

# DISCRETE STRUCTURES



- Theory assignments (30%)
  - Quiz (32%)
  - Mid-Sem (38%)
- } (H1)

## \* PROPOSITIONAL LOGIC:

### ◦ Proposition:

- A mathematical statement that is either True or False.

Ex:  $2+2=4$      $2+2=1$ , etc.

### ◦ Operations:

1] Negation: Let  $p$  be a proposition. Then the negation of  $p$  (denoted as  $\neg p$ ) is the complement of  $p$ .  
 "NOT  $P$ " → stays a proposition

Ex:	P	T	F	}	→ Truth Table
	$\neg P$	F	T		

2] Conjunction (AND): Let  $p, q$  be propositions. Then the conjunction of  $p \wedge q$  ( $p \wedge q$ ) is true only when both  $p \wedge q$  are true. → stays a propos?

Ex:	P	q	$p \wedge q$
	T	T	T
	T	F	F
	F	T	F
	F	F	F

3] Disjunction (OR):  $(p \vee q)$  is false only when both false.

4] Exclusive OR (XOR):  $(p \oplus q)$  is true only when one of  $p \oplus q$  is "exclusively" true.

promise or  
antecedent ← conclusion → exactly one of them is true

5] Implication:  $(p \rightarrow q)$  is false, when  $p$  is true &  $q$  is false.  
 $\rightarrow (\neg p \vee q)$  otherwise true.

Ex:	P	q	$p \rightarrow q$
	T	T	T
	T	F	F
	F	T	T
	F	F	T

} vacuously true statements

6] Bijmplication:  $(p \leftrightarrow q)$  is true, when  $p \wedge q$  have same truth value.  
 $\rightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$

1] Tautology: (T)

- When a compound proposition is always true.

2] contradiction: (F)

- When a compound proposition is always false.

#	P	q	$p \rightarrow q$	$q \rightarrow p$	$\neg p \rightarrow \neg q$	$\neg q \rightarrow \neg p$
	T	T	T	T	T	T
	T	F	F	T	T	F
	F	T	T	F	F	T
	F	F	T	T	T	T

⇒ 1)  $p \rightarrow q$  = implication

2)  $q \rightarrow p$  = converse

3)  $\neg q \rightarrow \neg p$  = contrapositive

4)  $\neg p \rightarrow \neg q$  = inverse

Logically Equivalent



Logically Equivalent



3] Elementary Laws:

$$1] p \wedge T \equiv p, p \vee T \equiv T$$

$$4] (p \vee q) \vee r \equiv p \vee (q \vee r)$$

$$2] p \vee F \equiv p, p \wedge F \equiv F$$

$$5] p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

$$3] p \wedge q \equiv q \wedge p, p \vee q \equiv q \vee p$$

$$6] p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

4] Interesting Identities:

$$1] p \vee (p \wedge q) \equiv p$$

2] De-Morgan's Laws:

$$\begin{cases} \neg(p \vee q) \equiv \neg p \wedge \neg q \\ \neg(p \wedge q) \equiv \neg p \vee \neg q \end{cases}$$

↳ Intuition necessary, less harsh approach

Q] Show that  $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$ .

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

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

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

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

$$= \neg p \wedge \neg q$$

∴ QED

## \* Predicates:

- Propositions whose truth values depend on the values of the variable assigned to it.

## \* Quantifiers:

1] Universal -  $p(x)$  is true  $\forall x$  in a domain  $D$ .

2] Existential -  $p(x)$  is true for at least one value in domain  
 $\Rightarrow \exists x \in D$  s.t.  $p(x)$  is true

#	Statement	When True?	When False?
	$\forall x \in D, p(x)$	$\forall x$ s.t. $p(x)$ true	$\exists x$ s.t. $p(x)$ false
	$\exists x \in D, p(x)$	$\exists x$ s.t. $p(x)$ true	$\forall x$ s.t. $p(x)$ false
$\rightarrow$	$\neg (\forall x, p(x)) \equiv \exists x, \neg p(x)$		
	i.e., $\neg (\exists x, p(x)) \equiv \forall x, \neg p(x)$		

Q) Break Goldbach's conjecture into predicate, quantifier, domain.

$\rightarrow$  [Goldbach's Conjecture: For every even integer  $n > 2$ ,  $\exists$  primes cause not proven  $p \in \mathbb{P}, q \in \mathbb{P}$  s.t.  $n = p+q$ ]

Let Evens = even  $\mathbb{Z} > 2$  & Primes = prime no.s

$\rightarrow \forall n \in \text{Evens}, \exists p, q \in \text{Primes} : n = p+q$

$\rightarrow (\forall n, n \in \text{Evens}) \longrightarrow (\exists p, q ; p \in \text{Primes} \wedge q \in \text{Primes} \wedge n = p+q)$

Imp: cannot write as:

$\exists p, q \in \text{Primes} : \forall n \in \text{Evens}, n = p+q$

$\therefore \rightarrow$  pick any  $p, q$  first they will add up to all Evens

check if  $\forall p, q \in \text{Primes}, \exists n \in \text{Evens}$  s.t.  $n = p+q$  is logically equivalent to Goldbach's conjecture

$\rightarrow$  NO its not as this states for any two primes an even exists, obviously does not work for 2.

Q] Form mathematical statements.

1) The sum of 2 +ve integers is always +ve.

$$\Rightarrow \forall x, y \in \mathbb{N} : x+y > 0$$

$$\text{OR } \forall x, y \in \mathbb{Z}, x > 0 \wedge y > 0 \rightarrow x+y > 0$$

Q] Show that:  $\exists x \forall y, P(x, y) \rightarrow \forall y \exists x P(x, y)$  is a valid assertion whenever  $x$  &  $y$  share the same domain.

Proof: Let  $D$  be the domain for  $x \in y \in P_0$  be some predicate over  $D$

If  $\exists x \in D, \forall y \in D, P_0(x, y)$  is true then ② is true

①

→ From 'exists'; for some  $d \in D \forall y \in D, P_0(x, y)$

→  $P_0(d, d)$  true &  $d \in D$

→ For any  $d \in D \exists$  atleast one  $d_0, P(x, y)$

→ ② ∴ QED

\* Satisfiability problem (SAT):

- Satisfactory result when prop<sup>n</sup> true.

- True = 1, False = 0

$$\rightarrow P(x_1, x_2, \dots, x_n) = (x_1 \vee x_2 \vee \neg x_3) \wedge (x_4 \vee \neg x_5 \vee x_6) \wedge \dots \wedge (\neg x_{n-2} \wedge \neg x_{n-1} \wedge x_n)$$

= 3-SAT as 3 literals per clause (3 literals per clause)

→ 1ly,  $k$ -SAT

→  $C(n)$  solves/decides problem  $P$  in 'T' time if:

&  $x \in P, C(n)$  outputs YES/ACCEPT in 'T' steps

&  $x \notin P, C(n)$  outputs NO/REJECT in 'T' steps

→ For an input of  $n$ -bits bit string, a computational model [here  $C(n)$ ] is said to be efficient if  $T = \underline{\text{polynomial}}(n)$ .

Solve 3-SAT in time  $T = \underline{\text{poly}}(n)$ .

MILLION DOLLAR QUESTS:

Theorem: Important prop<sup>n</sup>

Lemma: Preliminary prop<sup>n</sup> useful for proving later "prop"

Corollary: Prop<sup>n</sup> that follows in only a few logical steps from a theorem/lemma.

\* Direct Proofs:

Prop?: If  $n$  is even, then  $n^2$  is even. If  $n$  is odd then  $n^2$  odd.

Proof: Let  $n = 2k \Rightarrow n^2 = 4k^2 \Rightarrow$  even

Let  $n = 2k+1 \Rightarrow n^2 = 4k^2 + 4k + 1 = 2m+1 \Rightarrow$  odd

\* Proof by Contraposition:

$$\rightarrow P \rightarrow Q \equiv \neg Q \rightarrow \neg P$$

Prop?: If  $\sqrt{r} \notin \mathbb{Q}$ , then  $\sqrt{r} \in \mathbb{Q}$

Proof: forming contrapositive: if  $\sqrt{r} \in \mathbb{Q}$  then  $r \in \mathbb{Q}$

Let  $\sqrt{r} \in \mathbb{Q} \Rightarrow \sqrt{r} = \frac{p}{q}$  where  $p, q \in \mathbb{N}$

$$\Rightarrow r = \frac{p^2}{q^2} = \frac{a}{b} \text{ where } a, b \in \mathbb{N} \Rightarrow r \in \mathbb{Q}$$

$\therefore$  If  $r \notin \mathbb{Q}$  then  $\sqrt{r} \notin \mathbb{Q}$

Prop?: If  $n^2$  is even, then  $n$  is even

Proof: If  $n$  is odd,  $n^2$  odd (proven above)

\* Proof by Equivalence:

$$\rightarrow P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$$

Prop?: The std. dev<sup>n</sup> of a sequence of values  $x_1, x_2, \dots, x_n$  is zero iff all the values are equal to their mean.

Proof: Let  $\forall i \in [1, n] x_i = u \Rightarrow \sigma(x_1, x_2, \dots, x_n) = 0$

& let  $\sigma(x_1, x_2, \dots, x_n) = 0 \Rightarrow \sum (x_i - u)^2 = 0$

$\Rightarrow$  sum of  $^2 = 0 \Rightarrow$  all 0  $\Rightarrow \forall i x_i = u \therefore \text{QED}$

\* Proof by contradiction:

Steps: ① We use proof by contradiction

② "Suppose  $P$  is false"

③ " $\neg P \rightarrow F$ " holds

④ This is a # hence  $P$  is true.

Prop: Let  $x \in \mathbb{Z}, y \in \mathbb{Z}^+$ , then  $\frac{x+y}{2} \geq \sqrt{xy}$

Proof: We will use proof by contradiction

$$\text{say } \frac{x+y}{2} < \sqrt{xy} \Rightarrow \frac{(x+y)^2}{4} < xy$$

$$\Rightarrow x^2 + 2xy + y^2 < 4xy \Rightarrow (x-y)^2 < 0 \quad \# \quad \therefore \text{QED}$$

Prop:  $\sqrt{2}$  is irrational

Proof: Say  $\sqrt{2} \in \mathbb{Q} \rightarrow \exists p, q \in \mathbb{N}$  s.t.  $\sqrt{2} = \frac{p}{q}$  where  $\text{HCF}(p, q) = 1$

$$\Rightarrow 2 = \frac{p^2}{q^2} \rightarrow 2q^2 = p^2$$

$\rightarrow p^2$  is even  $\rightarrow p$  is even  $\Rightarrow p = 2k$

$$\rightarrow 2q^2 = 4k^2 \rightarrow q^2 \text{ even} \Rightarrow q \text{ even} \quad \# \quad \text{as HCF}(p, q) = 1 \quad \therefore \text{QED}$$

\* Proof by Induction:

o Inductive axiom by Peano:

- Given a set  $A$  of positive integers, suppose the following:

$$\rightarrow 1 \in A$$

$$\rightarrow \text{If } k \in A, \text{ then } k+1 \in A$$

Then,  $A = \mathbb{N}$

1] Show  $P(x)$  true for  $x=1$ . **Basic Step**

2] Whenever the  $\boxed{P(x)}$  true for  $x=k$ ,  $P(x)$  also true for  $x=k+1$

$\rightarrow$  Then  $P(x)$  holds  $\forall n \in \mathbb{N}$ .

\* Harmonic Numbers:

-  $H_j$  s.t.  $j \in \mathbb{N} \rightarrow H_j = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{j}$

Prop: Prove that  $H_{2n} \geq 1 + n/2$ ,  $\forall n \in \mathbb{N}_0$

Proof: Let  $P(x)$  be the prop<sup>n</sup> that  $H_{2x} \geq 1 + x/2$

$\therefore$  for  $n=0$ ,  $P(0)$  = True as  $H_{20} = 1 \geq 1 + 0/2$

Now, for  $n=k$ , let  $P(k)$  = True  $\Rightarrow H_{2k} = 1 + \frac{1}{2} + \dots + \frac{1}{2k} \geq 1 + k/2$

$n=k+1$ ,  $P(k+1) = 1 + \frac{1}{2} + \dots + \frac{1}{2k} + \frac{1}{2k+1} \geq 1 + (k+1)/2$

$$\Rightarrow H_{2k+1} = \frac{1}{2k+1} \geq \frac{1+k}{2} + \frac{1}{2k+1}$$

P.T.O.

$$H_{2^{k+1}} \Rightarrow H_{2^k} + \frac{1}{2^k+1} + \dots + \frac{1}{2^{k+1}} > 1 + \frac{k}{2} + \frac{1}{2^k+1} + \dots + \frac{1}{2^{k+1}}$$

→ as an expression lower than  $\geq 1 + k/2 + 2^k (1/2^k + 2^k)$   
current works (lowest thus taken)  $\geq 1 + k/2 + 2^k/2 \cdot 2^k$

∴ QED

$$\geq 1 + k/2 + 1/2$$

### • Strong Induction:

-  $P(1)$  is true

- If  $P(k)$  true  $\forall 1 \leq k \leq n$ , then  $P(n+1)$  is true

1)  $P(1)$  is true. Basic step

2) If  $P(k)$  true  $\forall 1 \leq k \leq n$  then  $P(n+1)$  also true

→  $P(n)$  true  $\forall n \in \mathbb{N}$ .

Inductive Hypothesis

Statement → Let  $P(n)$  be a prop over  $n$ . Let  $a \in \mathbb{N}$  & suppose:

i)  $p(a)$  is true

ii)  $\forall n \geq a$ , if  $p(k)$  true  $\forall a \leq k \leq n$ , then  $p(n+1)$  also true.

Then  $p(n)$  is true  $\forall n \geq a$ .

Proof: We suppose that  $p(a)$  is true. Define  $q(n) = \bigwedge_{k=a}^n p(k)$

→  $q(n)$  true, thus  $p(n)$  true, so it is sufficient to show that  $q(n)$  is true  $\forall n \geq a$ .

Thus:  $p(a)$  true  $\Rightarrow q(a)$  true

Now, assume for some  $n \geq a$ ,  $q(n)$  is true.  $\therefore q(n)$

This means  $p(k)$  is true  $\forall a \leq k \leq n$ . So by ②  $p(n+1)$  true.

→ So by "Weak Induction"  $p(n)$  is also true  $\forall n \geq a$ . ∴ QED

Prop? Given  $n \in \mathbb{N}_0$ , define  $a_n$  recursively as follows:

$$a_0 = 1, a_1 = 3, a_n = 2a_{n-1} - a_{n-2}, \forall n \geq 2$$

Prove that  $\forall n \geq 0$ ,  $a_n = 2n+1$ .

here weak induction doesn't hold as, for  $n+1$  is dependant on  $n \in \mathbb{N}-1$  & we have no assumptions about  $n-1$

Proof: Base cases:  $n=0$ ,  $a_0 = 2(0)+1 = 1$ ,  $a_1 = 2(1)+1 = 3$

Strong Inductive

Hypothesis: Let for some  $n \geq 1$  we have  $a_k = 2k+1, \forall 0 \leq k \leq n$

Now,  $a_{n+1} = 2a_n - a_{n-1} + n+1 \geq 2$

$$\Rightarrow a_{n+1} = 2(2n+1) - 2(n-1)+1 = 2(n+1)+1 \therefore \underline{\text{QED}}$$

## \* Elementary Set Theory:

- A set is an unordered collection of elements.

### • Equality of sets:

$$-(S=T) \leftrightarrow (\forall x, x \in S \leftrightarrow x \in T)$$

### • Subsets:

$$-(S \subseteq T) \leftrightarrow (\forall x, x \in S \rightarrow x \in T)$$

$$-(S \subset T) \leftrightarrow (\forall x, x \in S \rightarrow x \in T) \wedge (\exists x, x \in T \wedge x \notin S)$$

★ TPT for all sets  $S$ ,  $\emptyset \subseteq S$ .

$$\rightarrow (\emptyset \subseteq S) \leftrightarrow (\forall x, x \in \emptyset \rightarrow x \in S)$$

F  $\Rightarrow$  entire statement becomes vacuously true

$$- P(S) = \{x \mid x \subseteq S\}$$

★  $\emptyset = \{\}$ ,  $P(\emptyset) = \{\emptyset\}$ ,  $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ , ...

### • Cartesian Product:

$$-(S \times T) = \{(s, t) \mid (s \in S \wedge t \in T)\}$$

$$\rightarrow S_1 \times S_2 \times \dots \times S_n = \{(\underbrace{s_1, s_2, \dots, s_n}) \mid s_i \in S_i, 1 \leq i \leq n\}$$

*n-tuple*

★ Let  $S$  be the set of all sets that are not members of themselves, i.e.  $S = \{x \mid x \notin x\}$   $\rightarrow$  This kinda method is called diagonalization

★ Q) Does  $S \in S$ ? (Paradox)  $\rightarrow S \in S \leftrightarrow S \notin S$  ★

$\rightarrow$  ZFC axioms redefine set theory to avoid these paradoxes.

## \* Elementary Functions:

- For a  $f: S \rightarrow T$ , every  $s \in S$   $\exists$  exactly one  $t \in T$ .  
*domain*  $\hookrightarrow$  *co-domain*

- Range:  $\{y \mid y = f(x)\} \Rightarrow \text{Range} \subseteq \text{codomain}$

### • Injective function (one-one):

-  $f: S \rightarrow T$  is injective if for every  $t \in \text{Range}(f)$ ,  $\exists$  unique  $s \in S$ , s.t.  $f(s) = t$ , i.e.  $f(x) = f(y) \rightarrow x = y \wedge x \neq y \Rightarrow f(x) \neq f(y)$

### • Surjective function (onto):

-  $\forall y \in T, \exists x \in S$  s.t.  $y = f(x)$ , i.e.  $\text{Range}(f) = \text{codomain}(f)$

### • Bijective function:

-  $f: S \rightarrow T$  is bijective  $\leftrightarrow$  surjective  $\wedge$  injective

### \*] Schröder-Bernstein Theorem:

- For any pair of sets  $S$  and  $T$  if

(works for both finite & infinite sets)

**cardinality**

1)  $|S| \leq |T|$  ( $\exists$  an injection from  $S \rightarrow T$ )

2)  $|S| \geq |T|$  ( $\exists$  a surjection from  $S \rightarrow T$ )

3)  $|S| = |T|$  ( $\exists$  a bijection from  $S \rightarrow T$ )

### \*] Countable Sets:

- A set  $S$  is countable iff:

(i)  $S$  is finite OR (ii)  $S$  has same cardinality as  $\mathbb{N}$

→ For a countable set we can list its elements in same order.

Propn: Let  $A$  be a set and  $b \in A$ . Then  $A$  is infinite  $\leftrightarrow A \text{ bij } A \cup \{b\}$

Proof:  $P \leftrightarrow Q = (P \rightarrow Q) \wedge (\underbrace{Q \rightarrow P})$

$\neg P \rightarrow \neg Q$  i.e.  $A$  is finite  $\Rightarrow \neg(A \text{ bij } A \cup \{b\})$

as cardinality would ↑

$Q \rightarrow P \checkmark$

Proving  $P \rightarrow Q$ : Suppose  $A$  is infinite

Then there is a sequence of elements in  $A$ :  $a_0, a_1, a_2, \dots$

which are distinct.

Let  $f(a_0) = b \in f(a_{n+1}) = a_n + n \in \mathbb{N}_0$

$\in f(a) = a + a \in A - \{a_0, a_1, a_2, \dots\}$

$\therefore A \text{ bij } A \cup \{b\} \therefore P \rightarrow Q \checkmark \therefore \underline{\text{QED}}$

∴ Adding an element to an infinite set does not ↑ its cardinality

→ If  $A, B$  are countable then so is  $A \cup B$ .

\* ensure ordering of bijection s.t.  $\mathbb{N}$  does not exhaust before

Q] Is  $\bigcup_{i=1}^{\infty} A_i$  countably infinite?

→  $A_1 = a_1 \quad a_2 \quad a_3 \quad \dots$

$A_2 = b_1 \quad b_2 \quad b_3 \quad \dots$

$A_3 = c_1 \quad c_2 \quad c_3 \quad \dots$

⋮

⇒ bijection from  $\mathbb{N} \rightarrow \bigcup_{i=1}^{\infty} A_i$  exists. countably infinite.

o] Cross products of countable sets:

- Suppose  $A, B$  countable sets. Is  $C = A \times B$  countable?

$$\rightarrow A = \{a_0, a_1, a_2, \dots\} \quad \& \quad B = \{b_0, b_1, b_2, \dots\}$$

$$\therefore C = \{(a_i, b_j) \mid a_i \in A \wedge b_j \in B\}$$

$(a_0, b_0)$	$(a_0, b_1)$	$(a_0, b_2)$	$(a_0, b_3)$	$\dots$
$(a_1, b_0)$	$(a_1, b_1)$	$(a_1, b_2)$	$(a_1, b_3)$	$\dots$
$(a_2, b_0)$	$(a_2, b_1)$	$(a_2, b_2)$	$(a_2, b_3)$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

$$\Rightarrow f(1) = (a_0, b_0), f(2) = (a_0, b_1), f(3) = (a_1, b_0), \dots$$

ensures every ordered pair has a  $\in \mathbb{N}$  ensuring a bijection from  $\mathbb{N} \rightarrow A \times B$ . Thus,  $C$  is countably infinite.

o] Any subset  $S$  of  $\mathbb{N}$  is countable:

Proof: By the Well Ordering Principle  $\exists$  a least element in  $S$ .

Let that element be  $a_0$ . Then the set  $S \setminus \{a_0\}$  is either  $\emptyset$  ( $\Rightarrow$  countable) or the set  $\{S \setminus \{a_0\}\}$  has least element  $a_1$ , then  $S \setminus \{a_0, a_1\}$  is either  $\emptyset$  ( $\Rightarrow$  countable) or  $\{S \setminus \{a_0, a_1\}\}$  has least element  $a_2$ , ... on repeating as evident it either stops somewhere  $\Rightarrow$  finite and countable or  $S = \{a_0, a_1, \dots\} \Rightarrow$  countably infinite (ordering exists)

$$\rightarrow \exists \text{ bijection: } \mathbb{N} \rightarrow S.$$

o] Any subset of a countable set is countable:

Proof: Suppose  $S$  is a countable set (countably infinite). Clearly the prop<sup>n</sup> true if  $S = \mathbb{N}$ . For any such  $S$ , by definition,  $\exists f: S \rightarrow \mathbb{N}$ , s.t.  $f$  is a bijection.

Suppose  $T \subseteq S$ . Consider the set  $\tau = \{f(t) \mid t \in T\}$

Clearly,  $f: T \rightarrow \tau$  is a bijection.

But  $\tau \subseteq \mathbb{N}$ . So bijection:  $\tau \rightarrow \mathbb{N}$

$$\therefore (T \text{ bij. } \tau) \wedge (\tau \text{ bij. } \mathbb{N}) \implies (T \text{ bij. } \mathbb{N})$$

$\therefore \underline{\text{QED}}$

→ A set is countable if it has bij. with  $\mathbb{N}$  & is computably enumerable if  $\exists$  an algorithm that enumerates its members.  
All such sets together are known as recursively enumerable sets.

•]  $\mathbb{Z}$  is countable:

$$\rightarrow \mathbb{Z} = \{-\dots, -1, 0, 1, \dots\} \rightarrow f(1) = 0, f(2k) = k, f(2k+1) = -k$$

$\therefore \mathbb{Z}$  is countable

•]  $\mathbb{Q}^+$  is countable:

$$\rightarrow \mathbb{Q}^+ = \{f(a,b) \mid a \in \mathbb{N}, b \in \mathbb{N}\}_{a/b} \text{ (eliminating } 0 \text{ for simplicity)}$$

Now, cross product of  $a \times b$  gives set of  $a/b$  with duplicate elements (ex:  $1/2, 2/4, 4/8, \dots$ ) which is a countable set.

$\therefore \mathbb{Q}^+ \subseteq a \times b \therefore \mathbb{Q}^+$  is countable

\*] Uncountable Sets:

$$(S \text{ is infinite}) \wedge (\mathbb{Z} \text{ is b.f. N})$$

- Any set is uncountable if it is not countable.

•] The set of all infinite sequences of binary digits is uncountable:

Proof:  $d_i^{(j)} \in \{0,1\}$ ,  $f(1) = s_1 = d_1^{(1)} \oplus d_2^{(1)} \oplus d_3^{(1)} + \dots$   
 $f(2) = s_2 = d_1^{(2)} \oplus d_2^{(2)} \oplus d_3^{(2)} + \dots$   
 $\vdots$  → let it be countable (bij.)

Now using Cantor's diagonalisation we prove that a sequence  $(s^*)$  exists s.t. the bij. fails.

⇒ flip the  $n^{\text{th}}$  digit of the  $n^{\text{th}}$  sequence:

$$\therefore s^* = \neg d_1^{(1)} \neg d_2^{(2)} \neg d_3^{(3)} \dots \neg d_n^{(n)}$$

→  $\exists n \in \mathbb{N}$  s.t.  $f(n) = s^*$   $\therefore$  to earlier claimed bij.

∴ QED

•] The set  $\mathbb{R}$  is uncountable:

Proof: TPT:  $|\mathbb{N}| < |\mathbb{R}|$ ,  $f(x) = x \rightarrow \mathbb{N}$  inf.  $\mathbb{R}$ . ∵  $|\mathbb{N}| < |\mathbb{R}|$

∴ QED

•]  $|\mathbb{[0,1]}| = |\mathbb{R}|$ :

Proof: we use  $\tan x$ , converting the domain of  $\tan x$  from  $[-\frac{\pi}{2}, \frac{\pi}{2}]$  to  $[0,1]$ :  $\tan x \rightarrow \tan(\pi(x-\frac{1}{2}))$   
 $\therefore$  consider  $\tan(\pi(x-\frac{1}{2})) \Rightarrow [0,1]$  bij.  $\mathbb{R}$

∴ QED

•]  $|\mathbb{C}| = |\mathbb{R}|$ :

Proof:  $C = \text{ordered pair of } \mathbb{R} \therefore \underline{\text{QED}}$

→ cannot construct smaller  $\infty$ s than  $\mathbb{N}$ .

\* Can you construct larger infinities?

◦ Cantor's Theorem:

- For any set  $S$ ,  $|S| < |P(S)|$ .

Proof: We prove: i)  $\exists$  injection  $f: S \rightarrow P(S)$

ii)  $\nexists$  any surjection  $f: S \rightarrow P(S)$

Proving (i):  $f: S \rightarrow P(S)$  s.t.  $f(x) = \{x\}$  is an injection.

Proving (ii): For any  $f: S \rightarrow P(S)$ , we will provide a set  $T \subseteq S$  (i.e.  $T \in P(S)$ ) s.t.  $T$  has no pre-image in  $S$ .

•  $\forall x \in S$ ,  $f(x) \subseteq S$

• Either  $x \in f(x)$  or  $x \notin f(x)$

Define  $T = \{x \in S \mid x \notin f(x)\} \subseteq S$  ( $\in P(S)$ )

→ We will show  $T$  has no pre-image in  $S$  via #:

∴ Suppose  $\exists x$ , s.t.  $f(x) = T$ :

i)  $x \notin f(x)$ : We know  $x \in T$ , But  $f(x) = T$  so  $x \in f(x)$   $\#$

ii)  $x \in f(x)$ : We know  $x \in T$ , But  $f(x) = T$  so  $x \notin f(x)$   $\#$

∴  $T$  has no pre-image in  $S \Rightarrow |S| < |P(S)|$  ∴ QED

◦ Recipe to construct larger infinities:

→  $|S| < |P(S)| < |P(P(S))| < \dots$

◦ Continuum hypothesis:

- There is no set  $X$  s.t.  $|\mathbb{N}| < |X| < |\mathbb{R}|$

( $P \in \mathbb{R} \rightarrow P$  both can't be proven)

\* Methods of counting:

◦ Product Rule:

-  $n_i$  ways to do  $t_i$

$$\Rightarrow [\#_t = \prod_{i=1}^k n_i]$$

$$\equiv \left[ \prod_{i=1}^k |A_i| = \prod_{i=1}^k |A_i| \right]$$

cross product

◦ Sum Rule:

-  $n_i$  ways to do  $t_i$

$$\Rightarrow [\#_{vt} = \sum_{i=1}^k n_i]$$

$$\equiv \left[ \left| \bigcup_{i=1}^k A_i \right| = \sum_{i=1}^k |A_i| \right]$$

Ex: Find total number of subsets of  $S = \{s_1, s_2, \dots\}$ .

→ Let the possibility  $s_i$  included in subset = 1  
not included = 0

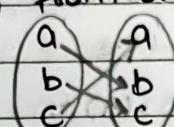
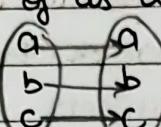
∴ each  $s_i$  either 0 or 1 → Let  $A = \{0, 1\}$

$$\therefore \text{Total subsets} = \left| \bigcup_{i=1}^n A \right| = 2^n$$

o) Permutation: (ordered selection)

- can also be thought of as a bij. from a set to itself.

i.e.  $\sigma: S \rightarrow S \Rightarrow$



, etc.

Ex:  $\sigma(\{1, 2, 3, \dots\}) \rightarrow (\{2, 3, \dots\}) \rightarrow \sigma(1) = 2$

⇒ cardinality of set of all permutations =  $n!$

∴ first element → n choices, 2<sup>nd</sup> → n-1, ... . . . . .

↳ K-Permutation:

- Pick a sequence of length K from n elements & form bij.

$\sigma: S(K) \rightarrow S(K)$

⇒ cardinality of set of all K-permutations =  ${}^n P_K = \frac{n!}{(n-K)!}$   $P(n, k)$

∴ first → n choices, K<sup>th</sup> → (n-(K-1)) choices

o) Combination: (unordered selection)

↳ K-combination:

- Selecting a subset of cardinality K from a set of cardinality n.  $C(n, k)$

⇒ cardinality of set of all K-combinations =  ${}^n C_K = \binom{n}{k} = \frac{n!}{k!(n-k)!}$

${}^n P_K = {}^n C_K \times K!$

↳ ordering K elements

# Prove  ${}^{n+1} C_K = {}^n C_K + {}^n C_{K-1}$  non-algebraically.

→ We need to form subset of length K from set of n+1

→ consider one element from n+1: Now from the leftover n, either form K from those n =  ${}^n C_K$

or form K-1 from those n =  ${}^n C_{K-1}$  and include the considered n+1 th element

$$\therefore {}^{n+1} C_K = {}^n C_K + {}^n C_{K-1}$$

•]  $k$ -permutations with repetitions:

- each element now has  $n$  choices  $\therefore n^k$

•]  $k$ -combinations with repetitions:

- Multisets = sets with repetition

-  $k$ -combination with repetition:

a] order does not matter

b] Repetitions are allowed

$| \text{Multiset} | \Rightarrow$  count repeated elements.

# From set  $S, |S| = n$ , Multisets with cardinality  $k$  can be built s.t.  $k$  can be  $> n$  & needn't be  $\leq n$ .

claim: The no. of  $k$  combinations with repetition from a set  $S$  of  $n$  elements is the total no. of multisets of cardinality  $k$  that can be made from  $S$ .

Q] How many multisets of cardinality 5 can be  $\{a, b, c, d\}$ ?

→ Multiset Separated by bars \* 1 encoding

$[a, a, b, c, d]$  aa|b|c|d \*\*\*|\*|\*|\*

$[a, a, a, a, a]$  aaaaa| ||| \*\*\*\*\*| | |

↳ 3 bars as set has 3 partitions

∴ Total no. of multisets possible = no. of placing 3 bars in  $\star$  1 config. of 8 elements

$$\Rightarrow {}^8C_3$$

K-combination with repetitions:  $\frac{{K+1-1}}{{n-1}}C_{n-1}^{K+1-1} \rightarrow K$  cardinality  
 $n-1$  bars

JEE:  $x_1 + x_2 + x_3 + x_4 = 20 \equiv 20$  cardinality multiset from 4 card. set

$$= {}^{20+4-1}C_{4-1} = {}^{23}C_3$$

\*] Inclusion - Exclusion Principle:

-  $|\bigcup_{i=1}^r A_i| = \sum_{i=1}^r |A_i| \rightarrow$  If mutually disjoint

$$= \sum_{i=1}^r |A_i| - (|A_1 \cap A_2| + \dots + |A_n \cap A_1|) + (|A_1 \cap A_2 \cap A_3| + \dots) \\ - (\dots)$$

Theorem:

$$\rightarrow \sum_{i=1}^k |A_i| = \sum_{\emptyset \neq K \subseteq \{1, 2, \dots, n\}} (-1)^{|K|+1} \cdot |\bigcap_{j \in K} A_j|$$

→ Meaning of  $\emptyset \neq K \subseteq \{1, 2, \dots, n\}$ : ① Exclude  $\emptyset$

- ② Form  ${}^n C _k$  cardinality subsets one by one i.e.  $k=1 \Rightarrow \{1\}, \{2\}, \{3\}, \dots$   
 ③ Ily, repeat for each cardinality.

Proof: Suppose  $s$  is present in  $K$  of these sets,  $s \in A_i; 1 \leq i \leq k$

$\#_s$

$$\begin{aligned} &\sum_{i=1}^k |A_i| \rightarrow s \text{ counted } k \text{ times} \\ &\rightarrow (-) \sum_{1 \leq i \leq j \leq k} |A_i \cap A_j| \rightarrow s \text{ subtracted } {}^k C _2 \text{ times} \\ &\rightarrow (+) \sum_{1 \leq m < n < r \leq k} |A_m \cap A_n \cap A_r| \rightarrow s \text{ added } {}^k C _3 \text{ times} \end{aligned}$$

$$\rightarrow \#_s = {}^k C _1 - {}^k C _2 + {}^k C _3 - \dots$$

$$\text{Now, } {}^k C _0 - (1-x)^n = {}^k C _1 \cdot x - {}^k C _2 \cdot x^2 + {}^k C _3 \cdot x^3 - \dots$$

$$x=1 \rightarrow 1 = {}^k C _1 - {}^k C _2 + {}^k C _3 - {}^k C _4 + \dots$$

$\Rightarrow \#_s = 1 \therefore s \text{ counted only once} \rightarrow \text{Holds defn. of union}$   
 $\therefore \underline{\text{QED}}$

### Applications:

→ Let  $X = \{\pi : [n] \rightarrow [n]\}$ ,  $|X| = n!$ ,  $[n] = \{1, 2, \dots, n\}$   
 total permutations

Now find:  $S = \{\pi : [n] \rightarrow [n] \mid \pi(i) \neq i \forall i \in [n]\}$ ,  $|S| = ?$   
 Derangement

$\Rightarrow |X| = n!$ , Define  $A_i$  where it is a set of all permutations such that pos<sup>n</sup> of  $i$  is fixed.  $\Rightarrow (n-1)!$  permutations

$\Rightarrow \bigcup_{i=1}^n A_i = \text{union of all sets where } i \text{ fixed}$

$$\Rightarrow |S| = - \bigcup_{i=1}^n A_i$$

$$= |S| = n! - \left| \bigcup_{i=1}^n A_i \right|, \left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq K \subseteq \{1, 2, \dots, n\}} (-1)^{|K|+1} \cdot \left| \bigcap_{j \in K} A_j \right|$$

$$\Rightarrow |S| = n! - \sum_{k=1}^n (-1)^{k+1} \cdot \frac{n!}{k!} = \sum_{k=1}^n (-1)^{k+1} \cdot {}^n C _k \cdot (n-k)!$$

$$= n! - \left( \frac{n!}{1!} - \frac{n!}{2!} + \frac{n!}{3!} - \dots + (-1)^{n!} \cdot \frac{n!}{n!} \right) = \sum_{k=1}^n (-1)^{k+1} \cdot \frac{n!}{k!} \rightarrow \sum_{k=0}^n (-1)^k \cdot \frac{n!}{k!}$$

$$= n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right] \therefore D_n = n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right]$$

$$\rightarrow \text{Probability } (D(n)) = \sum_{k=0}^n (-1)^k \cdot \frac{1}{k!}$$

OP 1 - ! check

$$n \rightarrow \infty = \frac{1}{e}$$

$$\therefore P(D(n)) \xrightarrow{n \rightarrow \infty} \frac{1}{e}$$

$\therefore$  If you take a set large enough, 30% chance of derangement

### \*] Pigeon-hole Principle:

- If we place  $\geq n$  pigeons into  $k$  holes then at least one hole contains  $\lceil n/k \rceil$  or more pigeons. ( $\lceil \cdot \rceil = \blacksquare$ )

Ex: During 30 days a student solves at least one problem every day from a list of 45 days. Show that there is a period of several consecutive days during which they solve exactly 14 Qs?

$\rightarrow$  Let  $a_i$  be the number of problems solved during the first  $i$  days.

$$0 < a_1 < a_2 < a_3 < \dots < a_{30} \leq 45 \Rightarrow 14 < a_1 + 14 < \dots < a_{30} + 14 \leq 59$$

30 int mutually distinct

30 int mutually distinct

$\therefore$  List of 60 int all  $\leq 59$   $\therefore$  by PHP  $\exists i, j$  s.t.  $a_j = a_i + 14$

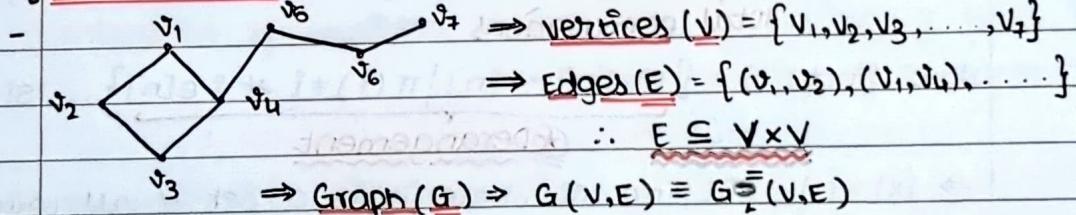
$\therefore$  day  $i+1 \rightarrow$  day  $j$

$$= 14 \text{ Qs.} \quad \therefore \underline{\text{QED}}$$

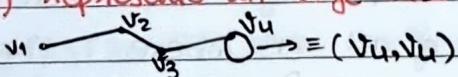
$$a_j - a_i = 14$$

as  $i, j$  mutually  
distinct amongst  
themselves

### \*] GRAPH THEORY:

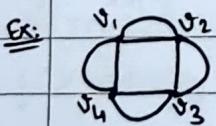


#  $(v_i, v_i)$  represents an edge that is a self loop



### o] Multigraphs:

- Graphs with more than 2 edges b/w vertices



$\rightarrow$  such graphs have "weighted edges"

thus, for such cases, edges redefined to <sup>not</sup> only  
b/w 2 vertices but also having a mapping with IR

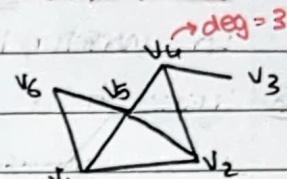
• Simple Graphs:

- A graph in which each edge connects 2 different vertices & where no 2 edges connect the same pair of vertices & where there are no self loops are called simple graphs.
- Vertices  $v \in V$  are said to be **adjacent** if  $\exists (v, v) \in E$ .  
 ↳ Degree of a vertex:

→  $\deg(v) \rightarrow \text{No.}$

→ No. of vertices adjacent to  $v$ .

→ Neighbours of  $v$  ( $\frac{\text{No. of edges}}{\text{incident to } v}$ )



Handshaking Lemma:

For  $G(V, E)$ ,  $\sum_{v \in V} \deg(v) = 2|E|$

↳ sum of degrees of all vertices

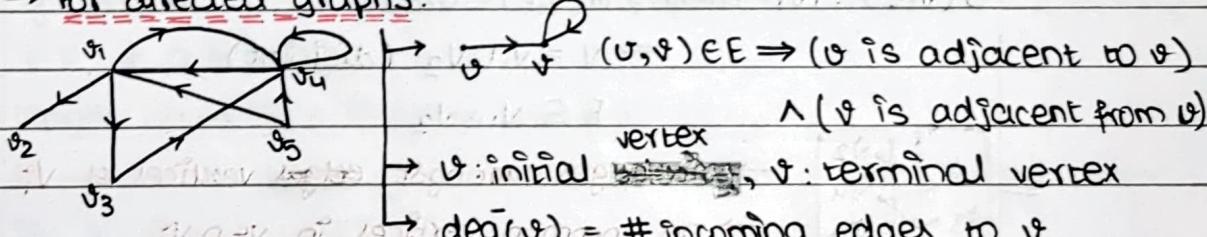
Corollary: An undirected graph has an even no. of vertices of odd degree

Proof:  $\sum_{v \in V} \deg(v) = \sum_{v: \deg(v) \text{ Even}} \deg(v) + \sum_{v: \deg(v) \text{ Odd}} \deg(v)$

Even      Even      Even      ... QED

→ Valid for multigraphs as well, although  $\deg(v)$  for multigraph is no. of edges incident at  $v$ , self loop <sup>thus</sup> contributes two to degree

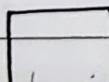
→ For directed graphs:



→ Handshaking Lemma for D.G.:  $\sum_{v \in V} \deg(v) = \sum_{v \in V} \deg^+(v) = |E|$

# If degree( $d$ ) of all vertices of a graph are equal then that graph is called a ' $d$ -regular' graph.

Ex:



= 2-regular graph

↳ some Examples:

### 1) Complete graph ( $K_n$ ):

- All vertices connected to each other.

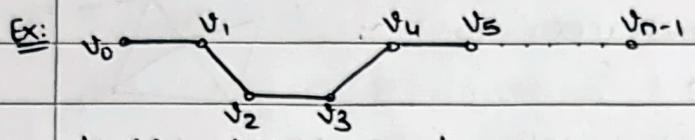
Ex:  $\bullet = K_1$ ,  $\longrightarrow = K_2$ ,  $\Delta = K_3$ ,  $\square = K_4$ ,  =  $K_5$ , etc.

- $(n-1)$ -regular graph

- $\binom{n}{2}$  edges

### 2) Line graph ( $L_n$ ):

- $L_n = (V, E)$ ,  $|V| = n$

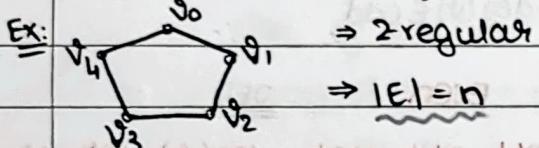


- $\deg(v_0), \deg(v_{n-1}) = 1$

- $\deg(\text{other } v) = 2$ ,  $\rightarrow |E| = n-1$

### 3) Cycle graph ( $C_n$ ):

- Join  $v_0 \in V_{n-1}$  of a line graph

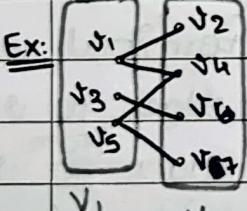


### 4) Bipartite graph ( $B_{m,n}$ ):

- $G(V, E)$ ,  $|V| = m+n$ ,  $G(V, E) = B_{m,n}$

$$\Rightarrow V = V_1 \cup V_2 \quad (\text{disjoint})$$

$$E \subseteq V_1 \times V_2$$



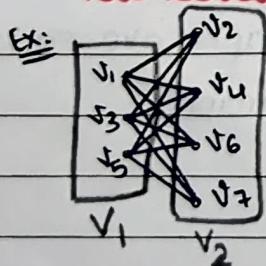
$\rightarrow$  no edges amongst ~~edges~~ vertices of  $V_i$

$\rightarrow$  no common vertices in  $V_i \cap V_j$

$\rightarrow$  Complete Bipartite graphs are those where each

element in  $V_1$  mapped to all in  $V_2$ .

### $\hookrightarrow$ complete Bipartite graphs ( $K_{m,n}$ ):



$$- G(V, E) = K_{m,n}$$

$$\Rightarrow V = V_1 \cup V_2 \quad (\text{disjoint}), |V_1| = m, |V_2| = n$$

$$\therefore |E| = m \times n = V_1 \times V_2$$

$\rightarrow$  for  $V_1$ ,  $\deg(v) = n$  for  $V_2$ ,  $\deg(v) = m$

### 1] Subgraph of a graph:

- Subgraph of  $G(V, E)$  is  $H(W, F)$  s.t.  $W \subseteq V, F \subseteq E$ .

Ex:

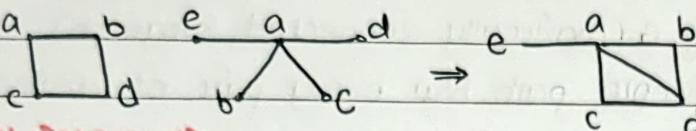


$= G(V, E)$  then  $= H(W, F)$   $\rightarrow$  Subgraph of simple graph need not be simple

### 2] Union of two graphs:

- $G(V_1, E_1) \cup G(V_2, E_2) \rightarrow G(V_1 \cup V_2, E_1 \cup E_2)$

Ex:

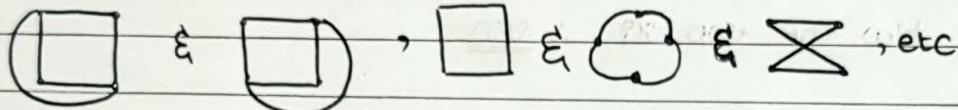


$\rightarrow$  Ill., intersection, cross product etc.

### 3] Graph Isomorphism:

- If  $G_1(V_1, E_1)$  &  $G_2(V_2, E_2)$  are two graphs, then  $G_1$  is isomorphic to  $G_2$  ( $G_1 \cong G_2$ ) iff  $\exists$  a bijection  $f: V_1 \rightarrow V_2$ , s.t. for every pair of vertices  $u, v \in V$ , if  $(u, v) \in E_1$ , then  $(f(u), f(v)) \in E_2$ .

Ex:



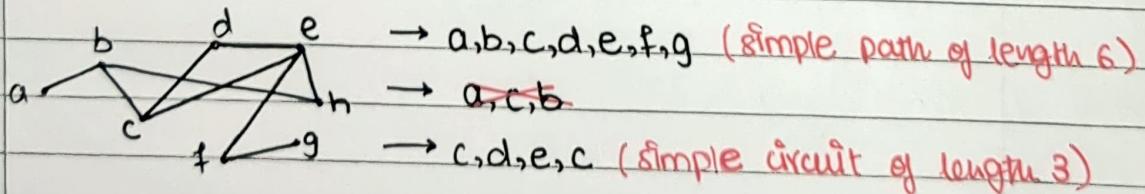
### 4] Path:

- Let  $K \in \mathbb{N}_0$  &  $G$  be an undirected graph. Then a path in  $G(V, E)$  of length  $K$  is a sequence of vertices & edges s.t.  $(v_i, v_{i+1}) \in E$  &  $0 \leq i \leq K-1$ .
- length of path = #edges traversed

$\Rightarrow$  A path of length  $> 0$  that starts & ends at the same vertex is a circuit/cycle.

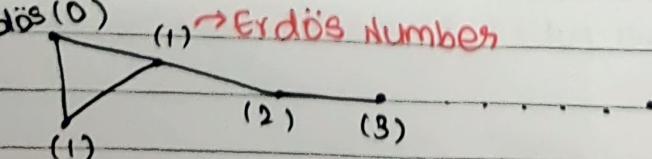
$\Rightarrow$  Any path is called simple if it doesn't contain the same edge more than once.

Ex:



### 5] Collaboration graph

Erdős (0)  $\xrightarrow{(1)}$  Erdős Number



Shortest r to Erdős

### •] Connected Graph:

- An undirected graph is connected if there is a path b/w every pair of distinct vertices in the graph.

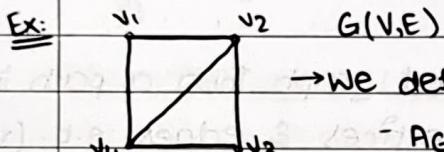
#### ↳ Connected Component:

→ A connected component of  $G$  is a connected subgraph of  $G$  that is not a proper subgraph of another connected subgraph of  $G$  (maximally connected subgraph).

Lemma: There is a simple path b/w every pair of distinct vertices in a connected graph.

Proof: Let  $u, x_1, x_2, \dots, v$  is the path of least length b/w  $u \in E, v$ . We claim this is a simple path, so let it not be a simple path  $\Rightarrow$  vertices:  $x_0, x_1, \textcircled{x}_2, \dots, x_j, \textcircled{x}_{j+1}, \dots, x_n$   $\textcircled{\#}$  as a shorter path can be formed by deleting edges b/w the two  $x_i$  : QED

### •] Representing a Graph using Matrices:



→ We define an adjacency matrix ( $A_G$ ):

-  $A_G \in \{0, 1\}$   $\xrightarrow{\text{Vertices} \times \text{Vertices}}$

$$- a_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \in E \\ 0 & \text{otherwise} \end{cases}$$

$$\Rightarrow A_G = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad \begin{array}{l} \xrightarrow{\text{Sum of each row gives degree of } v_i \text{ for simple directed graphs}} \\ \xrightarrow{\text{For undirected graphs: } A_G = A_G^T \text{ i.e. always symmetric}} \end{array}$$

as the edge  $v_i - v_j \equiv$  edge  $v_j - v_i$

Claim: For any graph  $G$ , let  $A_G$  be the adjacency matrix. Then

(Basic step)  $\#_k$ -paths from  $v_i$  to  $v_j$  equals to the  $(i, j)^{\text{th}}$  entry of  $A_G^K$ .

need not be simple Proof: Basic step: holds for  $K=1$

Inductive hypothesis: Let  $b_{i,j,r}$  be the  $(i, j)^{\text{th}}$  entry of  $A_G^K$ . Then

$b_{i,j,r}$  is the  $\#_r$ -paths b/w  $v_i \in E$  &  $v_j$ .

Let  $(A_G^{K+1})_{i,j} = c_{i,j}^r$ , Now,  $A_G^{K+1} = A_G^K \cdot A_G$

$\rightarrow c_{i,j}^r = \sum_{r=1}^{K+1} b_{i,j,r} * a_{r,j}$  → (Basically  $b_{i,j,r}$  gives  $K$ -length path to  $v_j \in E$ )

↳ TPT: this gives  $\#_{K+1}$ -paths

$a_{r,j}$  gives 1-length path from  $v_r \rightarrow v_j$  : QED

•] Euler & hamilton circuits:

- Can we travel along the edges of a graph starting at a vertex & returning to it by:

(Q1): traversing each edge of the graph exactly once.

(Q2): traversing each <sup>vertex</sup> of the graph exactly once.

→ (Q1): Euler Circuit: Simple circuit containing every edge of G.

Euler Path: simple path

(Q2): Hamilton Circuit: Simple circuit that passes through every <sup>vertex</sup> of G exactly once.

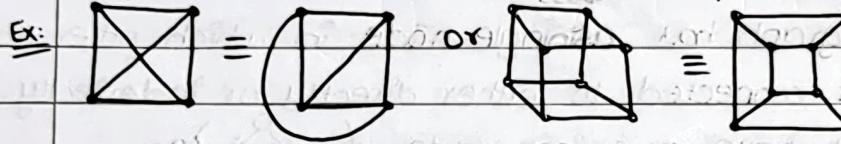
Hamilton Path: simple path

Lemma: A connected graph has an Eulerian circuit  $\leftrightarrow$  every  $\deg(v)$  = even

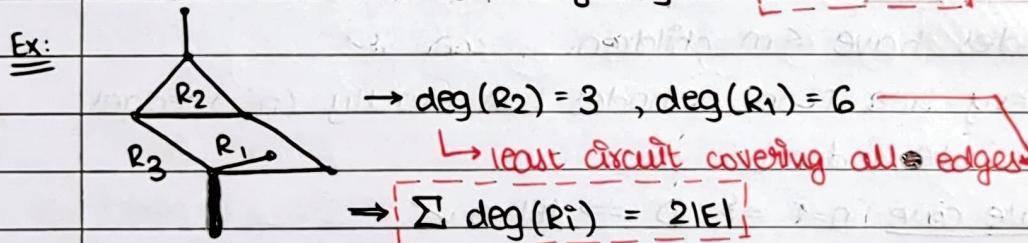
Lemma: G has an Eulerian path (but not Eulerian circuit)  $\leftrightarrow$  exactly two vertices have odd degree (first & last vertex)

•] Planar Graphs:

- Graphs that can be drawn on a plane so no 2 edges cross.



Lemma: Let G be a connected simple planar graph with e edges E, v vertices. Then, the no. of regions  $[r = e - v + 2]$



Corollary 1: If G is a connected planar simple graph, with e edges & v vertices where:  
i)  $v \geq 3$ , then  $e \leq 3v - 6$ .  
ii)  $v \geq 3 \wedge$  no circuits of length 3, then  $e \leq 2v - 4$ .  
If conditions not satisfied then not planar.

MID SEMESTER UNTIL HERE

Second half Taken by Professor Kannan Srinathan

## \* Trees:

Definition: Trees are graphs that are (a) connected (b) Acyclic

Ex: Family Tree, Factor Tree, Recursion Tree

Theorem: A simple graph is a tree iff  $\exists$  a unique path b/w any 2 nodes

Proof: if part:  $\exists$  unique path b/w any two nodes  $\Rightarrow G$  is connected

if  $\bullet$   $G$  has a cycle  $\Rightarrow$  two paths b/w adjacent vertices(nodes)

$\oplus$  Contradiction, as unique path  $\Rightarrow G$  is acyclic

$\therefore G$  is a tree

Only if part: Given a tree  $T$

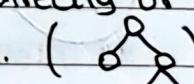
$\rightarrow T$  is connected & acyclic

$\rightarrow \exists$  a path b/w any two nodes  $\rightarrow \exists$  at most one path b/w

$\therefore \exists$  a unique path b/w any two nodes.

$\therefore \text{QED}$

## \* Rooted Trees:

- When the graph has a single node in which other nodes are rooted or connected to either directly or indirectly, i.e. they don't have a parent node. (  )

- Ily, a node with no child nodes = Leaf Node

## \* M-ary Tree:

- Nodes have  $\leq m$  children.

Theorem: Every tree  $T$  on  $n$  nodes has exactly  $(n-1)$  edges.

Proof: We use Induction:

Base case:  $n=1 \Rightarrow 0 \Rightarrow |E|=0 \checkmark$

Inductive hypothesis:  $n=k \Rightarrow |E|=k-1 \checkmark$

Induction step: Consider a tree on  $k+1$  nodes, it must have a leaf node.

Now, delete that leaf node  $\Rightarrow$  new tree generated with  $k$  nodes

$\Rightarrow$  from hypothesis, it has  $k-1$  edges

Now, add the leaf node back, i.e. add an edge

$\Rightarrow k+1$  nodes  $\rightarrow k$  edges.

$\therefore \text{QED}$

$\rightarrow$  If forest of  $n$  nodes, to make it one tree, exactly  $(n-1)$  edges required

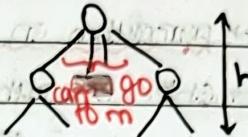
Theorem: Any m-ary tree of height 'h' has  $\leq m^h$  leaves.

Proof: can be done by induction on h. i.e. longest path from original parent to last child (leaf)  
base case:  $h=0$ ,  $m^0 = 1 \rightarrow$  Root ✓

Inductive Hypothesis: Suppose any m-ary tree of height = h-1 has  $\leq m^{h-1}$  leaves.

Induction Step: For tree of height = h

$$m^h = m \cdot m^{h-1} \leftarrow h-1$$



∴ QED

• Traversal Algorithms:

1] Pre-Order Traversal

① Root

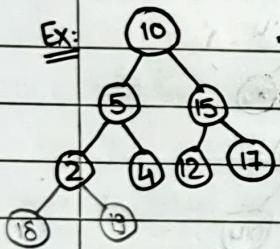
② Recursive on left

sub tree

③ Recursive on right

sub tree

Ex:



→ Pre-Order: 10, 5, 2, 4, 15, 12, 17

→ In-Order: 5, 2, 4, 10, 15, 12, 17 ; 2, 5, 4, 10, 12, 15, 17

→ Post-Order: 5, 2, 4, 15, 12, 17, 10 ; 2, 5, 4, 10, 12, 15, 17

③ Root

(Parent always before)

18, 19 (parent in middle)

18, 19, 4, 5, 12, 15 (parent in end)

17, 15 (parent in end)

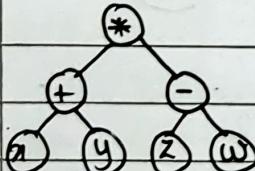
18, 19, 4, 5, 12, 15, 10 (parent in end)

17, 15 (parent in end)

→ applying in-order traversal to BST (Binary search tree)  
we get values in increasing order

Ex:

$$(x+y) * (z-w)$$



→ Pre-Order (Prefix): \* + xy - zw

→ In-Order (Infix): (x+y) \* (z-w)

→ Post-Order (Postfix): xy + zw - \*

• Applications:

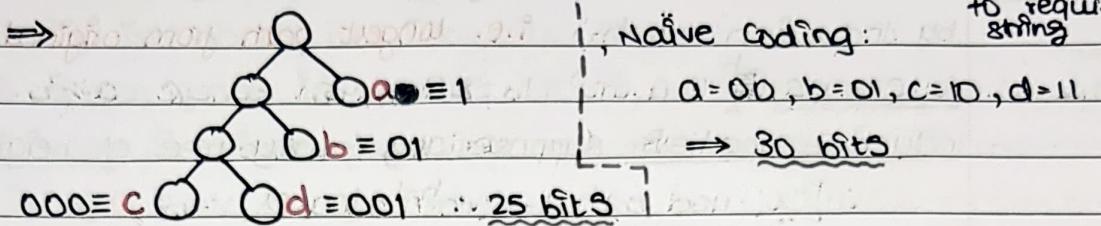
1] Huffman Trees/Codes:

↳ Prefix-Free Codes:

- NO code is a prefix of another code

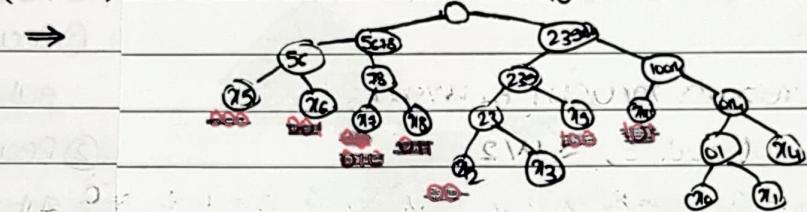
⇒ All leaves

→ Thus, for string  $abaabaaacaabcb$   
 we draw smallest binary tree with exactly 4 leaves, suited to required string

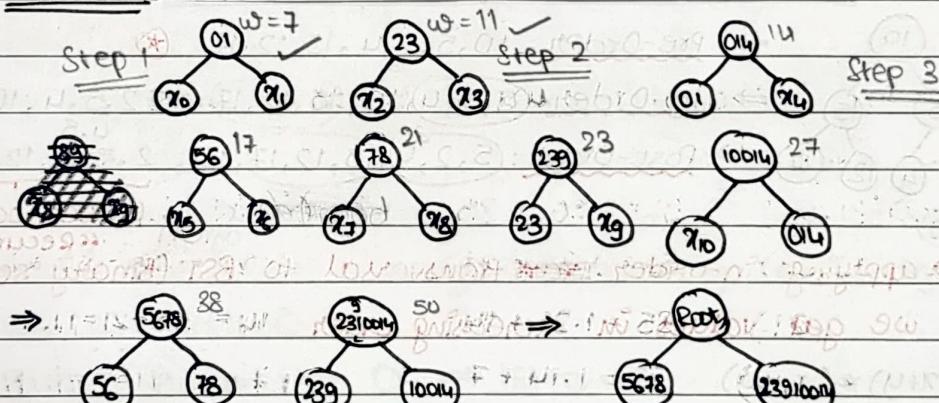


- ↳ Algorithm to Pick best Tree:
- Check weights / frequency
  - Lowest weight at bottom
  - Recurse

Ex:  $x_0(w_0=3), x_1(w_1=4), \dots, x_{10}(w_{10}=13)$

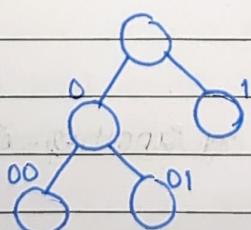


### Procedure



### Encoding:

- Give left subtree a zero & right a 1
- Increase no. of bits by 1 as you move down



## \* Modular Arithmetic:

Q) What is least? s.t.  $ax + by = ?$

→ least? = HCF(a,b)

Theorem: G.C.D. (a,b) = G.C.D. (b,  $a \pmod{b}$ ) where  $a \geq b$ .

Proof:  $c \mid a \wedge c \mid b$  ( $c$  divides  $a \wedge b$ )

$\Rightarrow c \mid a \pmod{b} \because (a \pmod{b}) \equiv a - kb$

$\therefore$  largest common factor same  $\therefore \text{QED}$

## ★ • Euclid's Algorithm: $O(\log(\min(a,b)))$

-  $\text{GCD}(a,b)$

if ( $b == 0$ )

    return  $a$ ;

else

    return  $\text{GCD}(b, a \% b)$ ;

Theorem:  $a \geq b$ ,  $a \pmod{b} \leq a/2$

Proof: Case:  $b \geq a/2 \Rightarrow a \% b = a - b \leq a - a/2 \leq a/2 \therefore \text{QED}$

Case:  $b < a/2 \Rightarrow a \% b < b < a/2 \therefore \text{QED}$

$\therefore$  In Euclid's algo, every 2 steps we're atleast halving

$\Rightarrow$  for  $\text{GCD}(a,b)$ :  $2 \log_2 a$  steps

Ex:  $91x + 56y = 7$

$\rightarrow \text{GCD}(91, 56) \quad 91 = 1 \cdot 56 + 35$

$$35 = [1, -1]$$

$\text{GCD}(56, 35) \quad 56 = 1 \cdot 35 + 21$

$$21 = 56 - 35 = [0, 1] - [1, -1]$$

$\text{GCD}(35, 21) \quad 35 = 1 \cdot 21 + 14$

$$14 = 35 - 21 = [1, -1] - [1, 2] = [-1, 2]$$

$\text{GCD}(21, 14) \quad 21 = 1 \cdot 14 + 7$

$$7 = 21 - 14 = [2, -3]$$

$\text{GCD}(14, 7) \quad 14 = 2 \cdot 7 + 0$

$$0 = 14 - 2 \cdot 7 = [2, -3] - [-6, 10]$$

$\text{GCD}(7, 0)$

$$= [8, -13]$$

Ex:  $187x + 88y = 11$

$\rightarrow \text{GCD}(187, 88) \quad 187 = 2 \cdot 88 + 11$

$$11 = [1, -2]$$

$\text{GCD}(88, 11) \quad 88 = 11 \cdot 8 + 0$

$\text{GCD}(11, 0)$

$\rightarrow$  This is called extended euclid's algorithm

P.T.O.

### 1] Extended Euclid's Algorithm:

-  $ax + by = \gcd(a, b)$   $\quad [x \ y] \begin{bmatrix} a \\ b \end{bmatrix}$

-  $\text{GCD}(a, b) \quad a = q_1 b + r_1$

$\text{GCD}(b, r_1) \quad b = q_2 r_1 + r_2$

$\text{GCD}(r_1, r_2) \quad r_1 = q_3 r_2 + r_3$

$\vdots \quad \vdots$

$r_1 = [x_1 \ y_1] \begin{bmatrix} a \\ b \end{bmatrix}$

$r_2 = [x_2 \ y_2] \begin{bmatrix} a \\ b \end{bmatrix}$

$r_3 = [x_3 \ y_3] \begin{bmatrix} a \\ b \end{bmatrix}$

$\vdots \quad \vdots$

### \* Chinese Remainder Theorem:

-  $x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2} \rightarrow n_i$  are all mutually co-prime

$\vdots \quad \vdots$

$x \equiv a_k \pmod{n_k}$

Ex:  $x < 210$

$x \% 2 = 10$

$x \% 3 = 1$

$x \% 5 = 2$

$x \% 7 = 3$

$x = 52$

- Thus,

$$x \equiv (?) \pmod{\prod_{i=1}^k n_i} \equiv \sum_{j=1}^k a_j \left[ \frac{\prod_{i=1}^k n_i}{n_j} \cdot x_j \right] \pmod{\prod_{i=1}^k n_i}$$

$\left\{ \left( \frac{\prod_{i=1}^k n_i}{n_j} \right)^{-1} \pmod{n_j} \right\}$

NOTE: If  $ab \equiv 1 \pmod{n} \Rightarrow b = a^{-1}$  & vice versa

Solve:  $x \equiv 9 \pmod{17} \quad \& \quad x \equiv 7 \pmod{19}$

$$\rightarrow x \equiv 7 \pmod{17} \quad x \equiv \{7 \cdot (17 \cdot [17^{-1} \pmod{19}]) + 9 \cdot (19 \cdot [19^{-1} \pmod{17}])\} \pmod{323}$$

$$\equiv \{7 \cdot 17 \cdot 9 + 9 \cdot 19 \cdot 9\} \pmod{323}$$

$x \equiv 26$

Solve:  $x \equiv 2 \pmod{11}$ ,  $x \equiv 3 \pmod{13}$  &  $x \equiv 1 \pmod{7}$

$$\rightarrow x \equiv [2[91 \cdot (91^{-1} \pmod{11})] + 3 \cdot [77 \cdot (77^{-1} \pmod{13})] + 1 \cdot [143 \cdot (143^{-1} \pmod{7})]] \pmod{1001}$$

$$91 \equiv 3 \pmod{11} \Rightarrow 91^{-1} \equiv 3^{-1} \pmod{11}$$

$$\Rightarrow 4 \pmod{11}$$

$$77 \equiv 12 \pmod{13} \Rightarrow 77^{-1} \equiv 12^{-1} \pmod{13}$$

$$\Rightarrow 12$$

$$143 \equiv 3 \pmod{7} \Rightarrow 143^{-1} \pmod{7} \equiv 3^{-1} \pmod{7}$$

$$\Rightarrow 5$$

$$x \equiv [2 \cdot 91 \cdot 4 + 3 \cdot 12 \cdot 77 + 143 \cdot 5 \cdot 1] \pmod{1001}$$

$$\therefore \underline{x \equiv 211 \pmod{1001}}$$

### \* Birthday Paradox:

Q) How many people are needed so that there's a clash of birthdays with probability  $\geq 0.5$ ?

$$\rightarrow 23.$$

Theorem: To pick  $q$  from  $N$  objects one at a time with replacement what probability of collision? picking an object again.

$$\frac{q(q-1)}{4N} \leq P[\text{collision}] \leq \frac{q(q-1)}{2N}$$

Proof:

$$P[\text{collision}_q] = 1 - P[\text{No collision}] = 1 - P[\text{No collision}_q]$$

$$= P[\text{No collision}_q] / P[\text{No collision}] - P[\text{No collision}]$$

$$P[\text{No collision}_q] = \left(1 - \frac{q-1}{N}\right) \cdot P[\text{No collision}_{q-1}]$$

$$= \left(1 - \frac{q-1}{N}\right) \left\{1 - \frac{q-2}{N} \cdot P[\text{No collision}_{q-2}]\right\}$$

$$= \left(\prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right)\right) \therefore P[\text{collision}] = 1 - \left(\prod_{i=1}^{q-1} \left(1 - \frac{i}{N}\right)\right)$$

Ex:  $0 < x < 1$

$$1-x < e^{-x} < 1 - \frac{x}{2}, \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right) < \prod_{i=0}^{q-1} e^{-i/N}$$

$$= e^{-1/N} \sum_{i=0}^{q-1} i = e^{-(q-1)q/2N} < \left(1 - \frac{(q-1)q}{4N}\right)$$

P.T.O.

$$\prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right) < \left(1 - \frac{(q-1)q}{4N}\right)$$

$$\text{Hence, } 1 - \prod_{i=0}^{q-1} \left(1 - \frac{i}{N}\right) \geq \left(\frac{(q-1)q}{4N}\right)$$

$\therefore \underline{\text{QED}}$

### \* Recurrence Relations:

- $a_0, a_1, a_2, \dots, a_n, \dots$
- Given by:  $a_n = f(n, a_{n-1}, \dots, a_{n-i})$   $\xrightarrow{i^{\text{th}} \text{ order}}$

E. Boundary cond'ns (like  $a_0 = A$ ,  $a_1 = B$ , etc.)

# Order	Linearity	Homogeneity	Constant Coefficients
First	Linear	Homogeneous	constant
Second	Non-linear	Non-homogeneous	Non-constant

### Examples: First order

linear

$$a_n = a_{n-1}$$

$$a_n = n a_{n-1} + \textcircled{n}$$

homogeneous

$\Rightarrow$  Geometric

$\rightarrow$  Non-constant

constant coefficients

Progressions

coefficients

Ex: Solve:  $a_n = a_{n-1} + f(n)$

(Telescopic)

$$a_{n-1} - a_{n-2} = f(n-1) \Rightarrow a_n = a_0 + \sum_{i=1}^n f(i)$$

$$a_1 - a_0 = f(1)$$

Ex: Solve:  $a_n = 3(a_{n-1})$

$$\Rightarrow a_n = 3[3a_{n-2}] \quad (\text{Expansion})$$

$$= 3^2 a_{n-2} \quad \therefore a_n = a_0 \cdot 3^n$$

Ex: Solve:  $a_n = 3a_{n-1} + n$

$$= 3[3a_{n-2} + (n-1)] + n$$

$$= 3^2 a_{n-2} + 3^1(n-1) + 3^0(n)$$

$$\Rightarrow a_n = 3^i a_{n-i} + \sum_{j=0}^{i-1} 3^j (n-j)$$

$$\rightarrow @ i=n \Rightarrow 3^n a_0 + \sum_{j=0}^n 3^j (n-j)$$

Solve:  $a_n^2 = 3a_{n-1}^2 + n$  (Substitution)

Let  $b_n = a_n^2$

$$\rightarrow b_n = 3b_{n-1} + n \Rightarrow b_n = 3^n b_0 + \sum_{i=0}^{n-1} 3^i (n-i)$$

$$\Rightarrow a_n^2 = 3^n a_0^2 + \sum_{i=0}^{n-1} 3^i (n-i) \Rightarrow a_n = \sqrt{3^n a_0^2 + \sum_{i=0}^{n-1} 3^i (n-i)}$$

Solve:  $a_n = n \cdot a_{n-1} + 1$

$$a_n = n(a_{n-1} + 1) + 1$$

$$= n(n-1)a_{n-2} + n + 1$$

$$\therefore a_n = \underbrace{n! a_0}_{2} + \cancel{n(n-1)} n + n(n-1) + n(n-1)(n-2) + \dots + 1$$

$$\Rightarrow a_n = \underbrace{\sum_{i=0}^{n-1} {}^n P_i a_{n-i}}_{n!} + \sum_{j=0}^{n-1} {}^n P_j$$

### • Second Order:

Ex:  $a_n = a_{n-1} + a_{n-2}$ ,  $a_0 = 0$ ,  $a_1 = 1$

→ Suppose:  $a_n = r^n$  & solve for  $r \Rightarrow r^n = r^{n-1} + r^{n-2}$

$$\Rightarrow r^2 = r + 1 \therefore r = \left( \frac{1 \pm \sqrt{5}}{2} \right)$$

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

$$a_0 = 0 = A+B$$

$$a_1 = 1 = A \left( \frac{1+\sqrt{5}}{2} \right) - A \left( \frac{1-\sqrt{5}}{2} \right) = \frac{A}{2} (1+\sqrt{5}-1+\sqrt{5}) \Rightarrow 1 = A \times 2\sqrt{5}$$

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

$$\therefore A = \frac{1}{\sqrt{5}}, B = -\frac{1}{\sqrt{5}}$$

Solve:  $a_n = 2a_{n-1} - a_{n-2}$

i.e. generalisation  $a_n = \lambda a_{n-1} + \mu a_{n-2}$

Let  $a_n = r^n \Rightarrow r^2 = \lambda r + \mu \therefore r = \lambda \pm \sqrt{4\mu + \lambda^2}$

$$\therefore a_n = A \left( \frac{\lambda + \sqrt{4\mu + \lambda^2}}{2} \right)^n + B \left( \frac{\lambda - \sqrt{4\mu + \lambda^2}}{2} \right)^n$$

$$\Rightarrow \text{if } 4\mu + \lambda^2 > 0 \quad \left| \begin{array}{l} a_n = K \left( \frac{\lambda}{2} \right)^n \\ a_n = (A+Bn) \left( \lambda/2 \right)^n \end{array} \right. \quad \rightarrow \text{if } 4\mu + \lambda^2 = 0$$

E.g. DNE if  $4\mu + \lambda^2 < 0$ .

as we must have 2 unknowns

$$\rightarrow a_n = 2a_{n-1} - a_{n-2}, a_0 = 0, a_1 = 1$$

↳ rigorous way of writing sequence of whole numbers

$$\text{Solve: } a_n = a_{n-1} - a_{n-2}, \quad a_0 = 0, \quad a_1 = 1$$

$$\Rightarrow a_n = r^n \quad \therefore r^2 - r + 1 = 0 \quad \therefore r = \underline{1 \pm i\sqrt{3}}$$

$$\rightarrow a_n = A \left( \frac{1+i\sqrt{3}}{2} \right)^n + B \left( \frac{1-i\sqrt{3}}{2} \right)^n$$

$$\Rightarrow a_0 = 0 = A+B, \Rightarrow a_1 = 1 = \frac{A+B}{2} + \frac{(A-B)i\sqrt{3}}{2}$$

$$\therefore A = \frac{1}{\sqrt{3}}, B = -\frac{1}{\sqrt{3}}$$

$$\therefore a_n = \frac{1}{\sqrt{3}} \left( \frac{1+i\sqrt{3}}{2} \right)^n + \frac{(-1)}{\sqrt{3}} \left( \frac{1-i\sqrt{3}}{2} \right)^n$$

$$= \frac{1}{\sqrt{3}} \left[ e^{in\pi/3} - e^{-in\pi/3} \right] \quad \therefore a_n = \frac{2}{\sqrt{3}} \sin\left(n\frac{\pi}{3}\right) =$$

## 0] Non-Homogeneous Recurrences: (Recommend referring to)

Ex:  $a_n = 2a_{n-1} + 7 \cdot 3^n$ ,  $a_0 > 0$ , ~~some other source~~ some other source)

→ Let  $a_n = B \cdot 3^n$

$$\Rightarrow B \cdot 3^A = \frac{2[B \cdot 3^{A-1}]}{3} + 7 \cdot 3^A$$

$\rightarrow 3B = 2B + 21 \quad \therefore B = 21$

This a 'PARTICULAR SOLUTION'.  $\downarrow$  from coeff??

'GENERAL SOLUTION':  $a_n = A2^n + B \cdot 3^n$

$$a_0 = 0 = A \cdot 2^0 + 21 \cdot 3^0 \Rightarrow A = -21$$

~~Yankee / or / / 0, / / 95 / / 2 / 8 / 20 / 11 / 3~~

$$\text{Verify } a_2 : a_2 = 20, \sqrt{3^2 - 2 \times 1 + 4 \times 9} = 65$$

$$O_2 = 21 \cdot 2^2 + 21 \cdot 3^2$$

$$\therefore a_n = -21 \cdot 2^n + 21 \cdot 3^n$$

$$\text{Solve: } a_n = 3a_{n-1} + 7 \cdot 3^n, a_0 = 1$$

$$a_n = A \cdot 3^n \quad \text{Guess: } a_n = B \cdot n \cdot 3^n : (a_n \text{ also } 3^n)$$

- B<sub>n</sub> if r<sub>n</sub> is not soln.
- ~~B<sub>n</sub>~~ if r<sub>n</sub> is soln for q<sub>n</sub>
- B<sub>n+1</sub> if r<sub>n</sub> is repeated w/ l < n

$$B_0 \cdot 3^n = 3 B(n-1) \cdot 3^{n-1} + 7 \cdot 3^n \Rightarrow B = 7$$

$$a_n = A \cdot 3^n + 7n \cdot 3^n \quad a_0 = A = 1$$

$$\therefore a_n = 3^n + 7n \cdot 3^n$$

$$\underline{\text{Solve:}} \quad a_n = 2a_{n-1} + 3a_{n-2} + 2 \cdot 3^n ; a_0 = 0, a_1 = 1$$

$$\rightarrow a_n^{(N)} = A \cdot (-1)^n + B \cdot 3^n, a_n^{(P)} = Cn \cdot 3^n$$

$$Cn3^n \Rightarrow 2(C(n-1))3^{n-1} + 3(C(n-2)) \cdot 3^{n-2} + 2 \cdot 3^n$$

$$9Cn = 6C(n-1) + 3C(n-2) + 18$$

$$0 = -6C - 6C + 18 \rightarrow C = 3/2$$

$$a_n = A \cdot (-1)^n + B \cdot 3^n + \frac{3}{2}n \cdot 3^n$$

$$a_0 = A + B = 0, a_1 = -A + 3B + \frac{3}{2} \cdot 3^1 = 1$$

$$= -A + 3B = -\frac{7}{2}$$

$$\Rightarrow 4B = -\frac{7}{2} \therefore B = -\frac{7}{8}, A = \frac{7}{8}$$

$$\therefore a_n = \frac{7}{8}(-1)^n + \left(-\frac{7}{8}\right)3^n + \frac{3}{2}n \cdot 3^n$$

$$\underline{\text{Solve:}} \quad a_n = 2a_{n-1} - a_{n-2} + 7, a_0 = 0, a_1 = 1$$

$$a_n^{(N)} = (A_n + B) \cdot 1^n, a_n^{(P)} = Cn^2$$

$$Cn^2 = 2(C(n-1))^2 - C(n-2)^2 + 7$$

$$\Rightarrow Cn^2 = Cn^2 - 2C + 7 \rightarrow C = 7/2$$

$$\therefore a_n = A_n + B + \frac{7}{2}n^2$$

$$a_0 = B = 0, a_1 = A + \frac{7}{2} = 1 \Rightarrow A = -5/2$$

$$\therefore a_n = \frac{-5}{2}n + \frac{7}{2}n^2$$

$$\underline{\text{Solve:}} \quad a_n = 4a_{n-1} - 3a_{n-2} + 5 \cdot 2^n \quad a_0 = 0, a_1 = 1$$

$$a_n^{(N)} = A \cdot 3^n + B, a_n^{(P)} = C \cdot 2^n$$

$$x^2 - 4x + 3$$

$$(x-3)(x-1)$$

$$\therefore C \cdot 2^n = 4C \cdot 2^{n-1} - 3 \cdot C \cdot 2^{n-2} + 5 \cdot 2^n$$

$$\Rightarrow C = -20$$

$$a_n = A \cdot 3^n + B - 20 \cdot 2^n$$

$$a_0 = B - 20 \cdot 2^0 = 20$$

$$a_1 = 3A + B = 401$$

$$\Rightarrow 2A = 201 \therefore A = \frac{201}{2}$$

$$\Rightarrow B = 40 - 201 = \frac{19}{2}$$

$$\therefore a_n = \frac{201}{2} \cdot 3^n + \frac{19}{2} - 20 \cdot 2^n$$

\*] Group Theory:

- A non-empty set  $G$  with an associated binary operator ' $\circ$ ' is a group if:

① Closure:  $\forall a, b \in G, a \circ b \in G$

② Associativity:  $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$

③ Identity:  $\exists e \in G$  s.t.  $\forall a \in G, a \circ e = e \circ a = a$

④ Inverse:  $\forall a \in G \exists b \in G$  s.t.  $a \circ b = b \circ a = e$   
an Abelian

Theorem:  $(\mathbb{Z}, +)$  is a group.

Proof: Closed ✓, Associative ✓, Identity ✓  $e=0$ , Inverse ✓  $b = -a$   
 $\Rightarrow$  Group ✓

NOW,  $\mathbb{Z}$  commutative with  $+$   $\Rightarrow$  Commutative Group = Abelian Group

$\therefore$  QED

Ex: Is the set of all  $2 \times 2$  matrices, say  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  over  $\mathbb{R}$ , s.t.  $ad - bc \neq 0$  with operation of matrix mult a group?

$\rightarrow$  Closure ✓, Associative ✓, Identity ✓  $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$   
Inverse ✓ =  $\frac{1}{|A|} \text{adj. } A$

$\therefore$  Group

Ex:  $(\{1, -1\}, *)$  is a group.

$\rightarrow$  Closure ✓, Associative ✓, Identity ✓  $e = 1$ , Inverse ✓

$\begin{cases} \rightarrow \text{Abelian} \\ \rightarrow \text{Finite} \\ \rightarrow o(G) = 2 \text{ (Group } G \text{ of order)} \rightarrow \text{Finite group order} = o(G) \end{cases}$ 
 $\therefore$  Group

Theorem:  $S$  is a finite set,  $A(S) = \{ f : S \rightarrow S \mid f \text{ is one-one} \}$ . Then

$(A(S), \circ)$  is a group.  $\circ$   $\xrightarrow{\text{composition}}$

$\rightarrow [o(S_n) = n!]$

Symmetric Group ( $S_n$ )  
 $n = 15!$

Theorem: In any group  $G$ :

- ①  $e$  is unique.
- ②  $a^{-1}$  is unique &  $a \in G$ .
- ③  $(a^{-1})^{-1} = a$  &  $a \in G$ .
- ④  $(ab)^{-1} = b^{-1} \cdot a^{-1}$  &  $a, b \in G$ .

Proof: ① Let  $e, f$  be two identity elements

$$\Rightarrow \forall a \in G, ae = a = ea \quad \boxed{e} \quad fe = f = ef \quad (@0=f)$$

$$+ a \in G \quad af = a = fa \quad \boxed{f} \quad ef = e = fe \quad (@a=e)$$

$$\therefore \boxed{e=f}$$

② Cancellation Law: if  $ax = ay$  then  $x = y$  ( $a \cdot a_1^{-1} = a \cdot a_2^{-1} \Rightarrow a_1^{-1} = a_2^{-1}$ )

Let  $b$  be the inverse of  $a$

$$\Rightarrow x = ex = (ba)x = b(ax) = b(ay) = (ba)y = ey = y$$

③  $a \cdot a^{-1} = e$  &  $(a^{-1}) \cdot (a^{-1})^{-1} = e$

$$\Rightarrow a \cdot a^{-1} = (a^{-1})^{-1} \cdot (a^{-1}) \quad \therefore \boxed{a = (a^{-1})^{-1}}$$

④  $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

$$(ab)(ab)^{-1} = e \Rightarrow (ab)(b^{-1}a^{-1}) = ?$$

$$= a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

$$\therefore \boxed{(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}}$$

### \* Subgroups:

- In a group  $(G, \circ)$ , if  $H \subseteq G$  s.t.  $(H, \circ)$  is a group, it is a subgroup of  $G$ .

Ex:  $(\mathbb{Z}, +)$  is a group  $\Rightarrow (\{n \in \mathbb{Z} \mid \exists k \in \mathbb{Z}, n = k\}, +)$  is a subgroup

Theorem: A subset  $H \subseteq G$  is a subgroup iff:

(a)  $\forall a, b \in H, a \cdot b \in H$

(b)  $\forall a \in H, a^{-1} \in H$

Proof: If  $\forall a, b \in H, a \cdot b \in H$  &  $\forall a \in H, a^{-1} \in H \Rightarrow e \in H$

$$a \cdot a^{-1} \in H \rightarrow e \in H$$

If  $G$  is finite:  $H \subseteq G$  is finite too

$a \in H, a^2 \in H, \forall i \in \mathbb{N} a^i \in H$

$$\exists i > j \quad a^i = a^j \rightarrow a^{i-j} = e \rightarrow a^{i-j-1} \cdot a = e$$

$$\Rightarrow a^{i-j-1} = a^{-1} \in H$$

/ /

Define:  $\forall a, b \in G$ ,  $a \equiv b \pmod{H}$  if  $ab^{-1} \in H$ ,  $(\rightarrow)$

Ex:  $G = \{\mathbb{Z}, +\}$ ,  $H = \{n \text{ s.t. } 3 \mid n\}, +) = H$

$$a \equiv b \pmod{H} \Rightarrow ab^{-1} \in H \text{ i.e. } a-b \text{ div. by 3}$$

subgroup of  $G$

Theorem: The relation  $a \equiv b \pmod{H}$  is an equivalence relation

Proof: 1] Reflexive:  $\forall a \in G$  TPT:  $a \equiv a \pmod{H}$

$$\rightarrow aa^{-1} \in H, e \in H \therefore \text{Proved}$$

2] Symmetric: TPT:  $\forall a, b \in G$ ,  $a \equiv b \pmod{H} \Leftrightarrow b \equiv a \pmod{H}$

$$\rightarrow ab^{-1} \in H \stackrel{?}{\Leftrightarrow} ba^{-1} \in H$$

$$\forall a \in H, a^{-1} \in H \Rightarrow (ab^{-1})^{-1} = (b \cdot a^{-1}) \therefore \text{QED}$$

3] Transitive: TPT:  $\forall a, b, c \in G$ ,  $a \equiv b \pmod{H} \wedge b \equiv c \pmod{H}$

$$\Rightarrow a \equiv c \pmod{H}$$

$$\rightarrow ab^{-1} \in H \wedge bc^{-1} \in H \Rightarrow ac^{-1} \in H \therefore (\stackrel{a, b \in H}{\Rightarrow} \stackrel{a, b \in H}{\Rightarrow} a \equiv b \pmod{H})$$

∴ QED

$\Rightarrow a \equiv b \pmod{H}$  is an equivalence relation.

NOTE:  $\equiv \pmod{H}$  partitions  $G$  into equivalence ~~classes~~ classes

◦ Equivalence classes:

- It is a subset of a set that contains elements that are related by an equivalence relation.

agelten 1.N. Bernstein

\*] Cosets:

Definition: Right coset of a wrt H is  $\{ha \in G \mid h \in H\}$ .

Similary likly Left coset is  $\{ah \mid h \in H\}$

$$\rightarrow [a] = \{x \mid a \equiv x \pmod{H}\} \\ = \{x \mid ax^{-1} \in H\}$$

Theorem:  $[a] = \{ha \mid h \in H\}$

Proof: Let  $x \in [a]$

$$\rightarrow ax^{-1} \in H \Rightarrow (ax^{-1})^{-1} \in H \Rightarrow xa^{-1} \in H$$

$$\Rightarrow \exists h \in H, xa^{-1} = h \Rightarrow x = ha, h \in H \Rightarrow x \in \{ha \mid h \in H\}$$

$$\Rightarrow [a] \subseteq \{ha \mid h \in H\}$$

$$\text{Let } x \in \{ha \mid h \in H\} \Rightarrow x = ha, h \in H \Rightarrow xa^{-1} = h \in H$$

$$\Rightarrow (xa^{-1})^{-1} \in H$$

$$\textcircled{1} \Rightarrow [a] \supseteq \{ha \mid h \in H\}$$

$$\Rightarrow ax^{-1} \in H \Rightarrow x \in [a] - \textcircled{1}$$

∴ QED

Ex: → Partitioning group G using right cosets:

$$\{ha \mid h \in H\}$$

$$ha_1, ha_2, \dots, o(H), o(ha) = o(hb)$$

•] Lagrange's Theorem:

- If G is a finite group, then every subgroup H of G is such that  $o(G)$  is a multiple of  $o(H)$ .

Proof: Let  $H = \{h_1, h_2, \dots, h_r\}$

Let  $a \notin H$ , but  $a \in G$

$$h_1, h_2, \dots, h_r \quad \left. \begin{array}{l} \text{2r distinct} \\ \text{elements} \end{array} \right\} \text{2r distinct elements}$$

$b$  s.t. R these  $2r \Rightarrow bh_1, bh_2, \dots, bh_r \quad \left. \begin{array}{l} \text{3r distinct} \\ \text{elements} \end{array} \right\} \text{3r distinct elements}$

→ Let  $ahi = h_j \Rightarrow a = h_j h_i^{-1} \in H$  # contradiction

∴ we have r distinct elements

∴ QED

\*] cyclic subgroup: Any subgroup is cyclic if it has a generator (like  $a$ ) (generated by  $a$ )

-  $G; a \in G$  consider:  $\{e, a, a^2, a^3, \dots\}$

- Order of cyclic subgroup generated by  $a$ ?

→  $\text{o}(a)$ : is the minimum  $z > 0$ , s.t.  $a^z = e$ .  
 $\text{o}(G) \% \text{o}(a) == 0$

\*] Euler's Theorem:

- If  $a$  is coprime to  $N$ , then  $a^{\phi(N)} \equiv 1 \pmod{N}$

where  $\phi(N)$  is the Euler Totient Function of  $N$

↳ #nos coprime to  $N \leq \phi(N)$ .

Proof:

Using above example:

~~$\text{o}(a) = \min \{n \mid n \in \mathbb{Z} \wedge a^n \equiv e\}$~~

~~$\mathbb{Z}_N^* = \{a \mid a \text{ is coprime to } N \leq a \in [1, N]\}$~~

forms a group with operator  $\star \pmod{N}$

$\text{o}(\mathbb{Z}_N^*) = \phi(N)$  since  $\text{o}(G) \% \text{o}(a) == 0$ ,  $a^{\text{o}(a)} = 1 \leq \text{o}(a) | \phi(N)$

→  $e$  is 1.

$a^{\phi(N)} = 1 \leftarrow$

\*] Fermat's Little Theorem:

- If  $p$  is prime then  $\forall a, a^p \equiv a \pmod{p}$

Proof:

$$N = p \Rightarrow \phi(N) = p - 1$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

∴ QED

# Generalising:

$$HK = \{x \in G \mid x = hk, h \in H, k \in K\}$$

$H, K$  are subgroups of  $G$ :

Q] Is  $HK$  a subgroup?

Theorem:  $HK$  is a subgroup if and only if  $HK = KH$

Proof: Suppose  $HK$  is a subgroup, TPT:  $HK = KH$

Let  $x \in HK, x = hk$ , s.t.  $h \in H, k \in K$

$$x^{-1} \in HK \Rightarrow (hk)^{-1} \in HK \Rightarrow k^{-1}h^{-1} \in HK \Rightarrow k^{-1}h^{-1} \in KH \Rightarrow HK \subseteq KH$$

$$\text{Ily, } h^{-1}k^{-1} \in HK \Rightarrow kh \in HK \Rightarrow KH \subseteq HK \Rightarrow \underline{HK = KH}$$

→ Suppose  $HK = KH$  TPT:  $HK$  is a subgroup.

$$h_1 K, \epsilon H K : h_2 K_2 \epsilon H K$$

$$\Rightarrow (h_1 k_1)(h_2 k_2) \in HK$$

$$h_1 K_1 h_2 K_2 = h_1 (h_1' K') K_2 = (h_1 h_1') (K' K_2) \in HK$$

$\xrightarrow{h_1' K' \in KH = HK}$

## \*] Normal Subgroups:

- A subgroup  $N$  of group  $G$  is normal if  $\forall g \in G, \forall n \in N$   
 $\Rightarrow gng^{-1} \in N$

$$\text{Ex: } G = (\mathbb{Z}, +) \quad E: N = (\{\text{multiples of } 3\}, +)$$

Theorem:  $N$  is normal subgroup if & only if  $\forall g \in G, N = \{gng^{-1} \mid n \in N\}$

Proof: Normality of  $N \rightarrow gNg^{-1} \subseteq N$

$$N = eNe^{-1} = g^{-1}(gNg^{-1})g \quad \longrightarrow \quad N = gNg^{-1}$$

$$\text{N} \Rightarrow \subseteq g^1 Ng \mid gNg^{-1} \supseteq N$$

Theorem:  $N$  is normal iff the set of all left cosets of  $N$  is same as the set of all right cosets of  $N$ .

Proof: If  $N$  is normal:  $gN \rightarrow$  left coset,  $Ng \rightarrow$  right cosets

$$\forall g \in G : gNg^{-1} = N \Rightarrow (gNg^{-1})g = gN$$

$$\overbrace{Ng} \quad \rightarrow \quad g_N = Ng$$

$$+ g \in G : gN = Ng$$

$$\Rightarrow gNg^{-1} = Ngg^{-1} \Rightarrow gNg^{-1} = N$$

∴ QED

Theorem: The product of two right cosets of a normal subgroup  $N$  is also a right coset of  $N$ .

Proof:  $(Na)(Nb) = \{ xy \mid x \in Na, y \in Nb\}$

$$\Rightarrow xy = (n_1 a) (n_2 b) \quad | \quad NN = \{n_1 n_2 | n_1 \in N, n_2 \in N\} = N$$

$$= n_1(a n_2)b \Rightarrow (Na)(Nb) = NNab = Nab$$

$$= D_1(n_2 a) b$$

$$= (n_1 n_2) ab$$

∴ QED

## \* Quotient Groups:

- $G|N = \left( \left\{ \begin{array}{l} \text{Set of all} \\ \text{right cosets of } N \end{array} \right\}, \text{Product} \right)$

Theorem:  $G|N$  is a group.

Proof: Closure: Yes ✓  $(Na)(Nb) = Nab$

Associativity: ?  $Na(NbNc) \stackrel{?}{=} (NaNb)Nc$

$$Na(Nbc) \quad (Nab)Nc$$

$$Nabc = Nabc \quad \checkmark$$

Identity:  $Ne$  is the identity

$$\Rightarrow (Na)(Ne) = Nae = N = Nea = (Ne)(Na) \quad \checkmark$$

Inverse: ✓  $\underbrace{(Na)(Na^{-})}_{\text{Inverse}} = Ne \quad \therefore \underline{\text{QED}}$

Ex:  $G = (\mathbb{Z}, +)$

$$N = \{ \text{all multiples of } 3 \}, + , G|N = ?$$

$$\rightarrow G|N = \{ N+0, N+1, N+2 \}, \text{Product}$$