= 213(11) - 117(20)$

$3 = 213(11) + 117(-20)$

$252x + 198y = 18$

~~$18 = 252 - 198$~~

$252 = 198(1) + 54$

$198 = 54(3) + 36$

$54 = 36(1) + 18$

$36 = 18(2) + 0$

GCD $= 18$

Date : 31-5-22

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

9^{-1} Mod 10 exists

$10 = 9(1) - 1$

$1 = 10 - 9(1)$

$1 = 10 + 9(-1)$

$9 = 3 \times 3 \times 1$

$10 = 2 \times 5 \times 1$

9 Mod 10

Affine Cipher $K(a, b) \Rightarrow K(5, 7)$

Encryption

$Y = (ax + b)$ Mod 26

$x_1\ x_2\ x_3\ x_4$

$21\ 19\ 19\ 4$

VOTE $\Leftrightarrow$ IZYB

$y_1 = ax_1 + b$ Mod 26

$= 5(21) + 7$ Mod 26 $= 112$

$= 8$ Mod 26

$y_2 = 5(14) + 7$ Mod 26 $= 77 = 25$ Mod

$y_2 = 5(19) + 7$ Mod 26 $= 24$ Mod 26

$y_3 = 5(4) + 7$ Mod 26 $= 27$ Mod 26

$y_4 = 1$ Mod 26

Decryption

$x = a^{-1}(y - b)$ Mod 26

$x = a^{-1}(y - b)$ Mod 26

4 Mod 10

$^{8}I\ Z^{25}\ Y^{24}\ B^{1}$

$x = a^{-1}(y - b)$ Mod 26

$x_1 = 21(8 - 7)$ Mod 26

$x_1 = 21$ Mod 26

$x_2 = 21(25 - 7)$ Mod 26 $= 21(18$ Mod 26

$x_2 = 378$ Mod 26 $= 14$ Mod 26

$x_3 = 21(24 - 7)$ Mod 26 $= 21(17)$ Mod 26

$x_3 = 357$ Mod 26 $= 19$ Mod 26

$x_4 = 21(1 - 7)$ Mod 26 $= 21(-6)$ Mod 26

$x_4 = -126$ Mod 26 $= 4$ Mod 26

Date : 1-6-2022

Random Process

-> Sample Space

All possible outcomes of a random process are called sample space

Ludo dic $S = \{1, \ldots 6\}$

Playing card $P = \{52 \text{ cards}\}$

Event

An event is a subset of sample space.

Equally likely event

All the outcome of event are equally likely because they have same probability.

52 - Playing card
- Diamond → Red
- Heart → Red
- Spade → Black
- Club → Black

Probability

$$\frac{\text{No. of favourable outcomes}}{\text{No. of Total outcomes}} = \frac{N(E)}{N(S)}$$

- Naive Defination of Probability

E.g: Event = {Face Card} $N(S) = 52$

$N(E) = 6$ (only Black)

$$P(E) = \frac{N(E)}{N(S)} = \frac{6}{52}$$

- Finite → Countable
- Countably finite → Natural numbe with one-to-one correspondence
- Finite → Uncountable

~~Eint~~ Counting technique

$N(E) = n - m + 1 = 0$

(n: End no., m: starting no.)

Q. What is the probability of getting a two digit integer dividable with 3

Sample Space = 90

$m = 4$, $n = 33$

$N(E) = 33 - 4 + 1 = 30$

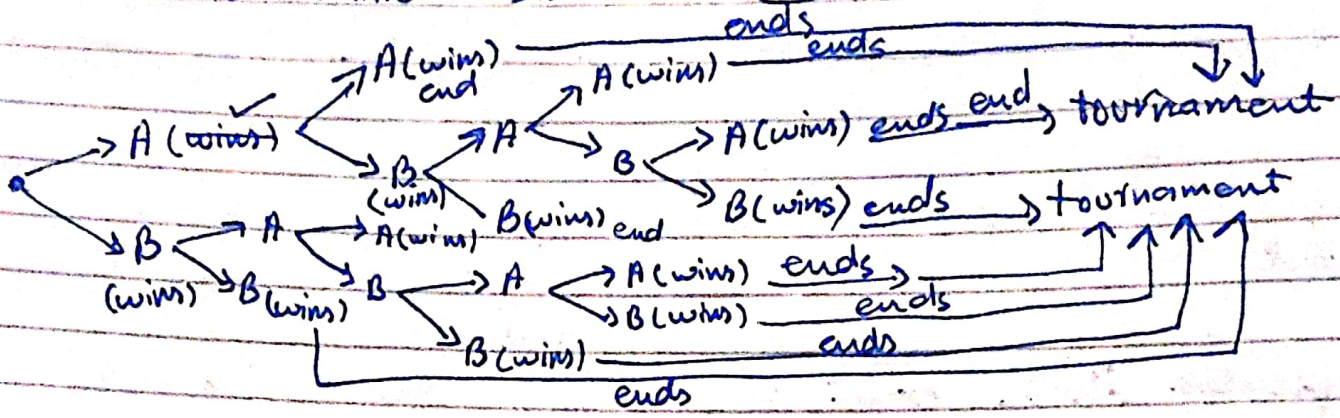
$$\text{Probability} = \frac{N(E)}{N(S)} = \frac{30}{90} = \frac{1}{3}$$

Tree

Team 1 = A , Team 2 = B

Consecutive 2nd = wins

~~1st Game~~ 3rd → end



Date: 2-6-2022

Buy a Graphic Card

→ Model of Vender = 3
→ Model of RTX = 2
→ Model of GPU = 2
→ 3 × 2 × 2

Multiplication Rule

If an experiment consist of 'k' steps:
1st step can be in n_1 ways
2nd " " n_2 "
3rd " " n_3 "
then the total outcomes of experiment are

$$n_1 \times n_2 \times n_3 \times \dots n_k$$

Permutation

A permutation of set of 'n' objects is an ordering of objects in a row.

COMPUTER
1 2 3 4 5 6 7 8

Date: 8-6-2022

Permutation

r - Permutation

$$nP_r = \frac{n!}{(n-r)!}$$

ways to choose 1st object = n

2nd = n-1

3rd = n-2

4th = n-3

rth object = n-(r-1)

= n-r+1

$$nP_r = n \times (n-1)(n-2)(n-3)(n-4)\ldots(n-r+1) \times \frac{(n-r)!}{(n-r)!}$$

$$nP_r = \frac{n!}{(n-r)!} \qquad {}^8P_3 = \frac{8!}{(8-3)!} = \frac{8!}{5!} = 8 \times 7 \times 6 = 336$$

Pigeonhole Principle

If 'n' pigeon fly into 'm' pigeonholes and $n > m$ then at least one pigeonhole must contain two or more pigeons.

Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$

Q: How many integers must be seleted from A if we want a pair of integers, having sum = 9

(1,8), (2,7), (3,6), (4,5)

(1,8) ... pigeonholes

(4,5) ... pigeon

→ Ordered Selection Permutation (Order)

→ Unordered Selection Combination (~~No repetition allowed~~) (Order doesn't matter)

Q: How many ordered-selection of two from set {0, 1, 2, 3}

$${}^nP_r = \frac{n!}{(n-r)!} = \frac{4!}{2!} = 4 \times 3 = 12$$

$${}^nC_r = \frac{n!}{r!(n-r)!}$$

Pascal's Formula

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Q: Calculate $\binom{7}{5}$

$$\binom{7}{5} = \binom{6}{4} + \binom{6}{5} = 21$$

Binomial Theorem

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

$$(a+b)^n = a^n + {}^nC_1 a^{n-1}b^1 + {}^nC_2 a^{n-2}b^2 + \dots + b^n$$

$$(a+b)^3 = a^3 + {}^3C_1 a^2 b + {}^3C_2 ab^2 + b^3$$

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

$$\boxed{{}^nC_r = {}^nC_{n-r}}$$

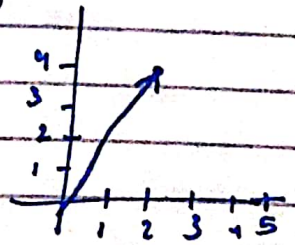
Date: 9-6-2022

Scalar

- One dimentional (25)

Vectors

- Direction
- Point in Space (N-D)



$$\begin{bmatrix} 2 \\ 4 \end{bmatrix}$$ ← Convention → 2-D

$$\begin{bmatrix} 2 \\ 4 \\ 3 \end{bmatrix}$$ → 3D

Date : 16-6-2022

- **Vector**

$\vec{N} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ 2D Vector $\quad \vec{M} = \begin{bmatrix} 4 \\ 2 \\ 1 \end{bmatrix}$ 3D Vector

$|v| = \sqrt{(3)^2 + (4)^2}$

$= \sqrt{9+16} = \sqrt{25} = 5$

- Magnitude / Length / Nohr
- **Unit Vector** ← To show the direction
- Magnitude of unit vector is 1

Unit Vector $= \frac{\text{Vector itself}}{\text{Mg. of Vector}}$ e.g. $\vec{V} = \frac{1}{5}\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ $\frac{1}{5} = \begin{bmatrix} \frac{3}{5} \\ \frac{4}{5} \end{bmatrix}$

Vector Addition

- Dimention must be same

$\vec{q} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ $\quad \vec{p} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ $\quad \vec{q} + \vec{p} = \begin{bmatrix} 1+3 \\ 2+4 \end{bmatrix} = \begin{bmatrix} 4 \\ 6 \end{bmatrix}$

Scalar Multiplication

$\vec{r} = \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix}$ $\quad a = 3$ $\quad \vec{a} \times r = 3\begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 9 \\ 6 \end{bmatrix}$

Linear Combination

$a(\vec{m} + \vec{n})$

$= 5\left(\begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} + \begin{bmatrix} 3 \\ 5 \\ 7 \end{bmatrix}\right)$ $\boxed{a = 5}$ $\quad \vec{n} = \begin{bmatrix} 3 \\ 5 \\ 7 \end{bmatrix}$

$= 5\begin{bmatrix} 4 \\ 8 \\ 9 \end{bmatrix} = \begin{bmatrix} 20 \\ 40 \\ 45 \end{bmatrix}$

Dot Product

$$\vec{v} = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \quad \vec{u} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Transpose

$$\vec{u}^T = \begin{bmatrix} 1 & -1 \end{bmatrix}$$

$$\vec{v} \cdot \vec{u} = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \end{bmatrix} = 1 - 1 = 0$$

$$\vec{r} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \quad \vec{q} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

$$\vec{r}^T \cdot \vec{q} = \begin{bmatrix} 2 & 3 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = 4 + 3 = 7$$

- If two vectors are perpendicular then their dot product is zero.
- Number of rows of 1st vector must be equal to Nuumber of colums of 2nd vector

Orthognal

$$\vec{n} \begin{bmatrix} 2 \\ 1 \\ -2 \\ 4 \end{bmatrix} \quad \vec{m} \begin{bmatrix} 3 \\ -6 \\ 4 \\ 2 \end{bmatrix} \qquad \vec{n}^T = \begin{bmatrix} 2 & 1 & -2 & 4 \end{bmatrix}$$

$$\vec{n}^T \cdot \vec{m} = \begin{bmatrix} 2 & 1 & -2 & 4 \end{bmatrix} \begin{bmatrix} 3 \\ -6 \\ 4 \\ 2 \end{bmatrix} = 6 - 6 - 8 + 8 = 0$$

- These two vectors are orthogonal / <u>orthonormal</u> to each other.
- If two vectors are normal to each other and both are unit vectors then they are orthonormal to each other.

Matrix / Matrices

$m \times n$

rows ↓ columns ↓

1. Square Matrix = $m \times m$
2. Transpose $A = A^t$ → Change row into columns

If $A^t = A$ then it is called Symmetric Matrix.

Matrix Multiplication

- $A \times B \neq B \times A$

1st 3×3 2nd 3×1 → 3×1

$$A \times B = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 7 \end{bmatrix} = \begin{bmatrix} 2+6+28 \\ 1+4+35 \\ 3+6+7 \end{bmatrix} = \begin{bmatrix} 36 \\ 40 \\ 16 \end{bmatrix}$$

Matrix Vector

Matrix - Matrix Multiplication

$$\begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 & 2 \\ 2 & 4 & 7 \\ 7 & 2 & 5 \end{bmatrix} = \begin{bmatrix} 2+6+28 & 6+12+8 & 4+21+20 \\ 1+4+35 & 3+8+20 & 2+14+25 \\ 3+6+7 & 9+12+2 & ~~3+14+5~~ \; 6+21+5 \end{bmatrix}$$

$$= \begin{bmatrix} 36 & 26 & 45 \\ 40 & 31 & ~~30~~ \; 41 \\ 16 & 23 & 32 \end{bmatrix}$$

Determinant

$$A = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \Rightarrow |A| = 5$$

Linear Dependent

$$A = \begin{bmatrix} 3 & 6 \\ 1 & 2 \end{bmatrix} \Rightarrow |A| = 0$$

Rank

No. of linear independent colum is the rank of Matrix.

$$B = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 3 \\ 4 & 1 & 5 \end{bmatrix}$$ ← Linear dependent

↑ ↑

linear independent = Rank = 2

Date : 17-6-2022

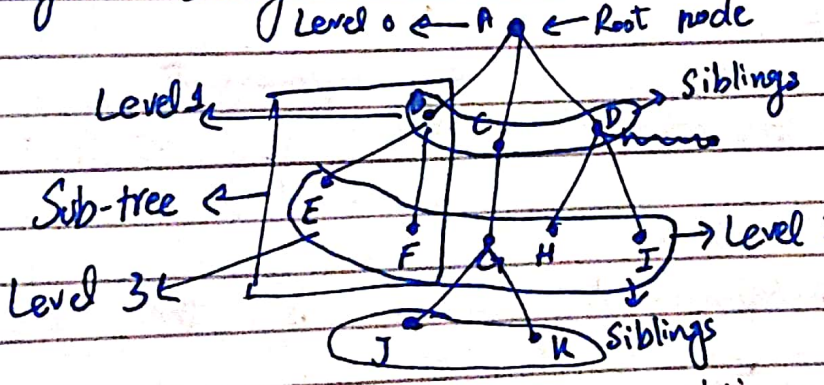
Introduction of Graph

- A simple graph $G = (V, E)$ consists of V, a non-empty set of vertices, and E, a set of unordered pairs of distinct element of V called edges.

Date : 21-6-2022

Introduction of Trees

- Graph having no cycle, loop or circuit.
- A tree is a connected undirected graph with no simple circuits.
- Posibility tree
- **Rooted tree** – One vertex of a tree has been designed designated as the root of the tree

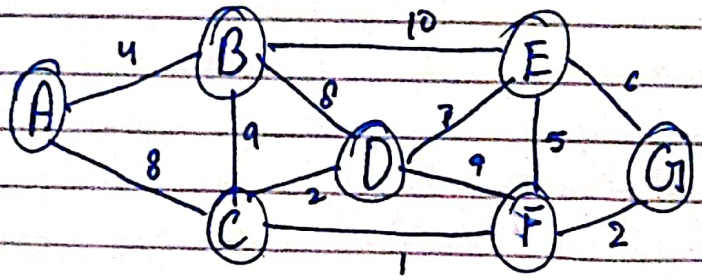


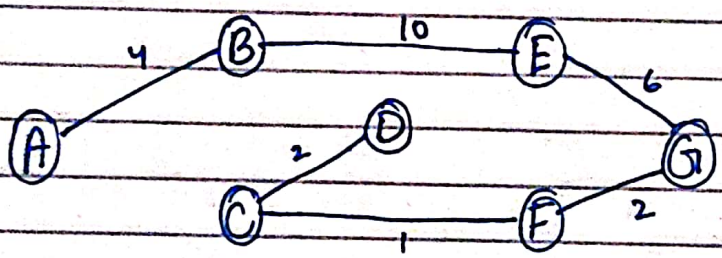
- Leaf node
- A tree can have a lot of sub-trees.

- EFGHI and BCD are siblings
- B has two children E, F and C has G. D has H and I children.
- Height - height of the tree from lowest node.
- The lowest node is the deepest node. - level

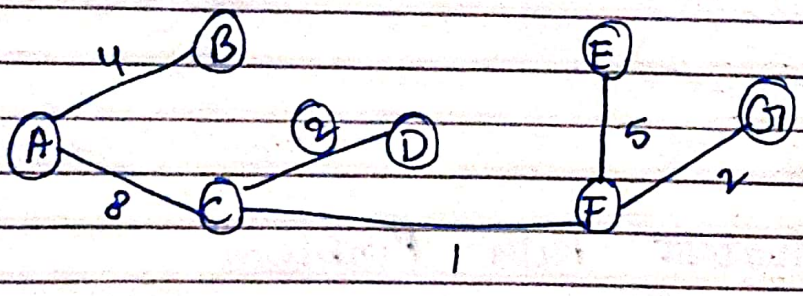
Spanning tree

- A tree with n vertices has n-1 edge.
- A spanning tree of a graph is a sub-graph that contains every vertex and the sub-graph is tree.
- A spanning tree having minimum length is called minimum-spanning. (MST).



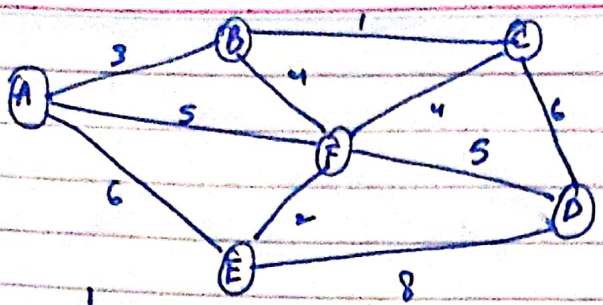


Length = 25



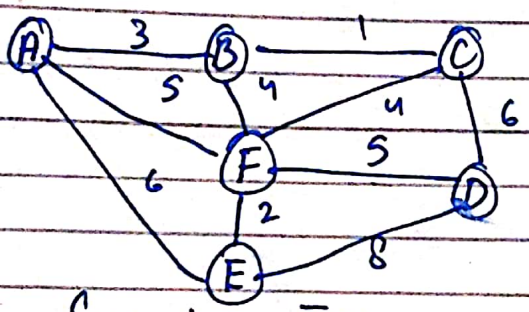
- Prims Algorithm

Task

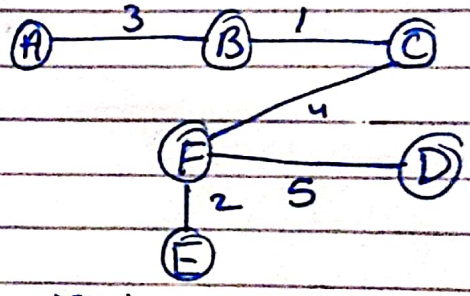


(2) (1)
a, b, c, f, e, d

Vertex in Tree (MST)	Remaining vertices
A(–,–)	B(A,3), e(A,6), F(A,5)
B(A,3)	C(B,1), F(B,4)
C(B,1)	F(C,4), D(C,6)
F(C,4)	B(F,4), E(F,2), F(C,4)
E(F,2)	D(E,8), ~~F(E,2)~~, A(E,6)
F(E,2)	D(F,5)
D(F,5)	

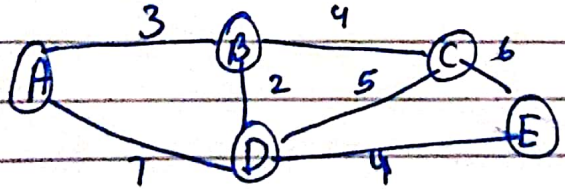


Spanning Tree



Minimum-Spanning Tree

Single Source Shortest Path Problem



- Dijkstra Algorithm

a(-,0) ✓	b(a,3), d(a,7), c(-,∞), e(-,∞)
b(a,3)	e(b,7), d(b,5), e(-,∞)
d(b,5)	c(b,7), e(d,9)
~~e(d,9~~	
c(b,7)	e(d,9)
e(d,9)	