Galois Connections and Abstract Interpretation

Viki

October 2, 2017

Preliminaries

Preliminaries

Definition

Complete lattice is a poset $(S, \leq)$ where for any $A \subseteq S$ there is $\sup(A) \in S$ and $\inf(A) \in S$.

Preliminaries

Definition

Complete lattice is a poset $(S, \leq)$ where for any $A \subseteq S$ there is $\sup(A) \in S$ and $\inf(A) \in S$.

Definition

A function $f : A \to B$ on posets $(A, \leq)$ and $(B, \sqsubseteq)$ is **monotone** iff:

$$\forall a, a' \in A \colon a \leq a' \implies f(a) \sqsubseteq f(a').$$

Preliminaries

Definition

Complete lattice is a poset $(S, \leq)$ where for any $A \subseteq S$ there is $\sup(A) \in S$ and $\inf(A) \in S$.

Definition

A function $f : A \to B$ on posets $(A, \leq)$ and $(B, \sqsubseteq)$ is **monotone** iff:

$$\forall a, a' \in A \colon a \leq a' \implies f(a) \sqsubseteq f(a').$$

Notation:

$$\mathbb{Z}^\infty = \mathbb{Z} \cup \{-\infty, \infty\}$$
$$\mathbb{Q}^\infty = \mathbb{Q} \cup \{-\infty, \infty\}$$
$$\mathbb{R}^\infty = \mathbb{R} \cup \{-\infty, \infty\}$$

Interval lattice

For any poset $(S, \leq)$ we define:

$$\mathtt{Int}_S = (I_S, \sqsubseteq),$$

where:

$$I_S = \{[a, b] \mid a, b \in S, a \leq b\} \cup \{\bot\}$$

$$\bot \sqsubseteq x \qquad \text{for all } x \in I_s$$
$$[a, b] \sqsubseteq [c, d] \iff c \leq a \wedge b \leq d$$

Interval lattice

For any poset $(S, \leq)$ we define:

$$\mathtt{Int}_S = (I_S, \sqsubseteq),$$

where:

$$I_S = \{[a, b] \mid a, b \in S, a \leq b\} \cup \{\bot\}$$

$$\bot \sqsubseteq x \qquad \text{for all } x \in I_s$$
$$[a, b] \sqsubseteq [c, d] \iff c \leq a \wedge b \leq d$$

If $(S, \leq)$ is a (complete) lattice, then $\mathtt{Int}_S$ is a (complete) lattice.

A good abstraction

Suppose we have posets $(C, \leq)$ and $(A, \sqsubseteq)$.

$$C \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} A$$

A good abstraction

Suppose we have posets $(C, \leq)$ and $(A, \sqsubseteq)$.

$$C \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} A$$

Functions α and γ should satisfy:

A good abstraction

Suppose we have posets $(C, \leq)$ and $(A, \sqsubseteq)$.

$$C \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} A$$

Functions α and γ should satisfy:

- α and γ are monotone,

A good abstraction

Suppose we have posets $(C, \leq)$ and $(A, \sqsubseteq)$.

$$C \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} A$$

Functions α and γ should satisfy:

- α and γ are monotone,
- $\alpha(c)$ is a correct abstraction of c:

$$c \leq \gamma(\alpha(c)),$$

A good abstraction

Suppose we have posets $(C, \leq)$ and $(A, \sqsubseteq)$.

$$C \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} A$$

Functions α and γ should satisfy:

- α and γ are monotone,
- $\alpha(c)$ is a correct abstraction of c:

$$c \leq \gamma(\alpha(c)),$$

- $\alpha(c)$ is the smallest abstraction of c:

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

A good abstraction

Suppose we have posets $(C, \leq)$ and $(A, \sqsubseteq)$.

$$C \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} A$$

Functions α and γ should satisfy:

- α and γ are monotone,
- $\alpha(c)$ is a correct abstraction of c:

$$c \leq \gamma(\alpha(c)),$$

- $\alpha(c)$ is the smallest abstraction of c:

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

  By setting $c = \gamma(a)$, we get:

$$\alpha(\gamma(a)) \sqsubseteq a.$$

Galois Connection – definition

Definition

Galois connection (α, γ) between partial orders $(C, \leq)$ and $(A, \sqsubseteq)$ is defined by two functions $\alpha : C \to A$ and $\gamma : A \to C$, such that:

- α and γ are monotone,
- $c \leq \gamma(\alpha(c))$,
- $\alpha(\gamma(a)) \sqsubseteq a$.

Galois Connection – definition

Definition

Galois connection (α, γ) between partial orders $(C, \leq)$ and $(A, \sqsubseteq)$ is defined by two functions $\alpha : C \to A$ and $\gamma : A \to C$, such that:

- α and γ are monotone,
- $c \leq \gamma(\alpha(c))$,
- $\alpha(\gamma(a)) \sqsubseteq a$.

Definition

Galois connection (α, γ) between partial orders $(C, \leq)$ and $(A, \sqsubseteq)$ is defined by two functions $\alpha : C \to A$ and $\gamma : A \to C$, such that:

$$\forall c \in C, a \in A. \quad \alpha(c) \sqsubseteq a \iff c \leq \gamma(a).$$

Galois Connection – example I

Suppose we have two posets $C = (2^{\mathbb{Z}}, \subseteq)$ and $A = \texttt{Int}_{\mathbb{Z}^\infty}$.
We define:

$$\alpha(S) = [\inf(S), \sup(S)]$$

$$\gamma(\bot) = \emptyset$$
$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

Galois Connection – example I

Suppose we have two posets $C = (2^{\mathbb{Z}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
We define:

$$\alpha(S) = [\inf(S), \sup(S)]$$

$$\gamma(\bot) = \emptyset$$
$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

Does the following hold?

Galois Connection – example I

Suppose we have two posets $C = (2^{\mathbb{Z}}, \subseteq)$ and $A = \texttt{Int}_{\mathbb{Z}^\infty}$.
We define:

$$\alpha(S) = [\inf(S), \sup(S)]$$

$$\gamma(\bot) = \emptyset$$
$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

Does the following hold?

- α and γ are monotone

Galois Connection – example I

Suppose we have two posets $C = (2^{\mathbb{Z}}, \subseteq)$ and $A = \texttt{Int}_{\mathbb{Z}^\infty}$.
We define:

$$\alpha(S) = [\inf(S), \sup(S)]$$

$$\gamma(\bot) = \emptyset$$
$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

Does the following hold?

- α and γ are monotone
- $S \subseteq \gamma(\alpha(S))$

Galois Connection – example I

Suppose we have two posets $C = (2^{\mathbb{Z}}, \subseteq)$ and $A = \texttt{Int}_{\mathbb{Z}^\infty}$.
We define:

$$\alpha(S) = [\inf(S), \sup(S)]$$

$$\gamma(\bot) = \emptyset$$
$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

Does the following hold?

- α and γ are monotone
- $S \subseteq \gamma(\alpha(S))$
- $\alpha(\gamma(I)) \sqsubseteq I$

Galois Connection – example I

Suppose we have two posets $C = (2^{\mathbb{Z}}, \subseteq)$ and $A = \texttt{Int}_{\mathbb{Z}^\infty}$.
We define:

$$\alpha(S) = [\inf(S), \sup(S)]$$

$$\gamma(\bot) = \emptyset$$
$$\gamma([a, b]) = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$$

Does the following hold?

- α and γ are monotone
- $S \subseteq \gamma(\alpha(S))$
- $\alpha(\gamma(I)) \sqsubseteq I$

The pair (α, γ) is a Galois connection.

Galois Connection – example II

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
Find Galois connection (α, γ).

Galois Connection – example II

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$

Galois Connection – example II

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$
- $\alpha(S) = [\lfloor \inf(S) \rfloor, \lceil \sup(S) \rceil]$

Galois Connection – example II

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$
- $\alpha(S) = [\lfloor \inf(S) \rfloor, \lceil \sup(S) \rceil]$

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Q}^\infty}$.
Find Galois connection (α, γ).

Galois Connection – example II

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$
- $\alpha(S) = [\lfloor \inf(S) \rfloor, \lceil \sup(S) \rceil]$

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Q}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$

Galois Connection – example II

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Z}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$
- $\alpha(S) = [\lfloor \inf(S) \rfloor, \lceil \sup(S) \rceil]$

Suppose we have two posets $C = (2^{\mathbb{Q}}, \subseteq)$ and $A = \mathtt{Int}_{\mathbb{Q}^\infty}$.
Find Galois connection (α, γ).

- $\gamma(\bot) = \emptyset$
  $\gamma([a, b]) = \{x \in \mathbb{Q} \mid a \leq x \leq b\}$
- there is no such α

Galois Connection – inf \ sup preserving

Given two complete lattices $(C, \leq)$ and $(A, \sqsubseteq)$ and Galois connection (α, γ):

- α preserves infima:

$$\alpha(\inf(X)) = \inf\{\alpha(x) \mid x \in X\},$$

  for any $X \subseteq C$.

- γ preserves suprema:

$$\gamma(\sup(Y)) = \sup\{\gamma(y) \mid y \in Y\},$$

  for any $Y \subseteq A$.

Galois Connection – uniqueness

Given two Galois connections (α, γ) and (α', γ') between the same posets, it holds:

$$\alpha = \alpha' \iff \gamma = \gamma'.$$

Galois Connection – uniqueness

Given two Galois connections (α, γ) and (α', γ') between the same posets, it holds:

$$\alpha = \alpha' \iff \gamma = \gamma'.$$

Proof.
Assume $\alpha = \alpha'$. From the definition with $\gamma(a) = c$:

$$\alpha'(\gamma(a)) \sqsubseteq a \iff \gamma(a) \leq \gamma'(a)$$

Galois Connection – determinacy

Given complete lattices $(C, \leq)$ and $(A, \sqsubseteq)$ and either α or γ, we define the other.

- Providing γ preserves suprema:

$$\alpha(x) = \inf\{y \mid x \leq \gamma(y)\}.$$

- Providing α preserves infima:

$$\gamma(y) = \sup\{x \mid \alpha(x) \sqsubseteq y\}.$$

Galois connection – product

Given posets $(C, \leq)$, $(A, \sqsubseteq)$ with GC (α, γ) and posets $(C', \leq')$, $(A', \sqsubseteq')$ with GC (α', γ'), there is a Galois connection on the Cartesian product of the posets:

$$(C \times C', \preceq) \qquad (A \times A', \trianglelefteq)$$

We define a Galois connection (Δ, Γ):

$$\Delta\big((a, b)\big) = (\alpha(a), \alpha'(b)),$$

$$\Gamma\big((a, b)\big) = (\gamma(a), \gamma'(b)).$$

Galois connection – example III

We want to find all possible values of a variable x.
We need to track the values on all program locations.

$$(2^{\mathbb{Z}})^n \underset{\Gamma}{\overset{\Delta}{\rightleftarrows}} (\mathtt{Int}_{\mathbb{Z}^\infty})^n$$

Recall the example from previous week.

Abstract transformer using GC

Abstract transformer using GC

Given two posets $(C, \leq)$ and $(A, \sqsubseteq)$ with GC (α, γ) and a transformer $f : C \to C$, we say $f^\sharp : A \to A$ overapproximates f if:

$$\alpha(f(\gamma(a))) \sqsubseteq f^\sharp(a).$$

Abstract transformer using GC

Given two posets $(C, \leq)$ and $(A, \sqsubseteq)$ with GC (α, γ) and a transformer $f : C \to C$, we say $f^\sharp : A \to A$ overapproximates f if:

$$\alpha(f(\gamma(a))) \sqsubseteq f^\sharp(a).$$

The best abstract transformer $f^\sharp$ is defined as:

$$f^\sharp(a) = \alpha(f(\gamma(a))).$$

Fixed point approximation

The least abstract fixed point overapproximates the least concrete fixed point:

$$\alpha(\mathsf{lfp}(f)) \sqsubseteq \mathsf{lfp}(f^\sharp).$$

Which is equivalent to:

$$\mathsf{lfp}(f) \leq \gamma(\mathsf{lfp}(f^\sharp)).$$