DISCRETE STRUCTURES

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

} (H1)

__/__/____

*] PROPOSITIONAL LOGIC:

◦] Proposition:

- A mathematical statement that is either True or False.

Ex: $2+2=4$ (True), $2+2=1$ (False), etc.

◦] Operations:

1] **Negation**: Let p be a proposition. Then the negation of p (denoted as $\neg p$) is the compliment of p.

"NOT p" → stays a proposition

Ex:

p	T	F
$\neg p$	F	T

→ Truth Table

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

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 & q is "exclusively" true.

↳ exactly one of them is true

premise or antecedant → ($p \rightarrow q$) ← conclusion

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

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

Ex:

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

} vaccuosly true statements

6] **Bi-implication**: ($p \leftrightarrow q$) is true, when p & q have same truth value.

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

__/__/__

◦] Tautology: (T)

- When a compound proposition is always True.

◦] Contradiction: (F)

- When a compound [redacted] proposition is always False.

(#)

p	q	$p \to q$	$q \to p$	$\neg p \to \neg q$	$\neg q \to \neg p$
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) $p \to q$ = implication
2) $q \to p$ = converse
3) $\neg q \to \neg p$ = contrapositive
4) $\neg p \to \neg q$ = inverse

Logically Equivalent

Logically Equivalent

◦] Elementary Laws:

1] $p \wedge T \equiv p$, $p \vee T \equiv T$
2] $p \vee F \equiv p$, $p \wedge F \equiv F$
3] $p \wedge q \equiv q \wedge p$, $p \vee q \equiv q \vee p$
4] $(p \vee q) \vee r \equiv p \vee (q \vee r)$
5] $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
6] $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

◦] Interesting Identities:

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

2] De-Morgan's Laws:

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

} ⊛ Intuition necessary, less harsh approach

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

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

∴ 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?
	$\forall\ x \in D,\ P(x)$	$\forall\ x$ st. $p(x)$ 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

$\Rightarrow$ $[\neg(\forall x, P(x)) \equiv \exists x, \neg P(x)]$

Ily, $[\neg(\exists x, P(x)) \equiv \forall x, \neg P(x)]$

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

→ [Goldbach's conjecture: For every even integer $n > 2$, $\exists$ primes p & q s.t. $n = p+q$] (cause not proven)

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

$\Rightarrow \forall n \in$ Evens, $\exists\ p,q \in$ Primes : $n = p+q$

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

Imp: Cannot write as:

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

$\because \Rightarrow$ pick any p,q first they will add up to all Evens

Hint: Check if $\forall\ p,q \in$ Primes, $\exists\ n \in$ Evens s.t. $n = p+q$ is logically equivalent to Goldbach's conjecture.

→ 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.

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

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

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

Proof: Let D be the domain for x & y & P_0 be some predicate over D

if $\exists x \in D, \forall y \in D, P_0(x,y)$ is true (1) then (2) is true

→ From '$\exists$'; for some $d_0 \in D$ $\forall y \in D, P_0(x,y)$

⇒ $P_0(d_0, d)$ true $\forall d \in D$

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

⇒ (2) ∴ QED

*] Satisfiability problem (SAT):

- Satisfactory result when prop^n True.
- True = 1, False = 0

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

= 3-SAT as 3 literals (3 literals e par kuch bhi allowed)

→ Ily, K-SAT

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

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

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

→ For an input of n-bits bit string, a computational model [here C(x)] is said to be effecient if T = polynomial(n).

MILLION DOLLAR QUES: Solve 3-SAT in time T = poly(n).

__/__/____

Theorem: Important propⁿ
Lemma: Preliminary propⁿ useful for proving later propⁿ
Corollary: Propⁿ that follows in only a few logical steps from a theorem/lemma.

*] **Direct Proofs:**

Propⁿ: 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 $n = 2k+1 \Rightarrow n^2 = 4k^2+4k+1 \equiv 2m+1 \Rightarrow$ odd

*] **Proof by contraposition:**

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

Propⁿ: If $x \notin \mathbb{Q}$, then $\sqrt{x} \notin \mathbb{Q}$

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

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

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

$\therefore$ if $x \notin \mathbb{Q}$ then $\sqrt{x} \notin \mathbb{Q}$

Propⁿ: If n^2 is even, then n is even

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

*] **Proof by Equivalence:**

→ $P \longleftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

Propⁿ: The std. devⁿ of a sequence of values $x_1, x_2, \ldots, x_n$ is zero iff all the values are equal to their mean.

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

& Let $\sigma(x_1, x_2, \ldots, x_n) = 0 \Rightarrow \sum (x_i - \mu)^2 = 0$

$\Rightarrow$ sum of $\hat{}^2 = 0 \Rightarrow$ all $0 \Rightarrow \forall i$ $x_i = \mu$ ∴ 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.

__/__/____

Propⁿ: Let x & $y \in \mathbb{Z}^+$ (& $\neq 0$), then $(x+y)/2 \geq \sqrt{xy}$

Proof: We will use proof by contradiction

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

$\Rightarrow x^2 + 2xy + y^2 < 4xy \Rightarrow (x-y)^2 < 0$ (#) ∴ QED

Propⁿ: $\sqrt{2}$ is irrational

Proof: Say $\sqrt{2} \in \mathbb{Q} \rightarrow \exists\ p,q \in \mathbb{N}$ s.t. $\sqrt{2} = \frac{p}{q}$ where 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 $\Rightarrow p = 2K$

$\rightarrow 2q^2 = 4K^2 \Rightarrow q^2$ even $\Rightarrow q$ even (#) as HCF $(p,q) = 1$ ∴ QED

*] **Proof by Induction:**

°] **Inductive axiom by Peano:**

- Given a set A of positive integers, suppose the following:
  - $1 \in A$
  - If $K \in A$, then $K+1 \in A$

Then, $A \equiv \mathbb{N}$

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

Inductive Hypothesis 2] Whenever the [redacted] $P(x)$ true for $x = K$, $P(x)$ also true for $x = K+1$

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

*] **Harmonic Numbers:**

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

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

Proof: Let $P(x)$ be the propⁿ that $H_{2^n} \geq 1 + n/2$

∴ for $n = 0$, $P(0)$ = True as $H_{2^0} = 1 \geq 1 + [redacted]0/2$

Now, for $n = K$, Let $P(K)$ = True $\Rightarrow H_{2^K} = 1 + \frac{1}{2} + \ldots + \frac{1}{2^K} \geq 1 + K/2$

~~$n = K+1$, $P(K+1) = 1 + \frac{1}{2} + \ldots + \frac{1}{K} + \frac{1}{K+1} \geq 1 + (K+1)/2$~~

~~$\Rightarrow$ [redacted] $H_{2^K} + \frac{1}{2^{K+1}} \geq 1 + \frac{K}{2} + \frac{1}{2^{K+1}}$~~

P.T.O.

__/__/____

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

→ as an expression lower than $\geq 1 + k/2 + 2^k(1/2^k + 2^k)$

current works (lowest thus taken) $\geq 1 + k/2 + 2^k/2 \cdot 2^k$

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

∴ QED

0] Strong Induction:

- P(1) is true
- if P(K) true ∀ $1 \leq K \leq n$, then P(n+1) is true

1] P(1) is true. Basic step

Inductive Hypothesis 2] if P(K) true ∀ $1 \leq K \leq n$ then P(n+1) also true

→ P(n) true ∀ $n \in \mathbb{N}$.

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

i) p(a) is true

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

Then p(n) is true ∀ $n \geq a$.

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 ∀ $n \geq a$

Thus: p(a) true ⇒ q(a) true

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

This means p(K) is true ∀ $a \leq K \leq n$. So by ii) q(n+1) true.

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

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

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

Prove that ∀ $n \geq 0$, $a_n = 2n+1$

here weak induction doesn't hold as, for n+1 is dependant on n & 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 $a_K = 2K+1$, ∀ $0 \leq K \leq n$

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

→ $a_{n+1} = 2(2n+1) - 2(n-1)+1 = 2(n+1)+1$ ∴ 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, $\phi \subseteq S$.

→ $(\phi \subseteq S) \leftrightarrow (\forall x,\ \underbrace{x \in \phi}_{F} \rightarrow x \in S)$ ⇒ entire statement becomes vacuously true

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

⊛ $P = \{\}$, $P(\phi) = \{\phi\}$, $P(\{\phi\}) = \{\phi, \{\phi\}\}$, ...

◦ Cartesian Product:

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

→ $S_1 \times S_2 \times \ldots \times S_n = \{\underbrace{(s_1, s_2, \ldots, s_n)}_{n\text{-tuple}} \mid s_i \in S_i,\ 1 \leq i \leq n\}$

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

⊛ Q] Does $S \in S$? (Russell's Paradox) → $S \in S \leftrightarrow S \notin S$ ⊛

→ ZFC axioms redefine set theory to avoid these paradoxes.

* Elementary Functions:

- For a $f: S \rightarrow T$ (S: Domain, T: Co-domain), for every $s \in S$ ∃ exactly one $t \in T$.
- Range: $\{y \mid y = f(x)\}$ ⇒ Range ⊆ codomain

◦ Injective function (one-one):

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

◦ Surjective function (onto):

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

◦ Bijective function:

- $f: S \rightarrow T$ is bijective ↔ surjective ∧ 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 $S \to T$)

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

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

*] **Countable Sets:**

- A set S is countable iff: (i.e. $\exists$ a bijection from $\mathbb{N} \to S$.)

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

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

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

Proof: $P \leftrightarrow Q = (P \to Q) \wedge (Q \to P)$

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

as cardinality would ↑

$\therefore Q \to P$ ✓

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

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

which are distinct.

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

& $f(a) = a \;\forall\; a \in A - \{a_0, a_1, a_2, \ldots\ldots\}$

$\therefore$ A bij. $A \cup \{b\}$ $\therefore P \to Q$ ✓ $\therefore$ QED

$\therefore$ 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?

→ $A_1 = a_1^{(1)} \; a_2^{(2)} \; a_3^{(4)} \ldots\ldots$

$A_2 = b_1^{(3)} \; b_2^{(5)} \; b_3 \ldots\ldots$

$A_3 = c_1^{(6)} \; c_2 \; c_3 \ldots\ldots$

$\vdots^{(7)}$

$\vdots$

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

__/__/____

◦] Cross products of countable sets:

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

→ $A = \{a_0, a_1, a_2, \ldots\}$ & $B = \{b_0, b_1, b_2, \ldots\}$

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

$(a_0, b_0)^1$ $(a_0, b_1)^2$ $(a_0, b_2)^4$ $(a_0, b_3)^7$ .....

$(a_1, b_0)^3$ $(a_1, b_1)^5$ $(a_1, b_2)^8$ (a_1, b_3) .....

$(a_2, b_0)^6$ $(a_2, b_1)^9$ (a_2, b_2) (a_2, b_3) .....

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

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

◦] 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 ϕ ($\Rightarrow$ countable) or the set $\{S \setminus \{a_0\}\}$ has least element a_1, then $S \setminus \{a_0, a_1\}$ is either ϕ ($\Rightarrow$ 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 $S = \{a_0, a_1, \ldots\} \Rightarrow$ countably infinite (ordering exists)

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

◦] Any subset of a countable set is countable:

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

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

clearly, $f : T \longrightarrow \tau$ is a bijection.

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

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

$\therefore$ 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.

0] $\mathbb{Z}$ is countable:

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

$\therefore \mathbb{N}$ bij. $\mathbb{Z} \Rightarrow$ countable

0] $\mathbb{Q}^+$ is countable:

→ $\mathbb{Q}^+ = \{(a,b) \mid a \in \mathbb{N}, b \in \mathbb{N}\}$ (eliminating 0 for simplicity)
$\equiv a/b$

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

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

*] Uncountable Sets: $\Rightarrow (S \text{ is infinite}) \wedge (\nexists\ (S \text{ bij. } \mathbb{N}))$

- Any set is uncountable if it is not countable.

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

Proof: $d_i^{(j)} \in \{0,1\}$, $f(1) = S_1 = d_1^{(1)}\ d_2^{(1)}\ d_3^{(1)} + \ldots\ldots$

$f(2) = S_2 = d_1^{(2)}\ d_2^{(2)}\ d_3^{(2)} + \ldots\ldots$

$\vdots$ → let it be countable (bij.)

Now using cantor's diagnolisation we prove that a sequence (S^*) exists s.t. the bij. fails.

⇒ Flip the n^{th} digit of the n^{th} sequence:

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

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

$\therefore$ QED

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

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

$\therefore$ QED

0] $|[0,1]| \equiv |\mathbb{R}|$!:

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. $\mathbb{R}$

$\therefore$ QED

0] $|\mathbb{C}| = |\mathbb{R}|$:

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

__/__/____

→ cannot construct smaller ∞s than ℕ.

*] Can you construct larger infinities? :

•] Cantor's Theorem:

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

Proof: We prove: i) ∃ injection $f: S \to P(S)$

ii) ∄ any surjection $f: S \to P(S)$

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

Proving (ii): For any $f: S \to P(S)$, 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 ∃ 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 $x \notin T$, 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:

→ $|S| < |P(S)| < |P(P(S))| < \dots\dots$

•] Continuum hypothesis:

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

(P & ¬P both can't be proven)

*] Methods of Counting:

•] Product Rule:

- n_i ways to do t_i

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

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

cross product

•] Sum Rule:

- n_i ways to do t_i

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

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

P.T.O.

°] K-permutations with repetitions:

- each element now has n choices ∴ n^k

°] K-combinations with repetitions:

- Multisets = sets with repetition
- K-combination with repetition:
  a] order does not matter
  b] Repetitions are allowed

∴ |Multiset| ⇒ count repeated elements.

(#) From set S, |S| = n, Multisets with cardinality K can be built s.t. K can be > n & need'nt be ≤ 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 made from {a,b,c,d}?

→

Multiset	Separated by bars	*·| 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 *·| config. of 8 elements

$\Rightarrow {}^{8}C_3$

∴ K-combination with repetitions: $\boxed{{}^{K+n-1}C_{n-1}}$ → K cardinality, n-1 bars

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

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

*] Inclusion - Exclusion Principle:

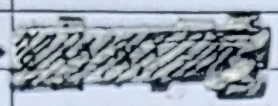
- $\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$ → If mutually disjoint

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

$- (\ldots\ldots)$

__/__/____

Theorem:

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

→ Meaning of $\phi \neq K \subseteq \{1,2,\ldots n\}$: ① Exclude ϕ

② Form all cardinality subsets one by one i.e. $K=1 \Rightarrow \{1\},\{2\},\{3\},\ldots$ (i)

③ Ily, repeat for each cardinality.

Proof: Suppose s is present in K of these sets, $s \in A_i \quad 1 \le i \le K$

no. of times s is counted (#s)

- $\sum_{i=1}^{K} |A_i|$ → s counted K times
- $(-)\sum_{1 \le i < j \le K} |A_i \cap A_j|$ → s subtracted ${}^{K}C_2$ times
- $(+)\sum_{1 \le m < n < r \le K} |A_m \cap A_n \cap A_r|$ → s added ${}^{K}C_3$ times
- ⋮

$\Rightarrow \#_s = {}^{K}C_1 - {}^{K}C_2 + {}^{K}C_3 - \ldots\ldots$

Now, ${}^{K}C_0 - (1-x)^n = {}^{K}C_1 \cdot x - {}^{K}C_2 \cdot x^2 + {}^{K}C_3 x^3 - \ldots\ldots$

$x=1 \Rightarrow 1 = {}^{K}C_1 - {}^{K}C_2 + {}^{K}C_3 - {}^{K}C_4 + \ldots\ldots$

$\Rightarrow \#_s = 1$ ∴ s counted only once → Holds ∀ defn of union

∴ QED

◦] Applications:

→ Let $X = \{\pi : [n] \to [n]\}$, $|X| = n!$, $[n] = \{1,2,\ldots,n\}$

total permutations

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

⊛ Derangement

$\Rightarrow |X| = n!$, Define A_i where it is a set of all permutat^{n}s such that posn of i is fixed. $\Rightarrow (n-1)!$ permutat^{n}s

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

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

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

$\Rightarrow |S| = n! - \sum_{K=1}^{n} (-1)^{K+1} \cdot \frac{n!}{K!} = \sum_{K=1}^{n} (-1)^{K+1} \cdot {}^{n}C_K \cdot (n-K)!$

$= n! - \left(\frac{n!}{1!} - \frac{n!}{2!} + \ldots (-1)^{n+1} \cdot \frac{n!}{n!}\right) = \sum_{K=1}^{n} (-1)^{K+1} \cdot \frac{n!}{K!}$ → $\equiv \sum_{K=0}^{n} (-1)^K \cdot n!/K!$

$= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \ldots\ldots - \frac{1}{n!}\right]$

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

__/__/____

→ OR $1 - \frac{1}{e}$ check

→ $\text{Probability}(D(n)) = \sum_{k=0}^{n} (-1)^k \cdot \frac{1}{k!}$ $\quad n \to \infty = \frac{1}{e}$

$\therefore P(D(n)) \xrightarrow[n\to\infty]{} \frac{1}{e}$

$\therefore$ 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. ($\lceil \cdot \rceil$ = ceiling func.)

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?

→ 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

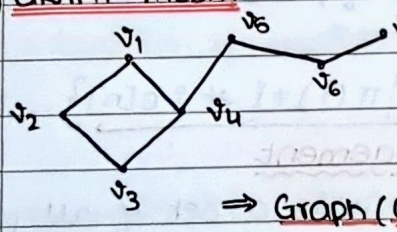
$\therefore$ list of 60 int all ≤ 59 $\therefore$ by PHP $\exists\ i, j$ s.t. $a_j = a_i + 14$

as i, j mutually distinct amongst themselves

$\therefore$ day $i+1 \longrightarrow$ day j $\quad a_j - a_i = 14 \Leftarrow$

$= 14$ Qs. $\quad \therefore$ QED

*] GRAPH THEORY:



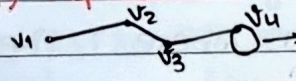
$\Rightarrow$ Vertices $(V) = \{v_1, v_2, v_3, \dots, v_7\}$

$\Rightarrow$ Edges $(E) = \{(v_1, v_2), (v_1, v_4), \dots\}$

$\therefore E \subseteq V \times V$

$\Rightarrow$ Graph $(G) \Rightarrow G(V, E) \equiv G \overset{=}{=} (V, E)$

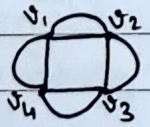
(v_i, v_i) represents an edge that is a self loop



o] Multigraphs:

- Graphs with more than 2 edges b/w vertices

Ex:



→ such graphs have "weighted edges"

thus, for such cases, edges redefined to not only b/w 2 vertices but also having a mapping with $\mathbb{R}$

__/__/__

• Simple Graphs:

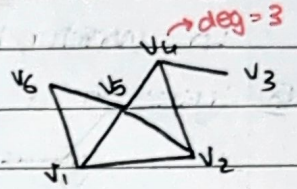
- A graph in which each edge connects 2 different vertices & where no 2 edges connect the same pair of vertices & where there are no self loops are called simple graphs.
- vertices v & v are said to be adjacent if $\exists\ (v,v) \in E$. (neighbours)

↳ Degree of a vertex:

→ deg. $V \longrightarrow \mathbb{N}_0$

→ No. of vertices adjacent to v.

→ Neighbours of v (No. of edges incident to v)



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

↳ Sum of degrees of all vertices

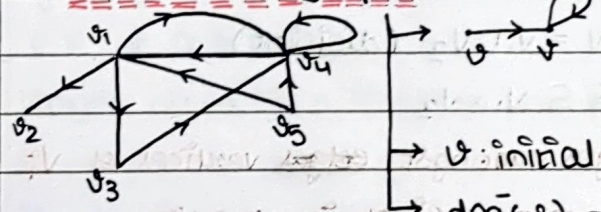
Corollary: An undirected graph has an even no. of vertices of odd degree

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

Even Even Even ∴ QED

→ Valid for Multigraphs as well, although deg(v) for Multigraph is no. of edges incident at v, self loop (thus) contributes two to degree.

→ For directed graphs:



$(v,v) \in E \Rightarrow (v$ is adjacent to $v)$
$\wedge\ (v$ is adjacent from $v)$

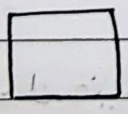
→ v: initial vertex, v: terminal vertex

→ $\deg^-(v)$ = # incoming edges to v

$\deg^+(v)$ = # outgoing edges from v

→ 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):

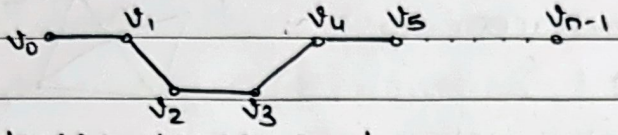
- All vertices connected to each other.

Ex: • = K_1 , — = K_2, △ = K_3,  = K_4,  = K_5, etc.

- $(n-1)$-regular graph
- ${}^nC_2$ edges

2) Line graph (L_n):

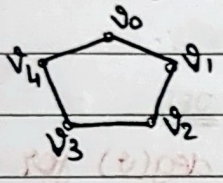
- $L_n = (V, E)$, $|V| = n$

Ex: 

- $\deg(v_0), \deg(v_{n-1}) = 1$
- $\deg(\forall \text{ other } v) = 2$; $\rightarrow |E| = n-1$

3) Cycle graph (C_n):

- Join v_0 & v_{n-1} of a Line graph

Ex: 

$\Rightarrow$ 2-regular

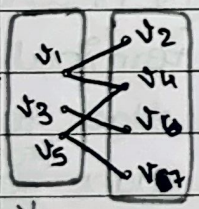
$\Rightarrow |E| = n$

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

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

$\Rightarrow V = V_1 \cup V_2$ (disjoint)

$E \subseteq V_1 \times V_2$

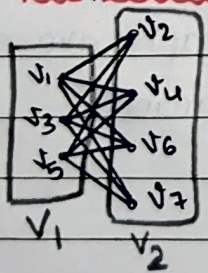
Ex: 

→ no edges amongst ~~edges~~ vertices of V_i

→ no common vertices in $V_i \cap V_j$

→ Complete Bipartite graphs are those where each element in V_1 mapped to all in V_2.

↳ Complete Bipartite graphs ($K_{m,n}$):

Ex: 

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

$\Rightarrow V = V_1 \cup V_2$ (disjoint) , $|V_1| = m$, $|V_2| = n$

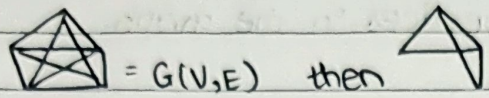
$\therefore |E| = m \times n = V_1 \times V_2$

→ For V_1, $\deg(v) = n$ & for V_2, $\deg(v) = m$

__/__/____

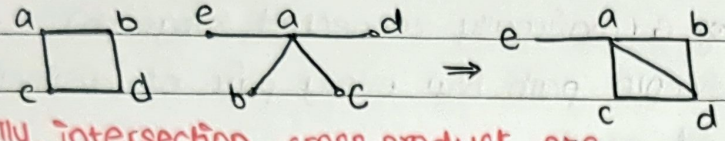
◦] Subgraph of a graph:

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

Ex:  → Subgraph of simple graph need not be simple

◦] Union of two graphs:

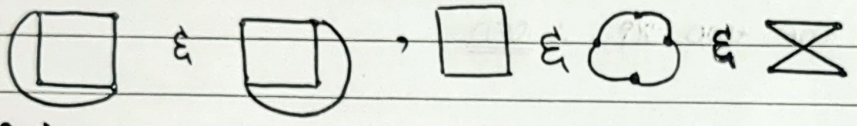
- $G(V_1,E_1)$ & $G(V_2,E_2) \rightarrow G(V_1 \cup V_2, E_1 \cup E_2)$

Ex: 

→ Ny, intersection, cross product etc.

◦] 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 $(f(u),f(v)) \in E_2$.

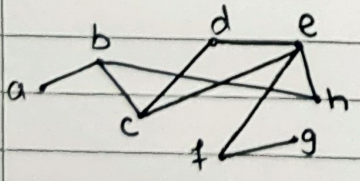
Ex:  & , & & , etc.

◦] Path:

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

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

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

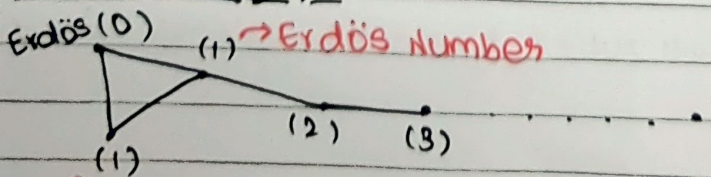
Ex: 

→ a,b,c,d,e,f,g (simple path of length 6)

→ ~~a,c,b~~

→ c,d,e,c (simple circuit of length 3)

Collaboration graph



__/__/____

◦] Connected Graph:

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

↳ **Connected Component:**

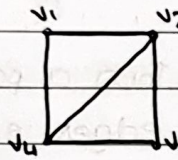
→ A connected component of G is a connected subgraph of G that is not a proper subgraph of another connected subgraph of G (maximally connected subgraph).

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

Proof: Let $u, x_1, x_2, \ldots, v$ is the path of least length b/w u & v. We claim this is a simple path, so let it not be a simple path $\Rightarrow$ vertices: $x_0, x_1, (x_i), \ldots, x_j, (x_j), \ldots, x_n$

(#) as a shorter path can be formed by deleting edges b/w the two x_i ∴ QED

◦] Representing a Graph using Matrices:

Ex: 

$G(V,E)$

→ We define an Adjacency Matrix (A_G): ↳ vertices × vertices

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

$$\Rightarrow A_G = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}_{4\times 4}$$

→ Sum of each row gives degree of v_i for simple directed graphs

→ For undirected graphs: $A_G = A_G^T$ i.e. always symmetric 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 $\#_K$-paths from v_i to v_j equals to the $(i,j)^{th}$ entry of A_G^K.

(need not be simple)

Proof: **Basic Step:** holds for $K=1$

Inductive Hypothesis: Let $b_{i,r}$ be the $(i,r)^{th}$ entry of A_G^K. Then $b_{i,r}$ is the $\#_K$-paths b/w v_i & v_r.

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

→ $c_{i,j} = \sum_{r=1}^{n} b_{i,r} * a_{r,j}$ → (Basically b_{ir} gives K-length path to v_r & $a_{r,j}$ gives 1-length path from v_r to v_j) ∴ QED

↳ TPT: this gives $\#_{K+1}$-paths

__/__/____

◦] 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 vertex of the graph exactly once.

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

Euler Path: simple path ——u——

(Q2): **Hamilton Circuit**: Simple circuit that passes through every vertex of G exactly once.

Hamilton Path: Simple path ——u—— once.

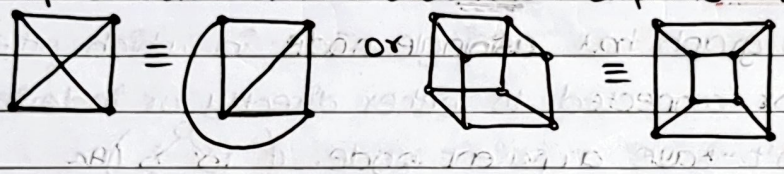
Lemma: A connected graph has an Eulerian circuit ⟷ every deg(v) = even

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

◦] Planar Graphs:

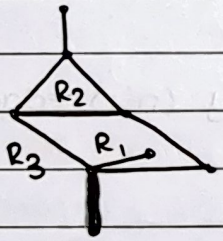
- Graphs that can be drawn on a plane s.t. no 2 edges cross.

Ex:



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

Ex:



→ deg(R2) = 3 , deg(R1) = 6

↳ least circuit covering all edges

→ $\sum \deg(R_i) = 2|E|$

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 Sinathan

__/__/____

*] **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 ∃ a unique path b/w any 2 nodes

Proof: **if part:** ∃ unique path b/w any two nodes ⇒ G is connected

if G has a cycle ⇒ two paths b/w adjacent vertices (nodes)

⊗ Contradiction, as unique path ⇒ G is acyclic

∴ G is a tree

Only if part: Given a tree T

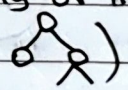
⇒ T is connected & acyclic

⇒ ∃ a path b/w any two nodes ⇒ ∃ atmost one path b/w any two nodes

∴ ∃ a unique path b/w any two nodes.

∴ 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. ()
- lly, a node with no child nodes = Leaf Node

[redacted]•] **M-ary Tree:**

- Nodes have ≤ m children.

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

Proof: We use Induction:

Base Case: n=1 ⇒ 0 ⇒ |E|=0 ✓

Inductive Hypothesis: n=K ⇒ |E| = K-1 ✓

Induction Step: Consider a tree on [redacted] K+1 nodes, it must have a leaf node.

Now, delete that leaf node ⇒ New tree generated with K nodes

⇒ From hypothesis, it has K-1 edges

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

⇒ K+1 nodes → K edges.

∴ QED

→ Or 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.

original parent to last child (leaf)

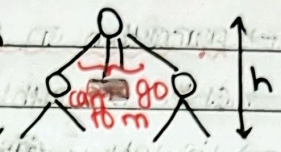
i.e. longest path from original parent to a leaf

Base case: $h = 0$, $m^0 = 1$ → 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

$m^h = m \cdot m^{h-1}$ ← h-1



∴ QED

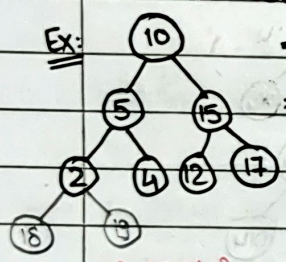
◦] Traversal Algorithms:

1] Pre-Order Traversal
① Root
② Recursive on left sub tree
③ Recursive on right sub tree

2] In-Order Traversal
① Recursive on left sub tree
② Root
③ Recursive on right sub tree

3] Post-Order Traversal
① Recursive on left sub tree
② Recursive on right sub tree
③ Root

Ex:



→ Pre-Order: 10,5,2,4,15,12,17 (parent always before) ✱

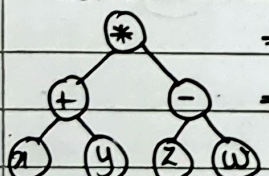
⇒ In-Order: 5,2,4,10,15,12,17 ; 2,5,4,10,12,15,17 ✱ (parent in middle)

⇒ Post-Order: 5,2,4,15,12,17,10 ; 2,4,5,12,15,17,10 ✱ (parent after)

correct way to write "Recursive"

⇒ applying in-order [redacted] transversal 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 Hoffmann Trees / Codes:

↳ Prefix-Free Codes:

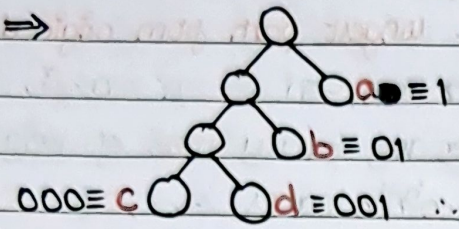
- NO code is a prefix of another code
  ⟹ All leaves

__/__/____

→ Thus, for: abaabaaacadabcb

we draw smallest binary tree with exactly 4 leaves, suited to required string

⇒



∴ 25 bits

, Naïve coding:

a = 00, b = 01, c = 10, d = 11

⇒ 30 bits

↳ Algorithm to Pick best Tree:

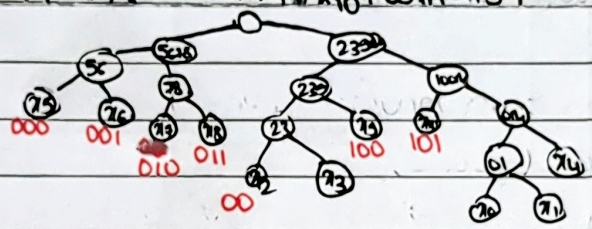
→ Check weights / frequency

→ Lowest 2 weight at bottom

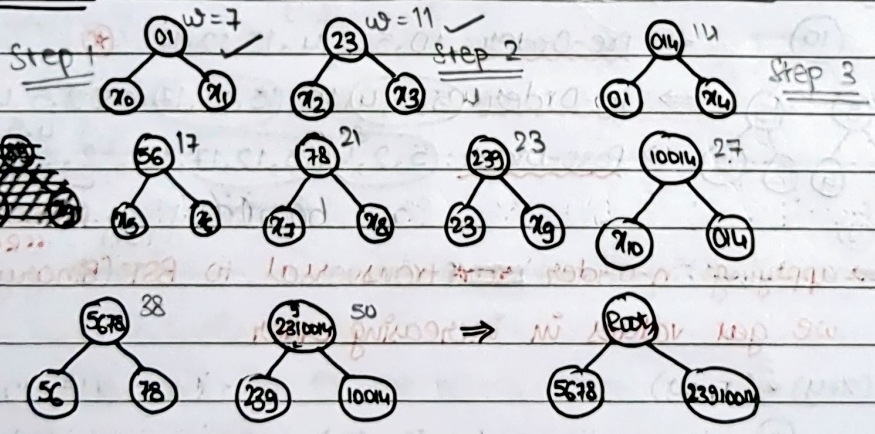
→ Recurse

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

→



Procedure



⇒

Encoding:

__/__/____

*] Modular Arithmetics:

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: $c \mid a$ & $c \mid b$ (c divides a & b)

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

$\therefore$ Largest common factor same $\therefore$ QED

⊛ ◦] **Euclid's Algorithm:** $O(\log(\min(a,b)))$

```
- GCD(a,b)
  if (b==0)
     return a;
  else
     return GCD(b, a%b);
```

Theorem: $a \geq b$. $a \pmod b \leq a/2$

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

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

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

→ for GCD(a,b) : $2\log_2 a$ steps

Ex: $91x + 56y = 7$

→

GCD(91,56)	$91 = 1 \cdot 56 + 35$	$35 = [1,-1]$
GCD(56,35)	$56 = 1 \cdot 35 + 21$	$21 = 56 - 35 \equiv [0,1] - [1,-1] = [-1,2]$
GCD(35,21)	$35 = 1 \cdot 21 + 14$	$14 = 35 - 21 = [1,-1] - [-1,2] = [2,-3]$
GCD(21,14)	$21 = 1 \cdot 14 + 7$	$7 = 21 - 14 = [-3,5]$
GCD(14,7)	$14 = 2 \cdot 7 + 0$	$0 = 14 - 2 \cdot 7 = [2,-3] - [-6,10] = [8,-13]$
GCD(7,0)		

Ex: $187x + 88y = 11$

→

GCD(187,88)	$187 = 2 \cdot 88 + 11$	$11 = [1,-2]$
GCD(88,11)	$88 = 11 \cdot 8 + 0$	
GCD(11,0)		

→ This is called extended euclid's algorithm

P.T.O.

__/__/____

o] **Extended Euclid's Algorithm:**

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

- $\text{GCD}(a,b)$	$a = q_1 b + r_1$	$r_1 = [x_1 \; y_1]\begin{bmatrix} a \\ b \end{bmatrix}$
$\text{GCD}(b, r_1)$	$b = q_2 r_1 + r_2$	$r_2 = [x_2 \; y_2]\begin{bmatrix} a \\ b \end{bmatrix}$
$\text{GCD}(r_1, r_2)$	$r_1 = q_3 r_2 + r_3$	$r_3 = [x_3 \; y_3]\begin{bmatrix} a \\ b \end{bmatrix}$
⋮	⋮	⋮

*] **Chinese Remainder Theorem:**

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

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

  ⋮

  $x \equiv a_K \pmod{n_K}$

Ex: $x < 210$

$x \% 2 = 0$

$x \% 3 = 1$

$x \% 5 = 2$

$x \% 7 = 3$

$x = 52$

- Thus,

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

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

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

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

→ ~~$x = 1 \pmod{17}$~~ ~~$x = 0 \pmod{19}$~~

$$x \equiv \left\{ 7 \left(17 \cdot [17^{-1} \pmod{19}] \right) + 9 \left(19 \cdot [19^{-1} \pmod{17}] \right) \right\} \pmod{17 \times 19}$$

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

$$x \equiv 26$$

P.T.O.

__/__/____

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

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

$\pmod{11}$ $\pmod{1001}$

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

$\Rightarrow 4 \pmod{13}$

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

$\Rightarrow 12$

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

$\Rightarrow 5$

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

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

*] Birthday Paradox:

Q] How many people are needed so that there's a clash of birthdays with probability ≥ 0.5?

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

$= P[\text{No collision on } q^{th} \text{ trial} \mid \text{No collision}] - P[\text{No collision}]$

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

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

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

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.

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

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

$\therefore$ QED

* Recurrence Relations:

- $a_0, a_1, a_2, \ldots\ldots, a_n, \ldots\ldots$
- Given by: $a_n = f(n, a_{n-1}, \ldots\ldots, a_{n-i})$ (i^{th} order)
  & Boundary cond^{n}s (like $a_0 = A$, $a_1 = B$, etc.)

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

Examples:

First order, Linear, Homogeneous, constant coefficients $\Rightarrow$ Geometric Progressions

- $a_n = a_{n-1}$
- $a_n = K \cdot a_{n-1}$
- $a_n = n a_{n-1} + n$ (→ Makes it Non-homo)
- → Non-constant coefficients

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

→ $a_n - a_{(n-1)} = f(n)$ (Telescopic)

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

$\vdots \quad \vdots$

$a_1 - a_0 = f(1)$

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

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

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

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

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

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

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

→ @ $i = n$ $\Rightarrow$ $3^n a_0 + \sum_{j=0}^{i-1} 3^j (n-j)$

__/__/____

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

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

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

$\therefore a_n = n! a_0 + n + n(n-1) + n(n-1)(n-2) + \dots + 1$

$\Rightarrow a_n = {}^nP_i \, a_{n-i} + \sum_{j=0}^{n-1} {}^nP_j$

-] **Second Order:**

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

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

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

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

$a_0 = 0 = A + B$

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

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

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

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

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

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

$\Rightarrow$ if $4\mu + \lambda^2 > 0$: $a_n = K\left(\frac{\lambda}{2}\right)^n$

$\rightarrow$ if $4\mu + \lambda^2 = 0$: $a_n = (A + Bn)(\lambda/2)^n$ ← as we must have 2 unknowns

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

__/__/____

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

↳ rigorous way of writing sequence of whole nums

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

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

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

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

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

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

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