Introduction to Lattice Theory

Bruno Teheux

June 18, 2024

DMATH

Goal

Elementary order and lattice theory for Computer Science.

Order

Poset

X, Y, Z... will be sets

Orders are meant to capture the "less or equal" relations.

Definition. A binary relation $\leq$ on X is an *order* if for all x, y, z

- $x \leq x$ (reflexivity)
- $(x \leq y$ and $y \leq x)$ implies $x = y$ (antisymmetry)
- $(x \leq y$ and $y \leq z)$ implies $x \leq z$ (transitivity)

We call $(X, \leq)$ a *partially ordered set* or *poset*.

Examples

We supercharge $\leq$.

Example. $(\mathbb{N}, \leq)$ where $\leq$ is the natural order is a poset

Examples

We supercharge $\leq$.

Example. $(\mathbb{N}, \leq)$ where $\leq$ is the natural order is a poset

Example. If $X \subseteq \mathbb{N}$ then $(X, \leq)$ is a poset

Example. $(\mathbb{R}, \leq)$ is a poset

Examples

We supercharge $\leq$.

Example. $(\mathbb{N}, \leq)$ where $\leq$ is the natural order is a poset

Example. If $X \subseteq \mathbb{N}$ then $(X, \leq)$ is a poset

Example. $(\mathbb{R}, \leq)$ is a poset

How to define $\leq$ on $\mathbb{N}$ and $\mathbb{R}$ is an interesting question.

These are examples of *total orders*, that is, that satisfies

$$\forall x, y \ (x \leq y \text{ or } y \leq x)$$

Example. $(\mathbb{N}, \leq)$ where $a \leq b$ if a divides b is a poset

Examples: natural orders

Example. $(2^X, \leq)$ where 2^X is the powerset of X and $\leq$ is the inclusion relation is a poset.

Definition. A *predicate* on X is a mapping $P\colon X \to \{\mathrm{True}, \mathrm{False}\}$.

Example. $x \geq 2$ is a predicate sur $\mathbb{N}$

Example. Let $\mathbb{P}(X)$ the set of predicates on X. $(\mathbb{P}, \implies)$ is a poset, where

$$P \implies Q \qquad \text{if} \qquad \{x \in X \mid P(X)\} \subseteq \{x \in X \mid Q(X)\}$$

Hasse diagrams

A (finite) poset $(X, \leq)$ can be represented by a diagram depicted according to the following rules:

1. Elements $x \in X$ are represented by dots.
2. If $x \leq y$ then x is represented below y and both are connected by a straight line unless ...

2 bis. the relation $x \leq y$ can de deduced from $x \leq z$ and $z \leq y$ for some z.

It is called the *Hasse diagram* of $(X, \leq)$

Hasse diagrams: examples

Draw the Hasse diagrams of $(\mathbb{N}, \leq)$, the divisors of 12 ordered by divisibility and the powerset $2^{\{0,1\}}$.

Order dual and strict order

Definition. The *(order) dual* of $(X, \leq)$ is the poset $(X, \leq^\partial)$ defined as

$$x \leq^\partial y \qquad \text{if} \qquad y \leq x.$$

How to obtain the Hasse diagram of $(X, \leq^\partial)$ from that of $(X, \leq)$?

Definition. We write $x < y$ if $(x \leq y$ and $y \not\leq x)$.

Such a $<$ is called a *strict partial order*.

Mappings

There are different natural classes of mappings betwen posets.

Definition. A map $f\colon (X, \leq) \to (Y, \leq)$ is

- *order-preserving* if $x \leq y \implies f(x) \leq f(y)$ for all x, y

Mappings

There are different natural classes of mappings betwen posets.

Definition. A map $f\colon (X,\leq) \to (Y,\leq)$ is

- *order-preserving* if $x \leq y \implies f(x) \leq f(y)$ for all x, y
- an *order-embedding* if $x \leq y \iff f(x) \leq f(y)$ for all x, y

Mappings

There are different natural classes of mappings betwen posets.

Definition. A map $f\colon (X,\leq) \to (Y,\leq)$ is

- *order-preserving* if $x \leq y \implies f(x) \leq f(y)$ for all x, y
- an *order-embedding* if $x \leq y \iff f(x) \leq f(y)$ for all x, y
- an *order-isomorphism* if f is an onto order-embedding.

Isomorphic posets can't be distinguished from the perspective of order theory.

Mappings: example

Example. Give two integers whose divisors posets are isomorphic

Example. The map $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x$ is an embedding.

Example. The powerset $(2^X, \subseteq)$ and the predicate poset $(\mathbb{B}, \implies)$ are isomorphic.

Poset consctructions: disjoint union

Definition. The *disjoint union* $(X, \leq) \mathbin{\dot\cup} (Y, \leq)$ is the poset defined on $X \mathbin{\dot\cup} Y$ by

$$s \leq t \qquad \text{if } (s, t \in X \text{ and } s \leq t) \text{ or } (s, t \in Y \text{ and } s \leq t)$$

Example.

Poset constructions: linear sum

Definition The *linear sum* $(X, \leq) \oplus (Y, \leq)$ is the poset defined on $X \uplus Y$ by

$$s \leq t \qquad \text{if} \qquad (s, t \in X \text{ and } s \leq t) \\ \text{or } (s, t \in Y \text{ and } s \leq t) \\ \text{or } (s \in X \text{ and } t \in Y).$$

Example.

Poset consctructions: Cartesian product

Given $(X, \leq)$ and $(Y, \leq)$ how to define a poset on $X \times Y$?

Definition. The *pointwise order* on $X \times Y$ is defined by

$$(x, y) \leq (x', y') \qquad \text{if} \qquad (x \leq x' \text{ and } y \leq y')$$

The *lexicographic order* on $X \times Y$ is defined by

$$(x, y) \leq (x', y') \qquad \text{if} \quad \big(x < x' \text{ or } (x = x' \text{ and } y \leq y')\big).$$

Exercise. Check that the lexicographic and pointiwse orders are orders.

Examples.

Exercise. Prove that the lexicographic order of total orders is a total order.

Bounds

Upper and lower bounds

Definition. Let $(X, \leq)$ be a poset and $S \cup \{u, \ell\} \subseteq X$.

1. u is an *upper bound* of S if $s \leq u$ for all $s \in S$
2. ℓ is a *lower bound* of S if $\ell \leq s$ for all $s \in S$

Examples.

Best bounds

One Bound to rule them all, One Bound to find them.

Definition. Let $(X, \leq)$ be a poset and $S \cup \{u, \ell\} \subseteq X$.

1. u is a *least upper bound (lub)* of S if u is an upper bound of S and $u \leq u'$ for every upper bound u' of S.
2. ℓ is a *greatest lower bound (glb)* of S if ℓ is a lower bound and $\ell' \leq \ell$ for every lower bound ℓ' of S.

Lub and glb are the best bounds.

Definition. If $S \subseteq X$ has a lup (glb, resp.) α and $\alpha \in S$, we say that S has a *greatest element* (*smallest element*, resp.) α.

Examples

Best bounds are unique

Lemma. If u and u' are two lub of S in $(X, \leq)$ then $u = u'$.

Proof. We have $u \leq u'$ and $u' \leq u$.

Unicity also holds for glb.

Bottom and top

Definition. A *top element* $\top$ *of* $(X, \leq)$ is a lup of $(X, \leq)$.

A *bottom element* $\perp$ *of* $(X, \leq)$ is a glb of $(X, \leq)$.

Sometimes top and bottom elements are denoted by 1 and 0, respectively.

Examples.

Powersets have top and bottom elements.

$(\mathbb{Z}, \leq)$ has neither a greatest element, nor a least element.

Lattices

Definition. A *lattice* is a poset in which every pair $\{x, y\}$ has a lub and a glb.

We denote by $x \wedge y$ and $x \vee y$ the glb and lub of $\{x, y\}$.

A lattice is *bounded* if it has a bottom and a top element.

Examples

Lattices as algebraic structures

A lattice $(L, \leq)$ can be seen as an algebraic structure $(L, \wedge, \vee)$ equipped with two binary operations

$$\wedge, \vee, : L \times L \to L,$$

It satisfies the following equations:

$$x \wedge y = y \wedge x \qquad \text{(symmetry)} \tag{1}$$

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \qquad \text{(associativity)} \tag{2}$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \qquad \text{(distributivity)} \tag{3}$$

$$x \wedge x = x \qquad \text{(idempotence)} \tag{4}$$

$$x \vee (x \wedge y) = x \qquad \text{(absorption)} \tag{5}$$

and their dual.

Lattices as algebraic structures

A bounded lattice $(L, \leq)$ can be seen as an algebraic structure $(L, \wedge, \vee 0, 1)$ equipped with two binary operations

$$\wedge, \vee, : L \times L \to L,$$

and constants 0 and 1.

It satisfies the following equations:

$$x \wedge y = y \wedge x \qquad \text{(symmetry)} \tag{1}$$

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \qquad \text{(associativity)} \tag{2}$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \qquad \text{(distributivity)} \tag{3}$$

$$x \wedge x = x \qquad \text{(idempotence)} \tag{4}$$

$$x \vee (x \wedge y) = x \qquad \text{(absorption)} \tag{5}$$

$$x \wedge 1 = 1, \quad x \vee 0 = 0$$

and their dual.

Lattices as posets $\equiv$ lattices as algebra

Proposition. In a lattice $(L, \leq)$, we can recover $\leq$ from $\wedge$ or $\vee$:

$$a \leq b \quad \Longleftrightarrow \quad a \wedge b = a \quad \Longleftrightarrow \quad a \vee b = b$$

Proposition. If $(L, \wedge, \vee)$ satisfies equations (1) - (5) then the relation $\leq$ defined as

$$a \leq b \quad \text{if } a \wedge b = a$$

is a lattice order. The glb and lub operations in $(L, \leq)$ coincide with $\wedge$ and $\vee$, respectively.

We use the order-theoretic and algebraic perspectives interchangeably.

Lattices and poset constructions

The disjoint union of lattices

Lattices and poset constructions

The disjoint union of lattices is not a lattice

The linear sum of lattices

Lattices and poset constructions

The disjoint union of lattices is not a lattice

The linear sum of lattices is a lattice

The lexicographic order on product of lattices

Lattices and poset constructions

The disjoint union of lattices is not a lattice

The linear sum of lattices is a lattice

The lexicographic order on product of lattices might not be a lattice (see exercises)

The pointwise order on product of lattices

Lattices and poset constructions

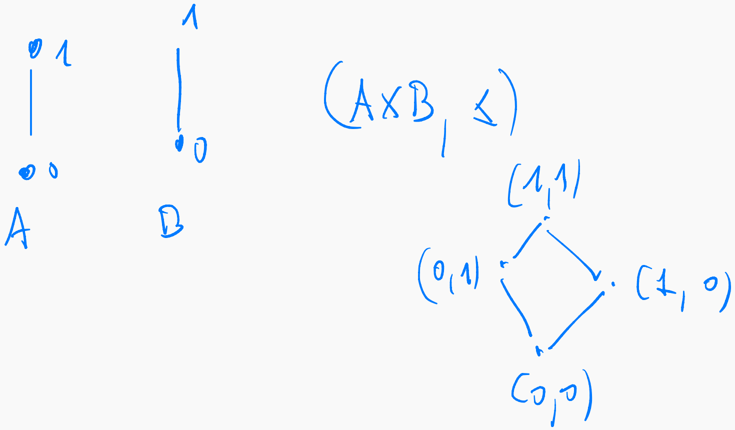
The disjoint union of lattices is not a lattice

The linear sum of lattices is a lattice

The lexicographic order on product of lattices might not be a lattice (see exercises)

The pointwise order on product of lattices *is* a lattice. Operations $\vee$ and $\wedge$ are computed pointwise.

Examples



Lattice constructions: sublattices

Definition. A subset S of a lattice $(L, \wedge, \vee)$ is called a *sublattice* if $x \wedge y$ and $x \vee y$ belongs to S for every $x, y \in S$.

Sublattices are lattices. They inherit their order and operations from their parent lattice.

Sublattice: Examples

Suitable maps between lattices

Definition. A map $f\colon (L, \wedge, \vee) \to (L', \wedge, \vee)$ is a *lattice homomorphism* if for every $a, b \in L$

$$f(a \vee b) = f(a) \vee f(b) \quad \text{and} \quad f(a \wedge b) = f(a) \wedge f(b).$$

A bijective lattice homomorphism is called a *lattice isomorphism*.

Examples.

Complete lattices: the best case scenario

Definition. A lattice $(L, \leq)$ is *complete* if every subset S of L has a lup and a glb, denoted by

$$\bigvee S \qquad \text{and} \qquad \bigwedge S,$$

and called the *supremum* and *infimum* of S, respectively.

A complete lattice $(L, \leq)$ has all joins and all meets. In particular,

$$\bigwedge L = \bigvee \varnothing \quad \text{and} \quad \bigvee L = \bigwedge \varnothing,$$

which are bottom and top element of $(L, \leq)$

Examples

Powerset lattices are complete.

$$\bigwedge S = \bigcap S \qquad \bigvee S = \bigcup S$$

Let $(L, \leq)$ be a complete lattice

X any set

$X \to L \equiv$ mappings from X to L

Define $\leq$ on $X \to L$ by

$$f \leq g \quad \text{iff} \quad \forall x \; f(x) \leq g(x)$$

Then $(X \to L, \leq)$ is complete

Completeness can be summarized

Lemma. A lattice $(L, \leq)$ is complete if and only if it has a top element $\top$ and every nonempty subset S of L a glb.

Proof. $\Leftarrow$ We have $\bigvee \varnothing = \top$ and if $T \subseteq L$ is nonempty

$$\bigvee T = \bigwedge \{\ell \in L \mid \forall t \in T \;\; t \leq \ell\}$$

Closure operator

Definition. A map $C\colon (X, \leq) \to (X, \leq)$ is a *closure operator* if for all $x \in X$

1. $x \leq C(x)$
2. $x \leq y \implies C(x) \leq C(y)$
3. $C(C(x)) = C(x)$.

Elements of the form $C(x)$ for some x are call *closed*.

Closure operators: Examples

Definition A subset S of $(X, \leq)$ is a *downset* if

$$(s \in S \quad \text{and} \quad x \leq s) \qquad \Longrightarrow \qquad x \in S.$$

For every susbet Y of X we set

$$Y{\downarrow} := \{x \in X \mid \exists y \in Y \; x \leq y\}.$$

Example. The map $-{\downarrow}$ is a closure operator on the powerset of X.

Closure operators: Examples

Definition A subset S of $(X, \leq)$ is a *downset* if

$$(s \in S \quad \text{and} \quad x \leq s) \qquad \Longrightarrow \qquad x \in S.$$

For every susbet Y of X we set

$$Y{\downarrow} := \{x \in X \mid \exists y \in Y \; x \leq y\}.$$

Example. The map $-{\downarrow}$ is a closure operator on the powerset of X.

Example. The linear span is a closure operator on the powerset of a vector space.

From Closure Opeators to Complete lattices

Theorem. For any complete lattice $(L, \leq)$ define $C\colon 2^L \to 2^L$ by

$$C(A) := \bigcap\{x\downarrow \mid A \subseteq x\downarrow\}.$$

Then,

1. C is a closure operator.

From Closure Opeators to Complete lattices

Theorem. For any complete lattice $(L, \leq)$ define $C\colon 2^L \to 2^L$ by

$$C(A) := \bigcap\{x{\downarrow} \mid A \subseteq x{\downarrow}\}.$$

Then,

1. C is a closure operator.
2. The set Γ of closed elements of C is a complete lattice for $\subseteq$ and

$$\bigwedge S = \bigcap S \qquad \text{and} \qquad \bigvee S = C(\bigcup S)$$

   for every $S \subseteq \Gamma$.

From Closure Opeators to Complete lattices

Theorem. For any complete lattice $(L, \leq)$ define $C\colon 2^L \to 2^L$ by

$$C(A) := \bigcap\{x{\downarrow} \mid A \subseteq x{\downarrow}\}.$$

Then,

1. C is a closure operator.
2. The set Γ of closed elements of C is a complete lattice for $\subseteq$ and
$$\bigwedge S = \bigcap S \qquad \text{and} \qquad \bigvee S = C(\bigcup S)$$
for every $S \subseteq \Gamma$.
3. The lattices $(\Gamma, \leq)$ and $(L, \leq)$ are isomorphic.

Fixpoints

Fixpoints

In general, a fix point of $F\colon X \to X$ is a $x \in X$ such that

$$F(x) = x.$$

Fixpoints are commonly used in CS in the context of posets.

We give a few existence and computation results for fixpoints.

Fixpoints in posets

$F\colon (X,\leq) \to (X,\leq)$

Notation.

$$\mathrm{fix}(F) := \{x \in X \mid F(x) = x\}$$
$$\mathrm{post}(F) := \{x \in X \mid x \leq F(x)\}$$
$$\mathrm{pre}(F) := \{x \in X \mid F(x) \leq x\}$$

These sets might be empty or nonempty, bounded or unbounded...

If $\bigvee \mathrm{fix}(F)$ exists and belongs to $\mathrm{fix}(F)$, it is denoted by $\nu(F)$.

If $\bigwedge \mathrm{fix}(F)$ exists and belongs to $\mathrm{fix}(F)$, it is denoted by $\mu(F)$.

Fixpoints in Complete Lattices

Theorem (Knaster - Tarski) Let $(L, \leq)$ be a complete lattice and $F\colon (L, \leq) \to (L, \leq)$ be an order-preserving map.

1. F has a least fixpoint $\mu(F)$ and a greatest fixpoint $\nu(F)$.
2. We have

$$\mu(F) = \bigwedge \mathrm{pre}(F),$$
$$\nu(F) = \bigvee \mathrm{post}(F).$$

Proof.[...]

This theorem does no help to compute or approximate fixpoints.

Complete Partial Orders (CPOs)

CPOs are the general environnement to state fixpoint theorems.

Definition. A subset D of $(X, \leq)$ is *directed* if every pair of elements of D has an upper bound in D.

Chains are examples of directed set.

Definition. A poset $(X, \leq)$ is a *complete partial order (CPO)* if

1. it has a bottom element $\bot$,
2. $\bigvee D$ exists for every directed $D \subseteq X$.

Complete lattices are instances of CPO.

Recognizing CPOs

Theorem ($).

$(P, \leq)$ is a CPO if and only if each chain has a lub (in P).

Continuous transformations

Definition. A map $f\colon (X,\leq) \to (Y,\leq)$ between CPOs is *continuous* if for every directed $D \subseteq X$,

$$f(D) \text{ is directed} \qquad \text{and} \qquad f(\bigvee D) = \bigvee f(D).$$

Continuous implies order-preserving but the converse is false.

Definition. $(X,\leq)$ satisfies the *ascending chain condition (AAC)* if every increasing sequence of P is eventually constant.

Lemma If $(X,\leq) \models$ AAC, then any order-preserving $f\colon (X,\leq) \to (Y,\leq)$ is continuous.

Next Fixpoint Theorem

Theorem. Let $F\colon (X, \leq) \to (X, \leq)$ be an order-preserving map on a CPO and set

$$\alpha := \bigvee \{ F_n(\perp) \mid n \geq 0 \}$$

1. If α is a fixpoint then it is the least fixpoint.
2. If F is continuous then it is a least fixpoint $\mu(F)$ and $\mu(F) = \alpha$.