Page No.
Date 16.11.2019

a system consisting of a non-empty set S and one or more n-ary operator.

algebraic structure
↓
closure property (groupoid)
↓
associative + ↑ (semigroup)
↓
identity + ↑ (monoid)
↓
inverse + ↑ (group)
↓
commutative + ↑ (abelian group). quasigroup

Q) $S = \{\Theta \times \Theta\}$ where Θ is set of rational nos. let an operation $*$ be defined on S by.

$$(a,b) * (c,d) = (ac, ad+b)$$

$\langle S, * \rangle$ is semigroup or not.

① $(a,b) * (c,d) = (ac, ad+b)$ ✓

② {

$\{(a,b) * (c,d)\} * (e,f)$

$= (ac, ad+b) * (e,f)$

$= (ace, acf + ad + b)$

$(a,b) * \{(c,d) * (e,f)\}$

$= (a,b) * (ce, cf+d)$

$= (ace, acf + ad + b)$

✓ associative property holds.

Commutative? ✗

$(a,b) * (c,d)$ $\qquad$ $(c,d) * (a,b)$

$= (ac, ad+b)$ $\qquad$ $= (ac, bc+d)$

identity element.

$(x,y) * (a,b)$

$= (xa, xb+y)$

$x=1 \quad y=0.$

$(1,0)$

$(a,b) * (1,0)$

$= (a, 0+b)$ ✓ $\quad e_l = e_r = (1,0)$

⇒ monoid

inverse

$(x, y) * (a, b) = (1, 0)$

$\Rightarrow (xa, xb+y) = (1, 0)$

$xa = 1 \qquad xb + y = 0$

$x = \frac{1}{a} \qquad \frac{b}{a} + y = 0$

$y = -\frac{b}{a}$

$(a, b) * \left(\frac{1}{a}, -\frac{b}{a}\right)$

$= \left(1, a \cdot -\frac{b}{a} + b\right) = (1, 0)$ ✓

$\Rightarrow$ group.

✗ abelian as not commutative

cyclic group. every element of the form g^k.

$g^k = g \circ g \circ g \ldots$

Quasi group:

a groupoid (G, o) is said to be a quasi group,

$$\left.\begin{aligned} a \circ x &= b \\ y \circ a &= b \end{aligned}\right\} \text{ has a unique soln.}$$

intersection of 2 subgroups is a subgroup.

union with condition

union of 2 subgroups is not a subgroup with a condition.

S_1	S_2	
$S_1 \cap S_2$	$a \in S_1$	$a \in S_2$	$a \in S_1 \cap S_2$
	$b \in S_1$	$b \in S_2$	$b \in S_1 \cap S_2$
$\Rightarrow ab^{-1} \in S_1$		$ab^{-1} \in S_2$	$ab^{-1} \in S_1 \cap S_2$

Page No. _____
Date _____

Let $[A, \bullet]$ be a semigroup.
further $\forall a, b \in A$, if $a \neq b$, then $a \bullet b \neq b \bullet a$

(i) $a \bullet b \bullet a = a$

let $a \bullet a = b$

then $(a \bullet a) \bullet a = a \bullet (a \bullet a)$

$\Rightarrow \quad b \bullet a = a \bullet b$

this is possible only when $a = b$, so

$a = a \bullet a$

let $a \bullet b \bullet a = c$

$a \bullet b \bullet a \bullet a = c \bullet a$

$a \bullet b \bullet a = c \bullet a$

$c = c \bullet a$

~~Let~~ $a \bullet b \bullet a = c$

$a \bullet a \bullet b \bullet a = a \bullet c$

$a \bullet b \bullet a = a \bullet c$

$c = a \bullet c$

$\therefore \quad c = c \bullet a = a \bullet c$

this is only possible when $c = a$, so

$a \bullet b \bullet a = a$

(ii) $a \cdot b \cdot c = a \cdot c \qquad a \cdot b \cdot a = a$

$a \cdot c = a \cdot b \cdot a \cdot c$

$a \cdot c \cdot c = a \cdot b \cdot a \cdot c \cdot c$

$a \cdot c = a \cdot c$

$a \cdot b \cdot c$

$a \cdot b \cdot a \cdot b \cdot c$

$a = a \cdot a$

$a \cdot b \cdot a = a$

$a \cdot b \cdot c = a \cdot c$

$a \cdot b \cdot c = a \cdot c$

$a \cdot a \cdot c \cdot c$

$a \cdot b \cdot a \cdot b \cdot b \cdot c \cdot b \cdot c$

$a \cdot b \cdot a \cdot b \cdot c \cdot b \cdot c$

$= a \cdot a \cdot b \cdot a \cdot c \cdot b \cdot c \cdot c$

$= a \cdot b \cdot a \cdot c \cdot b \cdot c$

$= a \cdot c$

$a \cdot c$

$= a \cdot b \cdot a$

$a \cdot c$

$= a \cdot a \cdot c \cdot c$

$= a \cdot a \cdot b \cdot a \cdot a \cdot b \cdot c \cdot c$

$= a \cdot b \cdot a \cdot b$

$a \cdot b = b \cdot a \qquad (a = b.)$

Page No.
Date

$a \cdot a = b$

$(a \cdot a) \cdot a = b \cdot a = a \cdot b$ $\quad a = b.$

$a = a \cdot a$

$a \cdot b \cdot a = a$

$a \cdot b \cdot a = c$ $\quad a \cdot b \cdot a = c$

$a \cdot b \cdot a \cdot a = c \cdot a$ $\quad a \cdot a \cdot b \cdot a = a \cdot c$

$a \cdot b \cdot a = c \cdot a$ $\quad a \cdot b \cdot a = a \cdot c$

$c = c \cdot a$ $\quad c = a \cdot c$

$c = c \cdot a = a \cdot c$

$a = c$

$a \cdot b \cdot a = a.$ $\quad d \cdot c = a \cdot d = d$

$\Rightarrow$ ~~$a \cdot b$~~ $\cdot\ c \cdot d \cdot c = c \cdot a \cdot d =$

$c \cdot d = c$ $\quad c \cdot d =$

(ii) $a \cdot b \cdot c = a \cdot c$ $\quad a \cdot b \cdot c = d.$

$a \cdot b \cdot c = d.$ $\quad a \cdot a \cdot b \cdot c = a \cdot d.$

$a \cdot b \cdot c \cdot c = d \cdot c$ $\quad a \cdot b \cdot a = a \cdot a$

$a \cdot b \cdot c = d \cdot c$ $\quad d = a \cdot a.$

$d = d.$

$a \cdot d = d \cdot a$

~~$a = d$~~ $\quad a = a b \cdot c$

$d \cdot c = a \cdot d = d$

$\Rightarrow d \cdot c \cdot a = a \cdot d \cdot a = d \cdot a$

$\Rightarrow d \cdot c \cdot a = a = d \cdot a$

$a \cdot c = (d \cdot a) \cdot (c \cdot d)$

$= d \cdot (a \cdot c) \cdot d$

$= d$

$a \cdot b \cdot c = a \cdot c$

$a \cdot b \cdot c = d$

$a \cdot b \cdot c \cdot c = d \cdot c$

$d = d \cdot c = a \cdot d$ ——— (1).

$c \cdot d = c \cdot d \cdot c = c a \cdot d$

$c \cdot d = c = c \cdot a \cdot d.$

$d \cdot c = d$

$c \cdot d = c$ ——— (2).

$d \cdot a = d \cdot c \cdot a = a \cdot d \cdot a$

$d \cdot a = d \cdot c \cdot a = a.$ ——— (3).

$a \cdot c = (d \cdot a) \cdot (c \cdot d)$

$= d \cdot (a \cdot c) \cdot d$

$= d.$

$\Rightarrow a \cdot c = a \cdot b \cdot c.$

Page No. _____
Date _____

PROOFS AND LOGIC

$\sqrt{2}$ 1.2 1 1.2 1.111...

$\frac{p}{q}$ $\frac{1}{2}$ 0.5 $\frac{1}{3}$ = 0.3333...

1.414....

π 3.1426...

if $a \rightarrow b$

$\sim a \rightarrow \sim b$ {1, 2, 3}

$b \rightarrow a$ $\frac{1}{4}$ $\frac{1}{2}$

$\sim b \rightarrow \sim a$

$\sqrt{2} = \frac{a}{b}$ $a, b \in \mathbb{Z}$

$2 = \frac{a^2}{b^2}$

$a^2 = 2b^2$

$a =$

a^2 = multiple of 2

a = multiple of 2

$a = 2k$

$\sqrt{2} = \frac{2k}{b}$ $2 = \frac{4k^2}{b^2}$ $b^2 = 2k^2$

$\Rightarrow b^2$ = multiple of 2

$\Rightarrow b$ = multiple of 2

a b

if mamu comes, then mama smiles.

$a \rightarrow b$

$\sim b \rightarrow \sim a$ $\sim a \rightarrow \sim b$

if mama does not smile, then mamu has not come.

if mamu does not come, then mama does

if a^2 is even, then a is even.

if a is odd, the a^2 is odd.

$a = 2k+1$

$a^2 = (2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$

a^2 even → a even

a odd → a^2 = odd.

odd

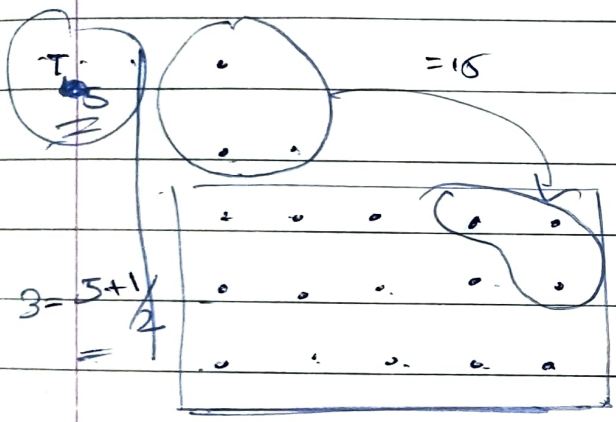
$2 \times 3 \times 5 \times 7 \times 11 + 1$ $6 \times 4 \times 16$

$2\ 3$ 2 $2\ 5$

Euclid. $2 \times 3 + 1$ 7

T_1 . $= 1$ T_2 . . $= 3$

T_3 . . . $= 6$ T_4 . . . . $= 10$



T_5 $= 15$

$3 = \frac{5+1}{2}$

$n \times \frac{(n+1)}{2}$

5

$T_n = \frac{n(n+1)}{2}$

$T_n = \frac{n(n+1)}{2}$

$\sum n = \frac{n(n+1)}{2}$ $\sum n^2 = \frac{n(n+1)(2n+1)}{2}$

$\sum 1 \; n \quad \sum n = \frac{n(n+1)}{2} \quad \sum n^2 = \frac{n(n+1)(2n+1)}{6}$

$\sum n^3 = \frac{n^2(n+1)^2}{4}$

$R \rightarrow W = \neg R \vee W$

$\neg\neg R = R$

distributive laws

$(R \vee W) \wedge S = (R \wedge S) \vee (W \wedge S)$

$(R \wedge W) \vee S = (R \vee S) \wedge (W \vee S)$

demorgan laws.

$\neg (A \vee B) = \neg A \wedge \neg B$

$\neg (A \wedge B) = \neg A \vee \neg B$

$\overline{(R \vee W) \wedge (R \wedge W)}$

$= (R \wedge \overline{(R \wedge W)}) \vee (W \wedge \overline{(R \wedge W)})$

$= (R \wedge (\neg R \vee \neg W)) \vee (W \wedge (\neg R \vee \neg W))$

$= (R \wedge \neg W) \vee (W \wedge \neg R)$

$= (R \wedge \neg W) \vee (\neg R \wedge W)$

Page No. _____
Date _____

COMPLETE SET OF CONNECTIVES, OPERATORS

- or, not
- and, not

✗ • or, and ⇒ not a complete set.

$a^{\log_b n} = n^{\log_b a}$

$a^{\log_b n} = n^{\log_b a}$

$n = 2^3$

$a = 2^2$

2^3

$(2^2)^3 \quad 2^6 \qquad (2^3)^2 = 2^6$

2^4

$a^{\log_b n} = n^{\log_b a}$

let $x = \log_b (a^{\log_b n})$

$= \log_b (LHS)$

let $x = \log (a^{\log_b n})$

$\Rightarrow x = \log_b n \cdot \log$

$= \log_b n \cdot \log_b a$

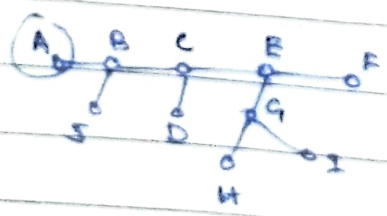
$= \log_b a \cdot \log_b n$

$= \log_b (n^{\log_b a})$

$= \log_b (RHS)$

$\therefore LHS = RHS$

factoring not get NPC.



A B C F G

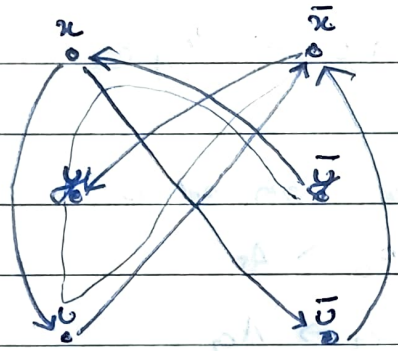
B D E H I

2SAT $\leq_p$ SCC Strongly connected components

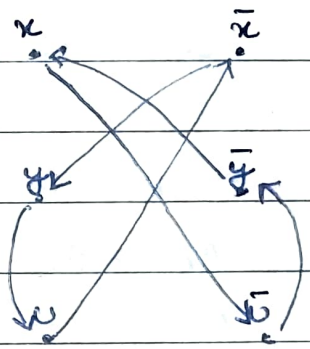
REDUCTION 2SAT $\leq_p$ SCC

$(x + v) \cdot$
$(\bar{v} + y) \cdot$
$(\bar{x} + \bar{y})$

3 vars. x, v, y $x = T$ $v = T/F$ $\bar{y} = T$



$(x + v) \cdot$
$(\bar{v} + y) \cdot$
$(\bar{x} + \bar{y})$



SCC's

$x\ \bar{v}\ \bar{y}$ $\bar{x}\ y\ v$ take a variable and connect to complement of other variable.

complexity of reduction SCC

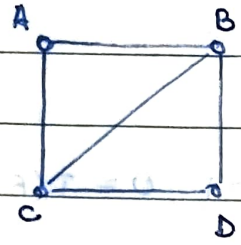
$\Theta(n) + \Theta(m)$ $\Theta(n+m)$

NP → SAT → minesweeper
~~3-colorability~~
↳ 3SAT → NAE 3SAT → MAX CUT
↳ vertex cover simple for planar
↳ dominating set easy for trees.

hamiltonian ckt.
↓
TSP

ex 3-colorability $\leq_p$ SAT

assigning colour to a node.



A can only take 1 colour

similarly for every vertex

$A_R \cdot \bar{A}_G \cdot \bar{A}_B +$
$\bar{A}_R \cdot A_G \cdot \bar{A}_B +$
$\bar{A}_R \cdot \bar{A}_G \cdot A_B$

converting edge info to logic.

if A and B have an edge $\Rightarrow$ A and B cannot be assigned the same colour. write 6 rules for all edges.

$A_R \rightarrow \bar{B}_R$ $\quad B_R \rightarrow \bar{A}_R$

$A_G \rightarrow \bar{B}_G$ $\quad B_G \rightarrow \bar{A}_G$

$A_Y \rightarrow \bar{B}_Y$ $\quad B_Y \rightarrow \bar{A}_Y$

XOR.

reductions can be used in settings.

(i) NP problem $\leq_p$ M $\leq_p$ Q

Q is a problem with unknown complexity

Q is harder than M.
M = NP-C and Q ∈ NP
$\Rightarrow$ Q = NP-C.

M is unknown p class.

Q is easy M is also easy.
sorting $\leq_p$ CH

Page No. _____
Date _____

REDUCTION

DNF ∨

CNF ∧

SAT $\leq_p$ 3-SAT

ONE VARIABLE CLASS

CNF (x).

using auxiliary variables.

$(y + \bar{x} + w + v)$.

$(x + y + z)$. $\leq_p$ 3SAT

$(x + \bar{z})$

$(x) = (x + a + b)$.
$(x + a + \bar{b})$.
$(x + \bar{a} + b)$.
$(x + \bar{a} + \bar{b})$

TWO VARIABLE CLASS

THREE VARIABLE CLASS

$(x + \bar{z}) = (x + \bar{z} + c)$.
$(x + \bar{z} + \bar{c})$

no work.

FOUR OR LARGE

$(y + \bar{x} + w + v) = (y + \bar{x} + l)$. $(\bar{l} + w + v)$

SAT complexity of reduction. $= O(n \cdot m)$

polynomial time.

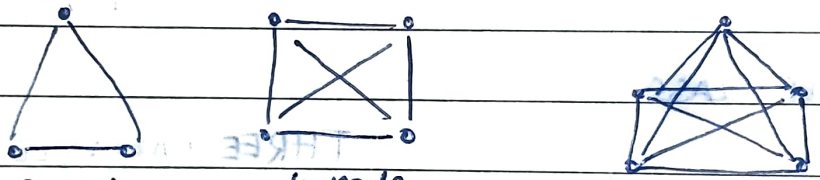
ex hamiltonian cycle in a graph.

NP time version

① guess a soln. in polynomial time : BAEFCD

② verify the guessing.

MAX CLIQUE PROBLE



3-node 4-node 5-node

(NP) time version.

① guess a solution : pick coll. of k nodes $\Theta(n)$

② verify a solution ; check if edges exist.

between every pair of k nodes $\Theta(n^2)$

ex 2 person game

is this in NP-class

exp. time (deterministic), thm of REDUCTIONS,

B is NP-C and

$B \leq_p C$ for for $C \in NP$

then C is also NP-C.

Steven cook every $NP \leq_p SAT \leq_p 3SAT$

Page No. _____
Date _____

thm if B is NPC and $B \leq_p C$ for some $C \in NP$ then C is also NP-C. (Proof?)

thm if any NP-C problem is polynomial time solvable, then P = NP.

NP → SAT → 3-SAT

3-SAT

$(x + y + \bar{z})$.

$(x + y + \bar{v})$.

⋮

no. of variables = (n)

no. of clauses = (m)

NP. non-deterministic polynomial time solvable.

(i) guess a soln. : $\Theta(n)$

(ii) verify the guess : $\Theta(m)$

} answer yes/no.

NPC problems and REDUCTIONS

DFNS FROM CLR BOOK

decision problem.

$L = \{x \in \Sigma^* \mid Q(x) = 1\}$ $\quad \Sigma = \{0, 1\}$.

dfn

a language L belongs to NP (non-deterministic polynomial class) iff there exists a 2-input polynomial time algorithm A and a constant c such that

there exists.

$L = \{x \in \Sigma^* : \exists$ a certificate y with,

$|y| = O(|x|^2)$

such that $A(x, y) = 1$

dfn

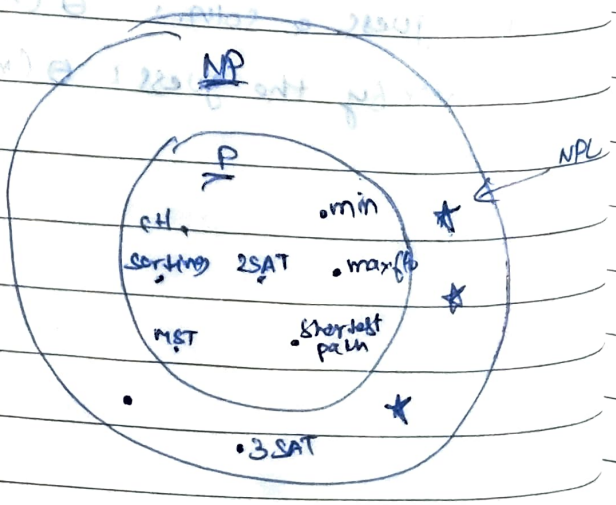
a language $L \subseteq \{0,1\}^*$

is NP complete if

① $L \in NP$ and

② $L' \leq_p L$ for ever $L' \in NP$

$\leq_p$ ← polynomial time reduction.



1972

COUNTING EXAMPLE

7
← Bkt
6
5
← Bkt
4 triangle no
3 $\Theta(n^2)$
2
1

MODIFIED

8
7 ← Bkt
6
5
4 ← BU
3
2
1

numbers are struck off only once "2n" $\Theta(n^2)$

(3) JARVIS' ALGO

$\Theta(n)$ (1) start at the lowest pt. (min. y, tie → min. x)

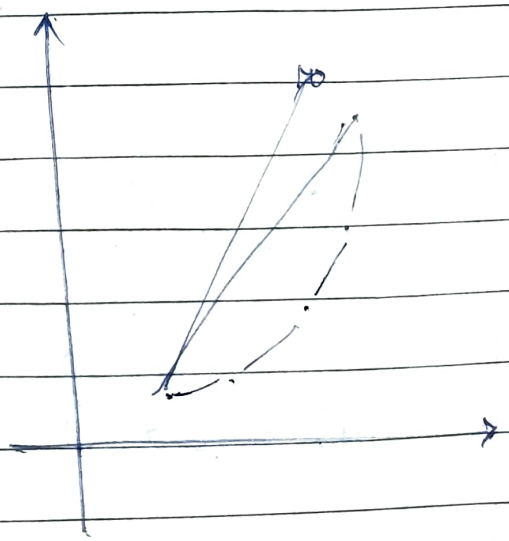
(2) find the right most pt. and add to CH

(3) find the right most pt. at the next pt.

T reduction sorting of nos. $\leq_p$ CH.

$\Theta(n \log n)$

x		(x, x^2)
6	→	(6, 36)
8	→	(8, 64)
1	→	(1, 1)
5	→	(5, 25)
9	→	(9, 81)
13	→	(13, 169)



CH is as hard a problem or harder than Sorting.

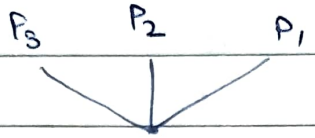
$P_1' = (5-4, 8-2) = (1, 6)$

$P_2' = (3-4, 6-2) = (-1, 4)$

$P_3' = (1-4, 4-2) = (-3, 2)$

b/t $-6-4 = -10 < 0 \Rightarrow P_2'$ ccw to P_1

$-12+2 = -10 < 0 \Rightarrow P_3'$ ccw to P_2



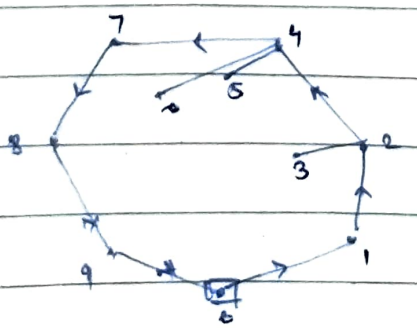
GRAHAM SCANNING ALGO

1. find the lowest pt. (min y, tie → min. x) $\Theta(n)$.
2. wrt lowest pt. sort the pts. in ccw direction $\Theta(n \log n)$.
3. graham scan procedure.

add a point to CH

every time you make a lft. turn, add point to CH.

but if you take rt. turn, backtrack and keep backtracking until you can make a lft. turn.



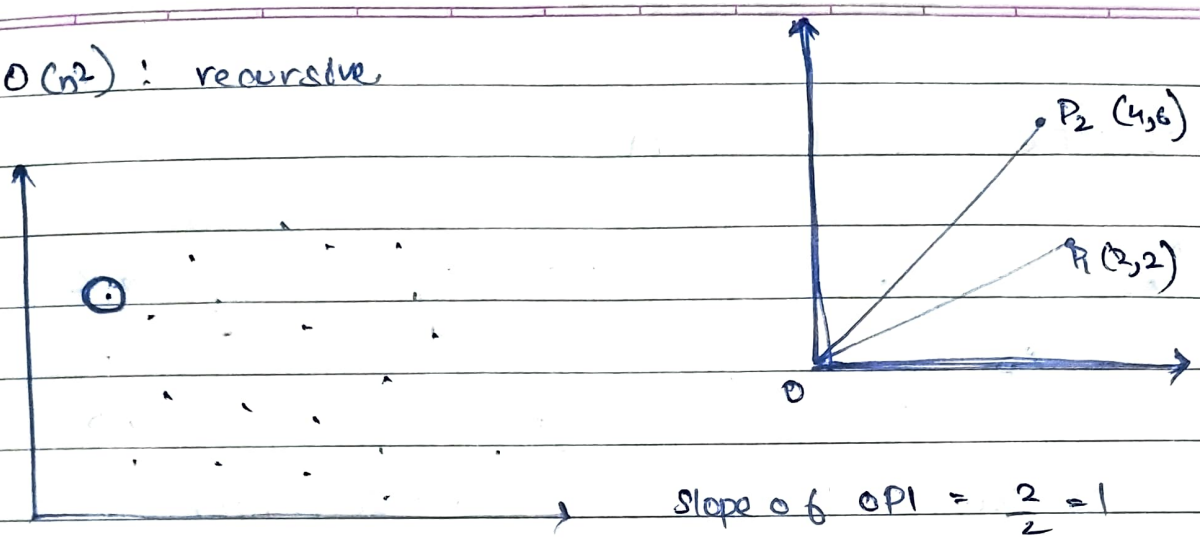
CH

0 - 1 - 2 - 4 - 7 - 8 - 9 - 0.

ccw.

Page No. _____
Date _____

$O(n^2)$: recursive

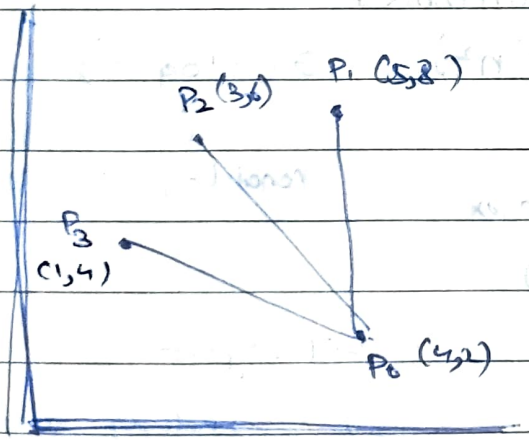


Slope of $OP_1 = \frac{2}{2} = 1 \quad \frac{y_1}{x_1}$

$T(n) = T(n-1) + \text{join the nth point}$

Slope of $OP_2 = \frac{6}{4} = 1.5 = \frac{y_2}{x_2}$

$\frac{y_1}{x_1} < \frac{y_2}{x_2} \Rightarrow P_1$ lt. of P_2



$y_1 x_2 - y_2 x_1 < 0 \Rightarrow P_1$ rt. of P_2

P_2 is ccw to P_1

P_1 cw to P_2 else clockwise.

$= 0$ $P_1 P_2$ collinear.

Subtract P_0 from $P_1 - P_3$