Abstract Interpretation

So far:

- we did not formally relate to the semantics of programs
- we did not formally relate the precision of the analyses

Now: formalize the notion of approximation in a unified framework

Abstract interpretation (Cousot & Cousot’79)

- theory of approximating sets and set operations
- formulated in mathematical (application independent) setting
- provides rigorous correctness guarantees for analyses
- allows for trade-off between precision and complexity
Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices. A pair \((\alpha, \gamma)\) of monotonic functions \(\alpha : L \to M\) and \(\gamma : M \to L\) is called a Galois connection, written \(L \xleftarrow[\alpha]{} M\), if it satisfies the conditions:

\[(G1) \quad \forall l \in L : l \leq_L \gamma(\alpha(l))\]
\[(G2) \quad \forall m \in M : \alpha(\gamma(m)) \leq_M m\]

\(\alpha : L \to M\) is an abstraction function

\(\gamma : M \to L\) is a concretization function
Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices. A pair \((\alpha, \gamma)\) of monotonic functions \(\alpha : L \to M\) and \(\gamma : M \to L\) is called a **Galois connection**, written \(L \xrightarrow{\gamma} M\), if it satisfies the conditions:

\[
\begin{align*}
\text{(G1)} & \quad \forall l \in L : \ l \leq_L \gamma(\alpha(l)) \\
\text{(G2)} & \quad \forall m \in M : \ \alpha(\gamma(m)) \leq_M m
\end{align*}
\]

**Example**

\((L, \leq_L) = (\mathcal{P}(V), \subseteq)\), where \(V\) is a set of concrete values

\((M, \leq_M) = (\mathcal{P}(A), \subseteq)\), where \(A\) is a set of abstract values

\[
\begin{array}{c}
\text{V} \\
\gamma(\alpha(l)) \\
\alpha(l) \\
\end{array}
\]

\[
\begin{array}{c}
\text{A} \\
\alpha(l) \\
\end{array}
\]

\(l \subseteq \gamma(\alpha(l))\): overapproximation
Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices. A pair \((\alpha, \gamma)\) of monotonic functions \(\alpha : L \to M\) and \(\gamma : M \to L\) is called a **Galois connection**, written \(L \xrightarrow{\gamma} \xleftarrow{\alpha} M\), if it satisfies the conditions:

(G1) \(\forall l \in L : l \leq_L \gamma(\alpha(l))\)

(G2) \(\forall m \in M : \alpha(\gamma(m)) \leq_M m\)

**Example**

\(L = \mathcal{P}(V)\), where \(V\) is a set of concrete values

\(M = \mathcal{P}(A)\), where \(A\) is a set of abstract values
Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices. A pair \((\alpha, \gamma)\) of monotonic functions \(\alpha : L \rightarrow M\) and \(\gamma : M \rightarrow L\) is called a Galois connection, written \(L \xrightarrow[\alpha\gamma]{} M\), if it satisfies the conditions:

1. *(G1)* \(\forall l \in L : \ l \leq_L \gamma(\alpha(l))\)
2. *(G2)* \(\forall m \in M : \ \alpha(\gamma(m)) \leq_M m\)

When \(l \neq \gamma(\alpha(l))\), we lose information by abstraction of \(l\).

If \(\alpha(\gamma(m)) = m\) for all \(m \in M\), \(L \xleftarrow[\alpha\gamma]{} M\) is a Galois insertion.
Galois connection: example

$(L, \leq_L) = (\mathcal{P}(\mathbb{Z}), \subseteq)$: concrete domain of all subsets of $\mathbb{Z}$

$(M, \leq_M) = (I \cup \{\bot\}, \sqsubseteq)$: abstract domain of intervals, where

$I = \{[l, h] \mid l, h \in \mathbb{Z} \cup \{-\infty, +\infty\} \land l \leq h\}$

We define a Galois connection $L \xleftarrow{\alpha} \xrightarrow{\gamma} M$ as follows:

for $Z \subseteq \mathbb{Z}$

$$\alpha(Z) := \begin{cases} \bot & \text{if } Z = \emptyset \\ [\inf(Z), \sup(Z)] & \text{if } Z \neq \emptyset \end{cases}$$

for $m \in I \cup \{\bot\}$

$$\gamma(m) := \begin{cases} \emptyset & \text{if } m = \bot \\ \{z \in \mathbb{Z} \mid l \leq z \leq h\} & \text{if } m = [l, h] \end{cases}$$
Properties of Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xrightarrow{\alpha} \gamma \xleftarrow{\alpha} M\) be a Galois connection.

**Property 1** For all \(l \in L\) and \(m \in M\) it holds that

\[
\alpha(l) \leq_M m \quad \text{if and only if} \quad l \leq_L \gamma(m).
\]

**Property 2**

a) The concretization function \(\gamma\) is uniquely determined by \(\alpha\):

\[
\gamma(m) = \bigsqcup \{ l \in L \mid \alpha(l) \leq_M m \} \quad \text{for all} \quad m \in M.
\]

b) The abstraction function \(\alpha\) is uniquely determined by \(\gamma\)

\[
\alpha(l) = \bigcap \{ m \in M \mid l \leq_L \gamma(m) \} \quad \text{for all} \quad l \in L.
\]
Properties of Galois connections

Let $(L, \leq_L)$ and $(M, \leq_M)$ be complete lattices and let $L \xrightarrow{\gamma} M \xleftarrow{\alpha} M$ be a Galois connection.

Proof of Property 1

$(\Rightarrow)$ Suppose that $\alpha(l) \leq_M m$. This implies $\gamma(\alpha(l)) \leq_L \gamma(m)$ since $\gamma$ is monotonic. By (G1) we have $l \leq_L \gamma(\alpha(l))$. Then, by transitivity, $l \leq_L \gamma(m)$.

$(\Leftarrow)$ Suppose that $l \leq_L \gamma(m)$. This implies $\alpha(l) \leq_M \alpha(\gamma(m))$ since $\alpha$ is monotonic. By (G2), $\alpha(\gamma(m)) \leq_M m$. Then, by transitivity, $\alpha(l) \leq_M m$. 
Properties of Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\gamma} M \xrightarrow{\alpha} M\) be a Galois connection.

Proof of Property 2 a)

Let \(L' = \{l \in L \mid \alpha(l) \leq_M m\}\).

\((\geq)\) To show that \(\gamma(m) \geq \bigsqcup L'\), we show that \(\gamma(m)\) is an upper bound for \(L'\). Let \(l \in L'\) be arbitrary. We will show \(l \leq_L \gamma(m)\). Since \(l \in L'\), we have \(\alpha(l) \leq_M m\). Then, by Property 1, \(l \leq_L \gamma(m)\).

\((\leq)\) To show that \(\gamma(m) \leq \bigsqcup L'\), we show that \(\gamma(m) \in L'\). From (G2), we have \(\alpha(\gamma(m)) \leq_M m\), and thus, \(\gamma(m) \in L'\).
Properties of Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\alpha} M\) be a Galois connection.

Property 3

a) The abstraction function \(\alpha\) is **completely additive**, i.e.,

\[
\alpha(\bigsqcup L') = \bigsqcup \{\alpha(l) \mid l \in L'\} \text{ for all } L' \subseteq L.
\]

b) The concretization function \(\gamma\) is **completely multiplicative**, i.e.,

\[
\gamma(\bigcap M') = \bigcap \{\gamma(m) \mid m \in M'\} \text{ for all } M' \subseteq M.
\]
Properties of Galois connections

Let $(L, \leq_L)$ and $(M, \leq_M)$ be complete lattices and let $L \xrightarrow{\gamma} M \xleftarrow{\alpha} M$ be a Galois connection.

Proof of Property 3 a)

Consider some $L' \subseteq L$. Let $M' = \{ \alpha(l) \in L \mid l \in L' \}$.

$(\geq)$ To show that $\alpha(\bigvee L') \geq_M \bigvee M'$, we show that $\alpha(\bigvee L')$ is an upper bound for $M'$. Let $l \in L'$. We show that $\alpha(l) \leq_M \alpha(\bigvee L')$. Since $l \leq \bigvee L'$ and $\alpha$ is monotonic, the claim follows.

$(\leq)$ According to Property 1, to show that $\alpha(\bigvee L') \leq_M \bigvee M'$, it suffices to show that $\bigvee L' \leq_L \gamma(\bigvee M')$. For this we show that $\gamma(\bigvee M')$ is an upper bound for $L'$. Let $l \in L'$ be arbitrary. We have $\alpha(l) \leq_M \bigvee M'$. By Property 1, $l \leq_L \gamma(\bigvee M')$. This concludes the proof.
Properties of Galois connections

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\alpha} M\) be a Galois connection.

**Property 4**

a) If \(\alpha' : L \to M\) is completely additive, then \(L \xleftarrow{\gamma'} M\) is a Galois connection, where the function \(\gamma' : M \to L\) is defined as:

\[
\gamma'(m) := \bigsqcup \{l \in L \mid \alpha'(l) \leq_M m\} \text{ for all } m \in M.
\]

b) If \(\gamma' : M \to L\) is completely multiplicative, then \(L \xleftarrow{\alpha'} M\) is a Galois connection, where the function \(\alpha' : L \to M\) is defined as:

\[
\alpha'(l) := \bigsqcap \{m \in M \mid l \leq_L \gamma'(m)\} \text{ for all } l \in L.
\]
Abstraction of functions

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\gamma} \xrightarrow{\alpha} M\) be a Galois connection. Let \(f : L \to L\) be a function.

A function \(f^\# : M \to M\) is an upper approximation to \(f\) if

\[
\alpha(f(\gamma(m))) \leq_M f^\#(m) \quad \text{for all } m \in M,
\]
denoted also \(\alpha \circ f \circ \gamma \leq f^\#\).

The function \(\alpha \circ f \circ \gamma\) is the most precise upper approximation to the function \(f\) in the Galois connection \(L \xleftarrow{\gamma} \xrightarrow{\alpha} M\).
Abstraction of functions

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\alpha} \xrightarrow{\gamma} M\) be a Galois connection. Let \(f : L \to L\) be a function.

A function \(f^\# : M \to M\) is an **upper approximation** to \(f\) if

\[
\alpha(f(\gamma(m))) \leq_M f^\#(m) \quad \text{for all} \quad m \in M,
\]

denoted also \(\alpha \circ f \circ \gamma \leq f^\#\).
Abstraction of functions

Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\gamma} M \xrightarrow{\alpha} M\) be a Galois connection. Let \(f : L \rightarrow L\) be a function.

A function \(f^\# : M \rightarrow M\) is an upper approximation to \(f\) if

\[
\alpha(f(\gamma(m))) \leq_M f^\#(m) \text{ for all } m \in M,
\]

denoted also \(\alpha \circ f \circ \gamma \leq f^\#\).

**Lemma**  If \(f : L \rightarrow L\) and \(f^\# : M \rightarrow M\) are monotonic, then

\[
\alpha \circ f \circ \gamma \leq f^\# \text{ if and only if } \alpha \circ f \leq f^\# \circ \alpha.
\]
Proof of the Lemma

(⇒) Let \( l \in L \).
Applying \( \alpha \circ f \circ \gamma \leq f^\# \) with \( \alpha(l) \) we get
\[ \alpha(f(\gamma(\alpha(l)))) \leq_M f^\#(\alpha(l)). \]
By (G1), we have \( l \leq_L \gamma(\alpha(l)) \). Since \( f, \alpha \) are monotonic,
\[ \alpha(f(l)) \leq_L \alpha(f(\gamma(\alpha(l)))) \]
By transitivity, \( \alpha(f(l)) \leq_M f^\#(\alpha(l)) \).

(⇐) Let \( m \in M \).
Applying \( \alpha \circ f \leq f^\# \circ \alpha \) with \( \gamma(m) \) we get
\[ \alpha(f(\gamma(m))) \leq_M f^\#(\alpha(\gamma(m))). \]
By (G2) we have \( \alpha(\gamma(m)) \leq_M m \). Since \( f^\# \) is monotonic, we get
\[ f^\#(\alpha(\gamma(m))) \leq_M f^\#(m). \]
By transitivity \( \alpha(f(\gamma(m))) \leq_M f^\#(m) \).
Abstraction of fixpoints

**Lemma** Let \((L, \leq_L)\) and \((M, \leq_M)\) be complete lattices and let \(L \xleftarrow{\gamma} \xrightarrow{\alpha} M\) be a Galois connection. Let \(f : L \to L\) and \(f^\# : M \to M\) be monotonic functions such that \(\alpha \circ f \circ \gamma \leq f^\#\). Then, it holds that

\[
\text{lfp}(f) \leq_L \gamma(\text{lfp}(f^\#))
\]

and

\[
\alpha(\text{lfp}(f)) \leq_M \text{lfp}(f^\#).
\]
Proof of the Lemma

We first show that $\text{lfp}(f) \leq L \gamma(\text{lfp}(f^\#))$.

By Tarski’s theorem (see Lecture 1) we have

$$
\text{lfp}(f) = \bigsqcap \{ l \mid f(l) \leq L l \}
$$

$$
\text{lfp}(f^\#) = \bigsqcap \{ m \mid f^\#(m) \leq M m \}
$$

From the second equation we get

$$
\gamma(\text{lfp}(f^\#)) = \gamma(\bigsqcap \{ m \mid f^\#(m) \leq M m \})
$$

$$
= \bigsqcap \{ \gamma(m) \mid f^\#(m) \leq M m \} \quad \text{by Property 3 b)}
$$

Thus, it suffices to show that

$$
\bigsqcap \{ l \mid f(l) \leq L l \} \leq L \bigsqcap \{ \gamma(m) \mid f^\#(m) \leq M m \}.
$$

For this we show that $\{ \gamma(m) \mid f^\#(m) \leq M m \} \subseteq \{ l \mid f(l) \leq L l \}$. 

Proof of the Lemma (continued)

We show that \( \{ \gamma(m) \mid f^\#(m) \leq_M m \} \subseteq \{ l \mid f(l) \leq_L l \} \).

Let \( m \in M \) be such that \( f^\#(m) \leq_M m \).

By \( \alpha \circ f \circ \gamma \leq f^\# \) we have \( \alpha(f(\gamma(m))) \leq f^\#(m) \).

Thus, by transitivity, \( \alpha(f(\gamma(m))) \leq m \).

By Property 1, \( f(\gamma(m)) \leq \gamma(m) \), which implies \( \gamma(m) \in \{ l \mid f(l) \leq_L l \} \), completing the proof.

To see that \( \alpha(\text{lfp}(f)) \leq_M \text{lfp}(f^\#) \), apply Property 1 with \( \text{lfp}(f) \leq_L \gamma(\text{lfp}(f^\#)) \).
Systematic construction of Galois connections

- Use functions that map concrete values to properties (extraction functions) to define Galois connections

- Develop program analysis in stages: functional (sequential) composition of Galois connections

- Develop program analysis in modular way: parallel composition of Galois connections
Galois connections defined by extraction functions

Let \((M, \leq_M)\) be a complete lattice and let \(\beta : V \to M\) be a function from some set \(V\) to \(M\). The function \(\beta\) gives rise to a Galois connection \(\mathcal{P}(V) \xrightleftharpoons{\alpha}{\gamma} M\) where \(\alpha\) and \(\gamma\) are defined by:

\[
\alpha(V') := \bigsqcup \{\beta(v) \mid v \in V'\} \text{ for } V' \in \mathcal{P}(V)
\]

\[
\gamma(m) := \{v \in V \mid \beta(v) \leq_M m\} \text{ for } m \in M
\]

(\(\alpha\) is monotonic) Let \(V_1 \subseteq V_2 \subseteq V\). Clearly \(\{\beta(v) \mid v \in V_1\} \subseteq \{\beta(v) \mid v \in V_2\}\), which implies \(\alpha(V_1) \leq_M \alpha(V_2)\).

(\(\gamma\) is monotonic) Let \(m_1 \leq_M m_2\). Clearly \(\{v \in V \mid \beta(v) \leq_M m_1\} \subseteq \{v \in V \mid \beta(v) \leq_M m_2\}\), which is exactly \(\gamma(m_1) \subseteq \gamma(m_2)\).
Galois connections defined by extraction functions

Let \((M, \leq_M)\) be a complete lattice and let \(\beta : V \rightarrow M\) be a function from some set \(V\) to \(M\). The function \(\beta\) gives rise to a Galois connection \(\mathcal{P}(V) \xleftarrow{\gamma} M\) where \(\alpha\) and \(\gamma\) are defined by:

\[
\alpha(V') := \bigsqcup \{ \beta(v) \mid v \in V' \} \text{ for } V' \in \mathcal{P}(V)
\]

\[
\gamma(m) := \{ v \in V \mid \beta(v) \leq_M m \} \text{ for } m \in M
\]

\((G1)\) Consider arbitrary \(V' \in \mathcal{P}(V)\).
Let \(v \in V'\). By the definition of \(\alpha\), we have \(\beta(v) \leq_M \alpha(V')\).
Thus, by the definition of \(\gamma\) applied to \(\alpha(V')\), we have \(v \in \gamma(\alpha(V'))\).
We conclude that \(V' \subseteq \gamma(\alpha(V'))\).
Galois connections defined by extraction functions

Let \((M, \leq_M)\) be a complete lattice and let \(\beta : V \to M\) be a function from some set \(V\) to \(M\). The function \(\beta\) gives rise to a Galois connection \(\mathcal{P}(V) \xrightarrow{\gamma} M\) where \(\alpha\) and \(\gamma\) are defined by:

\[
\alpha(V') := \bigsqcup \{\beta(v) \mid v \in V'\} \text{ for } V' \in \mathcal{P}(V)
\]

\[
\gamma(m) := \{v \in V \mid \beta(v) \leq_M m\} \text{ for } m \in M
\]

(G2) Consider arbitrary \(m \in M\).

By the definition of \(\gamma\), we have that \(m\) is an upper bound for the set \(\{\beta(v) \mid v \in \gamma(m)\}\). By the definition of \(\alpha\), we have that \(\alpha(\gamma(m))\) is the least upper bound of this set.

We conclude that \(\alpha(\gamma(m)) \leq_M m\).
Let $(M, \leq_M)$ be a complete lattice and let $\beta : V \to M$ be a function from some set $V$ to $M$. The function $\beta$ gives rise to a Galois connection $\mathcal{P}(V) \xleftarrow{\gamma} \xrightarrow{\alpha} M$ where $\alpha$ and $\gamma$ are defined by:

$$\alpha(V') := \bigsqcup \{\beta(v) \mid v \in V'\} \text{ for } V' \in \mathcal{P}(V)$$

$$\gamma(m) := \{v \in V \mid \beta(v) \leq_M m\} \text{ for } m \in M$$

Remark: Another way to establish (G1) and (G2) is to show that:

- The functions $\alpha$ and $\gamma$ defined above satisfy Property 1.
- Any pair of functions between complete lattices that satisfies Property 1 forms a Galois connection.
Galois connections defined by extraction functions

Important special case: \((M, \leq) = (\mathcal{P}(A), \subseteq)\) and we have an extraction function \(\eta : V \rightarrow A\). We define \(\beta_\eta : V \rightarrow \mathcal{P}(A)\) by

\[
\beta_\eta(v) := \{\eta(v)\}.
\]

This gives us the Galois connection \(\mathcal{P}(V) \xleftarrow{\gamma_\eta} \xrightarrow{\alpha_\eta} \mathcal{P}(A)\) where

\[
\alpha_\eta(V') = \bigcup \{\beta_\eta(v) \mid v \in V'\} = \{\eta(v) \mid v \in V'\}
\]
\[
\gamma_\eta(A') = \{v \in V \mid \beta_\eta(v) \subseteq A'\} = \{v \in V \mid \eta(v) \in A'\}.
\]
Consider the extraction functions $\text{sign} : \mathbb{Z} \to \{-, 0, +\}$ and $\text{parity} : \mathbb{Z} \to \{e, o\} = \{\text{even}, \text{odd}\}$ defined by

$$\text{sign}(z) = \begin{cases} - & \text{if } z < 0 \\ 0 & \text{if } z = 0 \\ + & \text{if } z > 0 \end{cases}$$

$$\text{parity}(z) = \begin{cases} e & \text{if } z = 0 \mod 2 \\ o & \text{if } z = 1 \mod 2 \end{cases}$$

These functions define Galois connections

$$\mathcal{P}(\mathbb{Z}) \xrightarrow{\gamma_{\text{sign}}} \mathcal{P}(\{-, 0, +\})$$

$$\mathcal{P}(\mathbb{Z}) \xrightarrow{\alpha_{\text{sign}}} \mathcal{P}(\{+\})$$

$$\mathcal{P}((\mathbb{Z}, \cdot)) \xrightarrow{\gamma_{\text{parity}}} \mathcal{P}(\{e, o\})$$

$$\mathcal{P}((\mathbb{Z}, \cdot)) \xrightarrow{\alpha_{\text{parity}}} \mathcal{P}(\{e, o\})$$