Galois Connections

Fabio Valentini

Specialization Seminar (CL), Summer Semester 2019

May 22, 2019

Contents

Motivation

- Performing fixed point calculations on the complete lattice L can be expensive, or even uncomputable.
- Idea: Introduce an abstraction over lattice L – a simpler lattice M.

Motivation

- Performing fixed point calculations on the complete lattice L can be expensive, or even uncomputable.
- Idea: Introduce an abstraction over lattice L – a simpler lattice M.

Example

The complete lattice over the powerset of integers $L = (\mathcal{P}(\mathbb{Z}), \sqsubseteq)$ is hard to use. By introducing an abstraction (describing sets of integers with intervals), interesting computations become easier.

Basic Idea

So, instead of performing program analysis $p \vdash l_1 \triangleright l_2$ over the lattice L, find descriptions (abstractions) M of elements in L and perform the simpler analysis $p \vdash m_1 \triangleright m_2$ over M instead.

Basic Idea

So, instead of performing program analysis $p \vdash l_1 \triangleright l_2$ over the lattice L, find descriptions (abstractions) M of elements in L and perform the simpler analysis $p \vdash m_1 \triangleright m_2$ over M instead.

Here, the lattice M and the transformation from elements of L to elements of M must have certain properties to maintain the requirement for safe results: the properties of a *Galois connection*.

Galois connections

Definition

A Galois connection is a 4-tuple (L, α, γ, M) with the properties:

- L and M are complete lattices, and
- α and γ are monotone functions

Galois connections

Definition

A Galois connection is a 4-tuple (L, α, γ, M) with the properties:

- L and M are complete lattices, and
- α and γ are monotone functions

$$\begin{aligned} \alpha &: L \to M && \text{(abstraction function)} \\ \gamma &: M \to L && \text{(concretization function),} \end{aligned}$$

where α and γ satisfy:

Galois connections

Definition

A Galois connection is a 4-tuple (L, α, γ, M) with the properties:

- L and M are complete lattices, and
- α and γ are monotone functions

$$
\begin{aligned}
\alpha &: L \to M && \text{(abstraction function)} \\
\gamma &: M \to L && \text{(concretization function)},
\end{aligned}
$$

where α and γ satisfy:

$$
\begin{aligned}
\gamma \circ \alpha &\sqsupseteq \lambda \ell . \ell \\
\alpha \circ \gamma &\sqsubseteq \lambda m . m
\end{aligned}
$$

Galois connections

Definition

A Galois connection is a 4-tuple (L, α, γ, M) with the properties:

- L and M are complete lattices, and
- α and γ are monotone functions

$$\begin{aligned} \alpha &: L \to M && \text{(abstraction function)} \\ \gamma &: M \to L && \text{(concretization function)}, \end{aligned}$$

where α and γ satisfy:

$$\begin{aligned} \gamma \circ \alpha &\sqsupseteq \lambda \ell . \ell \\ \alpha \circ \gamma &\sqsubseteq \lambda m . m \end{aligned}$$

These properties ensure safety, but precision may be lost.

Example: Integers and Intervals (1)

Example

Consider the example mentioned at the beginning – abstracting the powerset over the whole numbers as a set of intervals.

$$L : \mathcal{P}(\mathbb{Z}) = (\mathcal{P}(\mathbb{Z}), \subseteq)$$
$$M : \textbf{Interval} = (\textbf{Interval}, \sqsubseteq)$$

Example: Integers and Intervals (1)

Example

Consider the example mentioned at the beginning – abstracting the powerset over the whole numbers as a set of intervals.

$$L : \mathcal{P}(\mathbb{Z}) = (\mathcal{P}(\mathbb{Z}), \subseteq)$$
$$M : \textbf{Interval} = (\textbf{Interval}, \sqsubseteq)$$

Then, $(\mathcal{P}(\mathbb{Z}), \alpha_{ZI}, \gamma_{ZI}, \textbf{Interval})$ is a Galois connection with:

$$\alpha_{ZI}(Z) = \begin{cases} \bot & \text{if} Z = \emptyset \\ [\inf'(Z), \sup'(Z)] & \text{otherwise} \end{cases}$$
$$\gamma_{ZI}(int) = \{z \in \mathbb{Z} | \inf(int) \leq z \leq \sup(int)\}$$

Example: Integers and Intervals (2)

It is easy to show that α and γ are monotone, and they also have the desired properties $\alpha \circ \gamma \sqsubseteq \lambda m.m$ and $\gamma \circ \alpha \sqsupseteq \lambda \ell.\ell$:

$$\alpha_{ZI}(\gamma_{ZI}([z_1, z_2])) = [z_1, z_2]$$
$$\gamma_{ZI}(\alpha_{ZI}(Z)) \supseteq Z$$

Example: Integers and Intervals (2)

It is easy to show that α and γ are monotone, and they also have the desired properties $\alpha \circ \gamma \sqsubseteq \lambda m.m$ and $\gamma \circ \alpha \sqsupseteq \lambda \ell.\ell$:

$$\alpha_{ZI}(\gamma_{ZI}([z_1, z_2])) = [z_1, z_2]$$
$$\gamma_{ZI}(\alpha_{ZI}(Z)) \supseteq Z$$

Example

$$\gamma_{ZI}([0,3]) = \{0,1,2,3\}$$
$$\gamma_{ZI}([0,\infty]) = \{z \in \mathbb{Z} | z \geq 0\}$$

$$\alpha_{ZI}(\{0,1,3\}) = [0,3]$$
$$\alpha_{ZI}(\{2 \cdot z | z > 0\}) = [2,\infty]$$

Example: Using the representation function β

The representation function β, which associates properties ℓ to program states v, can also be used to define a Galois connection $(\mathcal{P}(V), \alpha, \gamma, L)$ with the following properties:

$$
\begin{aligned}
\alpha(V') &= \sqcup \{\beta(v) | v \in V'\} \\
\gamma(\ell) &= \{v \in V | \beta(v) \sqsubset \ell\}
\end{aligned}
$$

Example: Using the representation function β

The representation function β, which associates properties ℓ to program states v, can also be used to define a Galois connection $(\mathcal{P}(V), \alpha, \gamma, L)$ with the following properties:

$$\begin{aligned} \alpha(V') &= \sqcup\{\beta(v) | v \in V'\} \\ \gamma(\ell) &= \{v \in V | \beta(v) \sqsubset \ell\} \end{aligned}$$

$$\begin{tikzcd}
\mathcal{P}(V) \arrow[rr, bend left, "\alpha"] & & L \arrow[ll, bend left, "\gamma"] \\
& V \arrow[ul, "\times"] \arrow[ur, "\beta"'] &
\end{tikzcd}$$

Properties of Galois connections (1)

For a Galois connection (L, α, γ, M), the following statements hold:

Properties of Galois connections (1)

For a Galois connection (L, α, γ, M), the following statements hold:

- α uniquely determines γ:

$$\gamma(m) = \sqcup \{\ell | \alpha(\ell) \sqsubseteq m\}$$

Properties of Galois connections (1)

For a Galois connection (L, α, γ, M), the following statements hold:

- α uniquely determines γ:

$$\gamma(m) = \bigsqcup \{\ell | \alpha(\ell) \sqsubseteq m\}$$

- γ uniquely determines α:

$$\alpha(\ell) = \bigsqcap \{m | l \sqsubseteq \gamma(m)\}$$

Properties of Galois connections (1)

For a Galois connection (L, α, γ, M), the following statements hold:

- α uniquely determines γ:

$$\gamma(m) = \bigsqcup \{\ell | \alpha(\ell) \sqsubseteq m\}$$

- γ uniquely determines α:

$$\alpha(\ell) = \bigsqcap \{m | l \sqsubseteq \gamma(m)\}$$

- α is completely additive, γ is completely multiplicative

Properties of Galois connections (1)

For a Galois connection (L, α, γ, M), the following statements hold:

- α uniquely determines γ:

$$\gamma(m) = \bigsqcup \{\ell | \alpha(\ell) \sqsubseteq m\}$$

- γ uniquely determines α:

$$\alpha(\ell) = \bigsqcap \{m | l \sqsubseteq \gamma(m)\}$$

- α is completely additive, γ is completely multiplicative
- $\alpha(\bot) = \bot$ and $\gamma(\top) = \top$

Properties of Galois connections (2)

There are some additional important properties of functions over lattices:

Properties of Galois connections (2)

There are some additional important properties of functions over lattices:

- If a function $\alpha : L \to M$ is completely additive, then $\exists \gamma : M \to L$ such that (L, α, γ, M) is a Galois connection.

Properties of Galois connections (2)

There are some additional important properties of functions over lattices:

- If a function $\alpha : L \to M$ is completely additive, then $\exists\gamma : M \to L$ such that (L, α, γ, M) is a Galois connection.
- If a function $\gamma : M \to L$ is completely multiplicative, then $\exists\alpha : L \to M$ such that (L, α, γ, M) is a Galois connection.

Properties of Galois connections (2)

There are some additional important properties of functions over lattices:

- If a function $\alpha : L \to M$ is completely additive, then $\exists \gamma : M \to L$ such that (L, α, γ, M) is a Galois connection.
- If a function $\gamma : M \to L$ is completely multiplicative, then $\exists \alpha : L \to M$ such that (L, α, γ, M) is a Galois connection.

Additionally,

- both $\alpha \circ \gamma \circ \alpha = \alpha$,
- and $\gamma \circ \alpha \circ \gamma = \gamma$

hold because of the monotonicity of α and γ and the additional constraints on $\alpha \circ \gamma$ and $\gamma \circ \alpha$ for Galois connections.

Adapting the correctness relation (1)

Transforming L into M (and back) for performing calculations does *not* affect the result of program correctness and safety analyses.

- New correctness relation S, using R and (L, α, γ, M):
- before: $R : V \times L \rightarrow \{true, false\}$
- now: $S : V \times M \rightarrow \{true, false\}$
- with: $vSm \Leftrightarrow vR(\gamma(m))$

Adapting the correctness relation (1)

Transforming L into M (and back) for performing calculations does *not* affect the result of program correctness and safety analyses.

- New correctness relation S, using R and (L, α, γ, M):
- before: $R : V \times L \to \{true, false\}$
- now: $S : V \times M \to \{true, false\}$
- with: $vSm \Leftrightarrow vR(\gamma(m))$

If S is indeed a correctness relation, the following two properties must hold (Chapter 4.1):

$$vR\ell_1 \wedge \ell_1 \sqsubseteq \ell_2 \Rightarrow vR\ell_2$$
$$(\forall \ell \in L' \subseteq L : vR\ell) \Rightarrow vR(\sqcap L')$$

Adapting the correctness relation (2)

Proof.

With γ monotone, and R as correctness relation:

$$\begin{aligned}(vSm_1) \wedge m_1 \sqsubseteq m_2 &\Rightarrow vR(\gamma(m_1)) \wedge \gamma(m_1) \sqsubseteq \gamma(m_2)\\ &\Rightarrow vR(\gamma(m_2))\\ &\Rightarrow vSm_2\end{aligned}$$

Adapting the correctness relation (2)

Proof.

With γ monotone, and R as correctness relation:

$$\begin{aligned}(vSm_1) \wedge m_1 \sqsubseteq m_2 &\Rightarrow vR(\gamma(m_1)) \wedge \gamma(m_1) \sqsubseteq \gamma(m_2)\\ &\Rightarrow vR(\gamma(m_2))\\ &\Rightarrow vSm_2\end{aligned}$$

With γ completely multiplicative, and R as correctness relation:

$$\begin{aligned}(\forall m \in M' : vSm) &\Rightarrow (\forall m \in M' : vR(\gamma(m)))\\ &\Rightarrow vR(\sqcap \{\gamma(m) | m \in M'\})\\ &\Rightarrow vR(\gamma(\sqcap M'))\\ &\Rightarrow vS(\sqcap M')\end{aligned}$$

Adapting the correctness relation (2)

Proof.

With γ monotone, and R as correctness relation:

$$\begin{aligned}(vSm_1) \wedge m_1 \sqsubseteq m_2 &\Rightarrow vR(\gamma(m_1)) \wedge \gamma(m_1) \sqsubseteq \gamma(m_2)\\ &\Rightarrow vR(\gamma(m_2))\\ &\Rightarrow vSm_2\end{aligned}$$

With γ completely multiplicative, and R as correctness relation:

$$\begin{aligned}(\forall m \in M' : vSm) &\Rightarrow (\forall m \in M' : vR(\gamma(m)))\\ &\Rightarrow vR(\sqcap \{\gamma(m) | m \in M'\})\\ &\Rightarrow vR(\gamma(\sqcap M'))\\ &\Rightarrow vS(\sqcap M')\end{aligned}$$

Hence, S is a correctness relation, if R is a correctness relation and (L, α, γ, M) is a Galois connection. $\square$

Adapting the correctness relation (3)

S can be generated from the representation function β and the Galois connection (L, α, γ, M):

$$\beta : V \to L$$

$$\beta(v) = \ell \iff vR\ell$$

Adapting the correctness relation (3)

S can be generated from the representation function β and the Galois connection (L, α, γ, M):

$$\beta : V \to L$$
$$\beta(v) = \ell \iff vR\ell$$

$$\begin{aligned} vSm &\Leftrightarrow vR(\gamma(m)) \\ &\Leftrightarrow \beta(v) \sqsubseteq \gamma(m) \\ &\Leftrightarrow (\alpha \circ \beta)(v) \sqsubseteq m \end{aligned}$$

So, S can be generated from the function composition of the abstraction function α and and the representation function β.

Galois insertions

Due to the abstractions that are applied when constructing M from L, there can be several superfluous $m \in M$ that describe the same $l \in L$, and are hence redundant for performing analyses.

Galois insertions

Due to the abstractions that are applied when constructing M from L, there can be several superfluous $m \in M$ that describe the same $l \in L$, and are hence redundant for performing analyses.

Definition

For complete lattices $L = (L, \sqsubseteq)$ and $M = (M, \sqsubseteq)$, monotone functions $\alpha : L \to M$ and $\gamma : M \to L$, which have the properties

$$\gamma \circ \alpha \sqsupseteq \lambda \ell . \ell$$
$$\alpha \circ \gamma = \lambda m . m,$$

the 4-tuple (L, α, γ, M) is a Galois insertion. The equality in the second requirement is a stronger restriction than for Galois connections, where a $\sqsubseteq$ relation was sufficient.

Properties of Galois insertions (1)

The stronger constraints on α and γ ensure that no superfluous elements can be added (to M) when first applying the abstraction function, and then the concretization function.

Properties of Galois insertions (1)

The stronger constraints on α and γ ensure that no superfluous elements can be added (to M) when first applying the abstraction function, and then the concretization function.

Example

The Galois connection $(\mathcal{P}(\mathbb{Z}), \alpha_{ZI}, \gamma_{ZI}, \text{Interval})$ from the first example is also a Galois insertion, since the equality $\alpha \circ \gamma = \lambda m.m$ holds.

Properties of Galois insertions (2)

For a given Galois connection (L, α, γ, M), the following claims are equivalent:

- (L, α, γ, M) is a Galois insertion,

Properties of Galois insertions (2)

For a given Galois connection (L, α, γ, M), the following claims are equivalent:

- (L, α, γ, M) is a Galois insertion,
- α is surjective,

$$\forall m \in M : \exists \ell \in L : \alpha(\ell) = m$$

Properties of Galois insertions (2)

For a given Galois connection (L, α, γ, M), the following claims are equivalent:

- (L, α, γ, M) is a Galois insertion,
- α is surjective,

$$\forall m \in M : \exists \ell \in L : \alpha(\ell) = m$$

- γ is injective,

$$\forall m_1, m_2 \in M : \gamma(m_1) = \gamma(m_2) \Rightarrow m_1 = m_2$$

Properties of Galois insertions (2)

For a given Galois connection (L, α, γ, M), the following claims are equivalent:

- (L, α, γ, M) is a Galois insertion,
- α is surjective,

$$\forall m \in M : \exists \ell \in L : \alpha(\ell) = m$$

- γ is injective,

$$\forall m_1, m_2 \in M : \gamma(m_1) = \gamma(m_2) \Rightarrow m_1 = m_2$$

- γ is an order-similarity

$$\forall m_1, m_2 \in M : \gamma(m_1) \sqsubseteq \gamma(m_2) \Leftrightarrow m_1 \sqsubseteq m_2$$

(γ preserves lattice ordering)

Construction of Galois insertions

It is always possible to construct a Galois insertion from an existing Galois connection.

Proof.

By construction:

Construction of Galois insertions

It is always possible to construct a Galois insertion from an existing Galois connection.

Proof.

By construction:

- Introduce a *reduction operator* $\varsigma : M \to M$ with:

$$\varsigma(m) = \sqcap \{m' | \gamma(m) = \gamma(m')\}$$

Construction of Galois insertions

It is always possible to construct a Galois insertion from an existing Galois connection.

Proof.

By construction:

- Introduce a *reduction operator* $\varsigma : M \to M$ with:

$$\varsigma(m) = \sqcap \{m' | \gamma(m) = \gamma(m')\}$$

- Construct a complete lattice from ς and M:

$$\varsigma[M] = (\{\varsigma(m) | m \in M\}, \sqsubseteq_M)$$

Construction of Galois insertions

It is always possible to construct a Galois insertion from an existing Galois connection.

Proof.

By construction:

- Introduce a *reduction operator* $\varsigma : M \to M$ with:

$$\varsigma(m) = \sqcap \{m' | \gamma(m) = \gamma(m')\}$$

- Construct a complete lattice from ς and M:

$$\varsigma[M] = (\{\varsigma(m) | m \in M\}, \sqsubseteq_M)$$

Then, $(L, \alpha, \gamma, \varsigma[M])$ is a Galois insertion, by definition. □

Systematic Design of Galois connections

Systematic Design of Galois connections

$\Rightarrow$ Topic of next seminar

Literature

Chapter 4.3 (Galois connections, p.233 - 246) of [1]:

Flemming Nielson, Hanne R. Nielson, and Chris Hankin.
Principles of Program Analysis.
Springer Publishing Company, Incorporated, 2010.