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: Truth Table

p	T	F
$\neg p$	F	T

2] **Conjunction (AND)**: Let p, q be propositions. Then the conjunctⁿ of p & q ($p \land q$) is true only when both p & q are true. → stays a proposⁿ

Ex:

p	q	$p \land q$
T	T	T
T	F	F
F	T	F
F	F	F

3] **Disjunction (OR)**: ($p \lor q$) 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, conclusion

5] **Implication**: ($p \to q$) is false, when p is true & q is false. Otherwise true.
→ ($\neg p \lor q$)

Ex:

p	q	$p \to q$
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.
→ $(p \land q) \lor (\neg p \land \neg q)$

__/__/__

o] <u>Tautology:</u> (T)

- When a compound proposition is always True.

o] <u>Contradiction:</u> (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

$\Rightarrow$ 1) $p \to q$ = implication — Logically Equivalent

2) $q \to p$ = converse

3) $\neg q \to \neg p$ = contrapositive — Logically Equivalent

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

o] <u>Elementary Laws:</u>

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

o] <u>Interesting Identities:</u>

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

2] <u>De-Morgan's Laws:</u>

$$\left.\begin{aligned} &\neg(p \vee q) \equiv \neg p \wedge \neg q \\ &\neg(p \wedge q) \equiv \neg p \vee \neg q \end{aligned}\right\}$$

⊛ Intuition necessary, less harsh approach

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

$$\begin{aligned} \to \neg(p \vee (\neg p \wedge q)) &= \neg p \wedge \neg(\neg p \wedge q) \\ &= \neg p \wedge (p \vee \neg q) \\ &= (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\ &= F \vee (\neg p \wedge -q) \\ &= \neg p \wedge \neg q \end{aligned}$$

$\therefore$ <u>QED</u>

__/__/__

*] 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

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

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

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

$\rightarrow$ [Goldbach's Conjecture: For every even integer $n>2$, $\exists$ primes 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 : $n=p+q$

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

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

HW: Check if $\forall\, p,q \in$ Primes, $\exists\, n \in$ 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.

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

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

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 $\underbrace{\exists\, x \in D, \forall y \in D, P_0(x,y)}_{①}$ is true then ② is true

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

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

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

$\Rightarrow$ ② $\therefore$ QED

*] Satisfiability Problem (SAT):

- Satisfactory result when propⁿ True.
- True = 1, False = 0

$\rightarrow$ $P(x_1, x_2, \ldots x_n) = \underbrace{(x_1 \vee x_2 \vee \neg x_3)}_{= \text{3-SAT as 3 literals}} \wedge (x_4 \vee \neg x_5 \vee x_6) \wedge \ldots \wedge (\neg x_{n-2} \wedge \neg x_{n-1} \wedge x_n)$

(3 literals par kuch bhi allowed)

$\Rightarrow$ Ily, $\boxed{\text{K-SAT}}$

$\rightarrow$ $C(x)$ 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

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

*] Proof by contraposition:

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

Propⁿ: If $r \notin \mathbb{Q}$, then $\sqrt{r}$ [redacted] $\notin \mathbb{Q}$

Proof: forming [redacted] 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 $p, q \in \mathbb{N}$

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

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

Propⁿ: If n^2 is even, then n is even

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

*] Proof by Equivalence:

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

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

$\Rightarrow$ sum of ^2 $= 0 \Rightarrow$ all $0 \Rightarrow \forall i\ x_i = \mu$ $\therefore$ 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^n: Let x & $y \in \mathbb{Z}^+$ & $\{0\}$, then $(x+y)/2 \geq \sqrt{xy}$

Proof: We will use proof by contradiction

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

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

Prop^n: $\sqrt{2}$ 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 $HCF(p,q) = 1$ $\therefore$ QED

*] Proof by Induction:

o] 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 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. $j \in \mathbb{N} \Rightarrow H_j = 1 + \frac{1}{2} + \frac{1}{3} + \ldots\ldots + \frac{1}{j}$

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

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

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

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

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

$\Rightarrow \cancel{H_{2^K} + \frac{1}{2^{K+1}} \geq 1 + \frac{K}{2} + \frac{1}{2^{K+1}}}$

P.T.O.

__/__/____

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

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

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

∴ QED $\geq 1 + k/2 + 1/2$

• Strong Induction: diff?

- 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

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

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

Statement → Let P(n) be a propⁿ 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 ⇒ q(a) true

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

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

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