Order Theory

MPRI 2–6: Abstract Interpretation, application to verification and static analysis

Antoine Miné

Year 2022–2023

Course 1
19 September 2022
Plan

- Partially ordered structures
  - (complete) partial orders
  - (complete) lattices

- Fixpoints

- Abstractions
  - Galois connections, upper closure operators
    (first-class citizens)
  - Concretization-only framework
  - Operator abstraction
  - Fixpoint abstraction
Partial orders
Given a set $X$, a relation $\sqsubseteq \in X \times X$ is a partial order if it is:

1. reflexive: $\forall x \in X$, $x \sqsubseteq x$

2. antisymmetric: $\forall x, y \in X$, $(x \sqsubseteq y) \land (y \sqsubseteq x) \implies x = y$

3. transitive: $\forall x, y, z \in X$, $(x \sqsubseteq y) \land (y \sqsubseteq z) \implies x \sqsubseteq z$

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

If we drop antisymmetry, we have a preorder instead.
Examples: partial orders

Partial orders:

- \((\mathbb{Z}, \leq)\)
  (completely ordered)

- \((\mathcal{P}(X), \subseteq)\)
  (not completely ordered: \(\{1\} \not\subseteq \{2\}, \{2\} \not\subseteq \{1\}\))

- \((S, =)\) is a poset for any \(S\)

- \((\mathbb{Z}^2, \sqsubseteq)\), where \((a, b) \sqsubseteq (a', b') \iff (a \geq a') \land (b \leq b')\)
  (ordering of interval bounds that implies inclusion)
Examples: preorders

Preorders:

- \( (\mathcal{P}(X), \subseteq) \), where \( a \subseteq b \iff |a| \leq |b| \)
  (ordered by cardinal)

- \( (\mathbb{Z}^2, \subseteq) \), where \( (a, b) \subseteq (a', b') \iff \{ x \mid a \leq x \leq b \} \subseteq \{ x \mid a' \leq x \leq b' \} \)
  (inclusion of intervals represented by pairs of bounds)
  not antisymmetric: \([1, 0] \neq [2, 0]\) but \([1, 0] \subseteq [2, 0] \subseteq [1, 0]\)

Equivalence: \( \equiv \)

\[ X \equiv Y \iff (X \subseteq Y) \land (Y \subseteq X) \]

We obtain a partial order by quotienting by \( \equiv \).
Examples of posets (cont.)

- Given by a Hasse diagram, e.g.:

\[
\begin{align*}
g & \sqsubseteq g \\
f & \sqsubseteq f, g \\
e & \sqsubseteq e, g \\
d & \sqsubseteq d, f, g \\
c & \sqsubseteq c, e, f, g \\
b & \sqsubseteq b, c, d, e, f, g \\
a & \sqsubseteq a, b, c, d, e, f, g
\end{align*}
\]
Examples of posets (cont.)

- **Infinite Hasse diagram** for \((\mathbb{N} \cup \{\infty\}, \leq)\):

\[
\begin{array}{c}
\infty \\
\vdots \\
3 \\
2 \\
1 \\
0
\end{array}
\]

\[
\begin{align*}
\infty &\subseteq \infty \\
\cdots \\
1 &\subseteq 1, 2, \ldots, \infty \\
0 &\subseteq 0, 1, 2, \ldots, \infty
\end{align*}
\]
Partial orders

Use of posets (informally)

Posets are a very useful notion to discuss about:

- **logic**: formulas ordered by implication $\Rightarrow$

- **program verification**: program semantics $\sqsubseteq$ specification
  (e.g.: behaviors of program $\subseteq$ accepted behaviors)

- **approximation**: $\sqsubseteq$ is an information order
  ("$a \sqsubseteq b$" means: "$a$ caries more information than $b$")

- **iteration**: fixpoint computation
  (e.g., a computation is directed, with a limit: $X_1 \subseteq X_2 \subseteq \cdots \subseteq X_n$)
(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 $b$, $c \sqsubseteq d$
(Least) Upper bounds

If it exists, the lub of $a$ and $b$ is unique, and denoted as $a \sqcup b$.
(proof: assume that $c$ and $d$ are both lubs of $a$ and $b$; by definition of lubs, $c \sqsubseteq d$ and $d \sqsubseteq c$; by antisymmetry of $\sqsubseteq$, $c = d$)

Generalized to upper bounds of arbitrary (even infinite) sets $\sqcup Y$, $Y \subseteq X$
(well-defined, as $\sqcup$ is commutative and associative).

Similarly, we define greatest lower bounds (glb, meet) $a \sqcap b$, $\sqcap Y$.
($a \sqcap b \sqsubseteq a$) $\land$ ($a \sqcap b \sqsubseteq b$) and $\forall c$, ($c \sqsubseteq a$) $\land$ ($c \sqsubseteq b$) $\implies$ ($c \sqsubseteq a \sqcap b$)

Note: not all posets have lubs, glbs
(e.g.: $a \sqcup b$ not defined on ($\{a, b\}$, =))
A chain in $(X, \sqsubseteq)$ is a chain in $(X, \sqsubseteq)$ if it is totally ordered by $\sqsubseteq$: 

$$\forall x, y \in C, (x \sqsubseteq y) \lor (y \sqsubseteq x).$$

\[ a \sqsubseteq c \sqsubseteq f \sqsubseteq g \]
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 \(\bot\).

Examples, Counter-examples:

- \((\mathbb{N}, \leq)\) 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.
Complete partial order examples

\[ (\mathbb{N}, \leq) \]
non-complete

\[ (\mathbb{N} \cup \{\infty\}, \leq) \]
complete
Lattices
A lattice \((X, \sqsubseteq, \sqcup, \sqcap)\) is a poset with

1. a lub \(a \sqcup b\) for every pair of elements \(a\) and \(b\);
2. a glb \(a \sqcap b\) for every pair of elements \(a\) and \(b\).

Examples:

- integers \((\mathbb{Z}, \leq, \text{max}, \text{min})\)
- integer intervals (next slide)
- divisibility (in two slides)

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

Reference on lattices: Birkhoff \([Birk76]\).
Example: the interval lattice

Integer intervals: \( \{ [a, b] | a, b \in \mathbb{Z}, a \leq b \} \cup \{ \emptyset \}, \subseteq, \cup, \cap \)

where \([a, b] \cup [a', b'] \overset{\text{def}}{=} [\min(a, a'), \max(b, b')]\).
Example: the divisibility lattice

\[
\begin{array}{c}
\text{Divisibility} (\mathbb{N}^*, |, \text{lcm}, \text{gcd}) \text{ where } x \mid y \quad \overset{\text{def}}{\iff} \quad \exists k \in \mathbb{N}, \; kx = y
\end{array}
\]
Let $P \overset{\text{def}}{=} \{ p_1, p_2, \ldots \}$ be the (infinite) set of prime numbers.

We have a correspondence $\iota$ between $\mathbb{N}^*$ and $P \rightarrow \mathbb{N}$:

- $\alpha = \iota(x)$ is the (unique) decomposition of $x$ into prime factors
- $\iota^{-1}(\alpha) \overset{\text{def}}{=} \prod_{a \in P} a^{\alpha(a)} = x$
- $\iota$ is one-to-one on functions $P \rightarrow \mathbb{N}$ with finite support
  $(\alpha(a) = 0$ except for finitely many factors $a)$

We have a correspondence between $(\mathbb{N}^*, |, \text{lcm}, \text{gcd})$ and $(\mathbb{N}, \leq, \text{max}, \text{min})$.

Assume that $\alpha = \iota(x)$ and $\beta = \iota(y)$ are the decompositions of $x$ and $y$, then:

- $\prod_{a \in P} a^{\max(\alpha(a), \beta(a))} = \text{lcm}(\prod_{a \in P} a^{\alpha(a)}, \prod_{a \in P} a^{\beta(a)}) = \text{lcm}(x, y)$
- $\prod_{a \in P} a^{\min(\alpha(a), \beta(a))} = \text{gcd}(\prod_{a \in P} a^{\alpha(a)}, \prod_{a \in P} a^{\beta(a)}) = \text{gcd}(x, y)$
- $(\forall a: \alpha(a) \leq \beta(a)) \iff (\prod_{a \in P} a^{\alpha(a)}) | (\prod_{a \in P} a^{\beta(a)}) \iff x | y$
Complete lattices

A complete lattice \((X, \sqsubseteq, \sqcup, \sqcap, \bot, \top)\) is a poset with

1. a lub \(\sqcup S\) for every set \(S \subseteq X\)
2. a glb \(\sqcap S\) for every set \(S \subseteq X\)
3. a least element \(\bot\)
4. a greatest element \(\top\)

Notes:

- 1 implies 2 as \(\sqcap S = \sqcup \{y \mid \forall x \in S, y \sqsubseteq x\}\) (and 2 implies 1 as well),
- 1 and 2 imply 3 and 4: \(\bot = \sqcup \emptyset = \sqcap X\), \(\top = \sqcap \emptyset = \sqcup X\),
- a complete lattice is also a CPO.
Complete lattice examples

- **real segment** $[0, 1]$: $(\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}, \leq, \max, \min, 0, 1)$

- **powersets** $(\mathcal{P}(S), \subseteq, \cup, \cap, \emptyset, S)$
  (next slide)

- **any finite lattice**
  ($\sqcup Y$ and $\sqcap Y$ for finite $Y \subseteq X$ are always defined)

- **integer intervals** with finite and **infinite** bounds:
  $$(\{ [a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}, a \leq b \} \cup \{\emptyset\}, \subseteq, \sqcup, \cap, \emptyset, [-\infty, +\infty])$$

  with $\sqcup_{i \in I} [a_i, b_i] \overset{\text{def}}{=} [\min_{i \in I} a_i, \max_{i \in I} b_i]$.
  (in two slides)
Example: the powerset complete lattice

\[
(\mathcal{P}(\mathbb{Z}), \subseteq, \cup, \cap, \emptyset, \mathbb{Z})
\]
Example: the intervals complete lattice

The integer intervals with finite and infinite bounds:

\{(a, b) | a \in \mathbb{Z} \cup \{ -\infty \}, b \in \mathbb{Z} \cup \{ +\infty \}, a \leq b \} \cup \{ \emptyset \}, \subseteq, \sqcup, \cap, \emptyset, [-\infty, +\infty]\}
Derivation

Given a (complete) lattice or partial order \((X, \sqsubseteq, \sqcup, \sqcap, \bot, \top)\) we can derive new (complete) lattices or partial orders by:

- **duality**
  \((X, \sqsupseteq, \sqcap, \sqcup, \top, \bot)\)
  - \(\sqsubseteq\) is reversed
  - \(\sqcup\) and \(\sqcap\) are switched
  - \(\bot\) and \(\top\) are switched

- **lifting** (adding a smallest element)
  \((X \cup \{\bot'\}, \sqsubseteq', \sqcup', \sqcap', \bot', \top)\)
  - \(a \sqsubseteq' b \iff a = \bot' \lor a \sqsubseteq b\)
  - \(\bot' \sqcup' a = a \sqcup' \bot' = a\), and \(a \sqcup' b = a \sqcup b\) if \(a, b \neq \bot'\)
  - \(\bot' \sqcap' a = a \sqcap' \bot' = \bot'\), and \(a \sqcap' b = a \sqcap b\) if \(a, b \neq \bot'\)
  - \(\bot'\) replaces \(\bot\)
  - \(\top\) is unchanged
Derivation (cont.)

Given (complete) lattices or partial orders:
\((X_1, \sqsubseteq_1, \sqcup_1, \sqcap_1, \bot_1, \top_1)\) and \((X_2, \sqsubseteq_2, \sqcup_2, \sqcap_2, \bot_2, \top_2)\)

We can combine them by:

- **product**
  \((X_1 \times X_2, \sqsubseteq, \sqcup, \sqcap, \bot, \top)\) where
  - \((x, y) \sqsubseteq (x', y') \iff x \sqsubseteq_1 x' \land y \sqsubseteq_2 y'\)
  - \((x, y) \sqcup (x', y') \overset{\text{def}}{=} (x \sqcup_1 x', y \sqcup_2 y')\)
  - \((x, y) \sqcap (x', y') \overset{\text{def}}{=} (x \sqcap_1 x', y \sqcap_2 y')\)
  - \(\bot \overset{\text{def}}{=} (\bot_1, \bot_2)\)
  - \(\top \overset{\text{def}}{=} (\top_1, \top_2)\)

- **smashed product** (coalescent product, merging \(\bot_1\) and \(\bot_2\))
  \(((X_1 \setminus \{\bot_1\}) \times (X_2 \setminus \{\bot_2\})) \cup \{\bot\}, \sqsubseteq, \sqcup, \sqcap, \bot, \top)\)
  (as \(X_1 \times X_2\), but all elements of the form \((\bot_1, y)\) and \((x, \bot_2)\) are identified to a unique \(\bot\) element)
Lattices

Derivation (cont.)

Given a (complete) lattice or partial order \((X, \sqsubseteq, \sqcup, \sqcap, \bot, \top)\) and a set \(S:\)

- **point-wise lifting** (functions from \(S\) to \(X\))

  \((S \to X, \sqsubseteq', \sqcup', \sqcap', \bot', \top')\) where

  - \(x \sqsubseteq' y \iff \forall s \in S: x(s) \sqsubseteq y(s)\)
  - \(\forall s \in S: (x \sqcup' y)(s) \overset{\text{def}}{=} x(s) \sqcup y(s)\)
  - \(\forall s \in S: (x \sqcap' y)(s) \overset{\text{def}}{=} x(s) \sqcap y(s)\)
  - \(\forall s \in S: \bot'(s) = \bot\)
  - \(\forall s \in S: \top'(s) = \top\)

- **smashed point-wise lifting**

  \(((S \to (X \setminus \{\bot\})) \cup \{\bot'\}, \sqsubseteq', \sqcup', \sqcap', \bot', \top')\)

  as \(S \to X\), but identify to \(\bot'\) any map \(x\) where \(\exists s \in S: x(s) = \bot\)

  (e.g. map each program variable in \(S\) to an interval in \(X\))
A lattice \((X, \subseteq, \cup, \cap)\) is **distributive** if:

- \(a \cup (b \cap c) = (a \cup b) \cap (a \cup c)\) and
- \(a \cap (b \cup c) = (a \cap b) \cup (a \cap c)\)

**Examples, Counter-examples:**

- \((\mathcal{P}(X), \subseteq, \cup, \cap)\) is **distributive**

- **intervals are not distributive**
  - \(([0, 0] \cup [2, 2]) \cap [1, 1] = [0, 2] \cap [1, 1] = [1, 1]\) but
  - \(([0, 0] \cap [1, 1]) \cup ([2, 2] \cap [1, 1]) = \emptyset \cup \emptyset = \emptyset\)

  common cause of precision loss in static analyses:
  merging abstract information early, at control-flow joins
  vs. merging executions paths late, at the end of the program
Given a lattice \((X, \subseteq, \cup, \cap)\) and \(X' \subseteq X\), 
\((X', \subseteq, \cup, \cap)\) is a sublattice of \(X\) if \(X'\) is closed under \(\cup\) and \(\cap\).

Example, Counter-examples:

- if \(Y \subseteq X\), 
  \((\mathcal{P}(Y), \subseteq, \cup, \cap, \emptyset, Y)\) is a sublattice of 
  \((\mathcal{P}(X), \subseteq, \cup, \cap, \emptyset, X)\)

- integer intervals are not a sublattice of 
  \((\mathcal{P}(\mathbb{Z}), \subseteq, \cup, \cap, \emptyset, \mathbb{Z})\)

\([\min(a, a'), \max(b, b')] \neq [a, b] \cup [a', b']\)

...another common cause of precision loss in static analyses:
\(\cup\) cannot represent the exact union, and loses precision.
Functions and Fixpoints
A function $f : (X_1, \sqsubseteq_1, \sqcup_1, \bot_1) \to (X_2, \sqsubseteq_2, \sqcup_2, \bot_2)$ is

- **monotonic** if
  \[
  \forall x, x', \ x \sqsubseteq_1 x' \implies f(x) \sqsubseteq_2 f(x')
  \]
  (aka: increasing, isotone, order-preserving, morphism)

- **strict** if $f(\bot_1) = \bot_2$

- **continuous** between CPO if
  \[
  \forall C \text{ chain } \subseteq X_1, \ \{ f(c) \mid c \in C \} \text{ is a chain in } X_2
  \]
  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 $\forall x, \ x \sqsubseteq_1 f(x)$

- **reductive** if $X_1 = X_2$ and $\forall x, \ f(x) \sqsubseteq_1 x$
Fixpoints

Given \( f : (X, \sqsubseteq) \to (X, \sqsubseteq) \)

- \( x \) 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)

- \( \text{fp}(f) \overset{\text{def}}{=} \{ x \in X \mid f(x) = x \} \)
- \( \text{lfp}_x f \overset{\text{def}}{=} \min \sqsubseteq \{ y \in \text{fp}(f) \mid x \sqsubseteq y \} \) if it exists
  (least fixpoint greater than \( x \))
- \( \text{lfp} f \overset{\text{def}}{=} \text{lfp}_\perp f \)
  (least fixpoint)
- **dually:** \( \text{gfp}_x f \overset{\text{def}}{=} \max \sqsubseteq \{ y \in \text{fp}(f) \mid y \sqsubseteq x \} \), \( \text{gfp} f \overset{\text{def}}{=} \text{gfp}_\top f \)
  (greatest fixpoints)
Fixpoints: illustration
Fixpoints: example

Monotonic function with two distinct fixpoints
Monotonic function with a unique fixpoint
Non-monotonic function with no fixpoint
Uses of fixpoints: examples

Express solutions of mutually recursive equation systems

Example:

The solutions of
\[
\begin{align*}
x_1 &= f(x_1, x_2) \\
x_2 &= g(x_1, x_2)
\end{align*}
\]

with $x_1, x_2$ in lattice $X$

are exactly the fixpoint of $\vec{F}$ in lattice $X \times X$, where

\[
\vec{F} \left( \begin{array}{c} x_1 \\ x_2 \end{array} \right) = \left( \begin{array}{c} f(x_1, x_2) \\ g(x_1, x_2) \end{array} \right)
\]

The least solution of the system is \text{lfp} $\vec{F}$.
Uses of fixpoints: examples

- Close (complete) sets to satisfy a given property

Example:

\[ r \subseteq X \times X \text{ is transitive if:} \]
\[ (a, b) \in r \land (b, c) \in r \implies (a, c) \in r \]

The transitive closure of \( r \) is the smallest transitive relation containing \( r \).

Let \( f(s) = r \cup \{(a, c) \mid (a, b) \in s \land (b, c) \in s\} \), then \( \text{lfp } f \):

- \( \text{lfp } f \) contains \( r \)
- \( \text{lfp } f \) is transitive
- \( \text{lfp } f \) is minimal

\[ \implies \text{lfp } f \text{ is the transitive closure of } r. \]
Tarski’s fixpoint theorem

Tarski’s theorem

If $f : X \rightarrow X$ is monotonic in a complete lattice $X$ then $\text{fp}(f)$ is a complete lattice.

Proved by Knaster and Tarski [Tars55].
Tarski’s fixpoint theorem

**Tarski’s theorem**

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

**Proof:**

We prove \( \text{lfp} \ f = \bigsqcap \{ x \mid f(x) \sqsubseteq x \} \) (meet of post-fixpoints).
Tarski’s fixpoint theorem

**Tarski’s theorem**

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

**Proof:**

We prove \( \text{lfp } f = \bigcap \{ x \mid f(x) \sqsubseteq x \} \) (meet of post-fixpoints).

Let

\[
\begin{align*}
  f^* &= \{ x \mid f(x) \sqsubseteq x \} \quad \text{and} \quad a = \bigcap f^*. \\
  \forall x \in f^*, \ a \sqsubseteq x & \quad \text{(by definition of} \ \bigcap) \\
  \text{so } f(a) \sqsubseteq f(x) & \quad \text{(as } f \text{ is monotonic)} \\
  \text{so } f(a) \sqsubseteq x & \quad \text{(as } x \text{ is a post-fixpoint).} \\
  \text{We deduce that } f(a) \sqsubseteq \bigcap f^* \comma \text{i.e. } f(a) \sqsubseteq a. 
\end{align*}
\]
Tarski’s fixpoint theorem

Tarski’s theorem

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

Proof:
We prove \( \text{lfp} f = \bigsqcap \{ x \mid f(x) \sqsubseteq x \} \) (meet of post-fixpoints).

\[
f(a) \sqsubseteq a
\]
so \( f(f(a)) \sqsubseteq f(a) \) (as \( f \) is monotonic)
so \( f(a) \in f^* \) (by definition of \( f^* \))
so \( a \sqsubseteq f(a) \).

We deduce that \( f(a) = a \), so \( a \in \text{fp}(f) \).

Note that \( y \in \text{fp}(f) \) implies \( y \in f^* \).
As \( a = \bigsqcap f^* \), \( a \sqsubseteq y \), and we deduce \( a = \text{lfp} f \).
Tarski’s fixpoint theorem

Tarski’s theorem

If \( f : X \rightarrow X \) is monotonic in a complete lattice \( X \) then \( \text{fp}(f) \) is a complete lattice.

Proof:

Given \( S \subseteq \text{fp}(f) \), we prove that \( \text{lfp}_\sqcup S \ f \) exists.

Consider \( X' = \{ x \in X \mid \sqcup S \sqsubseteq x \} \).

\( X' \) is a complete lattice.

Moreover \( \forall x' \in X', \ f(x') \in X' \).

\( f \) can be restricted to a monotonic function \( f' \) on \( X' \).

We apply the preceding result, so that \( \text{lfp} f' = \text{lfp}_\sqcup S \ f \) exists.

By definition, \( \text{lfp}_\sqcup S \ f \in \text{fp}(f) \) and is smaller than any fixpoint larger than all \( s \in S \).
Tarski’s fixpoint theorem

Tarski’s theorem

If $f : X \rightarrow X$ is monotonic in a complete lattice $X$ then $\text{fp}(f)$ is a complete lattice.

Proof:
By duality, we construct $\text{gfp} f$ and $\text{gfp}_{\cap} f$.

The complete lattice of fixpoints is:

$$(\text{fp}(f), \sqsubseteq, \lambda S.\text{lfp}_{\cup} S f, \lambda S.\text{gfp}_{\cap} S f, \text{lfp} f, \text{gfp} f).$$

Not necessarily a sublattice of $(X, \sqsubseteq, \sqcup, \sqcap, \bot, \top)$!
Tarski’s fixpoint theorem: example

**Lattice:** \((\{ \text{lfp}, \text{fp}1, \text{fp}2, \text{pre}, \text{gfp} \}, \sqcup, \sqcap, \text{lfp}, \text{gfp})\)

**Fixpoint lattice:** \((\{ \text{lfp}, \text{fp}1, \text{fp}2, \text{gfp} \}, \sqcup', \sqcap', \text{lfp}, \text{gfp})\)

(not a sublattice as \(\text{fp}1 \sqcup' \text{fp}2 = \text{gfp}\) while \(\text{fp}1 \sqcup \text{fp}2 = \text{pre}\,
but \text{gfp} is the smallest fixpoint greater than \text{pre})
“Kleene” fixpoint theorem

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

Inspired by Kleene [Klee52].
"Kleene" fixpoint theorem

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

We prove that \( \{ f^n(a) \mid n \in \mathbb{N} \} \) is a chain and
\[
\text{lfp}_a f = \sqcup \{ f^n(a) \mid n \in \mathbb{N} \}.
\]
“Kleene” fixpoint theorem

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

We prove that \( \{ f^n(a) \mid n \in \mathbb{N} \} \) is a chain and
\[ \text{lfp}_a f = \sqcup \{ f^n(a) \mid n \in \mathbb{N} \}. \]

\( a \sqsubseteq f(a) \) by hypothesis.
\( f(a) \sqsubseteq f(f(a)) \) by monotony of \( f \).
(Note that any continuous function is monotonic.
Indeed, \( x \sqsubseteq y \implies x \sqcup y = y \implies f(x \sqcup y) = f(y) \);
by continuity \( f(x) \sqcup f(y) = f(x \sqcup y) = f(y) \), which implies \( f(x) \sqsubseteq f(y) \).)

By recurrence \( \forall n, f^n(a) \sqsubseteq f^{n+1}(a) \).
Thus, \( \{ f^n(a) \mid n \in \mathbb{N} \} \) is a chain and \( \sqcup \{ f^n(a) \mid n \in \mathbb{N} \} \) exists.
"Kleene" fixpoint theorem

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

\[
f(\bigsqcup \{ f^n(a) \mid n \in \mathbb{N} \}) \\
= \bigsqcup \{ f^{n+1}(a) \mid n \in \mathbb{N} \} \quad \text{(by continuity)} \\
= a \bigsqcup (\bigsqcup \{ f^{n+1}(a) \mid n \in \mathbb{N} \}) \quad \text{(as all } f^{n+1}(a) \text{ are greater than } a) \\
= \bigsqcup \{ f^n(a) \mid n \in \mathbb{N} \}.
\]

So, \( \bigsqcup \{ f^n(a) \mid n \in \mathbb{N} \} \in \text{fp}(f) \)

Moreover, any fixpoint greater than \( a \) must also be greater than all \( f^n(a), \ n \in \mathbb{N} \).

So, \( \bigsqcup \{ f^n(a) \mid n \in \mathbb{N} \} = \text{lfp}_a f \).
Well-ordered sets

\((S, \sqsubseteq)\) 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 \(\bigcap X \in X\)

Consequences:

- any element \(x \in S\) has a successor \(x + 1 \overset{\text{def}}{=} \bigcap \{ y \mid x \sqsubseteq y \}\)
  (except the greatest element, if it exists)
- if \(\forall y, x = y + 1, x\) is a limit and \(x = \bigcup \{ y \mid y \sqsubseteq x \}\)
  (every bounded subset \(X \subseteq S\) has a lub \(\bigcup X = \bigcap \{ y \mid \forall x \in X, x \sqsubseteq y \}\))

Examples:

- \((\mathbb{N}, \leq)\) and \((\mathbb{N} \cup \{\infty\}, \leq)\) are well-ordered
- \((\mathbb{Z}, \leq), (\mathbb{R}, \leq), (\mathbb{R}^+, \leq)\) are not well-ordered
- ordinals \(0, 1, 2, \ldots, \omega, \omega + 1, \ldots\) are well-ordered (\(\omega\) is a limit)
  well-ordered sets are ordinals up to order-isomorphism
  (i.e., bijective functions \(f\) such that \(f\) and \(f^{-1}\) are monotonic)
Constructive Tarski theorem by transfinite iterations

Given a function $f : X \to X$ and $a \in X$, the transfinite iterates of $f$ from $a$ are:

$$
\begin{align*}
    x_0 & \overset{\text{def}}{=} a \\
    x_n & \overset{\text{def}}{=} f(x_{n-1}) & \text{if } n \text{ is a successor ordinal} \\
    x_n & \overset{\text{def}}{=} \bigsqcup \{ x_m \mid m < n \} & \text{if } n \text{ is a limit ordinal}
\end{align*}
$$

Constructive Tarski theorem

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

Generalisation of “Kleene” fixpoint theorem, from [Cous79].
Proof

We prove that $\exists \delta$, $x_\delta = x_{\delta+1}$.

We note that $m \leq n \implies x_m \sqsubseteq x_n$.

Assume by contradiction that $\forall \delta$, $x_\delta = x_{\delta+1}$.

If $n$ is a successor ordinal, then $x_{n-1} \sqsubseteq x_n$.

If $n$ is a limit ordinal, then $\forall m < n$, $x_m \sqsubseteq x_n$.

Thus, all the $x_n$ are distinct.

By choosing $n > |X|$, we arrive at a contradiction.

Thus $\delta$ exists.
Proof

$f$ is monotonic in a CPO $X$,

\[
\begin{align*}
  x_0 & \overset{\text{def}}{=} a \sqsubseteq f(a) \\
  x_n & \overset{\text{def}}{=} f(x_{n-1}) \quad \text{if } n \text{ is a successor ordinal} \\
  x_n & \overset{\text{def}}{=} \sqcup \{ x_m \mid m < n \} \quad \text{if } n \text{ is a limit ordinal}
\end{align*}
\]

Proof:
Given $\delta$ such that $x_{\delta+1} = x_\delta$, we prove that $x_\delta = \text{lfp}_a f$.

$f(x_\delta) = x_{\delta+1} = x_\delta$, so $x_\delta \in \text{fp}(f)$.

Given any $y \in \text{fp}(f)$, $y \sqsupseteq a$, we prove by transfinite induction that

$\forall n, x_n \sqsubseteq y$.

By definition $x_0 = a \sqsubseteq y$.

If $n$ is a successor ordinal, by monotony,

$x_{n-1} \sqsubseteq y \implies f(x_{n-1}) \sqsubseteq f(y)$, i.e., $x_n \sqsubseteq y$.

If $n$ is a limit ordinal, $\forall m < n$, $x_m \sqsubseteq y$ implies

$x_n = \sqcup \{ x_m \mid m < n \} \sqsubseteq y$.

Hence, $x_\delta \sqsubseteq y$ and $x_\delta = \text{lfp}_a f$. 
An **ascending chain** $C$ in $(X, \sqsubseteq)$ is a sequence $c_i \in X$ such that $i \leq j \implies c_i \sqsubseteq c_j$.

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

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

**Examples:**

- the **powerset poset** $(\mathcal{P}(X), \subseteq)$ is ACC when $X$ is finite
- the **pointed integer poset** $(\mathbb{Z} \cup \{\bot\}, \sqsubseteq)$ where $x \sqsubseteq y \iff x = \bot \lor x = y$ is ACC and DCC
- the **divisibility poset** $(\mathbb{N}^*, |)$ is DCC but not ACC.
"Kleene" finite fixpoint theorem

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

Proof:
We prove $\exists n \in \mathbb{N}, \text{lfp}_a f = f^n(a)$.

By monotony of $f$, the sequence $x_n = f^n(a)$ is an increasing chain. By definition of ACC, $\exists n \in \mathbb{N}, x_n = x_{n+1} = f(x_n)$.
Thus, $x_n \in \text{fp}(f)$.

Obviously, $a = x_0 \sqsubseteq f(x_n)$.
Moreover, if $y \in \text{fp}(f)$ and $y \sqsupseteq a$, then $\forall i, y \sqsupseteq f^i(a) = x_i$.
Hence, $y \sqsupseteq x_n$ and $x_n = \text{lfp}_a(f)$. 

## Comparison of fixpoint theorems

<table>
<thead>
<tr>
<th>theorem</th>
<th>function</th>
<th>domain</th>
<th>fixpoint</th>
<th>method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tarski</td>
<td>monotonic</td>
<td>complete lattice</td>
<td>fp(f)</td>
<td>meet of post-fixpoints</td>
</tr>
<tr>
<td>Kleene</td>
<td>continuous</td>
<td>CPO</td>
<td>lfp&lt;sub&gt;α&lt;/sub&gt;(f)</td>
<td>countable iterations</td>
</tr>
<tr>
<td>constructive</td>
<td>monotonic</td>
<td>CPO</td>
<td>lfp&lt;sub&gt;α&lt;/sub&gt;(f)</td>
<td>transfinite iteration</td>
</tr>
<tr>
<td>ACC Kleene</td>
<td>monotonic</td>
<td>poset</td>
<td>lfp&lt;sub&gt;α&lt;/sub&gt;(f)</td>
<td>finite iteration</td>
</tr>
</tbody>
</table>
Galois connections
Galois connections

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

\[
\forall a \in A, \ c \in C, \ \alpha(c) \sqsubseteq a \iff c \leq \gamma(a)
\]

which is noted \((C, \leq) \xleftarrow{\gamma} \xrightarrow{\alpha} (A, \sqsubseteq)\).

- \(\alpha\) is the upper adjoint or abstraction; \(A\) is the abstract domain.
- \(\gamma\) is the lower adjoint or concretization; \(C\) is the concrete domain.
Galois connections

Galois connection example

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

We have: \((\mathcal{P}(\mathbb{Z}), \subseteq) \xleftrightarrow[\gamma]{\alpha} (I, \subseteq)\)

- \(I \overset{\text{def}}{=} (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{+\infty\})\)
- \((a, b) \subseteq (a', b') \iff (a \geq a') \land (b \leq b')\)
- \(\gamma(a, b) \overset{\text{def}}{=} \{ x \in \mathbb{Z} \mid a \leq x \leq b \}\)
- \(\alpha(X) \overset{\text{def}}{=} (\min X, \max X)\)

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

We have: $(\mathcal{P}(\mathbb{Z}), \subseteq) \overset{\gamma}{\leftrightarrow} (I, \sqsubseteq)$

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

proof:

\[
\begin{align*}
\alpha(X) & \subseteq (a, b) \\
& \iff \min X \geq a \land \max X \leq b \\
& \iff \forall x \in X : a \leq x \leq b \\
& \iff \forall x \in X : x \in \{ y | a \leq y \leq b \} \\
& \iff \forall x \in X : x \in \gamma(a, b) \\
& \iff X \subseteq \gamma(a, b)
\end{align*}
\]
Assuming $\forall a, c, \alpha(c) \sqsubseteq a \iff c \leq \gamma(a)$, we have:

1. **$\gamma \circ \alpha$ is extensive:** $\forall c, c \leq \gamma(\alpha(c))$
   
   **proof:** $\alpha(c) \sqsubseteq \alpha(c) \implies c \leq \gamma(\alpha(c))$

2. **$\alpha \circ \gamma$ is reductive:** $\forall a, \alpha(\gamma(a)) \sqsubseteq a$

3. **$\alpha$ is monotonic**
   
   **proof:** $c \leq c' \implies c \leq \gamma(\alpha(c')) \implies \alpha(c) \sqsubseteq \alpha(c')$

4. **$\gamma$ is monotonic**

5. **$\gamma \circ \alpha \circ \gamma = \gamma$**
   
   **proof:** $\alpha(\gamma(a)) \sqsubseteq \alpha(\gamma(a)) \implies \gamma(a) \leq \gamma(\alpha(\gamma(a)))$ and $a \sqsupseteq \alpha(\gamma(a)) \implies \gamma(a) \geq \gamma(\alpha(\gamma(a)))$

6. **$\alpha \circ \gamma \circ \alpha = \alpha$**

7. **$\alpha \circ \gamma$ is idempotent:** $\alpha \circ \gamma \circ \alpha \circ \gamma = \alpha \circ \gamma$

8. **$\gamma \circ \alpha$ is idempotent**
Alternate characterization

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

1. \(\gamma\) is monotonic
2. \(\alpha\) is monotonic
3. \(\gamma \circ \alpha\) is extensive
4. \(\alpha \circ \gamma\) is reductive

then \((\alpha, \gamma)\) is a Galois connection.

(proof left as exercise)
### Uniqueness of the adjoint

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

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

**Proof:** of 1

$\forall a, \ c \leq \gamma(a) \implies \alpha(c) \sqsubseteq a.$

Hence, $\alpha(c)$ is a lower bound of $\{ a \mid c \leq \gamma(a) \}$.

Assume that $a'$ is another lower bound.

Then, $\forall a, \ c \leq \gamma(a) \implies a' \sqsubseteq a$.

By Galois connection, we have then $\forall a, \ \alpha(c) \sqsubseteq a \implies a' \sqsubseteq a$.

This implies $a' \sqsubseteq \alpha(c)$.

Hence, the greatest lower bound of $\{ a \mid c \leq \gamma(a) \}$ exists, and equals $\alpha(c)$.

The proof of 2 is similar (by duality).
Properties of Galois connections (cont.)

If \((\alpha : C \to A, \gamma : A \to C)\), then:

1. \(\forall X \subseteq C, \text{ if } \lor X \text{ exists, then } \alpha(\lor X) = \bigsqcup \{ \alpha(x) \mid x \in X \}\)

2. \(\forall X \subseteq A, \text{ if } \land X \text{ exists, then } \gamma(\land X) = \bigwedge \{ \gamma(x) \mid x \in X \}\)

Proof: of 1

By definition of lubs, \(\forall x \in X, x \leq \lor X\).
By monotony, \(\forall x \in X, \alpha(x) \sqsubseteq \alpha(\lor X)\).
Hence, \(\alpha(\lor X)\) is an upper bound of \(\{ \alpha(x) \mid x \in X \}\).
Assume that \(y\) is another upper bound of \(\{ \alpha(x) \mid x \in X \}\).
Then, \(\forall x \in X, \alpha(x) \sqsubseteq y\).
By Galois connection \(\forall x \in X, x \leq \gamma(y)\).
By definition of lubs, \(\lor X \leq \gamma(y)\).
By Galois connection, \(\alpha(\lor X) \sqsubseteq y\).
Hence, \(\{ \alpha(x) \mid x \in X \}\) has a lub, which equals \(\alpha(\lor X)\).

The proof of 2 is similar (by duality).
Deriving Galois connections

Given \((C, \leq) \xleftarrow{\gamma} (A, \sqsubseteq)\), we have:

- **duality**: \((A, \sqsupseteq) \xleftarrow{\alpha} (C, \geq)\)

\[
(\alpha(c) \sqsubseteq a \iff c \leq \gamma(a) \text{ is exactly } \gamma(a) \geq c \iff a \sqsubseteq \alpha(c))
\]

- **point-wise lifting** by some set \(S\): \((S \rightarrow C, \leq) \xleftarrow{\dot{\gamma}} (S \rightarrow A, \sqsubseteq)\) where

\[
\begin{align*}
&\text{if } f \leq f' \iff \forall s, f(s) \leq f'(s), \quad (\dot{\gamma}(f))(s) = \gamma(f(s)), \\
&\text{if } f \sqsubseteq f' \iff \forall s, f(s) \sqsubseteq f'(s), \quad (\dot{\alpha}(f))(s) = \alpha(f(s)).
\end{align*}
\]

Given \((X_1, \sqsubseteq_1) \xleftarrow{\gamma_1} (X_2, \sqsubseteq_2) \xleftarrow{\gamma_2} (X_3, \sqsubseteq_3)\):

- **composition**: \((X_1, \sqsubseteq_1) \xleftarrow{\gamma_1 \circ \gamma_2} (X_3, \sqsubseteq_3)\)

\[
(\alpha_2 \circ \alpha_1(c) \sqsubseteq_3 a \iff \alpha_1(c) \sqsubseteq_2 \gamma_2(a) \iff c \sqsubseteq_1 (\gamma_1 \circ \gamma_2)(a))
\]
If \((C, \leq) \xleftarrow{\gamma} (A, \sqsubseteq)\), the following properties are equivalent:

1. \(\alpha\) is surjective \((\forall a \in A, \exists c \in C, \alpha(c) = a)\)
2. \(\gamma\) is injective \((\forall a, a' \in A, \gamma(a) = \gamma(a') \implies a = a')\)
3. \(\alpha \circ \gamma = id\) \((\forall a \in A, id(a) = a)\)

Such \((\alpha, \gamma)\) is called a Galois embedding, which is noted \((C, \leq) \xleftarrow{\gamma} (A, \sqsubseteq)\)

Proof:
Galois embeddings

If \((C, \leq) \xleftarrow{\gamma} \xrightarrow{\alpha} (A, \sqsubseteq)\), the following properties are equivalent:

1. \(\alpha\) is surjective
   \((\forall a \in A, \exists c \in C, \alpha(c) = a)\)

2. \(\gamma\) is injective
   \((\forall a, a' \in A, \gamma(a) = \gamma(a') \implies a = a')\)

3. \(\alpha \circ \gamma = id\)
   \((\forall a \in A, id(a) = a)\)

Such \((\alpha, \gamma)\) is called a Galois embedding, which is noted \((C, \leq) \xleftarrow{\gamma} \xrightarrow{\alpha} (A, \sqsubseteq)\)

Proof: \(1 \implies 2\)
Assume that \(\gamma(a) = \gamma(a')\).
By surjectivity, take \(c, c'\) such that \(a = \alpha(c), a' = \alpha(c')\).
Then \(\gamma(\alpha(c)) = \gamma(\alpha(c'))\).
And \(\alpha(\gamma(\alpha(c))) = \alpha(\gamma(\alpha(c'))))\).
As \(\alpha \circ \gamma \circ \alpha = \alpha\), \(\alpha(c) = \alpha(c')\).
Hence \(a = a'\).
Galois connections

Galois embeddings

If \((C, \leq) \xrightarrow{\gamma} (A, \sqsubseteq)\), the following properties are equivalent:

1. \(\alpha\) is surjective \((\forall a \in A, \exists c \in C, \alpha(c) = a)\)
2. \(\gamma\) is injective \((\forall a, a' \in A, \gamma(a) = \gamma(a') \implies a = a')\)
3. \(\alpha \circ \gamma = id\) \((\forall a \in A, id(a) = a)\)

Such \((\alpha, \gamma)\) is called a **Galois embedding**, which is noted \((C, \leq) \xleftarrow{\alpha} \xrightarrow{\gamma} (A, \sqsubseteq)\)

**Proof:** 2 \(\implies\) 3

Given \(a \in A\), we know that \(\gamma(\alpha(\gamma(a))) = \gamma(a)\).

By injectivity of \(\gamma\), \(\alpha(\gamma(a)) = a\).
Galois embeddings

If \((C, \leq) \xrightarrow{\gamma} (A, \sqsubseteq)\), the following properties are equivalent:

- **1.** \(\alpha\) is surjective  
  \[(\forall a \in A, \exists c \in C, \alpha(c) = a)\]

- **2.** \(\gamma\) is injective  
  \[(\forall a, a' \in A, \gamma(a) = \gamma(a') \implies a = a')\]

- **3.** \(\alpha \circ \gamma = id\)
  \[(\forall a \in A, id(a) = a)\]

Such \((\alpha, \gamma)\) is called a **Galois embedding**, which is noted \((C, \leq) \xleftarrow{\gamma} (A, \sqsubseteq)\)

**Proof:** 3 \(\implies\) 1

Given \(a \in A\), we have \(\alpha(\gamma(a)) = a\).

Hence, \(\exists c \in C, \alpha(c) = a\), using \(c = \gamma(a)\).
A Galois connection can be made into an embedding by quotienting $A$ by the equivalence relation $a \equiv a' \iff \gamma(a) = \gamma(a')$. 
Galois embedding example

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

We have: $(\mathcal{P}(\mathbb{Z}), \subseteq) \xrightarrow{\gamma} (I, \sqsubseteq)$

- $I \overset{\text{def}}{=} \{ (a, b) | a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}, a \leq b \} \cup \{\bot\}$
- $(a, b) \sqsubseteq (a', b') \iff (a \geq a') \land (b \leq b'), \forall x: \bot \sqsubseteq x$
- $\gamma(a, b) \overset{\text{def}}{=} \{ x \in \mathbb{Z} | a \leq x \leq b \}$, $\gamma(\bot) = \emptyset$
- $\alpha(X) \overset{\text{def}}{=} (\text{min } X, \text{max } X)$, or $\bot$ if $X = \emptyset$

proof:
Galois connections

Galois embedding example

Abstract domain of *intervals of integers* \( \mathbb{Z} \) represented as *pairs of ordered bounds* \((a, b)\) or \(\perp\).

We have: \((\mathcal{P}(\mathbb{Z}), \subseteq) \xrightarrow{\alpha} (I, \sqsubseteq)\)

- \(I \stackrel{\text{def}}{=} \{(a, b) \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}, a \leq b\} \cup \{\perp\}\)
- \((a, b) \sqsubseteq (a', b') \iff (a \geq a') \land (b \leq b'), \quad \forall x: \perp \sqsubseteq x\)
- \(\gamma(a, b) \stackrel{\text{def}}{=} \{x \in \mathbb{Z} \mid a \leq x \leq b\}, \quad \gamma(\perp) = \emptyset\)
- \(\alpha(X) \stackrel{\text{def}}{=} (\min X, \max X), \text{ or } \perp \text{ if } X = \emptyset\)

Proof:

Quotient of the “pair of bounds” domain \((\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{+\infty\})\) by the relation \((a, b) \equiv (a', b') \iff \gamma(a, b) = \gamma(a', b')\)
i.e., \((a \leq b \land a = a' \land b = b') \lor (a > b \land a' > b')\).
Upper closures

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

1. monotonic: \( x \sqsubseteq x' \implies \rho(x) \sqsubseteq \rho(x') \),
2. extensive: \( x \sqsubseteq \rho(x) \), and
3. idempotent: \( \rho \circ \rho = \rho \).

\[
\begin{align*}
\rho(X) \supseteq \rho(\rho(X)) \\
\rho(\rho(c)) \supseteq \rho(c) \\
\rho(c) \supseteq c \\
\rho(c) \supseteq \rho(\rho(c)) \\
\rho(\rho(c)) \supseteq \rho(\rho(\rho(c)))
\end{align*}
\]
Given \((C, \leq) \xleftarrow{\gamma} \xrightarrow{\alpha} (A, \sqsubseteq)\),
\(\gamma \circ \alpha\) is an upper closure on \((C, \leq)\).

Given an upper closure \(\rho\) on \((X, \sqsubseteq)\), we have a Galois embedding:
\((X, \sqsubseteq) \xleftarrow{id} \xrightarrow{\rho} (\rho(X), \sqsubseteq)\)

\(\implies\) we can rephrase abstract interpretation using upper closures instead of Galois connections, but we lose:

- the notion of abstract representation
  (a data-structure \(A\) representing elements in \(\rho(X)\))

- the ability to have several distinct abstract representations for a single concrete object
  (non-necessarily injective \(\gamma\) versus \(id\))
Operator approximations
Abstractions in the concretization framework

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

\((\gamma(a)\text{ is the “meaning” of } a\text{ in } C; \text{ we use intervals in our examples})\)

- \(a \in A\) is a **sound abstraction** of \(c \in C\) if \(c \leq \gamma(a)\).
  (e.g.: \([0, 10]\) is a sound abstraction of \(\{0, 1, 2, 5\}\) in the integer interval domain)

- \(g : A \rightarrow A\) is a **sound abstraction** of \(f : C \rightarrow C\) if \(\forall a \in A: (f \circ \gamma)(a) \leq (\gamma \circ g)(a)\).
  (e.g.: \(\lambda([a, b].[−\infty, +\infty]\) is a sound abstraction of \(\lambda X.\{x + 1 | x \in X\}\) in the interval domain)

- \(g : A \rightarrow A\) is an **exact abstraction** of \(f : C \rightarrow C\) if \(f \circ \gamma = \gamma \circ g\).
  (e.g.: \(\lambda([a, b].[a + 1, b + 1]\) is an exact abstraction of \(\lambda X.\{x + 1 | x \in X\}\) in the interval domain)
Assume now that \((C, \leq) \leftrightarrow (A, \sqsubseteq)\).

- **sound abstractions**
  - \(c \leq \gamma(a)\) is equivalent to \(\alpha(c) \sqsubseteq a\).
  - \((f \circ \gamma)(a) \leq (\gamma \circ g)(a)\) is equivalent to \((\alpha \circ f \circ \gamma)(a) \sqsubseteq g(a)\).

- Given \(c \in C\), its **best abstraction** is \(\alpha(c)\).
  
  (proof: recall that \(\alpha(c) = \cap \{a \mid c \leq \gamma(a)\}\), so, \(\alpha(c)\) is the smallest sound abstraction of \(c\))
  
  (e.g.: \(\alpha(\{0, 1, 2, 5\}) = [0, 5]\) in the interval domain)

- Given \(f : C \rightarrow C\), its **best abstraction** is \(\alpha \circ f \circ \gamma\)
  
  (proof: \(g\) sound \(\iff\) \(\forall a, (\alpha \circ f \circ \gamma)(a) \sqsubseteq g(a)\), so \(\alpha \circ f \circ \gamma\) is the smallest sound abstraction of \(f\))
  
  (e.g.: \(g([a, b]) = [2a, 2b]\) is the best abstraction in the interval domain of \(f(X) = \{2x \mid x \in X\}\); it is not an exact abstraction as \(\gamma(g([0, 1])) = \{0, 1, 2\} \supseteq \{0, 2\} = f(\gamma([0, 1]))\)
Operator approximations

Composition of sound, best, and exact abstractions

If \( g \) and \( g' \) soundly abstract respectively \( f \) and \( f' \) then:

- if \( f \) is monotonic,
  then \( g \circ g' \) is a sound abstraction of \( f \circ f' \),
  \( \text{(proof: } \forall a, (f \circ f' \circ \gamma)(a) \leq (f \circ \gamma \circ g')(a) \leq (\gamma \circ g \circ g')(a)\text{)} \)

- if \( g, g' \) are exact abstractions of \( f \) and \( f' \),
  then \( g \circ g' \) is an exact abstraction,
  \( \text{(proof: } f \circ f' \circ \gamma = f \circ \gamma \circ g' = \gamma \circ g \circ g'\text{)} \)

- if \( g \) and \( g' \) are the best abstractions of \( f \) and \( f' \),
  then \( g \circ g' \) is not always the best abstraction!
  \( \text{(e.g.: } g([a, b]) = [a, \min(b, 1)] \text{ and } g'([a, b]) = [2a, 2b] \text{ are the best abstractions of } f(X) = \{ x \in X \mid x \leq 1 \} \text{ and } f'(X) = \{ 2x \mid x \in X \} \text{ in the interval domain, but } g \circ g' \text{ is not the best abstraction of } f \circ f' \text{ as } (g \circ g')([0, 1]) = [0, 1] \text{ while } (\alpha \circ f \circ f' \circ \gamma)([0, 1]) = [0, 0]\text{)} \)
Fixpoint approximations
Fixpoint approximations

Fixpoint transfer

If we have:

- a Galois connection \((C, \leq) \xrightleftharpoons{\gamma}_\alpha (A, \sqsubseteq)\) between CPOs
- monotonic concrete and abstract functions \(f : C \to C, \, f^\# : A \to A\)
- a commutation condition \(\alpha \circ f = f^\# \circ \alpha\)
- an element \(a\) and its abstraction \(a^\# = \alpha(a)\)

then \(\alpha(\text{lfp}_a f) = \text{lfp}_{a^\#} f^\#.\)

(proof on next slide)
Proof:

By the constructive Tarski theorem, $\text{lfpa} f$ is the limit of transfinite iterations: $a_0 \overset{\text{def}}{=} a$, $a_{n+1} \overset{\text{def}}{=} f(a_n)$, and $a_n \overset{\text{def}}{=} \bigvee \{ a_m \mid m < n \}$ for limit ordinals $n$.

Likewise, $\text{lfpa}^\# f^\#$ is the limit of a transfinite iteration $a_n^\#$.

We prove by transfinite induction that $a_n^\# = \alpha(a_n)$ for all ordinals $n$:

- $a_0^\# = \alpha(a_0)$, by definition;
- $a_{n+1}^\# = f^\#(a_n^\#) = f^\#(\alpha(a_n)) = \alpha(f(a_n)) = \alpha(a_{n+1})$ for successor ordinals, by commutation;
- $a_n^\# = \bigsqcup \{ a_m^\# \mid m < n \} = \bigsqcup \{ \alpha(a_m) \mid m < n \} = \alpha(\bigvee \{ a_m \mid m < n \}) = \alpha(a_n)$ for limit ordinals, because $\alpha$ is always continuous in Galois connections.

Hence, $\text{lfpa}^\# f^\# = \alpha(\text{lfpa} f)$. 
If we have:

- a complete lattice \((C, \leq, \lor, \land, \bot, \top)\)
- a monotonic concrete function \(f\)
- a sound abstraction \(f^\#: A \rightarrow A\) of \(f\)
  \((\forall x^\#: (f \circ \gamma)(x^\#) \leq (\gamma \circ f^\#)(x^\#))\)
- a post-fixpoint \(a^\#\) of \(f^\#\) \((f^\#(a^\#) \sqsubseteq a^\#)\)

then \(a^\#\) is a sound abstraction of \(\text{lfp } f\): \(\text{lfp } f \leq \gamma(a^\#)\).

Proof:

By definition, \(f^\#(a^\#) \sqsubseteq a^\#\).
By monotony, \(\gamma(f^\#(a^\#)) \leq \gamma(a^\#)\).
By soundness, \(f(\gamma(a^\#)) \leq \gamma(a^\#)\).
By Tarski’s theorem \(\text{lfp } f = \land \{x \mid f(x) \leq x\}\).

Hence, \(\text{lfp } f \leq \gamma(a^\#)\).

Other fixpoint transfer / approximation theorems can be constructed...


