Mathematical Tools

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

Antoine Miné

CNRS, École normale supérieure

course 1, 2012–2013

Order theory

Partial orders

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: $\forall x, y \in X,\ x \sqsubseteq y \wedge y \sqsubseteq x \implies x = y$
3. transitive: $\forall x, y, z \in X,\ x \sqsubseteq y \wedge y \sqsubseteq z \implies x \sqsubseteq z$.

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

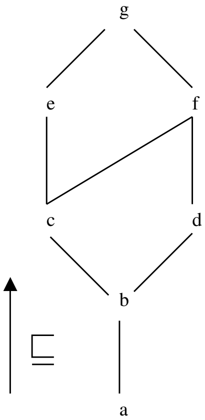
If we drop antisymmetry, we have a preorder instead.

Examples of posets

- $(\mathbb{Z}, \leq)$ is a poset (in fact, completely ordered)
- $(\mathcal{P}(X), \subseteq)$ is a poset (not completely ordered)
- $(S, =)$ is a poset for any S

Examples of posets (cont.)

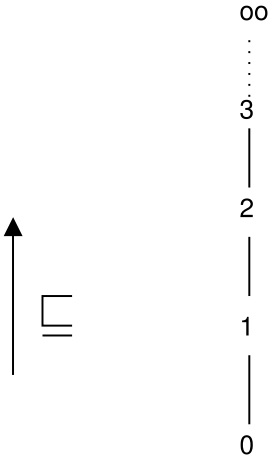
- Given by a Hasse diagram, e.g.:



$$
\begin{aligned}
g &\sqsubseteq g \\
f &\sqsubseteq f, g \\
e &\sqsubseteq e, g \\
d &\sqsubseteq d, f, g \\
c &\sqsubseteq c, e, f, g \\
b &\sqsubseteq b, c, d, e, f, g \\
a &\sqsubseteq a, b, c, d, e, f, g
\end{aligned}
$$

Examples of posets (cont.)

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



$\infty \sqsubseteq \infty$

$\dots$

$1 \sqsubseteq 1, 2, \dots, \infty$

$0 \sqsubseteq 0, 1, 2, \dots, \infty$

Informal uses of posets

Posets are a very useful notion to discuss about:

- logic: ordered by implication $\implies$
- approximations: $\sqsubseteq$ is an information order
- program verification: program semantics $\sqsubseteq$ specification

(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, $c \sqsubseteq d$

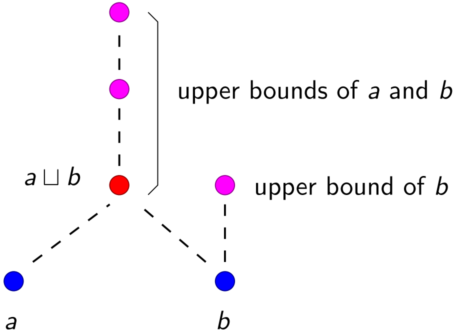
  The lub is unique and noted $a \sqcup b$.
  (proof: assume that c and d are both lubs of a and b; by definition of lubs, $c \sqsubseteq d$ and $d \sqsubseteq c$; by antisymmetry of $\sqsubseteq$, $c = d$)

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) $a \sqcap b$, $\sqcap Y$.
($a \sqcap b \sqsubseteq a, b$ and $\forall c,\ c \sqsubseteq a, b \implies c \sqsubseteq a \sqcap b$)

Note: not all posets have lubs, glbs; e.g., $(\{ a, b \}, =)$.

(Least) Upper bounds



Complete partial order (CPO)

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

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 $\perp$.

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.

Lattices

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.

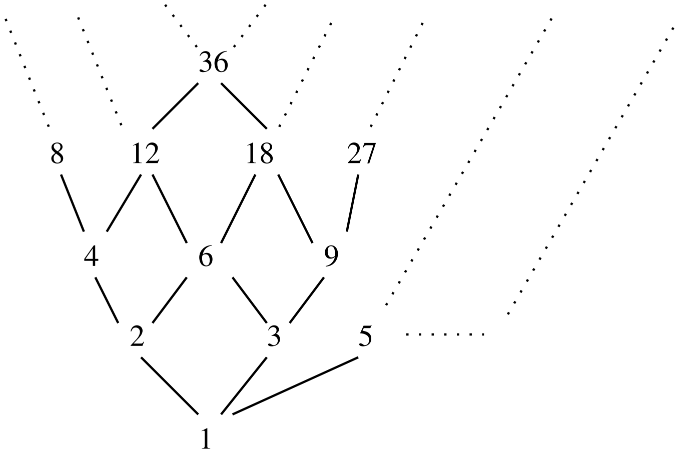
Examples:

- integer intervals $(\{\, [a, b] \mid a, b \in \mathbb{Z},\ a \leq b \,\} \cup \{\, \emptyset \,\}, \subseteq, \sqcup, \cap)$
  where $[a, b] \sqcup [a', b'] \stackrel{\text{def}}{=} [\min(a, a'), \max(b, b')]$.
- divisibility $(\mathbb{N}^*, |, \gcd, \mathrm{lcm})$
  where $x|y \stackrel{\text{def}}{\iff} \exists k \in \mathbb{N},\ kx = y$.

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

See Birkhoff [Birk76].

Example: the divisibility lattice



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:

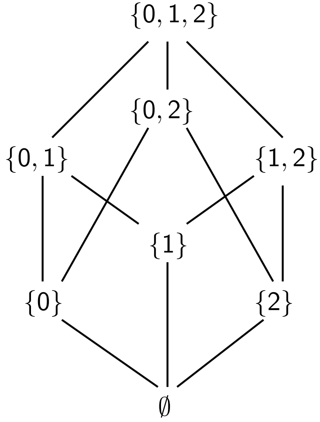
- 1 implies 2 as $\sqcap X = \sqcup \{ y \mid \forall x \in X,\ y \sqsubseteq x \}$ (and 2 implies 1 as well),
- 1 and 2 imply 3 and 4: $\bot = \sqcup \emptyset = \sqcap X$, $\top = \sqcap \emptyset = \sqcup X$,
- a complete lattice is also a CPO.

Complete lattice examples

- real segment $[0,1]$: $(\{\, x \in \mathbb{R} \mid 0 \leq x \leq 1 \,\}, \leq, \max, \min, 0, 1)$
- powersets $(\mathcal{P}(S), \subseteq, \cup, \cap, \emptyset, S)$
- 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 $\sqcup_{i \in I} [a_i, b_i] \stackrel{\text{def}}{=} [\min_{i \in I} a_i,\ \max_{i \in I} b_i]$.

Example: the powerset complete lattice

Example: $(\mathcal{P}(\{0,1,2\}), \subseteq, \cup, \cap, \emptyset, \{0,1,2\})$



Derivation

Given (complete) posets or lattices $(X, \sqsubseteq_X, \ldots)$, $(Y, \sqsubseteq_Y, \ldots)$ we can derive new ones by:

- duality $(X, \sqsupseteq_X, \ldots)$
  $\forall x, x', \ x \sqsupseteq_X x' \iff x' \sqsubseteq_X x$
- adding a least element $\perp$ (lifting)
  $(X \cup \{\perp\}, \sqsubseteq, \ldots)$
  $\forall x, x', \ x \sqsubseteq x' \stackrel{\text{def}}{\iff} x = \perp \vee x \sqsubseteq_X x'$
- product
  $(X \times Y, \sqsubseteq, \ldots)$
  $\forall x, x', y, y', \ (x, y) \sqsubseteq (x', y') \stackrel{\text{def}}{\iff} x \sqsubseteq_X x' \wedge y \sqsubseteq_Y y'$
- point-wise lifting by some set S
  $(S \to X, \sqsubseteq, \ldots)$
  $\forall x, x', \ x \sqsubseteq x' \stackrel{\text{def}}{\iff} \forall s \in S, \ x(s) \sqsubseteq_X x'(s)$
- sublattice
  $(X', \sqsubseteq_X, \sqcup_X, \sqcap_X)$ where $X' \subseteq X$ is closed by $\sqcup_X$ and $\sqcap_X$

Fixpoints

Functions

A function $f : (X, \sqsubseteq_X, \ldots) \to (Y, \sqsubseteq_Y, \ldots)$ is

- monotonic if
  $\forall x, x', \, x \sqsubseteq_X x' \implies f(x) \sqsubseteq_Y f(x')$

  (aka: increasing, isotone, order-preserving, morphism)

- strict if $f(\bot_X) = \bot_Y$

- continuous between CPOs if
  $\forall C$ chain $\subseteq X$, $\{\, f(c) \mid c \in C \,\}$ is a chain in Y
  and $f(\sqcup_X C) = \sqcup_Y \{\, f(c) \mid c \in C \,\}$

- a (complete) $\sqcup-$morphism between (complete) lattices
  if $\forall S \subseteq X$, $f(\sqcup_X S) = \sqcup_Y \{\, f(s) \mid s \in S \,\}$

- extensive if $X = Y$ and $\forall x$, $x \sqsubseteq_X f(x)$

Fixpoints

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

- x is a fixpoint of f if $f(x) = x$

- x is a prefixpoint of f if $x \sqsubseteq f(x)$
- x is a postfixpoint of f if $f(x) \sqsubseteq x$

We may have several (or none) fixpoints

- $\mathrm{fp}(f) \stackrel{\text{def}}{=} \{\, x \in X \mid f(x) = x \,\}$
- $\mathrm{lfp}_x\, f \stackrel{\text{def}}{=} \min_{\sqsubseteq} \{\, y \in \mathrm{fp}(f) \mid x \sqsubseteq y \,\}$ if it exists
  (least fixpoints)
- $\mathrm{lfp}\, f \stackrel{\text{def}}{=} \mathrm{lfp}_{\perp}\, f$
- dually, $\mathrm{gfp}_x\, f$, $\mathrm{gfp}\, f$ (greatest fixpoints)

Tarski's fixpoint theorem

Tarksi's theorem

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

Proved by Knaster and Tarski [Tars55].

Tarski's fixpoint theorem

Tarksi's theorem

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

Proof:

We prove $\mathrm{lfp}\, f = \sqcap \{\, x \mid f(x) \sqsubseteq x \,\}$ (meet of postfixpoints).

Let $f^* = \{\, x \mid f(x) \sqsubseteq x \,\}$ and $a = \sqcap f^*$.
$\forall x \in f^*,\ a \sqsubseteq x$ (by definition of $\sqcap$)
so $f(a) \sqsubseteq f(x)$ (as f is monotonic)
so $f(a) \sqsubseteq x$ (as x is a postfixpoint).

We deduce that $f(a) \sqsubseteq \sqcap f^*$, i.e. $f(a) \sqsubseteq a$.

Tarski's fixpoint theorem

Tarksi's theorem

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

Proof:

We prove $\mathrm{lfp}\, f = \sqcap \{\, x \mid f(x) \sqsubseteq x \,\}$ (meet of postfixpoints).

$f(a) \sqsubseteq a$
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 $f(a) = a$, so $a \in \mathrm{fp}(f)$.

Note that $y \in \mathrm{fp}(f)$ implies $y \in f^*$.
As $a = \sqcap f^*$, $a \sqsubseteq y$, and we deduce $a = \mathrm{lfp}\, f$.

Tarski's fixpoint theorem

Tarksi's theorem

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

Proof:

Given $S \subseteq \mathrm{fp}(f)$, we prove that $\mathrm{lfp}_{\sqcup S}\, f$ 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 $\mathrm{lfp}\, f' = \mathrm{lfp}_{\sqcup S}\, f$ exists.

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

Tarski's fixpoint theorem

Tarksi's theorem

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

<u>Proof:</u>

By duality, we construct $\text{gfp}\, f$ and $\text{gfp}_{\sqcap S}\, f$.

The complete lattice of fixpoints is:
$(\text{fp}(f), \sqsubseteq, \lambda S.\text{lfp}_{\sqcup S}\, f, \lambda S.\text{gfp}_{\sqcap S}\, f, \text{lfp}\, f, \text{gfp}\, f)$.

"Kleene" fixpoint 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.

Inspired by Kleene [Klee52].

"Kleene" fixpoint 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.

Proof:

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

$a \sqsubseteq f(a)$ by hypothesis.
$f(a) \sqsubseteq f(f(a))$ by monotony of f.
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

"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.

Proof:

$f(\sqcup \{\, f^n(a) \mid n \in \mathbb{N} \,\})$
$= \sqcup \{\, f^{n+1}(a) \mid n \in \mathbb{N} \,\})$ (by continuity)
$= a \sqcup (\sqcup \{\, f^{n+1}(a) \mid n \in \mathbb{N} \,\})$ (as all $f^{n+1}(a)$ are greater than a)
$= \sqcup \{\, f^n(a) \mid n \in \mathbb{N} \,\}$.
So, $\sqcup \{\, f^n(a) \mid n \in \mathbb{N} \,\} \in \mathrm{fp}(f)$

Moreover, any fixpoint greater than a must also be greater than all $f^n(a)$, $n \in \mathbb{N}$.
So, $\sqcup \{\, f^n(a) \mid n \in \mathbb{N} \,\} = \mathrm{lfp}_a\, f$.

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 $\sqcap X \in X$

Consequences:

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

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 (ω 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:

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

Constructive Tarski theorem

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

Generalisation of "Kleene" fixpoint theorem, from [Cous79].

Proof

f is monotonic in a complete lattice X,

$$\begin{cases} x_0 \stackrel{\text{def}}{=} a \sqsubseteq f(a) & \\ x_n \stackrel{\text{def}}{=} f(x_{n-1}) & \text{if } n \text{ is a successor ordinal} \\ x_n \stackrel{\text{def}}{=} \sqcup \{ x_m \mid m < n \} & \text{if } n \text{ is a limit ordinal} \end{cases}$$

<u>Proof:</u>

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 $\nexists \delta,\ x_\delta = x_{\delta+1}$.
If n is a successor ordinal, then $x_{n-1} \sqsubset x_n$.
If n is a limit ordinal, then $\forall m < n,\ x_m \sqsubset x_n$.
Thus, all the x_n are distinct.
By choosing $n > |X|$, we arrive at a contradiction.
Thus δ exists.

Proof

f is monotonic in a complete lattice X,

$$\begin{cases} x_0 \stackrel{\text{def}}{=} a \sqsubseteq f(a) & \\ x_n \stackrel{\text{def}}{=} f(x_{n-1}) & \text{if } n \text{ is a successor ordinal} \\ x_n \stackrel{\text{def}}{=} \sqcup \{ x_m \mid m < n \} & \text{if } n \text{ is a limit ordinal} \end{cases}$$

Proof:

Given δ such that $x_{\delta+1} = x_\delta$, we prove that $x_\delta = \mathrm{lfp}_a\, f$.

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

Given any $y \in \mathrm{fp}(f)$, $y \sqsupseteq a$, 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 $x_\delta = \mathrm{lfp}_a\, f$.

Ascending chain condition

An ascending chain C in $(X, \sqsubseteq)$ is a sequence $c_i \in X$ such that $i \leq j \implies c_i \leq c_j$.

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 (and DCC) iff X is finite
- the pointed integer poset $(\mathbb{Z} \cup \{\perp\}, \sqsubseteq)$ where $x \sqsubseteq y \iff x = \perp \vee x = y$ is ACC and DCC
- the divisibility poset $(\mathbb{N}^*, |)$ is DCC but not ACC.

Kleene fixpoints in ACC posets

"Kleene" finite fixpoint theorem

If $f : X \to X$ is monotonic in an AAC 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 AAC, $\exists n \in \mathbb{N},\ x_n = x_{n+1} = f(x_n)$.
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 $x_n = \text{lfp}_a\,(f)$.

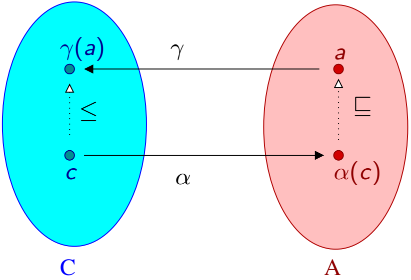
Galois connections

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



- α is the upper adjoint or abstraction; A is the abstract domain.
- γ is the lower adjoint or concretization; C is the concrete domain.

Properties of Galois connections

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. α is monotonic
   proof: $c \leq c' \implies c \leq \gamma(\alpha(c')) \implies \alpha(c) \sqsubseteq \alpha(c')$
4. γ 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 $(\alpha : C \to A, \gamma : A \to C)$ satisfies:

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

then (α, γ) is a Galois connection.

(proof left as exercise)

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

Proof: of 1

$\forall a,\ c \leq \gamma(a) \implies \alpha(c) \sqsubseteq a$.
Hence, $\alpha(c)$ is a lower bound of $\{ a \,|\, c \leq \gamma(a) \}$.

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 $\{ a \,|\, c \leq \gamma(a) \}$ 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. $\forall X \subseteq C$, 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 $\gamma(\sqcap X) = \wedge \{ \gamma(x) \mid x \in X \}$.

Proof: of 1

By definition of lubs, $\forall x \in X$, $x \leq \vee X$.
By monotony, $\forall x \in X$, $\alpha(x) \sqsubseteq \alpha(\vee X)$.
Hence, $\alpha(\vee X)$ 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, $\vee X \leq \gamma(y)$.
By Galois connection, $\alpha(\vee X) \sqsubseteq y$.
Hence, $\{ \alpha(x) \mid x \in X \}$ has a lub, which equals $\alpha(\vee X)$.

The proof of 2 is similar (by duality).

Deriving Galois connections

Given $(C, \leq) \xleftrightarrow[\alpha]{\gamma} (A, \sqsubseteq)$ and $(C', \leq') \xleftrightarrow[\alpha']{\gamma'} (A', \sqsubseteq')$,
we can construct new Galois connections by:

1. duality: $(A, \sqsupseteq) \xleftrightarrow[\gamma]{\alpha} (C, \geq)$
2. composition: $(C, \leq) \xleftrightarrow[\alpha' \circ \alpha]{\gamma \circ \gamma'} (A', \sqsubseteq')$ when $(A, \sqsubseteq) = (C', \leq')$
3. point-wise lifting by some set S:
   $(S \to C, \dot{\leq}) \xleftrightarrow[\dot{\alpha}]{\dot{\gamma}} (S \to A, \dot{\sqsubseteq})$ where
   $$f \dot{\leq} f' \iff \forall s,\ f(s) \leq f'(s), \quad (\dot{\gamma}(f))(s) = \gamma(f(s)),$$
   $$f \dot{\sqsubseteq} f' \iff \forall s,\ f(s) \sqsubseteq f'(s), \quad (\dot{\alpha}(f))(s) = \alpha(f(s)).$$
4. functional lifting of monotonic operators
   $(C \xrightarrow{\leq} C', \dot{\leq}') \xleftrightarrow[\hat{\alpha}]{\hat{\gamma}} (A \xrightarrow{\sqsubseteq} A', \dot{\sqsubseteq}')$
   where $\hat{\gamma}(f) = \gamma' \circ f \circ \alpha$ and $\hat{\alpha}(f) = \alpha' \circ f \circ \gamma$.

Galois embeddings

If $(C, \leq) \xleftrightarrow[\alpha]{\gamma} (A, \sqsubseteq)$, the following properties are equivalent:

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

Such (α, γ) is called a Galois embedding, which is noted
$(C, \leq) \xleftrightarrow[\alpha]{\gamma} (A, \sqsubseteq)$

Proof:

Galois embeddings

If $(C, \leq) \xleftrightarrows[\alpha]{\gamma} (A, \sqsubseteq)$, the following properties are equivalent:

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

Such (α, γ) is called a Galois embedding, which is noted $(C, \leq) \xleftrightarrows[\alpha]{\gamma} (A, \sqsubseteq)$

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 embeddings

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

1. α is surjective $(\forall a \in A, \exists c \in C, \alpha(c) = a)$
2. γ 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 (α, γ) is called a Galois embedding, which is noted
$(C,\leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows\!\!\!\!\!\rightarrow}} (A,\sqsubseteq)$

Proof: $2 \implies 3$

Given $a \in A$, we know that $\gamma(\alpha(\gamma(a))) = \gamma(a)$.
By injectivity of γ, $\alpha(\gamma(a)) = a$.

Galois embeddings

If $(C, \leq) \xleftrightarrow[\alpha]{\gamma} (A, \sqsubseteq)$, the following properties are equivalent:

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

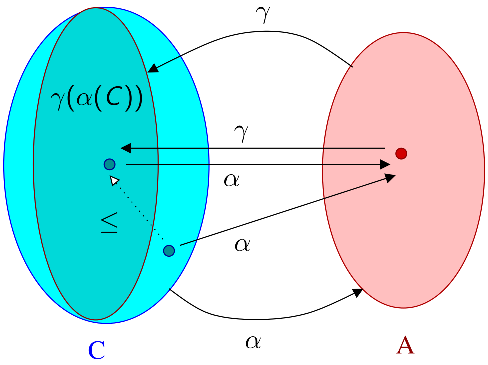
Such (α, γ) is called a Galois embedding, which is noted
$(C, \leq) \xleftrightarrow[\alpha]{\gamma} (A, \sqsubseteq)$

Proof: $3 \implies 1$

Given $a \in A$, we have $\alpha(\gamma(a)) = a$.
Hence, $\exists c \in C$, $\alpha(c) = a$, using $c = \gamma(a)$.

Galois embeddings (cont.)

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

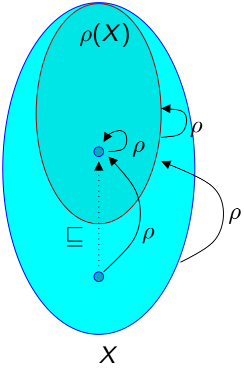


A Galois connection can be made into an embedding by quotienting A by the equivalence relation $a \equiv a' \iff \gamma(a) = \gamma(a')$.

Upper closures

$\rho : X \to X$ 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: $\rho \circ \rho = \rho$.



Upper closures and Galois connections

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:
$(X, \sqsubseteq) \underset{\rho}{\overset{id}{\leftrightarrows}} (\rho(X), \sqsubseteq)$

$\Longrightarrow$ 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 γ versus id)

Sound, best, and exact abstractions

Given $(C, \leq) \xleftarrow[\alpha]{\gamma} \hspace{-1em}\longrightarrow (A, \sqsubseteq)$

- $a \in A$ is a sound abstraction of $c \in C$ if $c \leq \gamma(a)$
  or, equivalently, $\alpha(c) \sqsubseteq a$.
- Given $c \in C$, its best abstraction is $\alpha(c)$.
  (proof: recall that $\alpha(c) = \sqcap \{ a \mid c \leq \gamma(a) \}$)
- $g : A \to A$ is a sound abstraction of $f : C \to C$
  if $\forall a \in A$, $(f \circ \gamma)(a) \leq (\gamma \circ g)(a)$
  or equivalently $\forall a \in A$, $(\alpha \circ f \circ \gamma)(a) \sqsubseteq g(a)$.
- Given $f : C \xrightarrow{\leq} C$, 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)
- $g : A \to A$ is an exact abstraction of $f : C \to C$ if
  $f \circ \gamma = \gamma \circ g$.

Composition of sound, best, and exact abstractions

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

- if f and f' are sound abstractions and f is monotonic, then $g \circ g'$ is a sound abstraction of $f \circ f'$,
  (proof: $\forall a, (f \circ f' \circ \gamma)(a) \leq (f \circ \gamma \circ g')(a) \leq (\gamma \circ g \circ g')(a)$)
- if g, g' are exact abstractions, then $g \circ g'$ is an exact abstraction,
  (proof: $f \circ f' \circ \gamma = f \circ \gamma \circ g' = \gamma \circ g \circ g'$)
- if g and g' are best abstractions, then $g \circ g'$ is not always a best abstraction!
  (we will see examples later)

Note: without α and a Galois connection, we can still define sound and exact abstractions.

Fixpoint abstraction example theorem

If:

- $(C, \leq, \vee, \wedge, \bot, \top)$ is a complete lattice,
- $g : A \to A$ is a sound abstraction of a monotonic $f : C \xrightarrow{\leq} C$,
- and a is a postfixpoint of g $\quad (g(a) \sqsubseteq a)$

then a is a sound abstraction of $\operatorname{lfp} f$.

Proof:

By definition, $g(a) \sqsubseteq a$.
By monotony, $\gamma(g(a)) \leq \gamma(a)$.
By soundness, $f(\gamma(a)) \leq \gamma(a)$.
By Tarski's theorem $\operatorname{lfp} f = \wedge \{ x \mid f(x) \leq x \}$.
Hence, $\operatorname{lfp} f \leq \gamma(a)$.

Notes:

- no α is required here,
- many other fixpoint abstraction theorems exist.

Bibliography

Bibliography

[Birk76] **G. Birkhoff**. *Lattice theory.* In AMS Colloquium Pub. 25, 3rd ed., 1976.

[Cous78] **P. Cousot**. *Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis, analyse sémantique des programmes.* In Thèse És Sc. Math., U. Joseph Fourier, Grenoble, 1978.

[Cous79] **P. Cousot & R. Cousot**. *Constructive versions of Tarski's fixed point theorems.* In Pacific J. of Math., 82(1):43–57, 1979.

[Cous92] **P. Cousot & R. Cousot**. *Abstract interpretation frameworks.* In J. of Logic and Comp., 2(4):511—547, 1992.

[Klee52] **S. C. Kleene**. *Introduction to metamathematics.* In North-Holland Pub. Co., 1952.

[Tars55] **A. Tarski**. *A lattice theoretical fixpoint theorem and its applications.* In Pacific J. of Math., 5:285–310, 1955.