Principles of Abstract Interpretation
MIT press

Ch. **11**, Galois Connections and Abstraction

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-11--Galois-connections-PrAbsInt.pdf

Chapter 11

Ch. **11**, Galois Connections and Abstraction

Galois connections

- Given posets $\langle \mathcal{C}, \sqsubseteq \rangle$ (the *concrete domain*) and $\langle \mathcal{A}, \preccurlyeq \rangle$ (the *abstract domain*), the pair $\langle \alpha, \gamma \rangle$ of functions $\alpha \in \mathcal{C} \rightarrow \mathcal{A}$ (the *lower adjoint* or *abstraction*) and $\gamma \in \mathcal{A} \rightarrow \mathcal{C}$ (the *upper-adjoint* or *concretization*) is a *Galois connection* (GC) if and only if

  $$\forall P \in \mathcal{C} \,.\, \forall \overline{P} \in \mathcal{A} \,.\, \alpha(P) \preccurlyeq \overline{P} \Leftrightarrow P \sqsubseteq \gamma(\overline{P}) \tag{11.1}$$

  which we write

  $$\langle \mathcal{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq \rangle \ .$$

`en.wikipedia.org/wiki/Galois_connection`

Example: homomorphic/partitioning abstraction

- Let C and A be sets, $h \in C \to A$
- $\alpha_h(S) \triangleq \{h(e) \mid e \in S\}$
- $\gamma_h(\overline{S}) \triangleq \{e \in C \mid h(e) \in \overline{S}\}$
- $\langle \wp(C),\ \subseteq \rangle \xleftarrow[\alpha_h]{\gamma_h} \xrightarrow{} \langle \wp(A),\ \subseteq \rangle$

Example: homomorphic/partitioning abstraction

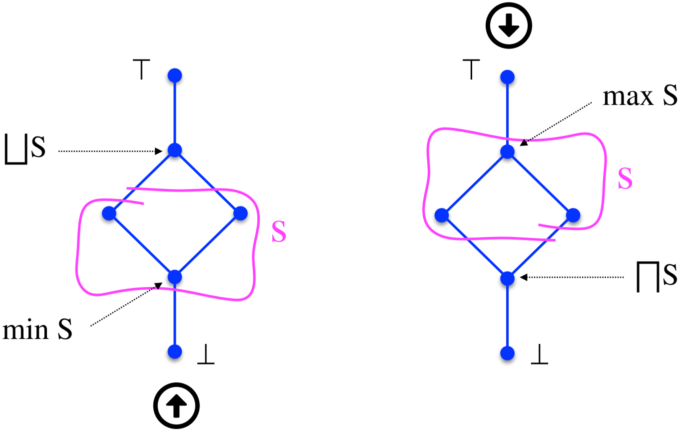
- Let C and A be sets, $h \in C \to A$
- $\alpha_h(S) \triangleq \{h(e) \mid e \in S\}$
- $\gamma_h(\overline{S}) \triangleq \{e \in C \mid h(e) \in \overline{S}\}$
- $\langle \wp(C), \subseteq \rangle \underset{\alpha_h}{\overset{\gamma_h}{\leftrightarrows}} \langle \wp(A), \subseteq \rangle$

Proof

$$\begin{array}{lll} & \alpha_h(S) \subseteq \overline{S} & \\ \Leftrightarrow & \{h(e) \mid e \in S\} \subseteq \overline{S} & \text{(def. } \alpha_h\text{)} \\ \Leftrightarrow & \forall e \in S \,.\, h(e) \in \overline{S} & \text{(def. } \subseteq\text{)} \\ \Leftrightarrow & S \subseteq \{e \in C \mid h(e) \in \overline{S}\} & \text{(def. } \subseteq\text{)} \\ \Leftrightarrow & S \subseteq \gamma_h(\overline{S}) & \text{(def. } \gamma_h\text{)} \quad \square \end{array}$$

Duality in order theory

- The order properties for $\sqsubseteq$, $\bot$, $\top$, $\sqcup$, $\max$, $\sqcap$, $\min$, *etc*. are valid for the dual $\sqsupseteq$, $\top$, $\bot$, $\sqcap$, $\min$, $\sqcup$, $\max$, *etc*.
- Intuition:



Dual of a Galois connection

- The dual of a Galois connection $\langle \mathcal{C}, \sqsubseteq \rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq \rangle$ is the Galois connection $\langle \mathcal{A}, \preccurlyeq \rangle \xrightleftharpoons[\gamma]{\alpha} \langle \mathcal{C}, \sqsubseteq \rangle$

Dual of a Galois connection

- The dual of a Galois connection $\langle \mathcal{C}, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ is the Galois connection $\langle \mathcal{A}, \preccurlyeq\rangle \xleftrightarrow[\gamma]{\alpha} \langle \mathcal{C}, \sqsubseteq\rangle$

Proof $\langle \mathcal{C}, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$

$$\begin{array}{lll}
\Leftrightarrow & \alpha(x) \preccurlyeq y \Leftrightarrow x \sqsubseteq \gamma(y) & \wr\text{def. Galois connection for all } x \in \mathcal{C} \text{ and } y \in \mathcal{A}\wr \\
 & \alpha(x) \succcurlyeq y \Leftrightarrow x \sqsupseteq \gamma(y) & \wr\text{dual statement}\wr \\
\Leftrightarrow & \gamma(y) \sqsubseteq x \Leftrightarrow y \preccurlyeq \alpha(x) & \wr\text{inverse order } x \sqsupseteq y \Leftrightarrow y \sqsubseteq x\wr \\
\Leftrightarrow & \gamma(x) \sqsubseteq y \Leftrightarrow x \preccurlyeq \alpha(y) & \wr\text{dummy variable renaming}\wr \\
\Leftrightarrow & \langle \mathcal{A}, \preccurlyeq\rangle \xleftrightarrow[\gamma]{\alpha} \langle \mathcal{C}, \sqsubseteq\rangle & \wr\text{def. Galois connection}\wr \quad \square
\end{array}$$

Dual of a Galois connection

- The dual of a Galois connection $\langle \mathcal{C},\ \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A},\ \preccurlyeq\rangle$ is the Galois connection $\langle \mathcal{A},\ \preccurlyeq\rangle \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \langle \mathcal{C},\ \sqsubseteq\rangle$

Proof $\langle \mathcal{C},\ \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A},\ \preccurlyeq\rangle$

$$\Leftrightarrow \quad \alpha(x) \preccurlyeq y \Leftrightarrow x \sqsubseteq \gamma(y) \qquad \wr\text{def. Galois connection for all } x \in \mathcal{C} \text{ and } y \in \mathcal{A}\wr$$

$$\alpha(x) \succcurlyeq y \Leftrightarrow x \sqsupseteq \gamma(y) \qquad \wr\text{dual statement}\wr$$

$$\Leftrightarrow \quad \gamma(y) \sqsubseteq x \Leftrightarrow y \preccurlyeq \alpha(x) \qquad \wr\text{inverse order } x \sqsupseteq y \Leftrightarrow y \sqsubseteq x\wr$$

$$\Leftrightarrow \quad \gamma(x) \sqsubseteq y \Leftrightarrow x \preccurlyeq \alpha(y) \qquad \wr\text{dummy variable renaming}\wr$$

$$\Leftrightarrow \quad \langle \mathcal{A},\ \preccurlyeq\rangle \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \langle \mathcal{C},\ \sqsubseteq\rangle \qquad \wr\text{def. Galois connection}\wr \quad \square$$

- Dualization of a statement involving Galois connections consists in exchanging the adjoints
- If an adjoint has a property, its adjoint has the dual property

Example of dualization

Lemma 1 If $\langle \mathcal{C},\ \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{A},\ \preccurlyeq\rangle$ then α is increasing. $\square$

Proof Assume $P \sqsubseteq P'$. By $\alpha(P') \preccurlyeq \alpha(P')$ we have $P' \sqsubseteq \gamma(\alpha(P'))$ so $P \sqsubseteq \gamma(\alpha(P'))$ by transitivity hence $\alpha(P) \preccurlyeq \alpha(P')$ by definition of a GC, proving that α is increasing. $\square$

Lemma 2 If $\langle \mathcal{C},\ \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{A},\ \preccurlyeq\rangle$ then γ is increasing. $\square$

Proof By duality (increasing is self-dual so the dual of "α is increasing" is "γ is increasing"). $\square$

Example of dualization

- In a Galois connection $\langle \mathcal{C}, \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ we have $\alpha \circ \gamma \circ \alpha = \alpha$

Example of dualization

- In a Galois connection $\langle C,\ \sqsubseteq\rangle \mathrel{\underset{\alpha}{\overset{\gamma}{\leftrightarrows}}} \langle \mathcal{A},\ \preccurlyeq\rangle$ we have $\alpha \circ \gamma \circ \alpha = \alpha$

Proof For all $x \in C$ and $y \in \mathcal{A}$,

— $\alpha(x) \preccurlyeq \alpha(x)$ $\wr$reflexivity$\int$

$\Rightarrow$ $x \sqsubseteq \gamma(\alpha(x))$ $\wr$def. GC$\int$

$\Rightarrow$ $\alpha(x) \preccurlyeq \alpha(\gamma(\alpha(x)))$ $\wr\alpha$ increasing$\int$

— $\gamma(y) \sqsubseteq \gamma(y)$ $\wr$reflexivity$\int$

$\Rightarrow$ $\alpha(\gamma(y)) \preccurlyeq y$ $\wr$def. GC$\int$

$\Rightarrow$ $\alpha(\gamma(\alpha(x))) \preccurlyeq \alpha(x)$ $\wr$for $y = \alpha(x)\int$

— $\alpha(x) = \alpha(\gamma(\alpha(x)))$ $\wr$antisymmetry$\int$ $\square$

Example of dualization

- In a Galois connection $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$ we have $\alpha \circ \gamma \circ \alpha = \alpha$

  Proof For all $x \in C$ and $y \in \mathcal{A}$,

  $$— \quad \alpha(x) \preccurlyeq \alpha(x) \qquad \wr\text{reflexivity}\int$$

  $$\Rightarrow \quad x \sqsubseteq \gamma(\alpha(x)) \qquad \wr\text{def. GC}\int$$

  $$\Rightarrow \quad \alpha(x) \preccurlyeq \alpha(\gamma(\alpha(x))) \qquad \wr\alpha\text{ increasing}\int$$

  $$— \quad \gamma(y) \sqsubseteq \gamma(y) \qquad \wr\text{reflexivity}\int$$

  $$\Rightarrow \quad \alpha(\gamma(y)) \preccurlyeq y \qquad \wr\text{def. GC}\int$$

  $$\Rightarrow \quad \alpha(\gamma(\alpha(x))) \preccurlyeq \alpha(x) \qquad \wr\text{for } y = \alpha(x)\int$$

  $$— \quad \alpha(x) = \alpha(\gamma(\alpha(x))) \qquad \wr\text{antisymmetry}\int \quad \square$$

- The dual is $\gamma \circ \alpha \circ \gamma = \gamma$.

Uniqueness of adjoints

- **Lemma 3** In a Galois connection one adjoint uniquely determines the other. $\square$

Uniqueness of adjoints

- **Lemma 3** In a Galois connection one adjoint uniquely determines the other. ☐

  Proof Observe that $\forall P \in C \mathrel{.} \alpha(P) = \sqcap\{\overline{P} \mid \alpha(P) \preccurlyeq \overline{P}\}$
  So, by definition of a GC, $\alpha(P) = \sqcap\{\overline{P} \mid P \sqsubseteq \gamma(\overline{P})\}$ *i.e.* γ uniquely determines α.

  Dually α uniquely determines γ since $\forall \overline{P} \in \mathcal{A} \mathrel{.} \gamma(\overline{P}) = \sqcup\{P \mid \alpha(P) \preccurlyeq \overline{P}\}$. ☐

Uniqueness of adjoints

- **Lemma 3** In a Galois connection one adjoint uniquely determines the other. □

  Proof Observe that $\forall P \in C \,.\, \alpha(P) = \sqcap\{\overline{P} \mid \alpha(P) \preccurlyeq \overline{P}\}$
  So, by definition of a GC, $\alpha(P) = \sqcap\{\overline{P} \mid P \sqsubseteq \gamma(\overline{P})\}$ *i.e.* γ uniquely determines α.

  Dually α uniquely determines γ since $\forall \overline{P} \in \mathcal{A} \,.\, \gamma(\overline{P}) = \sqcup\{P \mid \alpha(P) \preccurlyeq \overline{P}\}$. □

- This lemma is useful in situations where only one adjoint is defined explicitly since then the other is also uniquely determined.
- Note: for given concrete and abstract partial orders

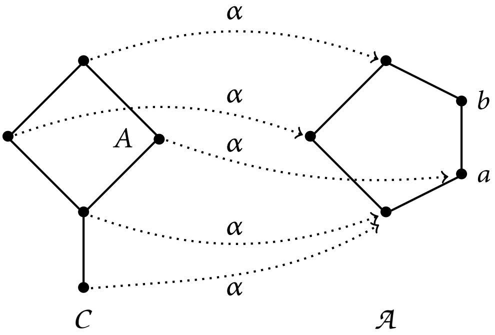
Galois retraction

- If $\langle C, \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma}\!\!\!\!\!\!\!\!\xrightarrow{} \langle \mathcal{A}, \preccurlyeq\rangle$ then
    - α is surjective, if and only if
    - γ is injective, if and only if
    - $\forall \overline{P} \in \mathcal{A} \mathrel{.} \alpha \circ \gamma(\overline{P}) = \overline{P}$.
- This is denoted $\langle C, \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma}\!\!\!\!\!\!\!\!\twoheadrightarrow \langle \mathcal{A}, \preccurlyeq\rangle$ and called a Galois retraction (Galois surjection, insertion, *etc.*).

(see solution to Exercise 11.49 in the book).

Counter-example

Not a retraction



Equivalent definition of Galois connections

- $\langle \mathcal{C}, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\longleftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$ if and only if $\alpha \in \mathcal{C} \to \mathcal{A}$ and $\gamma \in \mathcal{A} \to \mathcal{C}$ satisfy
  (1) α is increasing;
  (2) γ is increasing;
  (3) $\forall x \in \mathcal{C} \,.\, x \sqsubseteq \gamma \circ \alpha(x)$ (*i.e.* $\gamma \circ \alpha$ is extensive)
  (4) $\forall y \in \mathcal{A} \,.\, \alpha \circ \gamma(y) \preccurlyeq y$ (*i.e.* $\alpha \circ \gamma$ is reductive) ☐

α preserves existing lubs (I)

Lemma 4 If $\langle C, \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ then α preserves lubs that may exist in C *i.e.* let $\sqcup$ be the partially defined lub for $\sqsubseteq$ in C and $\curlyvee$ be the partially defined lub for $\preccurlyeq$ in $\mathcal{A}$. Let $S \in \wp(C)$ be any subset of C.

If $\bigsqcup S$ exists in C then the upper bound $\bigcurlyvee\{\alpha(e) \mid e \in S\}$ exists in C and is equal to $\alpha(\bigsqcup S)$. $\square$

α preserves existing lubs (I)

Lemma 4 If $\langle C, \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ then α preserves lubs that may exist in C *i.e.* let $\sqcup$ be the partially defined lub for $\sqsubseteq$ in C and $\curlyvee$ be the partially defined lub for $\preccurlyeq$ in $\mathcal{A}$. Let $S \in \wp(C)$ be any subset of C.

If $\bigsqcup S$ exists in C then the upper bound $\bigcurlyvee\{\alpha(e) \mid e \in S\}$ exists in C and is equal to $\alpha(\bigsqcup S)$. □

Proof ▪ $\alpha(\bigsqcup S)$ is an upper bound of $\alpha(S)$

- By existence and definition of the lub $\bigsqcup S$, we have $\forall e \in S \,.\, e \sqsubseteq \bigsqcup S$
- So $\alpha(e) \preccurlyeq \alpha(\bigsqcup S)$ since α is increasing.
- It follows that $\alpha(\bigsqcup S)$ is an upper bound of $\alpha(S) \triangleq \{\alpha(e) \mid e \in S\}$. □

…/…

α preserves existing lubs (II)

- $\alpha(\bigsqcup S)$ is the *least* upper bound of $\alpha(S)$
  - Let u be any upper bound of this set $\{\alpha(e) \mid e \in S\}$
  - $\forall e \in S \,.\, \alpha(e) \preccurlyeq u$ by def. upper bound.
  - By definition of a GC, $\forall e \in S \,.\, e \sqsubseteq \gamma(u)$.
  - So $\gamma(u)$ is an upper bound of S.
  - By existence and definition of the lub $\bigsqcup S$, $\bigsqcup S \sqsubseteq \gamma(u)$
  - By definition of a GC, $\alpha(\bigsqcup S) \preccurlyeq u$
  - This implies that $\alpha(\bigsqcup S)$, which exists since α is a total function, is the lub of $\alpha(S) \triangleq \{\alpha(e) \mid e \in S\}$ denoted $\curlyvee \alpha(S)$. □

By duality γ preserves existing meets

Abstraction of complete lattices

- If $\langle C, \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma} \hspace{-1em}\xrightarrow{} \langle \mathcal{A}, \preccurlyeq\rangle$ and $\langle C, \sqsubseteq, \sqcup\rangle$ is a complete lattice then $\langle \alpha(C), \preccurlyeq, \curlyvee\rangle$ is a complete lattice.

Abstraction of complete lattices

- If $\langle C, \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ and $\langle C, \sqsubseteq, \sqcup\rangle$ is a complete lattice then $\langle \alpha(C), \preccurlyeq, \curlyvee\rangle$ is a complete lattice.

Proof We have $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \alpha(C), \preccurlyeq\rangle$. Define $\curlyvee(S) \triangleq \alpha(\bigsqcup(\gamma(S)))$.

(1) $\curlyvee$ is an upper bound. If $e \in S \subseteq \alpha(C)$ then

$$\Rightarrow \gamma(e) \in \gamma(S) \qquad \text{≀since } e \in S\text{≀}$$

$$\Rightarrow \gamma(e) \sqsubseteq \bigsqcup \gamma(S) \qquad \text{≀def. lub in complete lattice } \langle C, \sqsubseteq, \sqcup\rangle\text{≀}$$

$$\Rightarrow e = \alpha(\gamma(e)) \preccurlyeq \alpha(\bigsqcup \gamma(S)) = \bigvee S \qquad \text{≀}\alpha \circ \gamma = \mathbb{1},\ \alpha \text{ increasing, def. } \curlyvee\text{≀}$$

Abstraction of complete lattices

- If $\langle C, \sqsubseteq\rangle \mathrel{\underset{\alpha}{\overset{\gamma}{\leftrightarrows}}} \langle \mathcal{A}, \preccurlyeq\rangle$ and $\langle C, \sqsubseteq, \sqcup\rangle$ is a complete lattice then $\langle \alpha(C), \preccurlyeq, \curlyvee\rangle$ is a complete lattice.

Proof We have $\langle C, \sqsubseteq\rangle \mathrel{\underset{\alpha}{\overset{\gamma}{\begin{smallmatrix}\longleftarrow\\ \twoheadrightarrow\end{smallmatrix}}}} \langle \alpha(C), \preccurlyeq\rangle$. Define $\curlyvee(S) \triangleq \alpha(\bigsqcup(\gamma(S)))$.

(1) $\curlyvee$ is an upper bound. If $e \in S \subseteq \alpha(C)$ then

$$\Rightarrow \gamma(e) \in \gamma(S) \qquad \wr\text{since } e \in S\int$$

$$\Rightarrow \gamma(e) \sqsubseteq \bigsqcup \gamma(S) \qquad \wr\text{def. lub in complete lattice } \langle C, \sqsubseteq, \sqcup\rangle\int$$

$$\Rightarrow e = \alpha(\gamma(e)) \preccurlyeq \alpha(\bigsqcup \gamma(S)) = \curlyvee S \qquad \wr\alpha \circ \gamma = \mathbb{1},\ \alpha \text{ increasing, def. } \curlyvee\int$$

(2) $\curlyvee$ is the lub. Assume $\forall e \in S \,.\, e \preccurlyeq u$ (u is an upper bound).

$$\Rightarrow \forall e \in S \,.\, \gamma(e) \sqsubseteq \gamma(u) \qquad \wr\gamma \text{ increasing}\int$$

$$\Rightarrow \bigsqcup \gamma(S) = \bigsqcup_{e \in S} \gamma(e) \sqsubseteq \gamma(u) \qquad \wr\text{def. lub in complete lattice } \langle C, \sqsubseteq, \sqcup\rangle\int$$

$$\Rightarrow \curlyvee S = \alpha(\bigsqcup \gamma(S)) \preccurlyeq u \qquad \wr\text{def. } \curlyvee\text{, Galois connection}\int \quad \Box$$

lub-preserving α

Lemma 5 If α preserves existing lubs and $\gamma(y) \triangleq \bigsqcup\{x \in C \mid \alpha(x) \preccurlyeq y\}$ is well-defined then $\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$. □

lub-preserving α

Lemma 5 If α preserves existing lubs and $\gamma(y) \triangleq \bigsqcup\{x \in C \mid \alpha(x) \preccurlyeq y\}$ is well-defined then $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$. □

Proof $x \sqsubseteq \gamma(y)$

$\Rightarrow\ x \sqsubseteq \bigsqcup\{x' \in C \mid \alpha(x') \preccurlyeq y\}$ $\qquad$ ⟅def. γ⟆

$\Rightarrow\ \alpha(x) \preccurlyeq \alpha(\bigsqcup\{x' \in C \mid \alpha(x') \preccurlyeq y\})$ $\qquad$ ⟅α preserves existing lubs so is increasing⟆

$\Rightarrow\ \alpha(x) \preccurlyeq \bigvee\{\alpha(x') \mid x' \in C \wedge \alpha(x') \preccurlyeq y\})$ $\qquad$ ⟅α preserves existing lubs⟆

$\Rightarrow\ \alpha(x) \preccurlyeq y$

⟅since y is an upper bound of $\{\alpha(x') \mid \alpha(x') \preccurlyeq y\}$ greater than or equal to the lub $\bigvee\{\alpha(x') \mid \alpha(x') \preccurlyeq y\}$⟆

$\Rightarrow\ x \preccurlyeq \bigsqcup\{x' \in C \mid \alpha(x') \preccurlyeq y\}$ $\qquad$ ⟅since $x \in \{x' \in C \mid \alpha(x') \preccurlyeq y\}$⟆

$\Rightarrow\ x \preccurlyeq \gamma(y)$ $\qquad$ ⟅def. γ⟆ □

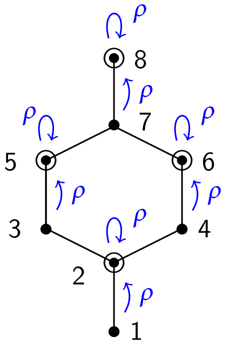
Closure operators

Definition of a closure operator

- Let $\langle \mathcal{P}, \sqsubseteq \rangle$ be a poset. By def., $\rho \in \mathcal{P} \rightarrow \mathcal{P}$ is an upper closure operator if and only if
    - ρ is increasing $(\forall x, y \in \mathcal{P} \,.\, x \sqsubseteq y \Rightarrow \rho(x) \sqsubseteq \rho(y))$
    - ρ is idempotent $(\rho \circ \rho = \rho)$
    - ρ is extensive $(\forall x \in \mathcal{P} \,.\, x \sqsubseteq \rho(x))$

Definition of a closure operator

- Let $\langle \mathcal{P}, \sqsubseteq \rangle$ be a poset. By def., $\rho \in \mathcal{P} \rightarrow \mathcal{P}$ is an upper closure operator if and only if
    - ρ is increasing $(\forall x, y \in \mathcal{P} \,.\, x \sqsubseteq y \Rightarrow \rho(x) \sqsubseteq \rho(y))$
    - ρ is idempotent $(\rho \circ \rho = \rho)$
    - ρ is extensive $(\forall x \in \mathcal{P} \,.\, x \sqsubseteq \rho(x))$



Examples of closure operators

- Example: reflexive transitive closure r^* of a relation $r \in \wp(S \times S)$
- Counter-example: transitive closure r^+ of a non-reflexive relation $r \in \wp(S \times S)$, not extensive, not idempotent

- The dual is a lower closure operator (increasing, idempotent, and reductive $\forall x \in \mathcal{P} \,.\, \rho(x) \sqsubseteq x$)

Galois connection and closure operators (I)

$\langle \mathcal{C}, \sqsubseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preceq \rangle$ is a Galois connection then $\gamma \circ \alpha$ is an upper closure operator (so, by duality, $\alpha \circ \gamma$ is a lower closure operator)

- α and γ so their composition $\gamma \circ \alpha$ are increasing
- $\gamma \circ \alpha$ is extensive
- $\gamma \circ \alpha \circ \gamma \circ \alpha = \gamma \circ \alpha$ proving idempotence

Galois connection and closure operators (II, Exercise 11.50)

If $\langle \mathcal{P},\ \sqsubseteq \rangle$ is a poset, $\rho \in \mathcal{P} \to \mathcal{P}$ is an upper closure operator then $\langle \mathcal{P},\ \sqsubseteq \rangle \xrightleftharpoons[\rho]{\mathbb{1}} \langle \rho(\mathcal{P}),\ \sqsubseteq \rangle$.

Galois connection and closure operators (II, Exercise 11.50)

If $\langle \mathcal{P}, \sqsubseteq \rangle$ is a poset, $\rho \in \mathcal{P} \to \mathcal{P}$ is an upper closure operator then $\langle \mathcal{P}, \sqsubseteq \rangle \underset{\rho}{\overset{\mathbb{1}}{\leftrightarrows}} \langle \rho(\mathcal{P}), \sqsubseteq \rangle$.

Proof For any $x \in \mathcal{P}$, $\overline{y} \in \rho(\mathcal{P})$,

$$
\begin{array}{ll}
 & \rho(x) \sqsubseteq \overline{y} \\
\Leftrightarrow & \rho(x) \sqsubseteq \rho(y) \qquad \langle \overline{y} \in \rho(\mathcal{P}) \text{ so } \overline{y} = \rho(y) \text{ for some } y \in \mathcal{P} \rangle \\
\Leftrightarrow & x \sqsubseteq \rho(y) \\
 & \qquad \langle (\Rightarrow) \quad x \sqsubseteq \rho(x) \text{ and transitivity} \\
 & \qquad\ \ (\Leftarrow)\ \rho(x) \sqsubseteq \rho(\rho(y)) = \rho(y),\ \rho \text{ increasing and idempotent} \rangle \\
\Leftrightarrow & x \sqsubseteq \overline{y} \qquad \langle \overline{y} = \rho(y) \rangle \\
\Leftrightarrow & x \sqsubseteq \mathbb{1}(\overline{y}) \qquad \langle \text{def. identity } \mathbb{1} \rangle
\end{array}
$$

$\rho \in \mathcal{P} \to \rho(\mathcal{P})$ obviously surjective. □

Using closure operator instead of Galois connections

- So the image of a complete lattice by a closure operator is a complete lattice

- $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preceq\rangle$ implies $\langle C, \sqsubseteq\rangle \underset{\gamma\circ\alpha}{\overset{\mathbb{1}}{\leftrightarrows}} \langle \gamma\circ\alpha(C), \sqsubseteq\rangle$ so we can reason only in the concrete using the closed concrete properties $\gamma\circ\alpha(C)$ for abstraction

- The encoding of abstract properties in the abstract domain $\langle \mathcal{A}, \preceq\rangle$ is lost!

Abstraction

Sound abstraction

- Assume $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$
- We say that $\overline{P} \in \mathcal{A}$ is a *sound abstraction* of $P \in C$ if and only if

$$P \sqsubseteq \gamma(\overline{P})$$

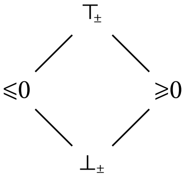
or equivalently

$$\alpha(P) \preccurlyeq \overline{P}$$

- Example, sign: $\{0\} \subseteq \gamma_{\pm}(=0) \subseteq \gamma_{\pm}(\geqslant 0) \subseteq \gamma_{\pm}(\top_{\pm})$. >0 is not a sound abstraction of $\{0\}$.
- Since $\langle C, \sqsubseteq\rangle \underset{\rho}{\overset{\mathbb{1}}{\leftrightarrows}} \langle \rho(C), \sqsubseteq\rangle$ with $\rho = \gamma \circ \alpha$, $P \in C$ is over-approximated by any $\rho(\overline{P})$ such that $P \sqsubseteq \rho(\overline{P})$ (*i.e.* over-approximations are restricted to the abstract domain $\rho(C)$)

Examples of sound abstractions

$\langle \overline{\mathbb{P}^{\pm}}, \sqsubseteq^{\pm} \rangle =$



$$\begin{array}{rcl}
\gamma_{\pm}(\bot_{\pm}) & \triangleq & \varnothing \\
\gamma_{\pm}(\leqslant 0) & \triangleq & \{z \mid z \leqslant 0\} \\
\gamma_{\pm}(\geqslant 0) & \triangleq & \{z \mid z \geqslant 0\} \\
\gamma_{\pm}(\top_{\pm}) & \triangleq & \mathbb{Z}
\end{array}$$

property	sound abstractions
$\{1, 42\}$	$\geqslant 0$ and $\top_{\pm}$
$\{0\}$	$\leqslant 0$, $\geqslant 0$, and $\top_{\pm}$

Better abstraction

- Assume $\langle C,\ \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A},\ \preccurlyeq\rangle$
- Let $\overline{P}_1, \overline{P}_2 \in \mathcal{A}$ be sound abstractions of the concrete property $P \in C$.
- We say that $\overline{P}_1$ is better/more precise/stronger/less abstract than $\overline{P}_2$ if and only if $\overline{P}_1 \preccurlyeq \overline{P}_2$.

Best abstraction

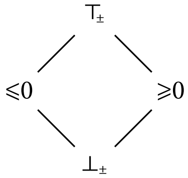
- Assume $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$
- Then $\alpha(P)$ is the best/most precise/strongest/least abstract property which is a sound abstraction of the concrete property P.

Proof

- $\alpha(P)$ is a sound abstraction of P since $P \sqsubseteq \gamma(\alpha(P))$.
- $\alpha(P)$ is the least sound abstraction of P since $\alpha(P) = \bigsqcap\{\overline{P} \mid P \sqsubseteq \gamma(\overline{P})\}$. $\square$

Examples of best abstractions

$\langle \overline{\mathbb{P}^{\pm}}, \sqsubseteq^{\pm} \rangle =$



$$
\begin{array}{rcl}
\gamma_{\pm}(\bot_{\pm}) & \triangleq & \emptyset \\
\gamma_{\pm}(\leqslant 0) & \triangleq & \{z \mid z \leqslant 0\} \\
\gamma_{\pm}(\geqslant 0) & \triangleq & \{z \mid z \geqslant 0\} \\
\gamma_{\pm}(\top_{\pm}) & \triangleq & \mathbb{Z}
\end{array}
$$

property	sound abstractions	best abstraction
$\{1, 42\}$	$\geqslant 0$ and $\top_{\pm}$	$\geqslant 0$
$\{0\}$	$\leqslant 0$, $\geqslant 0$, and $\top_{\pm}$	none

- There is no Galois connection between $\langle \wp(\mathbb{Z}), \subseteq \rangle$ and $\langle \overline{\mathbb{P}^{\pm}}, \sqsubseteq^{\pm} \rangle$.

Combination of Galois connections

Composition of Galois connections

- The composition of Galois connections $\langle \mathcal{P}_1,\ \sqsubseteq\rangle \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \langle \mathcal{P}_2,\ \preccurlyeq\rangle$ and $\langle \mathcal{P}_2,\ \preccurlyeq\rangle \underset{\alpha^2}{\overset{\gamma^2}{\leftrightarrows}} \langle \mathcal{P}_3,\ \trianglelefteq\rangle$ is the Galois connection $\langle \mathcal{P}_1,\ \sqsubseteq\rangle \underset{\alpha^2 \circ \alpha_1}{\overset{\gamma_1 \circ \gamma^2}{\leftrightarrows}} \langle \mathcal{P}_3,\ \trianglelefteq\rangle$.

Galois connections pairs

- Let $\langle C_1,\ \sqsubseteq_1\rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle \mathcal{A}_1,\ \preccurlyeq_1\rangle$ and $\langle C_2,\ \sqsubseteq_2\rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle \mathcal{A}_2,\ \preccurlyeq_2\rangle$;
- $\langle C_1 \times C_2,\ \dot{\sqsubseteq}\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}_1 \times \mathcal{A}_2,\ \dot{\preccurlyeq}\rangle$, where
- $\alpha(\langle x,\ y\rangle) = \langle \alpha_1(x),\ \alpha_2(y)\rangle$,
- $\gamma(\langle \overline{x},\ \overline{y}\rangle) = \langle \gamma_1(\overline{x}),\ \gamma_2(\overline{y})\rangle$, and
- $\dot{\sqsubseteq}$ and $\dot{\preccurlyeq}$ are componentwise.

Higher-order Galois connections

- Let $\langle C_1,\ \sqsubseteq_1\rangle \mathrel{\underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}}} \langle \mathcal{A}_1,\ \preccurlyeq_1\rangle$ and $\langle C_2,\ \sqsubseteq_2\rangle \mathrel{\underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}}} \langle \mathcal{A}_2,\ \preccurlyeq_2\rangle$;
- $\langle C_1 \xrightarrow{\nearrow} C_2,\ \dot{\sqsubseteq}_2\rangle \mathrel{\underset{\alpha}{\overset{\gamma}{\leftrightarrows}}} \langle \mathcal{A}_1 \xrightarrow{\nearrow} \mathcal{A}_2,\ \dot{\preccurlyeq}_2\rangle$, where
- $\alpha = f \mapsto \alpha_2 \circ f \circ \gamma_1$, and
- $\gamma = \overline{f} \mapsto \gamma_2 \circ \overline{f} \circ \alpha_1$.

$$\begin{tikzcd}
\mathcal{A}_1 \arrow[r, "\overline{f}"] \arrow[d, bend right, "\gamma_1"'] & \mathcal{A}_2 \arrow[d, bend right, "\gamma_2"'] \\
C_1 \arrow[r, "f"] \arrow[u, bend right, "\alpha_1"'] & C_2 \arrow[u, bend right, "\alpha_2"']
\end{tikzcd}$$

Conclusion on abstraction by Galois connections

- We can represent abstract program properties by posets and establish the correspondence with the concrete properties using a Galois connection.
- The concrete order structure is preserved in the abstract and inversely.
- Otherwise stated concrete and abstract implications coincide up to the Galois connection.
- So proofs in the abstract domain $\langle \mathcal{A}, \preccurlyeq \rangle$ using the abstract implication/order $\preccurlyeq$ is valid in the concrete $\langle \mathcal{C}, \sqsubseteq \rangle$ for $\sqsubseteq$, up to this GC.

Logical relation, and Tensor products

Logical relation (Definition 11.78)

A relation $\Vdash\, \in \wp(\mathcal{C} \times \mathcal{A})$ between complete lattices $\langle \mathcal{C}, \sqsubseteq, \bigsqcup \rangle$ and $\langle \mathcal{A}, \preccurlyeq, \curlywedge \rangle$ is a *logical relation* if and only if

(1) $(P \sqsubseteq P' \wedge P' \Vdash \overline{P}' \wedge \overline{P}' \preccurlyeq \overline{P}) \Rightarrow (P \Vdash \overline{P})$;

(2) $(\forall i \in \Delta \,.\, P_i \Vdash \overline{P}) \Rightarrow \bigsqcup\limits_{i \in \Delta} P_i \Vdash \overline{P}$;

(3) $(\forall i \in \Delta \,.\, P \Vdash \overline{P}_i) \Rightarrow P \Vdash \bigcurlywedge\limits_{i \in \Delta} \overline{P}_i$.

en.wikipedia.org/wiki/Logical_relations

Tensor product (Definition 11.79)

- The *tensor product* $\langle \mathcal{C}, \sqsubseteq\rangle \otimes \langle \mathcal{A}, \preccurlyeq\rangle$ of two complete lattices $\langle \mathcal{C}, \sqsubseteq\rangle$ and $\langle \mathcal{A}, \preccurlyeq\rangle$ is
$$\langle \mathcal{C}, \sqsubseteq\rangle \otimes \langle \mathcal{A}, \preccurlyeq\rangle \triangleq \{\Vdash\, \in \wp(\mathcal{C} \times \mathcal{A}) \mid\, \Vdash \text{ is a logical relation}\}$$

Soundness relation

- Let $\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$
- The relation

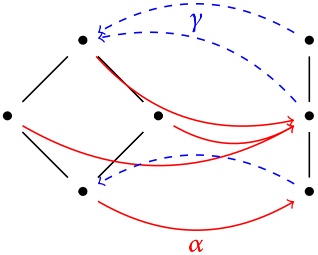
$$P \Vdash \overline{P} \triangleq P \sqsubseteq \gamma(\overline{P}) = \alpha(P) \preccurlyeq \overline{P}$$

is a logical relation called the *soundness relation*.

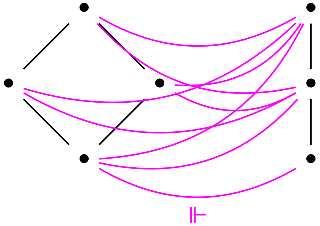
Mathematical equivalence of Galois connections and logical relations

- Let $\langle \mathcal{C}, \sqsubseteq \rangle$ and $\langle \mathcal{A}, \preccurlyeq \rangle$ be complete lattices.
- $\langle \mathcal{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq \rangle$ if and only if $\Vdash \in \langle \mathcal{C}, \sqsubseteq \rangle \otimes \langle \mathcal{A}, \preccurlyeq \rangle$.

Example



Galois connection



Logical soundness relation

$$
\begin{aligned}
P \Vdash \overline{P} \quad &\triangleq \quad P \sqsubseteq \gamma(\overline{P}) \quad = \quad \alpha(P) \preccurlyeq \overline{P} \\
\alpha(P) \quad &\triangleq \quad \bigwedge\{\overline{P} \mid P \Vdash \overline{P}\} \\
\gamma(\overline{P}) \quad &\triangleq \quad \bigsqcup\{P \mid P \Vdash \overline{P}\}
\end{aligned}
$$

Conclusion

- Closure operators formalize approximation in the complete lattice of properties (good for mathematicians)
- Galois connections add the possibility to reason on an encoding of the abstract properties (good for computer scientists who have to represent information in their machines)
- Galois connections are used everywhere in abstract interpretation and this Chapter **11**, "Galois Connections and Abstraction" should be studied carefully.
- Many complements, examples, exercises, and references in the book.

Home work

- Read Ch. **11** “Galois Connections and Abstraction” of

  Principles of Abstract Interpretation
  Patrick Cousot
  MIT Press

The End, Thank you