I. Partial orders

Definition (Partial order)

Given a set X, a relation $\sqsubseteq$ is a *partial order* if it is:
- **reflexive**: $\forall x \in X, x \sqsubseteq x$
- **antisymmetric**: $\forall x, y \in X, x \sqsubseteq y \land y \sqsubseteq x \Rightarrow x = y$
- **transitive**: $\forall x, y, z \in X, x \sqsubseteq y \land y \sqsubseteq z \Rightarrow x \sqsubseteq z$

$(X, \sqsubseteq)$ is a *partially ordered set* (*poset*).

If we drop antisymmetry, we get a **preorder**.

Example (Partial orders)

- $(\mathbb{Z}, \leq)$ is *completely ordered*
- $(\mathcal{P}, \subseteq)$ is not completely ordered

Example (Preorders)

- $(\mathcal{P}, \sqsubseteq)$ where $a \sqsubseteq b \Leftrightarrow |a| \leq |b|$

Definition ((Least) Upper bounds)

- c is an *upper bound* of a and b if $a \sqsubseteq c$ and $b \sqsubseteq c$.
- c is a *least upper bound* (*lub* or *join*) of a and b if
  - c is an upper bound of a and b
  - for every upper bound d of a and b, $c \sqsubseteq d$.

Prop (Unicity of least upper bound)

If it exists, the lub of a and b is **unique**, and denoted as $a \sqcup b$.

Similarly, we define the *greatest lower bound* (*glb*, *meet*) $a \sqcap b$.

Note: not all posets have lubs and glbs.
E.g. $a \sqcup b$ is not defined on $(\{a, b\}, =)$.

Definition (Chains)

$C \subseteq X$ is a *chain* in $(X, \sqsubseteq)$ if it is totally ordered by $\sqsubseteq$: $\forall x, y \in C, (x \sqsubseteq y) \lor (y \sqsubseteq x)$.

Definition (Complete partial orders (CPO))

A poset $(X, \sqsubseteq)$ is a *complete* partial order (CPO) if every chain C (including $\emptyset$) has a least upper bound $\sqcup C$.

A CPO has a **least element** $\sqcup \emptyset$ denoted $\perp$.

Example (CPO)

- $(\mathbb{N}, \leq)$ is not complete but $(\mathbb{N} \cup \{\infty\}, \leq)$ is complete.
- $(\{x \in \mathbb{Q} \mid 0 \leq x \leq 1\}, \leq)$ is not complete but
- $(\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}, \leq)$ is complete
- $(\mathcal{P}(Y), \subseteq)$ is complete for any Y
- $(X, \sqsubseteq)$ is complete if X is finite

II. Lattices

Definition (Lattice)

A *lattice* $(X, \sqsubseteq, \sqcup, \sqcap)$ is a poset with
- a lub $a \sqcup b$ for every pair of elements a and b
- a glb $a \sqcap b$ for every pair of elements a and b

Example (Lattice)

- integers $(\mathbb{Z}, \leq, \max, \min)$
- integer intervals $(\{[a, b] \mid a, b \in \mathbb{Z}, a \leq b\} \cup \{\emptyset\}, \subseteq, \cup, \cap)$
- divisibility $(\mathbb{N}^*, |, \mathrm{lcm}, \mathrm{gcd})$

If we drop one condition, we have a (join or meet) *semilattice*.

Definition (Complete lattice)

A *complete lattice* $(X, \sqsubseteq, \sqcup, \sqcap, \bot, \top)$ is a poset with:
- a lub $\sqcup S$ for every set $S \subseteq X$
- a glb $\sqcap S$ for every set $S \subseteq X$
- a least element $\bot$
- a greatest element $\top$

Remarks:
- 1 implies 2 as $\sqcap S = \sqcup \{y \mid \forall x \in S, y \sqsubseteq x\}$ (and vice-versa)
- 1 and 2 imply 3 and 4
- a complete lattice is also a CPO

Example (Complete lattice)

- powersets $(\mathcal{P}(S, \subseteq, \cup, \cap, \emptyset, S))$
- real segment $[0, 1]$: $([0, 1], \leq, \max, \min, 0, 1)$
- integer intervals with finite **and infinite** bounds
  $(\{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\} \cup \{\emptyset\}, \subseteq, \cup, \cap, \emptyset, [-\infty, +\infty])$

III. Functions and fixpoints

Definition (Functions)

A function $f : \left(X_1, \underset{1}{\sqsubseteq}, \sqcup_1, \bot_1\right) \to \left(X_2, \underset{2}{\sqsubseteq}, \sqcup_2, \bot_2\right)$ is:

- *monotonic* if $\forall x, x', x \underset{1}{\sqsubseteq}, x' \Rightarrow f(x) \underset{2}{\sqsubseteq} f(x')$
- *strict* if $f(\bot_1) = \bot_2$
- *continuous* between CPO if $\forall C$ chain $\subseteq X_1, \{f(c) \mid c \in C\}$ is a chain in X_2 and $f(\sqcup_1 C) = \sqcup_2 \{f(c) \mid c \in C\}$
- a (complete) $\sqcup$-*morphism* between (complete) lattices if $\forall S \subseteq X_1, f(\sqcup_1 S) = \sqcup_2 \{f(s) \mid s \in S\}$
- *extensive* if $X_1 = X_2$ and $\forall x, x \underset{1}{\sqsubseteq} f(x)$
- *reductive* if $X_1 = X_2$ and $\forall x, f(x) \underset{1}{\sqsubseteq} x$

Prop (Continuity implies monotony)

Any continuous function is monotonic.

Proof.

Let $x, x' \in X_1$ such that $x \underset{1}{\sqsubseteq} x'$. Then $\{x, x'\}$ is a chain.
By continuity of f, $\{f(x), f(x')\}$ is a chain and $f(\sqcup_1 \{x, x'\}) = \sqcup_2 \{f(x), f(x')\}$.
And $f(\sqcup_1 \{x, x'\}) = f(x \sqcup_1 x') = f(x')$ because $x \underset{1}{\sqsubseteq} x'$.
And $\sqcup_2 \{f(x), f(x')\} = f(x) \sqcup_2 f(x')$.
So we have $f(x') = f(x) \sqcup_2 f(x')$. By definition of the lub, $f(x) \underset{2}{\sqsubseteq} f(x) \sqcup_2 f(x')$, *i.e.* $f(x) \underset{2}{\sqsubseteq} f(x')$.

Definition (Fixpoints)

Given $f : (X, \subseteq) \to (X, \subseteq)$:

- x is a *fixpoint* of f if $f(x) = x$
- x is a *pre*-fixpoint of f if $x \sqsubseteq f(x)$
- x is a *post*-fixpoint of f if $f(x) \sqsubseteq x$

We may have several fixpoints (or none):

- $\mathrm{fp}(f) \overset{\text{def}}{=} \{x \in X \mid f(x) = x\}$
- least fixpoint greather than x: $\mathrm{lfp}_{x(f)} = \min_{\sqsubseteq}\{y \in \mathrm{fp}(f) \mid x \sqsubseteq y\}$ if it exists
- least fixpoint: $\mathrm{lfp}(f) = \mathrm{lfp}_{\bot}(f)$
- same definitions for greatest fixpoint $\mathrm{gfp}_x(f)$, $\mathrm{gfp}(f)$

Fixpoints can be used to express solutions of mutually recursive equation systems.

Theorem (Tarski's theorem)

If $f : X \to X$ is monotonic in a complete lattice X, then $\mathrm{fp}(f)$ is a complete lattice.

Theorem (Kleene fixpoint theorem)

If $f : X \to X$ is continuous in a CPO X and $a \sqsubseteq f(a)$ then $\mathrm{lfp}_a f$ exists.

Remark: in practice, we are often interested in applying the theorem with $a = \bot$.

Definition (Well-ordered set)

$(S, \sqsubseteq)$ is a *well-ordered set* if:
- $\sqsubseteq$ is a total order on S
- every $X \subseteq S$ such that $X \neq \emptyset$ has a least element $\sqcap X \in X$

Definition (Ordinals)

Ordinals are $0, 1, 2, ..., \omega, \omega + 1, ..., 2\omega, 2\omega + 1, ...$ where ω is a limit. Well-ordered sets are ordinals up to order-isomorphism.

Intuitively, ordinals provide a way to keep iterating after infinity.

Theorem (Constructive Tarski theorem)

If $f : X \to X$ is monotonic in a CPO X and $a \sqsubseteq f(a)$, then $\mathrm{lfp}_a f = x_\delta$ for some ordinal δ.

Definition (Ascending chain condition (ACC))

An *ascending chain* C in $(X, \sqsubseteq)$ is a ⊆uence $c_i \in X$ such that $i \leq j \Rightarrow c_i \sqsubseteq c_j$.

A poset $(X, \sqsubseteq)$ satisfies the *ascending chain condition* (*ACC*) iff for every ascending chain C, $\exists i, \forall j \geq i, c_i = c_j$.

Similarly, we can define a *descending chain condition* (*DCC*).

Theorem (Kleene finite fixpoint theorem)

If $f : X \to X$ is monotonic in an ACC poset X and $a \sqsubseteq f(a)$ then $\mathrm{lfp}_a f$ exists.

Comparison of fixpoint theorems				
theorem	**function**	**domain**	**fixpoint**	**method**
Tarski	monotonic	complete lattice	$\mathrm{fp}(f)$	meet of post-fixpoints
Kleene	continuous	CPO	$\mathrm{lfp}_a(f)$	countable iterations
constructive Tarski	monotonic	CPO	$\mathrm{lfp}_a(f)$	transfinite iterations
ACC Kleene	monotonic	ACC poset	$\mathrm{lfp}_a(f)$	finite iterations

IV. Galois connections

Definition (Galois connection)

Given two posets $(C, \leq)$ and $(A, \sqsubseteq)$, the pair $(\alpha : C \to A, \gamma : A \to C)$ is a *Galois connection* iff:

$$\forall a \in A, \forall c \in C, \alpha(c) \sqsubseteq a \Leftrightarrow c \leq \gamma(a)$$

which is noted $(C, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$.

We say that:

- A is the *abstract domain* and α is the *abstraction*.
- C is the *concrete domain* and γ is the *concretization*.

Example (Galois connection)

Abstract domain of intervals of integers $\mathbb{Z}$ represented as pair of bounds (a, b).

We have $(\mathcal{P}(\mathbb{Z}), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (I, \sqsubseteq)$ with

- $I \overset{\text{def}}{=} (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{+\infty\})$
- $(a, b) \sqsubseteq (a', b') \Leftrightarrow (a \geq a') \land (b \leq b')$
- $\alpha(X) \overset{\text{def}}{=} (\min X, \max X)$
- $\gamma((a, b)) = [a, b]$

Prop (Properties of Galois connections)

1. $\gamma \circ \alpha$ is extensive
2. $\alpha \circ \gamma$ is reductive
3. α is monotonic
4. γ is monotonic
5. $\gamma \circ \alpha \circ \gamma = \gamma$
6. $\alpha \circ \gamma \circ \alpha = \alpha$
7. $\alpha \circ \gamma$ is idempotent
8. $\gamma \circ \alpha$ is idempotent

Proof.

1. Goal: $\forall c \in C, c \leq \gamma \circ \alpha(c)$.
   Let $c \in C$, and consider $a = \alpha(c) \in A$. We have $\alpha(c) \sqsubseteq \alpha(c)$ which leads to $c \leq \gamma(\alpha(c))$.
2. Goal: $\forall a \in A, \alpha \circ \gamma(a) \sqsubseteq a$.
   Let $a \in A$ and consider $c = \gamma(a) \in C$. Same as above.
3. Let $c, c' \in C$ such that $c \leq c'$. Then $c' \leq \gamma \circ \alpha(c')$. Then, $c \leq \gamma \circ \alpha(c')$. Then, $\alpha(c) \sqsubseteq \alpha(c')$.
4. Same.
5. Let $a \in A$.
   - $\gamma \circ \alpha \circ \gamma(a) \leq \gamma(a)$: $\alpha \circ \gamma$ is reductive and γ is monotonic.
   - $\gamma \circ \alpha \circ \gamma(a) \geq \gamma(a)$: $\gamma \circ \alpha$ is extensive.
6. Same.
7. 8. Using above.

Prop (Galois connection characterization)

If the pair $(\alpha : C \to A, \gamma : A \to C)$ satisfies:

1. α is monotonic
2. γ is monotonic
3. $\gamma \circ \alpha$ is extensive
4. $\alpha \circ \gamma$ is reductive

then (α, γ) is a Galois connection.

Prop (Uniqueness of the adjoint)

Given $(C, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$, each adjoint can be uniquely defined in term of the other:

1. $\alpha(c) = \sqcap \{a \mid c \leq \gamma(a)\}$
2. $\gamma(a) = \vee \{c \mid \alpha(c) \sqsubseteq a\}$

Prop (Properties of Galois connections)

1. $\forall X \subseteq C$, if $\vee X$ exists, then $\alpha(\vee X) = \sqcup \{\alpha(x) \mid x \in X\}$
2. $\forall X \subseteq A$, if $\sqcap X$ exists, then $\gamma(\sqcap X) = \wedge \{\gamma(x) \mid x \in X\}$

Definition (Galois embeddings)

If $(C, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$, the following properties are equivalent:

1. α is surjective
2. γ is injective
3. $\alpha \circ \gamma = \mathrm{id}$

Such (α, γ) is called a *Galois embedding*, which is noted $(C, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightharpoons}} (A, \sqsubseteq)$.

Note: I used a non-standard notation for Galois embeddings. The proper notation would be the arrows of Galois connections with a doubled head for the arrow at the bottom (symbol not available in native Typst AFAIK).

Remark: a Galois connection can always be made into an embedding by quotienting A by the equivalence relation $a \equiv a' \Leftrightarrow \gamma(a) = \gamma(a')$.

Example (Galois embedding)

Using the previous example of Galois connection, but we add an extra element $\perp$: abstract domain of intervals of integers $\mathbb{Z}$ represented as pairs of ordered bounds (a, b) or $\perp$.

We have $(\mathcal{P}(\mathbb{Z}), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightharpoons}} (I', \sqsubseteq)$, using previous example:

- $I' = I \cup \{\perp\}$
- $\forall x, \perp \sqsubseteq x$
- $\gamma(\perp) = \emptyset$
- $\alpha(\emptyset) = \perp$

Definition (Upper closures)

$\rho : X \to X$ is an *upper closure* in the poset $(X, \sqsubseteq)$ if it is:

- **monotonic**: $x \sqsubseteq x' \Rightarrow \rho(x) \sqsubseteq \rho(x')$
- **extensive**: $x \sqsubseteq \rho(x)$
- **idempotent**: $\rho \circ \rho = \rho$

Given $(C, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$, $\gamma \circ \alpha$ is an upper closure on $(C, \leq)$.

Given an upper closure ρ on $(X, \sqsubseteq)$, we have a Galois embedding $(X, \sqsubseteq) \underset{\rho}{\overset{\mathrm{id}}{\leftrightarrows}} (\rho(X), \sqsubseteq)$.

We can rephrase abstract interpretation using upper closures instead of Galois connections, but we lose:

- the notion of **abstract representation**
- the ability to have several distinct abstract representations for a single concrete object.

V. Operator approximations

Definition (Sound abstraction, exact abstraction)

Given a concrete $(C, \leq)$ and an abstract $(A, \sqsubseteq)$ poset and a monotonic concretization $\gamma : A \to C$:

- $a \in A$ is a *sound abstraction* of $c \in C$ if $c \leq \gamma(a)$.
- $g : A \to A$ is a *sound abstraction* of $f : C \to C$ if $\forall a \in A, f \circ \gamma(a) \leq \gamma \circ g(a)$.
- $g : A \to A$ is an *exact abstraction* of $f : C \to C$ if $f \circ \gamma = \gamma \circ g$

Example (Sound abstraction, exact abstraction)

- $[0, 10]$ is a sound abstraction of $\{0, 1, 2, 5\}$ in the integer interval domain
- $\lambda[a, b].[-\infty, +\infty]$ is a sound abstraction of $\lambda X.\{x + 1 \mid x \in X\}$
- $\lambda[a, b].[a + 1, b + 1]$ is an exact abstraction of $\lambda X.\{x + 1 \mid x \in X\}$

Prop (Best abstractions)

- Given $c \in C$, its *best abstraction* is $\alpha(c)$.
- Given $f : C \to C$, its *best abstraction* is $\alpha \circ f \circ \gamma$.

Prop (Composition of sound, best, exact abstractions)

If g and g' soundly abstract respectively f and f':

1. if f is monotonic, then $g \circ g'$ is a sound abstraction of $f \circ f'$.
2. if g and g' are exact abstractions of f and f' then $g \circ g'$ is an exact abstraction.
3. if g and g' are the best abstractions of f and f', then **$g \circ g'$ is not always the best abstraction**.

Proof.

1. $\forall a \in A, f' \circ \gamma(a) \leq \gamma \circ g'(a)$ by soudness of g', then $f \circ f' \circ \gamma(a) \leq f \circ \gamma \circ g'(a)$ by monotonicity of f, then $f \circ f' \circ \gamma(a) \leq \gamma \circ g \circ g'(a)$ by soundess of g, *i.e.* the soudness of $g \circ g'$.

2. $f \circ f' \circ \gamma = f \circ \gamma \circ g'$ because g' exactly abstract f', then $f \circ \gamma \circ g' = \gamma \circ g \circ g'$ because g exactly abstract f, *i.e.* $g \circ g'$ exactly abstract $f \circ f'$.

Example (Best abstractions composition counterexample)

Consider $(\mathcal{P}(\mathbb{Z}), \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (I, \sqsubseteq)$ where I is the set of intervals of integers mentioned before.

The functions
- $g([a, b]) = [a, \min(b, 1)]$
- $g'([a, b]) = [2a, 2b]$

are the best abstractions of
- $f(X) = \{x \in X \mid x \leq 1\}$
- $f'(X) = \{2x \mid x \in X\}$

but $(g \circ g')([0, 1]) = [0, 1]$, whereas $(\alpha \circ f \circ f' \circ \gamma)([0, 1]) = [0, 0]$.

VI. Fixpoint approximations

Theorem (Fixpoint transfer)

If we have:
- a Galois connection $(C, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (A, \sqsubseteq)$ between **CPOs**
- **monotonic** concrete and abstract functions $f : C \to C$, $f^{\#} : A \to A$
- a **commutation condition** $\alpha \circ f = f^{\#} \circ \alpha$
- a **pre-fixpoint** a of f and its abstraction $a^{\#} = \alpha(a)$

Then $\alpha(\mathrm{lfp}_a f) = \mathrm{lfp}_{a^{\#}} f^{\#}$.

Theorem (Fixpoint approximation)

If we have:
- a **complete lattice** $(C, \leq, \vee, \wedge, \bot, \top)$
- a **monotonic** concrete function f
- a **sound abstraction** $f^{\#} : A \to A$ of f
- a **post-fixpoint** $a^{\#}$ of $f^{\#}$

Then $a^{\#}$ is a **sound abstraction of lfp f**: $\mathrm{lfp}\ f \leq \gamma(a^{\#})$.

Please refer to the slides for the proofs.

Remark: other fixpoint transfer / approximation theorems can be constructed.