CS615: Formal Specification and Verification of Programs 2019

Lecture 9: Lattice

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-09-10

Topic 9.1

Lattice theory

Partial order and poset

$\Delta_X = \{(x,x) | x \in X\}$

Definition 9.1

On a set X, $\leq \subseteq X \times X$ is a partial order if

- *reflexive:* $\Delta_X \subseteq \leq$
- *anti-symmetric:* $\leq \cap \leq^{-1} \subseteq \Delta_X$
- *transitive:* $\leq \circ \leq \subseteq \leq$

We will use $x \leq y$ to denote $(x,y) \in \leq$. Let $x < y \triangleq (x \leq y \wedge x \neq y)$.

Example 9.1

Is the following a partial order on $\{a, b, c\}$?

- $\leq = \{(a,a),(b,b),(c,c)\}$
- $\leq = \emptyset$
- $\leq = \{(a,a),(b,b),(c,c),(a,b)\}$
- $\leq = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$
- $\leq = \{(a,a),(b,b),(c,c),(a,b),(b,c)\}$

Poset

Definition 9.2

A poset $(X, \leq)$ is a set equipped with partial order $\leq$ on X

Example 9.2

Is the following a partial order?

- $(\mathbb{N}, \leq)$
- $(\mathbb{N} \times \mathbb{N}, \{(\ (a,b),(c,d)\ )|a \leq c\})$
- $(\mathbb{N} \times \mathbb{N}, \{(\ (a,b),(c,d)\ )|a \leq c \wedge b \leq d\})$
- $(\{a,b,c\}, \{(a,a),(b,b),(c,c),(a,b),(a,c)\})$

Covering relation

Definition 9.3

The covering relation $\lessdot$ *for poset* $(X, \leq)$ *is*

$$x \lessdot y \triangleq (x < y) \land \neg(\exists z. x < z \land z < y)$$

In other words, $\lessdot$ contains only immediate parents and has no self-edges.

Example 9.3

Consider poset $(\{a, b, c, d, e\}, \leq)$*, where*

$$\leq = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (a, c), (a, d), (b, e), (c, e), (d, e), (a, e)\}$$

Therefore,

$$\lessdot \ = \{(a, b), (a, c), (a, d), (b, e), (c, e), (d, e)\}$$

Hasse diagrams

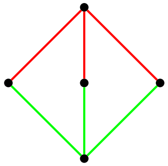
We draw posets $(X, \leq)$ as DAG. Nodes are from X and edges are from $\lessdot$.

DAG will be vertically aligned, i.e., if there is an edge between x and y, and x is located below y then $x \lessdot y$.

Example 9.4

Let us consider again our previous poset $(\{a, b, c, d, e\}, \leq)$, *where*

$$\lessdot \; = \{(a, b), (a, c), (a, d), (b, e), (c, e), (d, e)\}$$



Nodes at same level are incomparable.

Chain and antichain

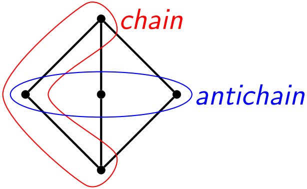
Definition 9.4

For a poset $(X, \leq)$*,* $C \subseteq X$ *is chain if* $\forall x, y \in C.\ x \leq y \lor y \leq x$

Definition 9.5

For a poset $(X, \leq)$*,* $C \subseteq X$ *is antichain if* $\forall x, y \in C.\ x \leq y \Rightarrow y = x$

Example 9.5



Ascending/descending chain condition

Definition 9.6

A poset $(X, \leq)$ *satisfies* ascending chain condition *if for any sequence* $x_0 \leq x_1 \leq x_2 \leq \dots, \exists k. \forall n > k\ x_k = x_n$

Symmetrically, we define descending chain condition

Definition 9.7

A poset $(X, \leq)$ *is called* well ordered *if it satisfies descending chain condition*

Example 9.6

$(\mathbb{N}, \leq)$ *satisfies descending chain condition but not ascending chain condition.*

Exercise 9.1

Prove $(X, \leq)$ *has no infinite chains if it satisfies both ascending and descending chain condition*

Minimal and Maximal elements

Definition 9.8

For poset $(X, \leq)$ *and* $S \subseteq X$,

$minimal(S) \triangleq \{x \in S | \neg\exists y \in S.\ y < x\}$

$maximal(S) \triangleq \{x \in S | \neg\exists y \in S.\ y > x\}$

Exercise 9.2

Consider poset $\mathbb{N}^2 = \{\mathbb{N} \times \mathbb{N}, \{(\ (a, b), (c, d)\ ) | a \leq c \wedge b \leq d\}\}$

Give the following sets

- $minimal(\mathbb{N} \times \mathbb{N}) =$
- $minimal(\{(a, b) | b \geq 2 \vee (a \geq 1 \wedge b \geq 1)\}) =$

Exercise 9.3

Give a subset S *of the above poset such that* $|minimal(S)|$ *is infinite.*

Minimum and maximum

Definition 9.9

For poset $(X, \leq)$ *and* $S \subseteq X$,

$min(S) \triangleq x$ *if* $\{x\} = minimal(S)$ *//*$min(S)$ *may not exist*

$max(S) \triangleq x$ *if* $\{x\} = maximal(S)$

Exercise 9.4

Consider poset $\mathbb{N}^2$

Give the following sets

- $minimum(\mathbb{N} \times \mathbb{N}) =$
- $minimum(\{(a, b) | b \geq 2 \vee (a \geq 1 \wedge b \geq 1)\}) =$

Top and bottom

Consider poset $(X, \leq)$

If $min(X)$ exists, we denote $min(X)$ by $\bot$

If $max(X)$ exists, we denote $max(X)$ by $\top$

Example 9.7

For poset $(\mathbb{N}, \leq)$, $min(\mathbb{N}) = 0$.

Exercise 9.5

Give a poset that has no minimum?

Upper bound and lower bound

Definition 9.10

For poset $(X, \leq)$ and $S \subseteq X$,

- $x \in X$ *is upper bound of* S *if* $\forall y \in S.\ y \leq x$
- $x \in X$ *is lower bound of* S *if* $\forall y \in S.\ x \leq y$

Exercise 9.6

Is the following lower bound of $\{(a,b) | b \geq 2 \vee (a \geq 1 \wedge b \geq 1)\} \subset \mathbb{N}^2$*?*

- $(0, 0)$
- $(0, 2)$
- $(1, 1)$
- $(0, 1)$

Least upper bound and greatest upper bound

Definition 9.11

$x \in X$ is least upper bound(lub) of S if x is upper bound of S and

$$\forall u.\ (\forall y \in S.\ y \leq u) \Rightarrow x \leq u$$

lub is usually denoted by $\vee, \sqcup$ (called join).

Definition 9.12

$x \in X$ is greatest lower bound(glb) of S if x is lower bound of S and

$$\forall u.\ (\forall y \in S.\ u \leq y) \Rightarrow u \leq x$$

lub is usually denoted by $\wedge, \sqcap$ (called meet).

Note: lub and glb may not exist.

Example: Least upper bound($\sqcup$) and greatest lower bound($\sqcap$)

Exercise 9.7

Is the following $\sqcap$ *of* $\{(a,b) | b \geq 2 \vee (a \geq 1 \wedge b \geq 1)\} \subset \mathbb{N}^2$*?*

- $(0,0)$
- $(0,2)$
- $(1,1)$
- $(0,1)$

Exercise 9.8

Give $\sqcup/\sqcap$ *for the following subsets of poset* $\mathbb{N}^2$*.*

- $\sqcup\{(a,b) | a^2 + b^2 \leq 16\}$
- $\sqcup\{(a,b) | a + 2b \leq 20\}$
- $\sqcap\{(a,b) | a + 2b \geq 20\}$

Uniqueness of lub an glb

Note that the uniqueness is not obvious by the definition of $\sqcup$

Theorem 9.1

For poset $(X, \leq)$ and $S \subseteq X$, if $\sqcup S$ exists then it is unique.

Proof.

- Suppose x and y are $\sqcup S$.
- By definition of $\sqcup$, x and y both are upper bounds of S.
- Since x is upper bound and y is $\sqcup S$, therefore $y \leq x$.
- Symmetrically, $x \leq y$.
- Due to anti-symmetry, $x = y$. □

Therefore, $\sqcup$ and $\sqcap$ are partial functions : $2^X \hookrightarrow X$

- If $S = \{x, y\}$, we will write $x \sqcup y$
- The infix usage usually means, lub of finite elements

Semi-lattice

Definition 9.13

A join semi-lattice $(X, \sqsubseteq, \sqcup)$ *is a poset* $(X, \sqsubseteq)$ *such that*

$$\forall x, y \in X.\ x \sqcup y \text{ exists.}$$

Definition 9.14

A meet semi-lattice $(X, \sqsubseteq, \sqcap)$ *is a poset* $(X, \sqsubseteq)$ *such that*

$$\forall x, y \in X.\ x \sqcap y \text{ exists.}$$

Example 9.8

$\mathbb{N}^2$ *is a meet semi-lattice.*

Exercise 9.9

a. Is $\mathbb{N}^2$ *is a join semi-lattice?*

b. Give a poset that is not a meet semi-lattice?

Properties of semi-lattice

Theorem 9.2

A join semi-lattice $(X, \sqsubseteq, \sqcup)$ *satisfies*

- $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$ *(associativity)*
- $(a \sqcup b) = (b \sqcup a)$ *(commutativity)*
- $a = (a \sqcup a)$ *(idempotence)*

Exercise 9.10

Prove 9.2

Exercise 9.11

For a join semi-lattice $(X, \sqsubseteq, \sqcup)$*, show that* $\sqcup S$ *exists for each finite set* $S \subseteq X$.

Equivalent definition of semi-lattice

Theorem 9.3

Let X be a set with function $\sqcup : X \times X \to X$ satisfying

$$(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c), \qquad (a \sqcup b) = (b \sqcup a), \quad \textit{and} \quad (a \sqcup a) = a.$$

Let $a \sqsubseteq b \triangleq (a \sqcup b) = b$.

Then, $(X, \sqsubseteq, \sqcup)$ is a join semi-lattice.

Proof.

We need to show that $\sqsubseteq$ is a partial order, i.e.,

- $\sqsubseteq$ is reflexive,
- $\sqsubseteq$ is transitive, and
- $\sqsubseteq$ is anti-symmetric.

We also need to show $\sqcup$ is lub with respect to $\sqsubseteq$. …

Commentary: Please read the theorem carefully. It says that the three conditions characterizes semi-lattices.

Equivalent definition of semi-lattice II

Proof(contd.)

claim: $\sqsubseteq$ is reflexive

- $a \sqsubseteq a$ holds because $(a \sqcup a) = a$.

claim: $\sqsubseteq$ is transitive

1. Assume $a \sqsubseteq b$ and $b \sqsubseteq c$
2. def of $\sqsubseteq$,
$$(a \sqcup b) = b \text{ and } (b \sqcup c) = c.$$
3. By substitution, $((a \sqcup b) \sqcup c) = c$.
4. Due to associativity, $a \sqcup (b \sqcup c) = c$.
5. Due to 4, $a \sqcup c = c$.(why?)
6. Therefore $a \sqsubseteq c$.

…

Equivalent definition of semi-lattice III

Proof(contd.)

claim: $\sqsubseteq$ is anti-symmetric

1. Assume $a \sqsubseteq b$ and $b \sqsubseteq a$
2. By def of $\sqsubseteq$, $(a \sqcup b) = b$ and $(b \sqcup a) = a$
3. By commutativity, $a = b$

claim: $\sqcup$ is lub

1. $b \sqsubseteq a \sqcup b$, because $a \sqcup (a \sqcup b) = (a \sqcup a) \sqcup b = a \sqcup b$.
2. Similarly, $a \sqsubseteq a \sqcup b$.
3. Let x be such that $a \sqsubseteq x$ and $b \sqsubseteq x$.
4. Therefore, $(a \sqcup x) = x = (b \sqcup x)$
5. After substitution, $(a \sqcup (b \sqcup x)) = x$
6. Apply associativity, $((a \sqcup b) \sqcup x) = x$, which is $(a \sqcup b) \sqsubseteq x$
7. Therefore, $a \sqcup b = lub(\{a, b\})$

☐

Notational redundancy in semi-lattice

We write $(X, \sqsubseteq, \sqcap)$ to describe a semi-lattice.

Due to the previous theorem, if we know something is a semi-lattice, we need not write both the second and third component.

One defines the other.

We may only write $(X, \sqcap)$.

Lattice

$\sqcap$ and $\sqcup$ are forced to exist for finite sets

Definition 9.15

A lattice $(X, \sqsubseteq, \sqcup, \sqcap)$ *is a poset* $(X, \sqsubseteq)$ *such that*

$$\forall x, y \in X \text{ both } x \sqcup y \text{ and } x \sqcap y \text{ exist.}$$

Exercise 9.12

Is $\mathbb{N}^2$ *a lattice?*

Properties of lattice

Properties of lattice

1. $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$ (associativity)
2. $(a \sqcup b) \sqcup c = a \sqcup (b \sqcup c)$
3. $(a \sqcap b) = (b \sqcap a)$ (commutativity)
4. $(a \sqcup b) = (b \sqcup a)$
5. $(a \sqcap a) = a$ (idempotence)
6. $(a \sqcup a) = a)$
7. $a \sqcap (a \sqcup b) = a$ (absorption)
8. $b \sqcup (a \sqcap b) = b$

Properties 1-6 were already present in semi-lattices.

The above properties are axiomatization of lattice

Observe that distributivity is missing!!!

Exercise

Exercise 9.13

a. Prove absorption.

$$a \sqcap (a \sqcup b) = a$$

b. Show that semi-lattices $(X, \sqsubseteq_1, \sqcup)$ *and* $(X, \sqsubseteq_2, \sqcap)$*, and absorption properties imply* $(X, \sqsubseteq_1, \sqcup, \sqcap)$ *is a lattice.*

Due to the above exercise, the properties 1-8 characterizes lattice.

Complete partial order/lattice

Definition 9.16

A complete partial order(cpo) is a poset $(X, \sqsubseteq)$ *such that every increasing chain in* X *has a lub in* X

Definition 9.17

A complete lattice is a poset $(X, \sqsubseteq)$ *such that for all* $S \subseteq X$ *has* $\sqcup S$ *in* X.

Example 9.9

$\mathbb{N}^2$ *is not a complete lattice.*

Complete lattice properties

Theorem 9.4

Let $(X, \sqsubseteq)$ be a complete lattice.

a. complete lattice has $\bot$

b. complete lattice has $\top$

Proof.

a. $\bot = \sqcup\emptyset$ (why?)

b. $\bot = \sqcup X$ (why?) □

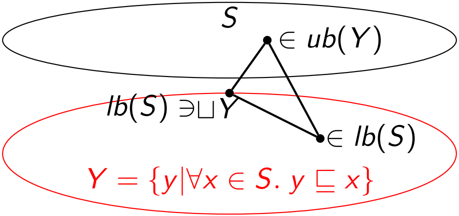
Complete lattice properties II

Theorem 9.5

Let $(X, \sqsubseteq)$ *be a complete lattice. For all* $S \subseteq X$, $\sqcap S$ *exists.*

Proof.

claim: $\sqcap S = \sqcup \{y | \forall x \in S.\ y \sqsubseteq x\}$



□

Exercise: complete lattices

Exercise 9.14

a. Finite lattices are complete

b. Show if $(X, \sqsubseteq, \sqcup, \sqcap)$ satisfies ACC and has $\bot$ then it is a complete lattice.

Moore family

Definition 9.18

For a poset $(X, \sqsubseteq)$ *with* $\top$ *element, a moore family* $M \subseteq X$ *is such that*

- $\top \in M$
- $\forall S \subseteq M. \sqcap S$ *exists and* $\sqcap S \in M$

Theorem 9.6

Let $(X, \leq)$ *be a poset with* $\top$ *element. If* $M \subseteq X$ *is a moore family then* $(M, \sqsubseteq, \top, \sqcap M)$ *is a complete lattice.*

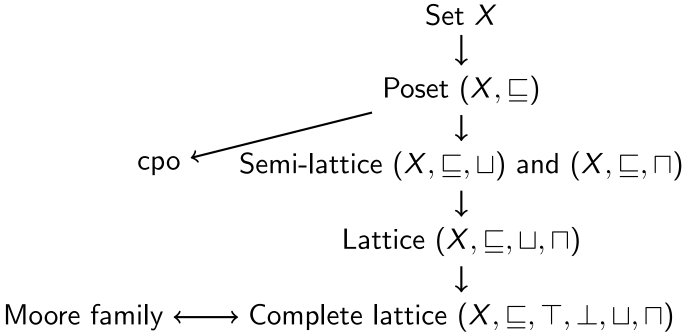
Proof.

1. $(X, \leq)$ is poset then $(M, \leq)$ is a poset
2. Since $\forall S \subseteq M.\ \sqcap S$ exists, M is a complete lattice due to Theorem 9.4.

□

Hierarchy of objects

We have seen the following objects



Set X

Poset $(X, \sqsubseteq)$

cpo

Semi-lattice $(X, \sqsubseteq, \sqcup)$ and $(X, \sqsubseteq, \sqcap)$

Lattice $(X, \sqsubseteq, \sqcup, \sqcap)$

Moore family ⟷ Complete lattice $(X, \sqsubseteq, \top, \bot, \sqcup, \sqcap)$

Topic 9.2

Exercises

Inverse

Exercise 9.15

Show inverse of a partial order is a partial order.

Successor-preserving linear extension

Exercise 9.16

Let $(X, \leq)$ be a partially ordered set. Let $S : A \hookrightarrow A$ be a partial function, such that $a < b$ iff $S(a) \leq b$ for each $a \in dom(S)$ and $b \in A$. Show that there is a total order $\sqsubseteq$ that is extension of $\leq$ and $a \sqsubset b$ iff $S(a) \sqsubseteq b$ for each $a \in dom(S)$ and $b \in A$.

End of Lecture 9