DMS

Modular Arithmetic:

Important Points:

→ It is all about remainder.

→ It operates only on integers $Z = (-\infty, +\infty)$.

→ All even integers are congrent to each other.

→ And all odd integers are congrent to each other.

→ Two integers ('a') and ('b') mod n are congrent to each other if their remainder mode 'n' is same.

e.g:

$$18 \equiv 0 \bmod 2$$

$$16 \equiv 0 \bmod 2$$

18 and 16 are congrent to each other as their remainder mod '2' is same i.e (0).

In the above example:

≡ is congrent to

0 is Congrence (remainder)

2 is modulus of congrence.

Writting Ways:

- $19 \equiv 1 \bmod 2$
  $2 \mid 19 - 1$
- $25 \equiv 4 \bmod 7$
  $7 \mid 25 - 4$
- $-5 \equiv 2 \bmod 7$
  $7 \mid -5 - 2$

Z_n:

Z_n reads as Z mod n.

$Z \bmod n$ = remainder

e.g:

$Z_1 = \{0\}$

$Z_{02} = \{0, 1\}$

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

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

Modular Addition:

1- $3 \bmod 5 + 4 \bmod 5$

$= (3+4) \bmod 5$

$= 7 \bmod 5$

$\equiv 2 \bmod 5$

Modular addition is closed under $Z_n (Z_5)$.

Ans 2 belongs to Z_n i.e (Z_5).

2- $3 \bmod 7 + 6 \bmod 7$

$= (3+6) \bmod 7$

$= 9 \bmod 7$

$\equiv 2 \bmod 7$

It is also closed under modular addition. Closure property holds.

Modular Subtraction:-

$Z_7 = \{0, 1, 2, 3, 4, 5, 6, \}$

1* $3 \bmod 7 - 6 \bmod 7$

$= (3-6) \bmod 7$

$= -3 \bmod 7$

$\equiv 4 \bmod 7$

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

2. $2 \bmod 7 - 6 \bmod 7$

$= (2-6) \bmod 7$

$= (-4) \bmod 7$

$\equiv 3 \bmod 7$

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

Closure property also holds for modular subtraction. The congrence should be from the

set of Z_n.

Modular Multiplication:

1. $4 \bmod 7 \times 5 \bmod 7$

$= (4 \times 5) \bmod 7$

$= 20 \bmod 7$

$= 6 \bmod 7$

$7 \overline{)20}$ quotient 2, remainder $20 - 14 = 6$

2. $5 \bmod 7 \times 6 \bmod 7$

$= (5 \times 6) \bmod 7$

$= 30 \bmod 7$

$= 2 \bmod 7$

$7 \overline{)30}$ quotient 4, remainder $30 - 28 = 2$

Modular multiplication is also closed w.r.t Z_n.

NOTE:

The congrence should be smallest non-negative integer.

e.g:

* $-2 \bmod 7$

$-2 \bmod 7 \equiv 5 \bmod 7$

So the congrence is 5 i.e smallest non-negative integer.

$7 \overline{)-2}$ quotient 1, remainder $-2 - (-7) = 5$

* $-22 \bmod 7$
$\equiv 6 \bmod 7$

$7 \overline{)-22}$
28
6

As 6 is non-negative integer.

Cipher

Encryption:

Let we have to encrypt the message "CAT" with key $k = 9$.

$Z_n = Z_{26} = \{0, 1, 2, 3, \ldots 25\}$

A	F	K	P	U	Z
0	5	10	15	20	25

To encrypt a message we have the following ~~(message:)~~ formula:

$$y_n = (x_n + k) \bmod 26$$

C	A	T
↓	↓	↓
2	0	19
x_1	x_2	x_3

$y_1 = (x_1 + k) \bmod 26$

$y_1 = (2+9) \bmod 26$

$y_1 = 11 \bmod 26$

$y_1 = L$

Also,

$y_2 = (x_2 + k) \bmod 26$

$y_2 = (0+9) \bmod 26$

$y_2 = 9 \bmod 26$

$y_2 = J$

Also,

$y_3 = (x_3 + k) \bmod 26$

$y_3 = (19+9) \bmod 26$

$y_3 = 28 \bmod 26$

$y_3 = 2 \bmod 26$

$y_3 = C$

Now the CAT is encrypted in LJC.

Decryption:

L	J	C
↓	↓	↓
11	9	2
y_1	y_2	y_3

Formula for decryption is:

$$x_n = (y_n - k) \bmod 26$$

$x_1 = (11-9) \bmod 26$

$x_1 = 2 \bmod 26$

$x_1 = C$

$x_2 = (9-9) \bmod 26$

$x_2 = 0 \bmod 26$

$x_2 = A$

$x_3 = (2-9) \bmod 26$

$x_3 = -7 \bmod 26$

$x_3 = 19 \bmod 26$

$x_3 = T$

$$26 \overline{)-7}^{\,1}$$
$$\underline{26}$$
$$19$$

Now the decrypt message is CAT.

For finding key we use

$$k = (y - x) \bmod 26$$

Modular Division

→ For modular division we require multiplicative inverse.

→ Modular multiplicative inverse can be found by greatest common divisor (GCD).

→ Multiplicative inverse exists iff their GCD is 1.

e.g:

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

$a \in Z_6$

$a^{-1} \bmod 6$ exists iff

$GCD(a, 6) = 1$

So

$5^{-1} \bmod 6$ only exists

* $Z_5 = \{0, 1, 2, 3, 4\}$

$2^{-1} \bmod 5$ exists

$3^{-1} \bmod 5$ exists

$4^{-1} \bmod 5$ exists

If n is a prime number than the maximum members

have multiplicative inverse

→ Two Multiplicative inverse also exists when the num and mod n are relatively prime to each other.

→ Two integers are relatively prime to each other iff their GCD = 1.

Euclidean Algorithm

It is a way to fi GCD.

Lets have an example:

(85, 34)

85 = (34×2) + 17

34 = (17×2) + 0

Now,

GCD = 17

(1331, 1001)

1331 = (1001×1) + 330

1001 = (330×3) + 11

330 = (11×30) + 0

Now GCD = 11

(9888 , 6060)

$9888 = 6060 + 3828$

$6060 = 3828 + 2232$

$3828 = 2232 + 1596$

$2232 = 1596 + 636$

$1596 = 636(2) + 324$

$636 = 324 + 312$

$324 = 312 + 12$

$312 = 12(26) + 0$

GCD = 12.

Find the values of unknow

$1331x + 1001y = 11$

extended
evcledeo
method

$11 = 1001 - 330(3)$

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

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

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

So

$x = -3$

$y = 4$

$213x + 117y = 3$

Eucledean Algorithm

$213 = 117 + 96$

$117 = 96(1) + 21$

$96 = 21(4) + 12$

$21 = 12 + 9$

$12 = 9 + 3$

$9 = 3(3) + 0$

$GCD = 3$

Extended eucledean Algorithm

$3 = 12 - 9$

$3 = 12 - (21 - 12)$

$3 = 12 - 21 + 12$

$3 = 12(2) + 21(-1)$

$3 = [96 - 21(4)]2 + 21(-1)$

$3 = 96(2) - 21(8) + 21(-1)$

$3 = 96(2) + 21(-9)$

$3 = 96(2) + [117 - 96](-9)$

$3 = 96(2) + 117(-9) + 96(9)$

$3 = 96(11) + 117(-9)$

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

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

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

Now

$x = 11$

$y = -20$

$252x + 198y = 18$

Eucledean Algorithm

$252 = 198(1) + 54$

$198 = 54(3) + 36$

$54 = 36 + 18$

$36 = 18(2) + 0$

$GCD = 18$

Extended Eucledean Algorithm

$18 = 54 - 36$

$18 = 54 - [198 - 54(3)]$

$18 = 54 - 198 + 54(3)$

$18 = 54(4) + 198(-1)$

$18 = (252 - 198)4 + 198(-1$

$18 = 252(4) + 198(-4) + 198(-1$

$18 = 252(4) + 198(-5)$

Now

$x = 4$

$y = -5$

Calculate multiplicative inverse using eucledean method:

1- Calaulate $5^{-1} \bmod 7$.

$$7 = 5(1) + 2$$

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

Now:

$$1 = 5 - 2(2)$$

$$1 = 5 - (7 - 5)2$$

$$1 = 5 + 7(-2) + 5(2)$$

$$1 = 5(3) + 7(-2)$$

Now

$$5^{-1} \bmod 7 = 3 \bmod 7$$

Verification:

$$= (5 \cdot 3) \bmod 7$$

$$= 15 \bmod 7$$

$$= 1 \bmod 7$$

Hence verified that

$$5^{-1} \bmod 7 = 3 \bmod 7$$

2- $8^{-1} \bmod 11 = ?$

$11 = 8(1) + 3$

$8 = 3(2) + 2$

$3 = 2 + 1$

Now:

$1 = 3 - 2$

$1 = 3 - [8 - 3(2)]$

$1 = 3 - 8 + 3(2)$

$1 = 3(3) + 8(-1)$

$1 = (11 - 8)3 + 8(-1)$

$1 = 11(3) + 8(-3) + 8(-1)$

$1 = 11(3) + 8(-4)$

$-4 \bmod 11 = 7 \bmod 11$

The inverse is $7 \bmod 11$

verification:

$8^{-1} \bmod 11 = 7 \bmod 11$

$= (8 \cdot 7) \bmod 11$

$= 56 \bmod 11$

$= 1 \bmod 11$

Hence verified that

$8^{-1} \bmod 11 = 7 \bmod 11$

3- $6^{-1} \bmod 9 = ?$

$6^{-1} \bmod 9$ does not exist as they are not relatively prime to each other.

4- $7^{-1} \bmod 9 = ?$

$9 = 7(1) + 2$

$7 = 2(3) + 1$

Now:

$1 = 7 - 2(3)$

$1 = 7 - [9 - 7]3$

$1 = 7 - 9(3) + 7(3)$

$1 = 7(4) + 9(-3)$

$7^{-1} \bmod 9 = 4 \bmod 9$

Verification:

$(7 \cdot 4) \bmod 9$

$= 28 \bmod 9$

$= 1 \bmod 9$

Hence verified

$7^{-1} \bmod 9 = 4 \bmod 9$

P.G

Subject: All

BRITISH SCHOOL

5- $9^{-1} \bmod 10 = ?$

$10 = 9(1) + 1$

Extended euclidian method

$1 = 10 - 9$

$1 = 10 + 9(-1)$

$-1 \bmod 10 = 9 \bmod 10$

So

$9^{-1} \bmod 10 = 9 \bmod 10$

Verification:

$(9 \cdot 9) \bmod 10$

$= 81 \bmod 10$

$= 1 \bmod 10$

Hence verified that

$9^{-1} \bmod 10 = 9 \bmod 10$

* It also shows that an integer can be an inverse of itself.

Affine cipher

- key k (a, b)

a should be that number whose multiplicative inverse exists.

- It operates on $Z_{26} = \{A, B, .. Z\}$

A	F	K	P	U	Z
0	5	10	15	20	25

- Encrypit:

$$y = (ax + b) \bmod 26$$

- Decrypit:

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

Example:

VOTE k (5, 7)

V	O	T	E
↓	↓	↓	↓
21	14	19	4
x_1	x_2	x_3	x_4

$$y_1 = (ax_1 + b) \bmod 26$$
$$y_1 = [5(21) + 7] \bmod 26$$
$$y_1 = 112 \bmod 26$$

$y_1 = 8 \bmod 26$

$y_1 = I$

$y_2 = [5(14) + 7] \bmod 26$

$y_2 = 77 \bmod 26$

$y_2 = 25 \bmod 26$

$y_2 = Z$

$y_3 = [5(19) + 7] \bmod 26$

$y_3 = 102 \bmod 26$

$y_3 = 24 \bmod 26$

$y_3 = Y$

$y_4 = [5(4) + 7] \bmod 26$

$y_4 = 27 \bmod 26$

$y_4 = 1 \bmod 26$

$y_4 = B$

Now VOTE is encrypted into

I Z Y B

Decryption:

I	Z	Y	B
↓	↓	↓	↓
8	25	24	1
y_1	y_2	y_3	y_4

$a = 5$

$5^{-1} \bmod 26$

$26 = 5(5) + 1$

Extended eucledean method

$1 = 26 - 5(5)$

$1 = 26 + 5(-5)$

$-5 \bmod 26 = 21 \bmod 26$

So $a^{-1} = 21$

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

$x_1 = 21(8 - 7) \bmod 26$

$x_1 = 21 \bmod 26$

$x_1 = V$

$x_2 = 21(25 - 7) \bmod 26$

$x_2 = 21(18) \bmod 26$

$x_2 = 378 \bmod 26$

$x_2 = 14 \bmod 26$

$x_2 = 0$

$x_3 = 21(24-7) \bmod 26$

$x_3 = 21(17) \bmod 26$

$x_3 = 357 \bmod 26$

$x_3 = 19 \bmod 26$

$x_3 = T$

$x_4 = 21(1-7) \bmod 26$

$x_4 = 21(-6) \bmod 26$

$x_4 = -126 \bmod 26$

$x_4 = 4 \bmod 26$

$x_4 = E$

The decrypted message is VOTE.

ii- SKY key (11, 2)

S	K	Y
↓	↓	↓
18	10	24
x_1	x_2	x_3

$y_1 = (ax_1 + b) \bmod 26$

$y_1 = [11(18) + 2] \bmod 26$

$y_1 = 200 \bmod 26$

$y_1 = 18 \bmod 26$

$y_1 = S$

$y_2 = [11(10) + 2] \bmod 26$

$y_2 = 112 \bmod 26$

$y_2 = 8 \bmod 26$

$y_2 = I$

$y_3 = [11(24) + 2] \bmod 26$

$y_3 = 266 \bmod 26$

$y_3 = 6 \bmod 26$

$y_3 = G$

The SKY is encrypted into SIG.

$a = 11$; $a^{-1} = ?$

$26 = 11(2) + 4$

$11 = 4(2) + 3$

$4 = 3 + 1$

Extended Eucledean Method.

$$1 = 4 - 3$$
$$1 = 4 - [11 - 4(2)]$$
$$1 = 4 + 11(-1) + 4(2)$$
$$1 = 4(3) + 11(-1)$$
$$1 = [26 - 11(2)]3 + 11(-1)$$
$$1 = 26(3) + 11(-6) + 11(-1)$$
$$1 = 26(3) + 11(-7)$$

$-7 \bmod 26 = 19 \bmod 26$

so

$$a^{-1} = 19$$

Decryption:-

S	I	G
↓	↓	↓
18	8	6
y_1	y_2	y_3

$$x_1 = a^{-1}(y - b) \bmod 26$$
$$x_1 = 19(18 - 2) \bmod 26$$
$$x_1 = 304 \bmod 26$$
$$x_1 = 18 \bmod 26$$
$$x_1 = S$$

$x_2 = 19(8-2) \bmod 26$

$x_2 = 114 \bmod 26$

$x_2 = 10 \bmod 26$

$x_2 = K$

$x_3 = 19(6-2) \bmod 26$

$x_3 = 76 \bmod 26$

$x_3 = 24 \bmod 26$

$x_3 = Y$

Decrypted message is SKY.

Probability

Random Processes:

Those processes whose outcome can be predicted but not gaurantted are called random processes.

e.g:

- Rolling a die
- Rolling a coin
- Choosing a card from a deck.

Sample Space:

→ All possible outcomes of a random process are called sample space.

→ It is written in the form of a set.

- **Rolling a coin:**
  $S = \{H, T\}$
- **Rolling a die:**
  $S = \{1, 2, 3, 4, 5, 6\}$
- **Choosing a card**
  $S = \{52 \text{ cards}\}$
- **Rolling two dice**
  $S = \{HH, HT, TH, TT\}$

Event:

A subset of a sample space is called an event.

Equally likely event:

Events having equal chances to occurr.

Probability : (Naive definition)

Probability = $\frac{\text{No. of favorable ou}}{\text{No. of total outc}}$

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

Probability of choosing a f card.

$N(E) = 12$

$N(S) = 52$

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

Heart →

Spade →

Diamond →

Club →

$$P = \frac{12}{52} = \frac{3}{13}$$

Probability of getting only b face card.

$N(E) = 6$

$N(S) = 52$

$$P = \frac{N[E]}{N[S]} = \frac{6}{52} = \frac{3}{26}$$

Two dice are rolled. What is the probability that their sum is 8.

$S = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6),$
$(2,1), (2,2), (2,3), (2,4), (2,5), (2,6),$
$(3,1), (3,2), (3,3), (3,4), (3,5), (3,6),$
$(4,1), (4,2), (4,3), (4,4), (4,5), (4,6),$
$(5,1), (5,2), (5,3), (5,4), (5,5), (5,6),$
$(6,1), (6,2), (6,3), (6,4), (6,5), (6,6)\}$

$N(S) = 36$

$E = \{(2,6), (3,5), (4,4), (5,3), (6,2)\}$

$N(E) = 5$

$$P = \frac{N(E)}{N(S)} = \frac{5}{36}$$

Finite countable
Infinite uncountable
Countably finite: One to one correspondence with natural numbers.

Counting:

What is the probability of getting two digit numbers tha are divisible by 3?

$S = \{10, 11, \underset{\downarrow 4}{12}, 13, 14, \underset{\downarrow 5}{15}, \ldots \underset{\downarrow 33}{99}\}$

$$N(S) = n - m + 1$$
$$= 99 - 10 + 1$$
$$= 90$$

$$E = \{4, 5, \ldots 33\}$$
$$N(E) = n - m + 1$$
$$= 33 - 4 + 1$$
$$= 30$$
$$P = \frac{N(E)}{N(S)}$$
$$P = \frac{30}{90}$$
$$P = \frac{1}{3}$$

What is the probability of gettin a three digit number that divisible by 5.

$S = \{100, 101, 102, \ldots 999\}$

20 ; 998 → 199

$N(S) = n - m + 1$

$= 999 - 100 + 1$

$= 900$

$E = \{20, \ldots 199\}$

$N(E) = 199 - 20 + 1$

$= 180$

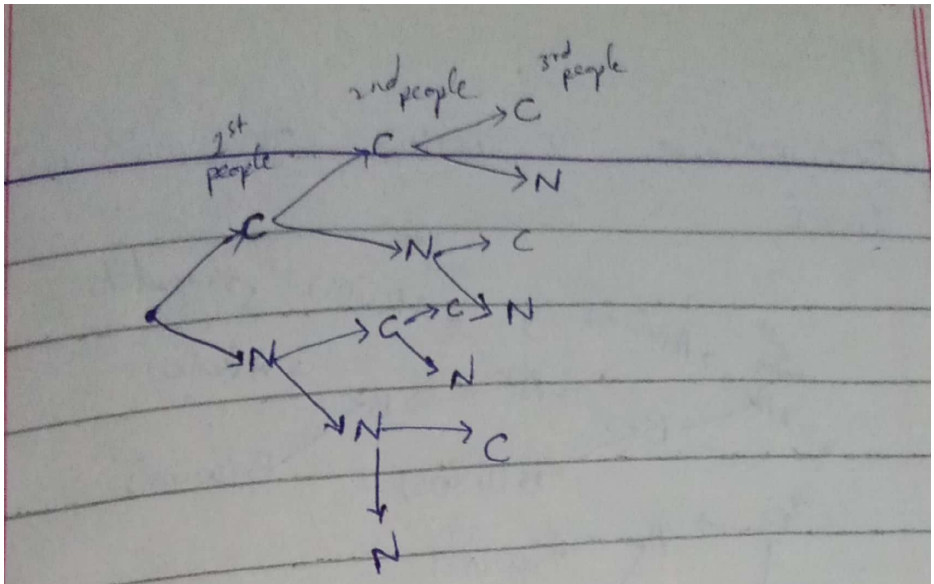
$P = \frac{N(E)}{N(S)}$

$P = \frac{18\cancel{0}}{90\cancel{0}}$

$P = \frac{1}{5}$.

Possibility Tree:

Three people went to meet covid patient. Probability of getting covid.



$S = \{ CCC, CCN, CNC, CNN, NCC, NCN, NNC, NNN \}$

$N(S) = 8$

Find the probability that at least one people get covid.

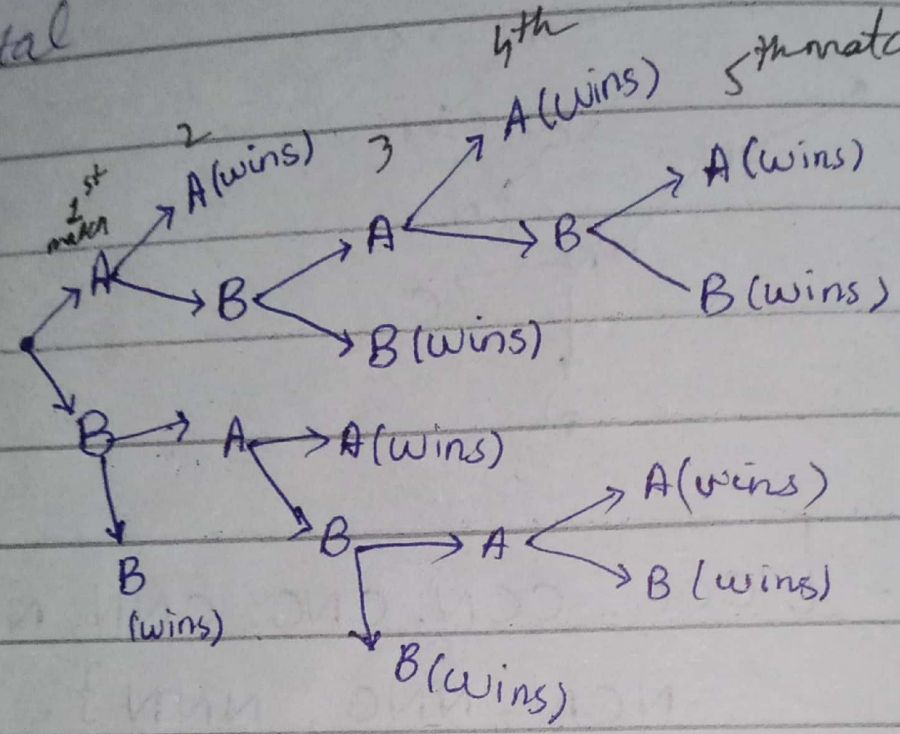
$E = \{ CCC, CCN, CNC, CNN, NCC, NCN, NNC, \}$

$N(E) = 7$

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

$$P = \frac{7}{8}$$

Consective 2 wins or 3 wi
total



Winning total possible outcom
are 10.

02-06-2022

Buy a computer.

Models of CPU

02-06-2022

Buy a Computer:

Models of CPU box = 3

Models of keyboard = 2

Models of LED = 2

How many models of computer can be made using these models?

Models of Computer = $3 \times 2 \times 2$

$= 12$

Multiplication Rule:

If an experiment consists of k steps, 1st step can be done in n_1 ways, 2nd step can be done in n_2 ways. k step can be done in n_k ways, then total outcomes of experiment are

$$n_1 \times n_2 \times n_3 \times \cdots n_k.$$

Example:

Suppose we have two pots P_1 and P_2. P_1 has two black balls (B_1 and B_2) and one white ball (W). P_2 has two

white balls (w_1 & w_2) and a black ball (B).

Experiment:

Choose a pot randomly
Choose a ball randomly
Choose 2nd ball randomly without replacement.
Calculate total no. of outcomes of experiment.

No. of ways of choosing a pot = 2
No. of ways of choosing a ball = 3
No. of ways of choosing 2nd ball without replacement = 2
Total no. of ways of outcomes of experiment = 2 X 3 X 2
= 12

What is the probability of choosing two black balls?

No. of ways of choosing a pot = 1
No. of ways of choosing a ball = 2
No. of ways of choosing 2nd ball = 1
Total no. of ways of choosing two

black balls = N(E) = 1 × 2 × 1

= 2

Probability = $\frac{2}{12} = \frac{1}{6}$

What is the probability of getting opposite color balls?

NO. of ways of choosing a pot = 2

NO. of ways of choosing a ball = 2

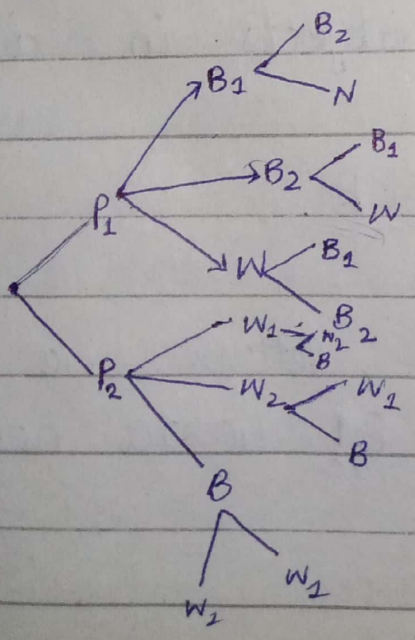
NO. of ways of choosing 2nd ball = 2

Total number of ways of getting opposite color balls = 2 × 2 × 2

N(E) = 8

Probability P(E) = $\frac{8}{12} = \frac{2}{3}$

Possibility Tree



Suppose three cities A, B and C.

The routes from A to B = 3

The routes from B to C = 5

routes from A to C = ?

routes from A to C = 3×5

= 15

routes from C to A = 3×5

= 15

Total round trip routes from A to C = 15×15

= 225.

Permutations: (A device for counting)

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

COMPUTER

8 7 6 5 4 3 2 1

using these 8 letters we can make 8! = 40320 new words.

What is the probability of getting such words in which 'C' and 'O' comes together?

No. of ways of getting CO together = 7!

Probability = $\frac{7!}{8!} = \frac{7!}{8 \cdot 7!}$

$= \frac{1}{8}$

ALGORITHM

9! new words can be made from {A, L, G, O, R, I, T, H, M}.
Find the probability of getting 'ALGO' at same place.

No. of ways of getting 'ALGO' at same place = 6!

Probability = $\frac{6!}{9!} = \frac{6!}{9 \cdot 8 \cdot 7 \cdot 6!}$

$= \frac{1}{504}$

08-06-2022

Permutation:

Ordered Selection (AB ≠ BA)

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

Proof:

Ways to choose 1st object = n

Ways to choose 2nd object = n-1

ways to choose 3rd object = n-2

ways to choose 4th object = n-3

ways to choose r object = n-(r-1)

= n-r+1

$$^nP_r = n \times (n-1) \times (n-2) \times (n-3) \times \cdots (n-r+1)$$

Multiply and divided by (n-r)!

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

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

Hence proved!

Examples:

* Find permutation when $n = 7$ and $r = 4$.

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

$$^7P_4 = \frac{7!}{(7-4)!}$$

$$^7P_4 = \frac{7!}{3!} = \frac{7.6.5.4.3!}{3!}$$

$$^7P_4 = 840$$

* How many arrangements in a row of no more than three letters for word 'NETWORK' can be made?

Total arrangement for 1 letter word = $^7P_1 = 7$

Total arrangement for 2 letters word = $^7P_2 = 42$

Total arrangement for 3 letters word = $^7P_3 = 210$

Total arrangement for no more

than three letters word = 7+42+210
= 259

Pigeonhole principle:

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

Example:

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

How many integers must be selected from A if we want a pair of integers having Sum = 9?

Possible pair of integers having Sum = 9 are (1,8), (2,7), (3,6) and (4,5).

So 5 integers must be selelted from A for a pair of integer having sum is equal to 9.

Combi

nC

* How
two
be

n

n

Or

Combination:

Unordered Selection (AB = BA)

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

* How many unordered selection of two elements from set (0, 1, 2, 3) be made?

$n = 4$

$r = 2$

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

$$^4C_2 = \frac{4!}{(4-2)!\,2!}$$

$$= \frac{4!}{2!.2!} = \frac{4.3.2!}{2!.2!}$$

$$= \frac{12}{2} = 6$$

Ordered Selection:

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

$$^4P_2 = \frac{4!}{(4-2)!} = \frac{4.3.2!}{2!}$$

$^4P_2 = 12$

$S = \{0, 1, 2, 3\}$

ordered Selection:

$E_1 = \{01, 02, 03, 10, 12, 13, 20, 21, 23, 30, 31, 32\}$

unordered selection:

$E_2 = \{01, 02, 03, 12, 13, 23\}$

* How many unordered and ordered selection of two letter word can be made from $S = \{a, b, c, d\}$

Ordered Selection (Permeutation)

$$^4P_2 = \frac{4!}{2!} = 4 \times 3 = 12$$

$E_1 = \{(ab), (ac), (ad), (ba), (bc), (b,d), (ca), (cb), (cd), (da), (db), (dc)\}$

unordered Selection (combination)

$$^4C_2 = \frac{4!}{(4-2)!\,2!} = \frac{4!}{2!\cdot 2!}$$

$$^4C_2 = \frac{^2 4\cdot 3\cdot 2!}{2\cdot 2!} = 6$$

$$\mathcal{E}_2 = \{(ab),(ac),(ad),(bc),(bd),(cd)\}$$

* Suppose two members of a 12 person group insist on working together. Select a team containing either both person or none. How many 5 person tearms are possible? Also find the probability of each.

When both are present in team:

Total arrangement of 5 members team when both are present = $^{10}C_3$

$$N(B) = 120$$

Total possible arrangements of 5 team member = $^{12}C_5$

$N(S) = 792$

$$\text{Probability} = \frac{N(E)}{N(S)}$$

$$= \frac{120}{792}$$

$$= \frac{5}{33}$$

When both are not present:

Total arrangement when both are not present in team = $^{10}C_5$

$N(E) = 252$

$$\text{Probability} = \frac{N(E)}{N(S)}$$

$$= \frac{252}{792}$$

$$= \frac{7}{22}$$

Pascal's Formula:

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

Let $\binom{6}{2} = 15$, $\binom{6}{3} = 20$, $\binom{6}{4} = 15$ and $\binom{6}{5} = 6$ then find $\binom{7}{3}$, $\binom{7}{4}$ and $\binom{7}{5}$ by using pascal's formula:

$$\binom{7}{3} = \binom{6}{2} + \binom{6}{3}$$

$$= 15 + 20$$

$$= 35$$

$$\binom{7}{4} = \binom{6}{3} + \binom{6}{4}$$

$$= 20 + 15$$

$$= 35$$

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

$$= 15 + 6$$

$$= 21$$

Binomial theorem

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots \binom{n}{n-1}ab^{n-1} + b^n.$$

* Find $(a+b)^3$ by binomial theorem.

$$(a+b)^3 = a^3 + \binom{3}{1}a^{3-1}b + \binom{3}{2}a^{3-2}b^2 + \binom{3}{3}a^{3-3}b^3$$

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

* Find the co-efficient of term x^6y^3 in $(x+y)^9$ by using binomial expansion.

Let b be the co-efficient

$$(b)\, x^6y^3 = \binom{9}{3}x^{9-3}y^3$$

$$b = \binom{9}{3}$$

$$b = 84$$

84 be the coefficient of x^6y^3.

=

In General

$${}^{n}C_{r} = {}^{n}C_{n-r}$$

16-06-2022

Linear Algebra

Vectors:

A vector is a point in space. It is represented in the form of $\begin{bmatrix} a \\ b \end{bmatrix}$ (column matrix).

Magnitude

$$\vec{V} = \begin{bmatrix} a \\ b \end{bmatrix}$$

$$|\vec{V}| = \sqrt{a^2 + b^2}$$

It is represented by $|\vec{V}|$ and also called length or norm.

$$\vec{V} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$|\vec{V}| = \sqrt{(3)^2 + (4)^2} = \sqrt{9 + 16} = \sqrt{25}$$

$$|\vec{V}| = 5$$

Unit Vector/Normal Vector

A vector whose norm is always 1 is called unit vector.

It tells us about the direction

of a vector.
It is represented by $\hat{V}$.

$$\hat{V} = \frac{\vec{V}}{|\vec{V}|} \qquad \because \vec{V} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$\hat{V} = \frac{\begin{bmatrix} 3 \\ 4 \end{bmatrix}}{5}$$

$$\hat{V} = \frac{1}{5}\begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$\hat{V} = \begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix}$$

Vector Addition:

Vector addition is possible if both vectors have same dimensions.

$$\vec{q} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad \vec{P} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \quad \vec{x} \begin{bmatrix} 5 & 6 \end{bmatrix}$$

Vector addition of $\vec{P}$ and $\vec{q}$ is possible while with $\vec{x}$ it is not possible.

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

Scalar Multiplication:

Multiplication of a vector with a scalar quant

$$a = 3 \quad , \quad \vec{x} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$$

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

Linear Combination:

It has only two operations.

Vector Addition

Scalar Multiplication

$$a = 5 \qquad \vec{x} = \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} \qquad \vec{n} = \begin{bmatrix} 3 \\ 5 \\ 7 \end{bmatrix}$$

$$a(\vec{x} + \vec{n}) = 5\left(\begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} + \begin{bmatrix} 3 \\ 5 \\ 7 \end{bmatrix}\right) = 5\left(\begin{bmatrix} 4 \\ 8 \\ 9 \end{bmatrix}\right)$$

$$a(\vec{x} \times \vec{n}) = \begin{bmatrix} 20 \\ 40 \\ 45 \end{bmatrix}$$

In vectors, linear combination is very important.

Any vector in a plane is represented in the form of a vector combination/linear combination.

Dot product (Inner product)

$$\vec{V} = \begin{bmatrix} 1 \\ -1 \end{bmatrix} \qquad \vec{U} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\vec{V}^t = [1 \quad -1]$$

$$\vec{V} \cdot \vec{U} = \vec{V}^t \vec{U} = [1 \quad -1] \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$= [1-1] = [0]$$

Orthogonal:

Two vectors are said to be orthogonal to each other if their dot product is equal to zero.

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

$$\vec{n}^t = \begin{bmatrix} 2 & 1 & -2 & 4 \end{bmatrix}$$

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

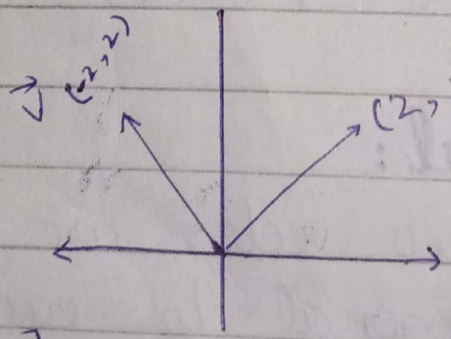
$$= \begin{bmatrix} 6-6-8+8 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \end{bmatrix}$$

Both vectors are orthogonal t
each other.

Orthonormal:

If two unit vectors
are perpendicular to each oth
than they are called orthon



$$\vec{U} = \begin{bmatrix} 2 \\ 2 \end{bmatrix} \Rightarrow |\vec{U}| = \sqrt{(2)^2 + (2)^2} = \sqrt{4+}$$

$$|\vec{U}| = \sqrt{8} = 2\sqrt{2}$$

$$\hat{U} = \frac{\begin{bmatrix} 2 \\ 2 \end{bmatrix}}{2\sqrt{2}} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

$\vec{v} = \begin{bmatrix} -2 & 2 \end{bmatrix}$, $|\vec{v}| = \sqrt{(-2)^2+(2)^2} = \sqrt{4+4}$

$\vec{v} = \sqrt{8} = 2\sqrt{2}$

$\hat{v} = \frac{\begin{bmatrix} -2 \\ 2 \end{bmatrix}}{2\sqrt{2}} = \cdot \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$

For orthonormal:

$\hat{u} \cdot \hat{v} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \cdot \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$

$\hat{u}^t \cdot \hat{v} = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$

$= \begin{bmatrix} -\frac{1}{2} + \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$

Hence proved that u and v are orthonormal to each other.

Matrices:

Matrices are a sort of functions.

They transform vectors.

dimension:

The dimension of a matrix is represented by m x n where m is no. of rows

and n is no. of columns.

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

dimension = 2 x 3

Square Matrix:

A matrix of dimensi
mxm is called square matrix

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

dimension = 2x2

Transpose of a matrix:

Converting rows into columns or columns into ro

$$A = \begin{bmatrix} 1 & 4 \\ 3 & 5 \end{bmatrix} \quad , A^t = \begin{bmatrix} 1 & 3 \\ 4 & 5 \end{bmatrix}$$

Symmetric matrix:

If $A^t = A$ then matri
A is called symmetric matrix

$$A = \begin{bmatrix} 12 & 7 \\ 7 & 12 \end{bmatrix} \quad , A^t = \begin{bmatrix} 12 & 7 \\ 7 & 12 \end{bmatrix}$$

$$\boxed{A = A^t}$$

Multiplication:

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 2 \\ 7 \end{bmatrix}$$

$$\vec{A}.\vec{B} = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 7 \end{bmatrix} = \begin{bmatrix} 2+6+28 \\ 1+4+35 \\ 3+6+7 \end{bmatrix}$$

$$\vec{A}.\vec{B} = \begin{bmatrix} 36 \\ 40 \\ 16 \end{bmatrix}$$

A vector '$\vec{B}$' is transformed matrix A.

Finding unknowns

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 1 \\ 3 & 6 & 1 \end{bmatrix} \begin{bmatrix} \quad \\ \quad \\ \quad \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 1 \\ 3 & 6 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} \quad \\ \quad \\ \quad \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \\ 9 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \\ 9 \end{bmatrix}$$

Matrix - Matrix multiplication:

$$A = \begin{bmatrix} 2 & 3 & 4 \\ 1 & 2 & 5 \\ 3 & 3 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 4 & 7 \\ 7 & 2 & 5 \end{bmatrix}$$

$$A \cdot B = \begin{bmatrix} 2+6+28 & 6+12+8 & 4+21+20 \\ 1+4+35 & 3+8+10 & 2+14+25 \\ 3+6+7 & 9+12+2 & 6+21+5 \end{bmatrix}$$

$$AB = \begin{bmatrix} 36 & 26 & 45 \\ 40 & 21 & 41 \\ 16 & 23 & 32 \end{bmatrix}$$

Determinants:

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

$$|A| = (2)(4) - (1)(3)$$

$$= 8 - 3 = 5$$

Singular Matrix:

A matrix whose determinant is equal to zero is called singular matrix.

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

$$|A| = 3(2) - 1(6)$$
$$= 6 - 6$$
$$= 0$$

- Inverse of a singular matrix does not exist.
- Columns are linearly dependent.

Rank:

Number of linearly independent columns is called rank of a matrix.

It cannot be zero.

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

Rank is 3

$|I| = 1$

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

As one column is dependent on other two so the rank of this matrix is **2**.

Inverse of a matrix:

Inverse of a 2x2 matrix is defined as:

$$A^{-1} = \frac{\text{Adj } A}{|A|}$$

$\because A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$

where $\text{Adj } A = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$

Let:

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

$$|A| = 3(5) - 2(1)$$
$$= 15 - 2 = 13$$

$$\text{Adj } A = \begin{bmatrix} 5 & -1 \\ -2 & 3 \end{bmatrix}$$

$$A^{-1} = \frac{\text{Adj } A}{|A|}$$

$$A^{-1} = \frac{\begin{bmatrix} 5 & -1 \\ -2 & 3 \end{bmatrix}}{13} = \begin{bmatrix} 5/13 & -1/13 \\ -2/13 & 3/13 \end{bmatrix}$$

Identity Matrix:

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