New York University, CIMS, CS, Course CSCI-GA.3140-001, Spring 2024

"Abstract Interpretation"

Ch. 10, Posets, Lattices, and Complete Lattices

(Prerequisites to be self-studied)

Patrick Cousot

pcousot@cs.nyu.edu   cs.nyu.edu/~pcousot

Class 3, Monday, February 5th, 2024, 4:55-6:55 PM, Online class, Room C15

These slides are available at
http://cs.nyu.edu/~pcousot/courses/spring24/CSCI-GA.3140-001/slides/03--2024-02-05-structural-fixpoint-prefix-trace-semantics/slides-10--posets-lattices-complete-lattices-AI.pdf

Chapter 10

Ch. 10, Posets, Lattices, and Complete Lattices

Order theory

- Order theory emerged from the work of George Boole, Ernst Schröder, Charles Peirce, and was mainly developed by Garrett Birkhoff [Birkhoff, 1973].
- Order theory is an abstraction of set theory where $\in$ is expressed in terms of $\subseteq$ ($x \in S \Leftrightarrow \{x\} \subseteq S$) and $\subseteq$ is abstracted as a partial order $\sqsubseteq$
- The abstract partial order $\sqsubseteq$ retains the essential properties of inclusion (reflexive, antisymmetric, and transitive).
- Many theorems of set theory remain valid, but not all, and this widely broaden the scope of applicability of order theory (see introductions in [Birkhoff, 1973; Davey and Priestley, 1990, 2002; Grätzer, 2011]).

`en.wikipedia.org/wiki/Order_theory`
`en.wikipedia.org/wiki/Glossary_of_order_theory`

Posets

Partially ordered set (Poset)

- A *poset* $\langle \mathbb{P}, \sqsubseteq \rangle$ is a set $\mathbb{P}$ equipped with a *partial order* $\sqsubseteq$ which is

  Reflexive: $\forall x \in \mathbb{P} \,.\, x \sqsubseteq x$;

  Antisymmetric: $\forall x, y \in \mathbb{P} \,.\, ((x \sqsubseteq y) \wedge (y \sqsubseteq x)) \Rightarrow (x = y)$;

  Transitive: $\forall x, y, z \in \mathbb{P} \,.\, ((x \sqsubseteq y) \wedge (y \sqsubseteq z)) \Rightarrow (x \sqsubseteq z)$.

en.wikipedia.org/wiki/Partially_ordered_set

Total order

- Two elements x and y are *comparable* when either $x \sqsubseteq y$ or $y \sqsubseteq x$ and *incomparable* when neither $x \sqsubseteq y$ nor $y \sqsubseteq x$.
- A partial order $\sqsubseteq$ is *total* whenever any two elements are comparable.

  Total: $\forall x, y \in \mathbb{P} \,.\, (x \sqsubseteq y) \vee (y \sqsubseteq x)$.

en.wikipedia.org/wiki/Total_order

Strict partial order

- A *strict partial order* $\sqsubset$ is irreflexive ($\forall x \in \mathbb{P} \,.\, x \not\sqsubset x$) and transitive.
- If $\sqsubseteq$ is a partial order then $x \sqsubset y \triangleq x \sqsubseteq y \wedge x \neq y$ is strict.
- If $\sqsubset$ is a strict partial order then $x \sqsubseteq y \triangleq x \sqsubset y \vee x = y$ is a partial order.

en.wikipedia.org/?title=Strict_partial_order&redirect=no

Preorder

- A *preorder* $\preceq$ is reflexive and transitive.
- Then $x \equiv y \triangleq x \preceq y \wedge y \preceq x$ is an *equivalence relation* (reflexive, symmetric ($\forall x, y \in \mathbb{P} \,.\, x \equiv y \Rightarrow y \equiv x$), and transitive).
- The *equivalence class* of $x \in \mathbb{P}$ for the equivalence relation $\equiv$ is $[x]_{\equiv} \triangleq \{y \in \mathbb{P} \mid x \equiv y\}$.
- The *quotient* of $\mathbb{P}$ by $\equiv$ is $\mathbb{P}|_{\equiv} \triangleq \{[x]_{\equiv} \mid x \in \mathbb{P}\}$.
- The *extension* of the preorder $\preceq$ to the quotient $\mathbb{P}|_{\equiv}$ is

$$[x]_{\equiv} \preceq_{\equiv} [y]_{\equiv} \Leftrightarrow \exists x' \in [x]_{\equiv}, y' \in [y]_{\equiv} \,.\, x' \preceq y'$$

- If $\preceq$ is a preorder on $\mathbb{P}$ then $\preceq_{\equiv}$ is a partial order on $\mathbb{P}|_{\equiv}$.

en.wikipedia.org/wiki/Preorder
en.wikipedia.org/wiki/Equivalence_relation
en.wikipedia.org/wiki/Equivalence_class

Equality

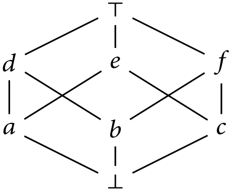
- Equality $=$ is the only relation which is both a partial order and an equivalence relation.

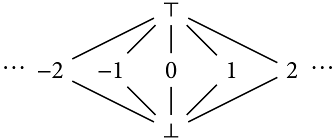
en.wikipedia.org/wiki/Equality_(mathematics)

Hasse diagrams

Hasse diagrams

- Finite posets $\langle \mathbb{P}, \sqsubseteq \rangle$ can be represented by a Hasse diagram





- This is a set of points $\{p_x \mid x \in \mathbb{P}\}$ in the plane, different two by two, and such that
  - if $x \sqsubset y$ then p_x is strictly below p_y;
  - p_x and p_y are linked by a segment when $x \lessdot y$ (y covers x) where $x \lessdot y \triangleq x \sqsubset y \wedge \nexists z \in \mathbb{P} \,.\, x \sqsubset z \wedge z \sqsubset y$.
- $\sqsubseteq$ is derived from $\lessdot$ by reflexivity and transitivity.
  Two unlinked elements are incomparable.

  en.wikipedia.org/wiki/Hasse_diagram

Least upper bound (lub), greatest lower bound (glb), minimum, maximum, infimum, supremum (section 10.3)

Bounds and extrema

- Let $\langle \mathbb{P}, \sqsubseteq \rangle$ be a poset and $S \in \wp(\mathbb{P})$ be a subset.
- This subset S has

An upper bound u: if and only if $u \in \mathbb{P}$ and $\forall x \in S \,.\, x \sqsubseteq u$;

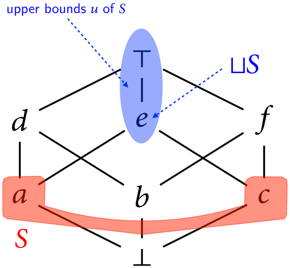
A least upper bound (lub/join) $\sqcup S$: if and only if

  - $\sqcup S \in \mathbb{P}$
  - $\sqcup S$ is an upper bound of S (i.e. $\forall x \in S \,.\, x \sqsubseteq \sqcup S$)
  - $\sqcup S$ is smaller that other upper bound of S (i.e. $\forall u \in \mathbb{P} \,.\, (\forall x \in S \,.\, x \sqsubseteq u) \Rightarrow (\sqcup S \sqsubseteq u)$).

$\sqcup\{x, y\}$ is denoted with the infix notation $x \sqcup y$;

A maximum M: if and only if $M = \sqcup S \in S$;

A supremum $\top$: if and only if $\top = \sqcup \mathbb{P} \in \mathbb{P}$.

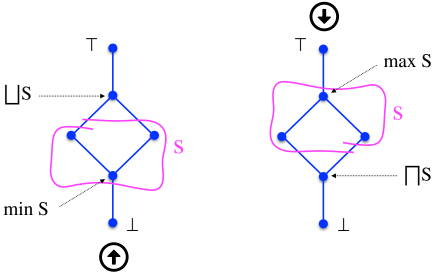


en.wikipedia.org/wiki/Upper_and_lower_bounds
en.wikipedia.org/wiki/Least-upper-bound_property
en.wikipedia.org/wiki/Maxima_and_minima
en.wikipedia.org/wiki/Infimum_and_supremum

Duality principle (section 10.4)

Order dual

- The *order dual* of an order-theoretic definition or statement is obtained by replacing
  - $\sqsubseteq$ by its inverse $\sqsupseteq$,
  - upper by lower,
  - least by greatest,
  - $\sqcup$ by $\sqcap$,
  - $\sqcap$ by $\sqcup$,
  - join by meet,
  - meet by join,
  - maximum by minimum,
  - etc.



en.wikipedia.org/wiki/Duality_(order_theory)

Duality principle

- If a definition or statement is valid for all partially ordered sets then the dual definition or dual statement is also valid for all partially ordered sets [Birkhoff, 1973].

Example 10.2 Let $f \in \langle A, \leqslant\rangle \xrightarrow{\nearrow} \langle B, \sqsubseteq\rangle$ be increasing ie i.e.

$$\forall x, y \in A \,.\, (x \leqslant y) \Rightarrow (f(x) \sqsubseteq f(y))$$

- The dual of "f is increasing" is "f is increasing".
- Note that if duality is applied to $\langle A, \leqslant\rangle$ or $\langle B, \sqsubseteq\rangle$ only, then the semi-dual of "f is increasing" would be "f is decreasing" i.e. $\forall x, y \in A \,.\, (x \leqslant y) \Rightarrow (f(x) \sqsupseteq f(y))$.

en.wikipedia.org/wiki/Duality_principle

Lattices

Lattices

Lattices are posets with the following properties.

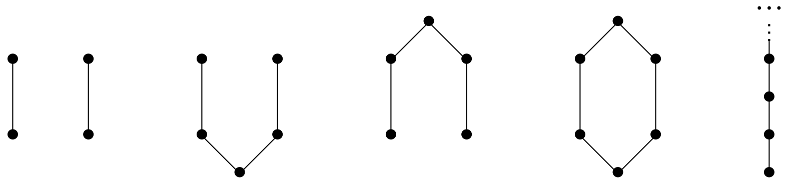
Join semilattice: $\forall x, y \in \mathbb{P} \,.\, x \sqcup y$ exists in $\mathbb{P}$ (hence any non-empty finite subset of $\mathbb{P}$ has a lub);

Meet semilattice: $\forall x, y \in \mathbb{P} \,.\, x \sqcap y$ exists in $\mathbb{P}$ (hence any non-empty finite subset of $\mathbb{P}$ has a glb);

Lattice: $\forall x, y \in \mathbb{P} \,.\, x \sqcup y$ and $x \sqcap y$ exist in $\mathbb{P}$ (hence any non-empty finite subset of $\mathbb{P}$has a lub/join and a glb/meet).

`en.wikipedia.org/wiki/Semilattice`
`en.wikipedia.org/wiki/Lattice_(order)`

Examples of lattices

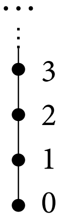


poset meet-lattice join-lattice lattices

Joins and meets of lattices

- Lattices have unique joins/meets of two-elements hence, by associativity of finite subsets.
- For example $\langle \mathbb{N}, \leqslant \rangle$ is a lattice where
  - the glb/meet is $\min$
  - the lub/join is $\max$

  taken on non-empty finite subsets of $\mathbb{N}$.



Algebraic definition of lattices

- The lub $\sqcup$ and glb $\sqcap$ of a lattice $\langle \mathbb{P},\ \sqsubseteq \rangle$ have the following properties.

$x \sqcap x = x$	$x \sqcup x = x$	idempotency
$x \sqcap y = y \sqcap x$	$x \sqcup y = y \sqcup x$	commutativity
$x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$	$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$	associativity
$(x \sqcap y) \sqcup x = x$	$(x \sqcup y) \sqcap x = x$	distributivity

- Conversely, a set equipped with binary operations $\sqcup$ an $\sqcap$ satisfying the above properties is a lattice by defining

$$x \sqsubseteq y \triangleq x \sqcap y = x \text{ (or equivalently } x \sqcup y = y\text{).}$$

en.wikipedia.org/wiki/Algebraic_structure

Complete lattices (section 10.6)

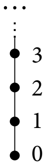
Complete lattice

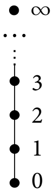
- A *complete lattice* is a poset $\langle \mathbb{P}, \sqsubseteq \rangle$ in which *any* subset $S \in \wp(\mathbb{P})$ has a lub/join $\sqcup S$ (not only the finite ones).
- Therefore a complete lattice has a supremum $\top = \sqcup \mathbb{P}$ and an infinum $\bot = \sqcup \emptyset$.
- Any element x of $\mathbb{P}$ is an upper bound of $\emptyset$ since $\forall y \in \emptyset \; . \; y \sqsubseteq x$. So the lub of $\emptyset$ is the least element of $\mathbb{P}$.

en.wikipedia.org/wiki/Complete_lattice

Examples of complete lattice

- $\langle \mathbb{N},\ \leqslant \rangle$ is not a complete lattice since $\mathbb{N}$ has no lub.
- $\langle \mathbb{N} \cup \{\infty\},\ \leqslant \rangle$ where $\forall n \in \mathbb{N} \ .\ n < \infty \leqslant \infty$ is a complete lattice with supremum ∞ and infimum 0.





- The powerset of a set S is a complete lattice $\langle \wp(S),\ \subseteq,\ \emptyset,\ S,\ \cup,\ \cap \rangle$.

Properties of complete lattices (exercise 10.7)

- A complete lattice $\langle \mathbb{P}, \sqsubseteq, \bot, \top, \sqcup \rangle$ has a glb $\sqcap$ for arbitrary subsets.
- $\sqcap S = \sqcup\{\ell \mid \forall x \in S \,.\, \ell \sqsubseteq x\}$

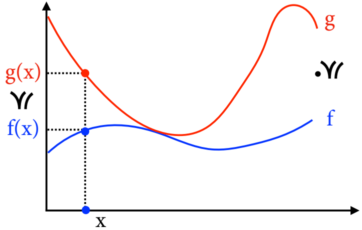
Properties of complete lattices (exercise 10.8)

- In a complete lattice $\langle \mathbb{P}, \sqsubseteq, \bot, \top, \sqcup \rangle$, if $X, Y \in \wp(\mathbb{P})$ and $X \subseteq Y$ then $\sqcup X \sqsubseteq \sqcup Y$.

Pointwise extension

Pointwise extension

- Let $\langle \mathbb{P}, \sqsubseteq \rangle$ be a poset and S be a set.
- The pointwise extension $\dot{\sqsubseteq}$ of $\sqsubseteq$ to S is $\langle S \to \mathbb{P}, \dot{\sqsubseteq} \rangle$ where $f \mathrel{\dot{\sqsubseteq}} g$ if and only if $\forall x \in S \,.\, f(x) \sqsubseteq g(x)$.
- The pointwise join is $f \mathbin{\dot{\sqcup}} g \triangleq x \in S \mapsto f(x) \sqcup g(x)$
- The pointwise meet is $f \mathbin{\dot{\sqcap}} g \triangleq x \in S \mapsto f(x) \sqcap g(x)$, etc.



- The pointwise extension of $\dot{\sqsubseteq}$ is denoted $\ddot{\sqsubseteq}$, that of $\ddot{\sqsubseteq}$ is $\dddot{\sqsubseteq}$, etc.

  en.wikipedia.org/wiki/Pointwise

Properties of the pointwise extension

- The pointwise extension of a poset (respectively semi-lattice, lattice, complete lattice, etc.) is a poset (respectively semi-lattice, lattice, complete lattice, etc.).
- Let $\langle \mathbb{P}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ be a complete lattice.
  - The increasing functions $\mathbb{P} \xrightarrow{\nearrow} \mathbb{P} \triangleq \{f \in \mathbb{P} \to \mathbb{P} \mid \forall x, y \in \mathbb{P} \,.\, (x \sqsubseteq y) \Rightarrow f(x) \sqsubseteq f(y)\}$,
  - The arbitrary join preserving functions $\mathbb{P} \xrightarrow{\sqcup} \mathbb{P} \triangleq \{f \in \mathbb{P} \to \mathbb{P} \mid \forall S \in \wp(\mathbb{P}) \,.\, (\sqcup S \in \mathbb{P}) \Rightarrow (\sqcup f(S) \in \mathbb{P} \wedge f(\sqcup S) = \sqcup f(S))\}$ where $f(S) \triangleq \{f(x) \mid x \in S\}$
  - Dually, the arbitrary meet preserving functions $\mathbb{P} \xrightarrow{\sqcap} \mathbb{P}$

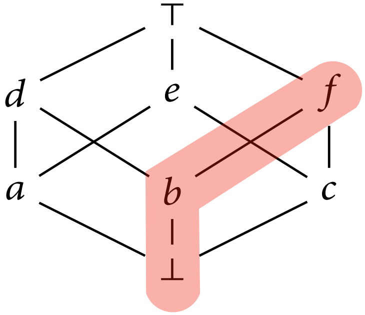
  are a complete lattice for the pointwise ordering

$$f \mathrel{\dot{\sqsubseteq}} g \Leftrightarrow \forall x \in \mathbb{P} \,.\, f(x) \sqsubseteq g(x)$$

Chain (section 10.8)

Chains I

- A *chain* C of a poset $\langle \mathbb{P}, \sqsubseteq \rangle$ is a subset of the poset $\mathbb{P}$ such that any two elements of the chain are comparable i.e. $C \subseteq \mathbb{P} \wedge \forall x, y \in C \,.\, x \sqsubseteq y \vee y \sqsubseteq x$.



- A *denumerable increasing/ascending chain* is a sequence $\langle x_i,\ i \in \mathbb{N} \rangle$ such that $x_0 \sqsubseteq x_1 \sqsubseteq \ldots x_n \sqsubseteq x_{n+1} \ldots$ i.e. $\forall i < j \in \mathbb{N} \,.\, x_i \sqsubseteq x_j$ (so $x \in \mathbb{N} \stackrel{\nearrow}{\longrightarrow} \mathbb{P}$)

Chains II

- An increasing chain $\langle x_i,\ i \in \mathbb{N}\rangle$ is *ultimately stationary* if and only if $\exists \ell \in \mathbb{N}\ .\ \forall i \geqslant \ell\ .\ x_i = x_\ell$.
- A poset $\langle \mathbb{P},\ \sqsubseteq\rangle$ is *noetherian* (or satisfies the *increasing chain condition* (also called ascending chain condition (ACC)[1]) if and only if any increasing chain is ultimately stationary (so that any strictly ascending chain is finite).
- The *descending chain condition (DCC)* is dual.

en.wikipedia.org/wiki/Ascending_chain_condition
en.wikipedia.org/wiki/Noetherian

[1] (*Voraussetzung des Teilerkettensatz*) [Noether, 1921, Satz I], [Noether, 1927, Satz II]

CPO (section 10.9)

Chain complete partial order (CPO)

- A *complete partial order (CPO)* or (*countably chain-complete poset*) is a poset $\langle \mathbb{P}, \sqsubseteq, \perp, \sqcup \rangle$ with infimum $\perp$ such that any denumerable ascending chain $\langle x_i, i \in \mathbb{N} \rangle$ has a least upper bound $\bigsqcup_{i \in \mathbb{N}} x_i \in \mathbb{P}$.
- A dual-cpo is defined dually.

en.wikipedia.org/wiki/Complete_partial_order
en.wikipedia.org/wiki/Chain-complete_partial_order

This concludes our presentation of

- Pointwise extension
- Chains and CPOs

from chapter 10, “Posets, Lattices, and Complete Lattices”

Conclusion

Conclusion

- The poset representation $\langle \mathbb{P}, \sqsubseteq \rangle$ of program properties $\mathbb{P}$ with an abstract implication $\sqsubseteq$ provides a unified theory of program properties and their abstraction
- Much more freedom and diversity is allowed in the choice of the possible encodings of abstract properties than with logic.
- [Aït–Kaci, Boyer, Lincoln, and Nasr, 1989] is an example of efficient implementation of finite lattices.
- In program verification and analysis, lattices need not be computer-representable, only their elements must be implemented.
- Posets, lattices, and complete lattices are used everywhere in abstract interpretation. It is essential to master these concepts!

Bibliography

Bibliography I

Aït–Kaci, Hassan, Robert S. Boyer, Patrick Lincoln, and Roger Nasr (1989). "Efficient Implementation of Lattice Operations.". *ACM Trans.Program.Lang.Syst.* 11.1, pp. 115–146.

Birkhoff, Garrett (1973). *Lattice Theory.* 3rd ed. American Mathematical Society, Colloquium Publications, Volume XXV.

Davey, Brian A. and Hilary A. Priestley (1990, 2002). *Introduction to Lattices and Order.* 2nd ed. Cambridge University Press.

Grätzer, George (2011). *Lattice Theory: Foundation.* Birkhäuser.

Noether, Emmy (1921). "Idealtheorie in Ringbereichen.". *Mathematische Annalen.* 83 (1–2), pp. 24–66.

— (1927). "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- Und Funktionenkörpern.". *Mathematische Annalen.* 96 (1–2), pp. 26–61.

The End, Thank you