CS615: Formal Specification and Verification of Programs 2019

Lecture 12: Galois connection and abstraction

Instructor: Ashutosh Gupta

IITB, India

Compile date: 2019-09-27

Topic 12.1

Galois connection

Galois connection

Definition 12.1

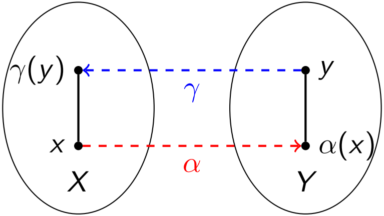
For posets $(X, \leq)$ *and* $(Y, \sqsubseteq)$*, a pair of maps* (α, γ) *of maps* $\alpha : X \rightarrow Y$ *and* $\gamma : Y \rightarrow X$ *is a Galois connection if*

$$\forall x \in X \forall y \in Y.\ \alpha(x) \sqsubseteq y \Leftrightarrow x \leq \gamma(y)$$

which is usually written

$$(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$$

α and γ are called upper and lower adjoints respectively.

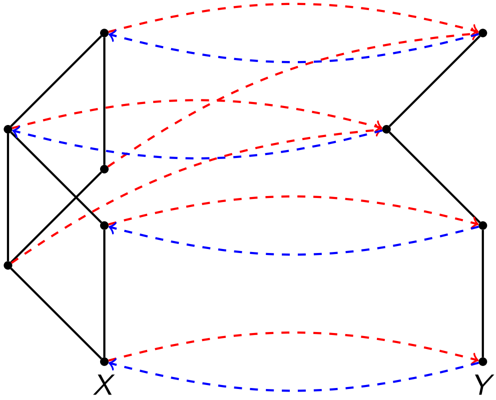


Example: Galois connection

Example 12.1

The following is a Galois connection.

$$(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$$

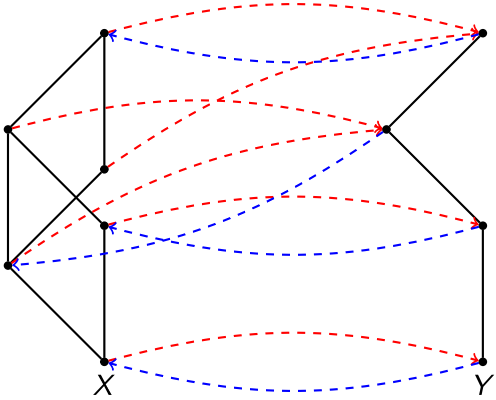


Exercise: not Galois

Exercise 12.1

Why the following mappings do not satisfy the condition of Galois connection?

$$(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$$



Unique adjoints

Theorem 12.1
In $(X, \leq) \xrightleftharpoons[\alpha]{\gamma} (Y, \sqsubseteq)$*,* α *uniquely defines* γ *and vice-versa.*

$$\alpha(x) = \sqcap\{y | x \leq \gamma(y)\} \qquad \gamma(y) = \vee\{x | \alpha(x) \sqsubseteq y\}$$

Proof.

- By definition of meet, $\sqcap\{y|\alpha(x) \sqsubseteq y\}$ exists(why?) and

$$\alpha(x) = \sqcap\{y|\alpha(x) \sqsubseteq y\}$$

- By def. of Galois connection, we may replace the set definition.

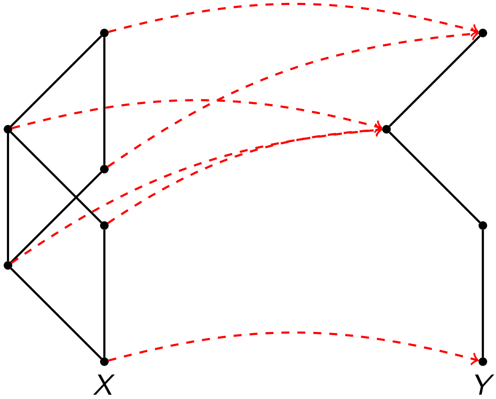
$$\alpha(x) = \sqcap\{y|x \leq \gamma(y)\}$$

Symmetrically for $\gamma(x)$. □

Exercise: unique adjoints

Exercise 12.2

Construct γ for the following α



Exercise 12.3

Give an example α such that there is no γ?

Exercise : unique adjoints II

Exercise 12.4

Let us suppose $\{x|\alpha(x) \sqsubseteq y\}$ *is empty for some* x. *What will be* $\gamma(x)$? *Will* α *and* γ *form Galois connection?*

Exercise 12.5

Prove or disprove: if α *is monotonic,* γ *is monotonic.*

Exercise 12.6

In $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (X, \leq)$, *if* α *is an upper closure operator. Give* γ?

Properties of Galois connection: extensive/reductive compose

Theorem 12.2

Let $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$ *then*

1. $\forall x \in X.\ x \leq \gamma \circ \alpha(x)$ *($\gamma \circ \alpha$ is extensive)*
2. $\forall y \in Y.\ \alpha \circ \gamma(y) \sqsubseteq y$ *($\alpha \circ \gamma$ is reductive)*

Proof.

claim: $\gamma \circ \alpha$ is extensive

1. $\alpha(x) \sqsubseteq \alpha(x)$
2. Due to the def. of connection, $x \leq \gamma \circ \alpha(x)$.
3. $\gamma \circ \alpha$ is extensive.

Symmetrically, $\alpha \circ \gamma$ is reductive. □

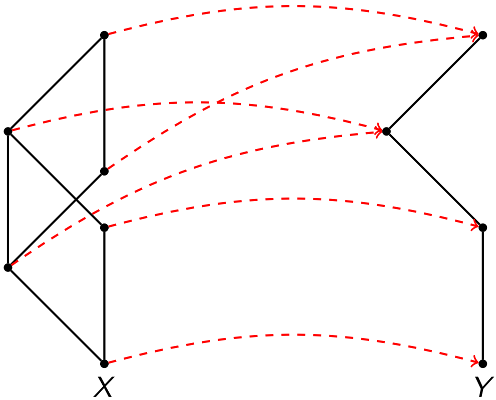
Exercise: compose

Exercise 12.7

Consider the following Galois connection.

$$(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$$

Draw $\gamma \circ \alpha$ *and* $\alpha \circ \gamma$



Properties of Galois connection : monotone

Theorem 12.3

Let $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$ *then*

1. α *is monotone*
2. γ *is monotone*

Proof.

claim: α is monotone

1. Let $x, x' \in X$. Assume, $x \leq x'$.
2. Since $\gamma \circ \alpha$ is extensive, $x \leq \gamma \circ \alpha(x')$.
3. Due to the def. of connection, $\alpha(x) \sqsubseteq \alpha(x')$.

Symmetrically, γ is monotone. □

Characterization of Galois connection

Theorem 12.4

Let $(X, \leq)$ and $(Y, \sqsubseteq)$ be posets. Let $\alpha : X \rightarrow Y$ and $\gamma : Y \rightarrow X$ such that

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

Then,

$$(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$$

Proof.

Let $x \in X$ and $y \in Y$.

1. Assume $\alpha(x) \sqsubseteq y$
2. Since γ is monotone, $\gamma \circ \alpha(x) \leq \gamma(y)$
3. Since $\gamma \circ \alpha$ is extensive, $x \leq \gamma(y)$.

The other direction is also symmetric. □

Exercise: violate characterization

Exercise 12.8

Let $(X, \leq)$ *and* $(Y, \sqsubseteq)$ *be posets. For each subset of the conditions of lhs of theorem 12.4, give an example of* $\alpha : X \to Y$ *and* $\gamma : Y \to X$ *such that exactly the condition in subset are satisfied and* α *and* γ *do not form Galois connection.*

More properties of Galois connection

Theorem 12.5

Let $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$ *then*

1. $\alpha \circ \gamma \circ \alpha = \alpha$
2. $\gamma \circ \alpha \circ \gamma = \gamma$

Proof.

1. Since $\gamma \circ \alpha$ is extensive, $x \leq \gamma \circ \alpha(x)$.
2. Since α is monotone, $\alpha(x) \sqsubseteq \alpha \circ \gamma \circ \alpha(x)$.
3. Since $\alpha \circ \gamma$ is reductive, $\alpha \circ \gamma \circ \alpha(x) \sqsubseteq \alpha(x)$.

Therefore, $\alpha \circ \gamma \circ \alpha = \alpha$.

Symmetrically, $\gamma \circ \alpha \circ \gamma = \gamma$. $\square$

Exercise 12.9

a. $\gamma \circ \alpha$ *is an upper-closure operator.*

b. $\alpha \circ \gamma$ *is a lower-closure operator.*

Onto/into Galois connections

Theorem 12.6

Let $(X, \leq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (Y, \sqsubseteq)$ *then*

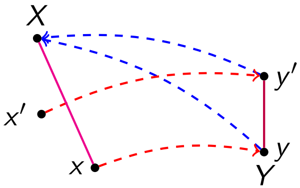
1. α *is onto* $\Leftrightarrow$ γ *is one-to-one* $\Leftrightarrow$ $\alpha \circ \gamma = \Delta_X$
2. γ *is onto* $\Leftrightarrow$ α *is one-to-one* $\Leftrightarrow$ $\gamma \circ \alpha = \Delta_Y$

Proof.

Assume α is onto.

claim: γ is one-to-one

1. Let $y, y' \in Y$ such that $\gamma(y) = \gamma(y')$.
2. Since α is onto, there are $x, x' \in X$ such that $\alpha(x) = y$ and $\alpha(x') = y'$
3. Therefore, $\gamma \circ \alpha(x) = \gamma \circ \alpha(x')$
4. Since $\gamma \circ \alpha$ is extensive, $x \leq \gamma \circ \alpha(x')$.
5. Due to the def. of connection, $\alpha(x) \sqsubseteq \alpha(x')$.
6. Therefore, $y \sqsubseteq y'$. Symmetrically, $y' \sqsubseteq y$
7. Therefore, $y = y'$



...

Onto/into Galois connections

Proof.

Assume γ is one-to-one.
claim: $\alpha \circ \gamma = \Delta_X$

1. We know $\gamma \circ \alpha \circ \gamma = \gamma$.
2. Let $y \in Y$. So, $\gamma \circ \alpha \circ \gamma(y) = \gamma(y)$
3. After rewrite, $\gamma(\alpha \circ \gamma(y)) = \gamma(y)$
4. Since γ is one-to-one, $\alpha \circ \gamma(y) = y$

$\alpha \circ \gamma = \Delta_X$
claim: α is onto

1. For each $y \in Y$, we have $\alpha \circ \gamma(y) = y$.
2. Therefore, for each y, there is an $x \in X$ such that $\alpha(x) = y$.

□

Topic 12.2

Abstraction and Galois connection

Abstract interpretation

Definition 12.2

Concrete objects of analysis or domain — $C = \mathfrak{p}(\mathbb{Q}^V)$

- *not all sets are concisely representable in computer*
- *too (infinitely) many of them*

Definition 12.3

Abstract domain — only simple to represent sets $D \subseteq C$

- D *should allow efficient algorithms for desired operations*
- *far fewer, but possibly infinitely many*
- *Sets in* $C \setminus D$ *are not precisely representable in* D

How to use D to capture semantics of a program?

Note: C naturally forms a complete lattice

$$(C, \subseteq, \emptyset, \mathbb{Q}^V, \cup, \cap)$$

Abstracting and concretization function

This is not the most general definition!
Any partial order can replace $\supseteq$.

Definition 12.4

An abstraction function $\alpha : C \rightarrow D$ *maps each set* $c \in C$ *to* $\alpha(c) \supseteq c$.

Definition 12.5

A concretization function $\gamma : D \rightarrow C$ *maps each set* $d \in D$ *to* d.

The above definitions become more meaningful, if we think of D as the representation of sets on a computer instead of the sets themselves.

Lemma 12.1

D contains $\mathbb{Q}^V$

Example: abstraction – intervals

Example 12.2

Let us assume $V = \{\mathtt{x}\}$

Consider $D = \{\bot, \top\} \cup \{[a,b] | a, b \in \mathbb{Q}\}$.

Ordering among elements of D *are defined as follows:*

D forms a lattice.

$\bot \sqsubseteq [a,b] \sqsubseteq \top$ *and* $[a_1, b_1] \sqsubseteq [a_2, b_2] \Leftrightarrow a_2 \leq a_1 \land b_1 \leq b_2$

Let $\alpha(c) \triangleq [inf(c), sup(c)]$ *and* $\gamma([a,b]) \triangleq [a,b]$

Exercise 12.10

Give the following value

- $\alpha(\{0,3,5\}) =$
- $\alpha((0,3)) =$
- $\alpha([0,3] \cup [5,6]) =$
- $\alpha(\{1/x | x \geq 1\}) =$

Exercise 12.11

Is D *a complete lattice?*

Choices for α: minimal abstraction principle

It is always better to choose smaller abstraction.

Choose $\alpha(c)$ as small as possible, therefore more precise abstraction

Therefore, if $d \in D$ then $\alpha(d) = d$ and α must be monotonic

There may be multiple minimal abstractions.

Even worse, there may be no minimal approximation,
e. g., approximating a circle with a polytope
(In this lecture, we assume minimal abstractions exist.)

Properties of D, α, and γ

Now on we will ignore that D is set of sets. We assume D is a topped poset

$$(D, \sqsubseteq, \top)$$

- α is monotone (due to minimality principle)
- γ is monotone
- $c \subseteq \gamma \circ \alpha(c)$
- $\alpha \circ \gamma(d) \sqsubseteq d$ (due to minimality principle)

Therefore,

$$(C, \subseteq) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (D, \sqsubseteq)$$

We always choose D, α, and γ such that the above Galois connection holds and usually referred

abstract domain.

Onto abstraction

Due to the principle of minimal abstraction, α must be onto

$$\forall p \in D.\ \alpha(p) = p \qquad (\text{assuming } D \subseteq C)$$

Therefore, one-to-one γ

However, in practice we may relax the onto condition on α. A set can be represented multiple ways on a computer.

Therefore, multiple abstract objects may have same concretization.

Example 12.3

BDDs and clauses both can be used to represent set of states.

Topic 12.3

Examples of abstract domains

Sign abstract domain

Sign abstraction

$C = \mathfrak{p}(\mathbb{Q})$

$D = \{+, -, 0, \bot, \top\}$

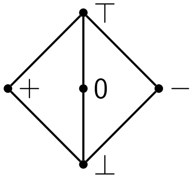
$\alpha(p) = +$ if $min(p) > 0$

$\alpha(p) = -$ if $max(p) < 0$

$\alpha(0) = 0$

$\alpha(\emptyset) = \bot$

$\alpha(p) = \top$, otherwise



Exercise 12.12

Give the following value

- $\alpha(\{0.1, 0.3\}) =$
- $\alpha(\{0\}) =$
- $\alpha(\{0.1, 0\}) =$
- $\alpha(\{-1/x | x \geq 1\}) =$

Congruence abstraction domain

A domain may be parameterized.

Congruence abstraction

For some $n \in \mathbb{N}$,
$C = \mathbb{Z}$
$D = \{0, \ldots, n-1\}$
$\alpha(c) = c \bmod n$

Exercise 12.13
Give the following value for $n = 11$

- $\alpha(6) =$
- $\alpha(-1) =$
- $\alpha(3000) =$
- $\alpha(\{0, 4, 5\}) =$

Cartesian predicate abstraction

Let V be a vector of variables. Cartesian predicate abstraction is defined by a set of predicates

$$P = \{p_1, \dots, p_n\}$$

over variables V. Naturally, $C = \mathfrak{p}(\mathbb{Q}^{|V|})$

Let $D = \perp \cup \mathfrak{p}(P)$. // $\emptyset$ represents $\top$

Ordering over the elements of $S_1, S_2 \in D$ is as follows.

$$\perp \sqsubseteq S_1 \sqsubseteq S_2 \text{ if } S_2 \subseteq S_1$$

Example 12.4

Let $V = \{\mathrm{x}, \mathrm{y}\}$. *Let* $P = \{\mathrm{x} \leq 1, -\mathrm{x} - \mathrm{y} \leq -1, \mathrm{y} \leq 5\}$

Exercise 12.14

Does the following hold?

- $\{\mathrm{x} \leq 1\} \sqsubseteq \{\mathrm{x} \leq 1, -\mathrm{x} - \mathrm{y} \leq -1\}$
- $\{\mathrm{x} \leq 1, -\mathrm{x} - \mathrm{y} \leq -1\} \sqsubseteq \{\mathrm{x} \leq 1\}$
- $\{\mathrm{x} \leq 1, -\mathrm{x} - \mathrm{y} \leq -1\} \sqsubseteq \emptyset$
- $\{\mathrm{x} \leq 1\} \sqsubseteq \perp$

Cartesian predicate abstraction II

Let us define the abstraction and concretization functions

$$\alpha(c) = \{p \in P | c \Rightarrow p\} \qquad \gamma(S) = \bigwedge S$$

Example 12.5

Let $V = \{\mathtt{x}, \mathtt{y}\}$ *and* $P = \{\mathtt{x} \leq 1, -\mathtt{x} - \mathtt{y} \leq -1, \mathtt{y} \leq 5\}$.

$\alpha(\{(0,0)\}) = \{\mathtt{x} \leq 1, \mathtt{y} \leq 5\}$
$\alpha((\mathtt{x}-1)^2 + (\mathtt{y}-3)^2 = 1) = \{-\mathtt{x} - \mathtt{y} \leq -1, \mathtt{y} \leq 5\}$

Exercise 12.15

Give the following value

- $\alpha(\{(8,8)\}) =$
- $\alpha(\{(0,0),(8,8)\}) =$
- $\alpha(\{(0,2)\}) =$
- $\alpha(\emptyset) =$

Topic 12.4

Some properties of abstract domains

Best approximation

Definition 12.6

α performs best approximation if $\forall c \in C, d \in D.\ c \subseteq \gamma(d) \Rightarrow \alpha(c) \sqsubseteq d$.

The above is one of the Galois conditions. So, $\alpha(c) = \sqcap\{d \in D | c \subseteq \gamma(d)\}$.

Theorem 12.7

An abstract domain is complete lattice iff best approximations exists.

Proof.

If abstract domain is complete lattice then $\sqcap\{d \in D | c \subseteq \gamma(d)\}$ always exists.
For the other direction, consider $S \subseteq D$.

1. Since $\bigcap \gamma(S)$ and best approximations exists, $\alpha(\bigcap \gamma(S)) = \sqcap\{d | \bigcap \gamma(S) \subseteq \gamma(d)\}$
2. $(\forall c \in S.\ c \in \{d | \bigcap \gamma(S) \subseteq \gamma(d)\}) \Rightarrow \alpha(\bigcap \gamma(S)) \in lb(S)$
3. Assume $d \in lb(S)$. Due to monotone γ, $\gamma(d) \in lb(\gamma(S))$. Therefore, $\gamma(d) \subseteq \bigcap \gamma(S)$
4. Due to monotone α, $\alpha \circ \gamma(d) \sqsubseteq \alpha(\bigcap \gamma(S))$
5. Since $\alpha \circ \gamma = 1_D$, $d \sqsubseteq \alpha(\bigcap \gamma(S))$. Therefore, $\alpha(\bigcap \gamma(S)) = \sqcap S$ □

Note: If we do not have best approximation then we are breaking conditions of Galois connection, namely monotone α.

End of Lecture 12