30 September 2020 09:02

Cover only the topics discussed in the class:

Unit-3: Lattice and Boolean Algebra → ch-14 → Schaum's Series (pdf) → a lot of exercise

→ Poset → Hasse diagram, max/min, Greatest/least, sup, inf.

→ Lattice theory → Lattice → Complete, Bounded, Distributive → Quiz → Lattice cryst

→ BCO → Boolean Algebra.

→ ~~Abp~~ of Lattice →

→ Unit-1 → Cryptography → ⇒ < 2 hours

Assignment-3 (Unit-3)

Quiz 3 → Monday → Unit-3

Applications of lattice theory

30 September 2020 09:24

The lattice model of information flow
→ diff. info^n flow policies → Lattice can be used to represent it.

for eg. multi-level security policies.

→ piece of info → Security class (A, C)

A 1

info → Unclassified (0)
Confidential (1)
secret (2)
top-secret (3)

A = { spies, moles, double agents }

Authority level

Category.
11
Subset of set of all compartments.

$2^{|A|}$ = 8 → Category →

arb → (V)
11

info^n →

(A_1, C_1) (A_2, C_2)

$\leq$ →

Rule:
Info^n is permitted to flow $(A_1, C_1) \rightarrow (A_2, C_2)$ iff

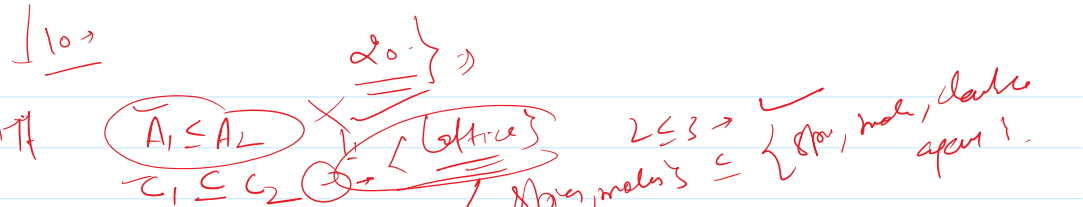
$(A_1, C_1) \leq (A_2, C_2)$

30 September 2020 09:31

Procedure:-

$(A_1, C_1) \preceq (A_2, C_2)$ iff $A_1 \leq A_2$ and $C_1 \subseteq C_2$

Info is permitted to flow from (A_1, C_1) to (A_2, C_2)



e.g. $(\underset{1}{\text{Secret}}, \{\text{Spies, moles}\}) \Rightarrow \{\underset{3}{\text{Top Secret}}, \{\text{Spies, moles, double agents}\}\}$

$\{\text{Top Secret, } \{\text{Spies, moles}\}\} \rightarrow \{\text{Secret, } \{\text{Spies, moles, double agents}\}\}$

$(A_1, C_1) \preceq (A_2, C_2)$ ✗

Set-S → Set of Security classes, $(A_1, C_1) \leq (A_2, C_2)$ iff $A_1 \leq A_2$, $C_1 \subseteq C_2$

→ Prove that $(S, \leq)$ is a lattice.

5-min

→ Poset
→ Inf(S) exist.
→ Sup(S) exist.
⇓
lattice

Poset → 1) Reflexive → $(A, C) \leq (A, C)$ $A \leq A$, $C \subseteq C$

2) Anti-Symmetric → $(A_1, C_1) \leq (A_2, C_2) \rightarrow A_1 \leq A_2$, $C_1 \subseteq C_2$ —

↪ $(A_2, C_2) \leq (A_1, C_1) \rightarrow A_2 \leq A_1$, $C_2 \subseteq C_1$ —

$A_1 = A_2$, $C_1 = C_2$ }

3) ✓

Set-S is a Poset ✓

30 September 2020 09:45

(A_1, C_1) (A_2, C_2) $\inf \to (\min(A_1, A_2),\ C_1 \cap C_2)$

$\inf(S)$: → g.l.b. → (a, b)

$x \leq a$

$x \leq b$

$\min(A_1, A_2) \leq A_1$ $C_1 \cap C_2 \subseteq C_1$

$\min(A_1, A_2) \leq A_2$ $C_1 \cap C_2 \subseteq C_2$

$(\min(A_1, A_2),\ C_1 \cap C_2) \leq (A_1, C_1)$

$(\min(A_1, A_2),\ C_1 \cap C_2) \leq (A_2, C_2)$

$x \leq (A_1, C_1)$

$x \leq (A_2, C_2)$

$\Rightarrow$ x is lower bound

$(A_1, C_1) \leq (A_2, C_2)$ iff $A_1 \leq A_2$, $C_1 \subseteq C_2$ $\Rightarrow$ $(\min(A_1, A_2),\ C_1 \cap C_2)$ is lower bound

If (A, C) is lower bound, then

$A \leq A_1$ $C \subseteq C_1$

$A \leq A_2$ $C \subseteq C_2$

$\Rightarrow$ $A \leq \min(A_1, A_2)$, $C \subseteq C_1 \cap C_2$

$(A, C) \leq (\min(A_1, A_2),\ C_1 \cap C_2))$

$\min((A_1, A_2), C_1 \cap C_2)$ is g.l.b. $\Rightarrow$ $\inf(S)$ exist

$\sup(S) \to (\max(A_1, A_2),\ C_1 \cup C_2)$

30 September 2020 09:57

Topological Sorting :-> Data & Algo :- CS ->

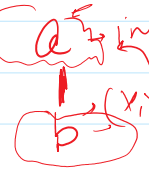
mathematics -> linearization of a partial-ordering

Topology in CS -> Arrangement to the objects that can be connected with edges :-

Problem :- 20 tasks, -> Some task dependent on other tasks.

Computer architecture

data dependency
control



find the order of the tasks.

Prob: find the order of these tasks.

Solution: find a partial order with Relation $a < b$ iff b cannot be started until task a has finished.

A total ordering $\leq$ is compatible with partial order Relation R.

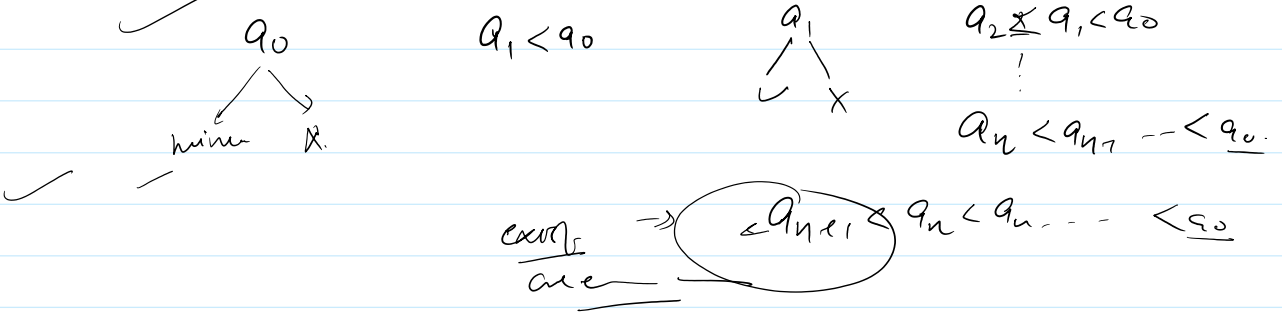
If $a \leq b$, then aRb.

→ Constructing a compatible total ordering from a partial ordering is called topological sorting.

Topological Sorting :→

$\preceq$

Lemma :→ Every finite non-empty poset $(S, \preceq)$ has atleast one minimal element



30 September 2020 10:10

→ topological sort

$T_1, T_2 \cdots T_n$ → find an order — $\preceq$ on A : $a < b$ → b is called dependent on task a.

1. choose the minimal element: a_1

2. $(A - \{a_1\}, \preceq)$ → also poset, then choose the next minimal element a_2.

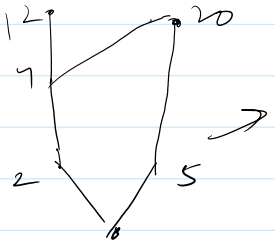
3. $(A - \{a_1, a_2\}, \preceq)$ → → a_3 … $a_1, a_2, \cdots a_n$

$a_1 < a_2 < a_3 \cdots < a_n$ → $a_1 \cdots a_n$

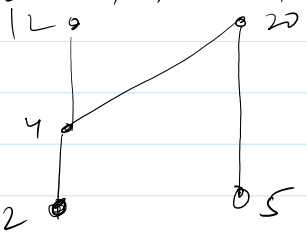
= = } multiple ordering possible

more than one minimal element → select any one

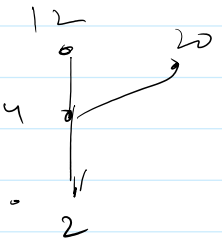
Example:- Poset $(\{1,2,4,5,12,20\}, |)$



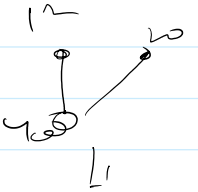
(1)



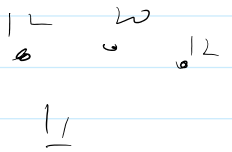
(5)



(2)



(4)



(20) (12)

(3)

$1 < 5 < 2 < 4 < 20 < 12$

quiz

(2)

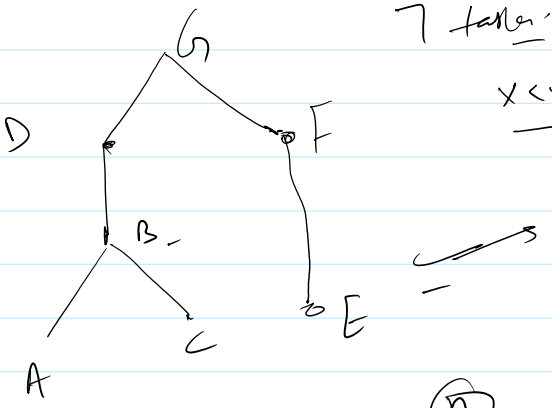
$1 < 5 < 2 < 4 < 20 < 12$

$n_1, n_2, \ldots n_6$

$n \to n!$

$4 \to 4!$

(n)



7 tasks.

x < y.

A < C < B < E < F < D < G.

Home exercise

→ how many possible.