

AAA616: Program Analysis

Lecture 6 — Abstract Interpretation Framework

Hakjoo Oh
2025 Fall

Step 1: Define Concrete Semantics

The concrete semantics describes the real executions of the program.
Described by semantic domain and function.

- A *semantic domain* D , which is a CPO:
 - ▶ D is a partially ordered set with a least element \perp .
 - ▶ Any increasing chain $d_0 \sqsubseteq d_1 \sqsubseteq \dots$ in D has a least upper bound $\bigsqcup_{n \geq 0} d_n$ in D .
- A *semantic function* $F : D \rightarrow D$, which is continuous: for all chains $d_0 \sqsubseteq d_1 \sqsubseteq \dots$,

$$F\left(\bigsqcup_{n \geq 0} d_i\right) = \bigsqcup_{n \geq 0} F(d_n).$$

Then, the concrete semantics (or collecting semantics) is defined as the least fixed point of *semantic function* $F : D \rightarrow D$:

$$fix F = \bigsqcup_{i \in \mathbb{N}} F^i(\perp).$$

Step 2: Define Abstract Semantics

Define the abstract semantics of the input program.

- Define an *abstract semantic domain* CPO \hat{D} .
 - ▶ Intuition: \hat{D} is an abstraction of D
- Define an *abstract semantic function* $\hat{F} : \hat{D} \rightarrow \hat{D}$.
 - ▶ Intuition: \hat{F} is an abstraction of F .
 - ▶ \hat{F} must be monotone:

$$\forall \hat{x}, \hat{y} \in \hat{D}. \hat{x} \sqsubseteq \hat{y} \implies \hat{F}(\hat{x}) \sqsubseteq \hat{F}(\hat{y})$$

$$(\text{or extensive: } \forall x \in \hat{D}. x \sqsubseteq \hat{F}(x))$$

Then, static analysis is to compute an upper bound of:

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\perp)$$

How can we ensure that the result soundly approximate the concrete semantics?

Requirement 1: Galois Connection

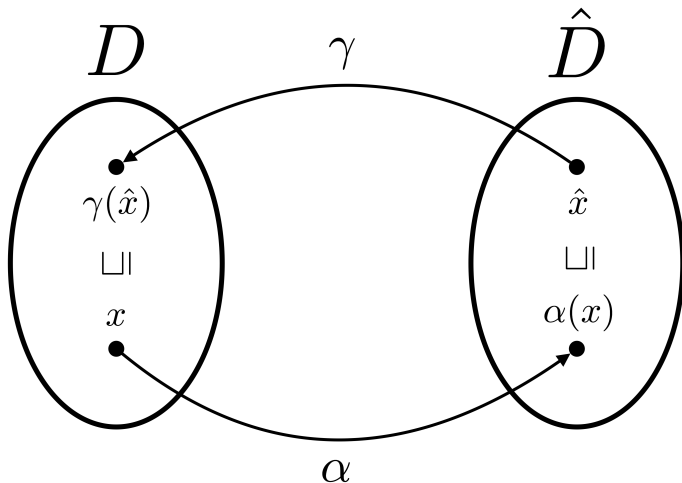
D and \hat{D} must be related with Galois-connection:

$$D \xrightleftharpoons[\alpha]{\gamma} \hat{D}$$

That is, we have

- *abstraction function*: $\alpha \in D \rightarrow \hat{D}$
 - ▶ represents elements in D as elements of \hat{D}
- *concretization function*: $\gamma \in \hat{D} \rightarrow D$
 - ▶ gives the meaning of elements of \hat{D} in terms of D
- $\forall x \in D, \hat{x} \in \hat{D}. \alpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$
 - ▶ α and γ respect the orderings of D and \hat{D}
 - ▶ If an element $x \in D$ is safely described by $\hat{x} \in \hat{D}$, i.e., $\alpha(x) \sqsubseteq \hat{x}$, then the element described by \hat{x} is also safe w.r.t. x , i.e., $x \sqsubseteq \gamma(\hat{x})$

Galois-Connection



Example: Sign Abstraction

$$\wp(\mathbb{Z}) \xleftrightarrow[\alpha]{\gamma} (\{\perp, +, 0, -, \top\}, \sqsubseteq)$$

$$\alpha(Z) = \begin{cases} \perp & Z = \emptyset \\ + & \forall z \in Z. z > 0 \\ 0 & Z = \{0\} \\ - & \forall z \in Z. z < 0 \\ \top & \text{otherwise} \end{cases}$$

$$\gamma(\perp) = \emptyset$$

$$\gamma(\top) = \mathbb{Z}$$

$$\gamma(+)= \{z \in \mathbb{Z} \mid z > 0\}$$

$$\gamma(0) = \{0\}$$

$$\gamma(-) = \{z \in \mathbb{Z} \mid z < 0\}$$

Example: Interval Abstraction

$$\wp(\mathbb{Z}) \xrightleftharpoons[\alpha]{\gamma} \{\perp\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$

$$\begin{aligned}\gamma(\perp) &= \emptyset \\ \gamma([a, b]) &= \{z \in \mathbb{Z} \mid a \leq z \leq b\}\end{aligned}$$

$$\begin{aligned}\alpha(\emptyset) &= \perp \\ \alpha(X) &= [\min X, \max X]\end{aligned}$$

cf) Alternate Formulation

D and \hat{D} are related with Galois-connection:

$$D \xrightleftharpoons[\alpha]{\gamma} \hat{D}$$

iff (α, γ) satisfies the following conditions:

- α and γ are monotone functions
- $\gamma \circ \alpha$ is extensive, i.e., $\gamma \circ \alpha \sqsupseteq \lambda x.x$
 - ▶ abstraction typically loses precision
 - ▶ $(\gamma \circ \alpha)(\{1, 3\}) = \{1, 2, 3\}$
- $\alpha \circ \gamma$ is reductive: i.e., $\alpha \circ \gamma \sqsubseteq \lambda x.x$
 - ▶ If $\alpha \circ \gamma = \lambda x.x$, Galois-insertion.
 - ▶ With Galois-insertion, no two abstract elements describe the same concrete element, which may be true with Galois-connection.

Proof (\Rightarrow)

If we have a Galois-connection:

$$\forall x \in D, \hat{x} \in \hat{D}. \alpha(x) \sqsubseteq \hat{x} \iff x \sqsubseteq \gamma(\hat{x})$$

then

- $\lambda x.x \sqsubseteq \gamma \circ \alpha$: $\alpha(x) \sqsubseteq \alpha(x)$ and hence $x \sqsubseteq \gamma(\alpha(x))$ by Galois-connection.
- $\alpha \circ \gamma \sqsubseteq \lambda x.x$: $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{x})$ and hence $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{x}$ by Galois-connection.
- γ is monotone: if $\hat{x} \sqsubseteq \hat{y}$, then $\alpha(\gamma(\hat{x})) \sqsubseteq \hat{y}$. Hence $\gamma(\hat{x}) \sqsubseteq \gamma(\hat{y})$ by Galois-connection.
- α is monotone: if $x \sqsubseteq y$, then $x \sqsubseteq \gamma(\alpha(y))$. Hence $\alpha(x) \sqsubseteq \alpha(y)$ by Galois-connection.

Proof (\Leftarrow)

- Assume $\alpha(x) \sqsubseteq \hat{x}$. Since γ is monotone, $\gamma(\alpha(x)) \sqsubseteq \gamma(\hat{x})$.
Because $\gamma \circ \alpha$ is extensive, we have $x \sqsubseteq \gamma(\hat{x})$.
- Assume $x \sqsubseteq \gamma(\hat{x})$. Since α is monotone, $\alpha(x) \sqsubseteq \alpha(\gamma(\hat{x}))$.
Because $\alpha \circ \gamma$ is reductive, we have $\alpha(x) \sqsubseteq \hat{x}$.

Properties of Galois-Connection (1)

Given $D \xleftrightarrow[\alpha]{\gamma} \hat{D}$, we have:

- $\gamma \circ \alpha \circ \gamma = \gamma$
 - ▶ From $\alpha \circ \gamma \sqsubseteq \lambda x.x$ and monotonicity of γ , we have $\gamma \circ \alpha \circ \gamma \sqsubseteq \gamma$.
We have $\gamma \circ \alpha \circ \gamma \sqsupseteq \gamma$ from $\gamma \circ \alpha \sqsupseteq \lambda x.x$.
- $\alpha \circ \gamma \circ \alpha = \alpha$
- $\alpha \circ \gamma$ and $\gamma \circ \alpha$ are idempotent:

$$(\alpha \circ \gamma)^2 = \alpha \circ \gamma, (\gamma \circ \alpha)^2 = \gamma \circ \alpha$$

- γ uniquely determines α (D, \hat{D} complete lattices):

$$\alpha(d) = \bigsqcap \{\hat{d} \mid d \sqsubseteq \gamma(\hat{d})\}$$

which implies that $\alpha(d)$ is the best abstraction of d .

- α uniquely determines γ :

$$\gamma(\hat{d}) = \bigsqcup \{d \mid \alpha(d) \sqsubseteq \hat{d}\}$$

Properties of Galois-Connection (2)

- α is strict, i.e., $\alpha(\perp) = \hat{\perp}$. Proof. From $\perp \sqsubseteq \gamma(\hat{\perp})$, we have $\alpha(\perp) \sqsubseteq \hat{\perp}$ by Galois-connection.
- α is continuous: for any chain S in D ,

$$\alpha\left(\bigsqcup_{x \in S} x\right) = \bigsqcup_{x \in S} \alpha(x).$$

Proof. Since α is monotonic,

$$\bigsqcup_{x \in S} \alpha(x) \sqsubseteq \alpha\left(\bigsqcup_{x \in S} x\right).$$

Since $\lambda x.x \sqsubseteq \gamma \circ \alpha$ and γ is monotonic,

$$\bigsqcup_{x \in S} x \sqsubseteq \bigsqcup_{x \in S} \gamma(\alpha(x)) \sqsubseteq \gamma\left(\bigsqcup_{x \in S} \alpha(x)\right)$$

By Galois-connection, we have

$$\alpha\left(\bigsqcup_{x \in S} x\right) \sqsubseteq \bigsqcup_{x \in S} \alpha(x)$$

Deriving Galois-Connections

- Pointwise lifting: Given $D \xleftrightarrow[\alpha]{\gamma} \hat{D}$ and a set S , then

$$S \rightarrow D \xleftrightarrow[\alpha']{\gamma'} S \rightarrow \hat{D}$$

with $\alpha'(f) = \lambda s \in S. \alpha(f(s))$ and $\gamma(f) = \lambda s \in S. \gamma(f(s))$.

- Composition: Given $X_1 \xleftrightarrow[\alpha_1]{\gamma_1} X_2 \xleftrightarrow[\alpha_2]{\gamma_2} X_3$, we have

$$X_1 \xleftrightarrow[\alpha_2 \circ \alpha_1]{\gamma_1 \circ \gamma_2} X_3$$

Requirement 2: \hat{F} and F

- \hat{F} is a sound abstraction of F :

$$F \circ \gamma \sqsubseteq \gamma \circ \hat{F} \quad (\alpha \circ F \sqsubseteq \hat{F} \circ \alpha)$$

- or, alternatively,

$$\alpha(x) \sqsubseteq \hat{x} \implies \alpha(F(x)) \sqsubseteq \hat{F}(\hat{x})$$

Best Abstract Semantics

From $D \xleftrightarrow[\alpha]{\gamma} \hat{D}$ and $F \circ \gamma \sqsubseteq \gamma \circ \hat{F}$, we have

$$\begin{aligned} \alpha \circ F \circ \gamma &\sqsubseteq \alpha \circ \gamma \circ \hat{F} && \alpha \text{ is monotone} \\ &\sqsubseteq \hat{F} && \alpha \circ \gamma \sqsubseteq \lambda x.x \end{aligned}$$

The result means that $\alpha \circ F \circ \gamma$ is the best abstraction of F and any sound abstraction \hat{F} of F is greater than $\alpha \circ F \circ \gamma$.

Composition

When F, F' are concrete operators and \hat{F}, \hat{F}' are abstract operators, if \hat{F} and \hat{F}' are sound abstractions of F and F' , respectively, then $\hat{F} \circ \hat{F}'$ is a sound abstraction of $F \circ F'$.

Fixpoint Transfer Theorems

Theorem (Fixpoint Transfer)

Let D and \hat{D} be related by Galois-connection $D \stackrel{\gamma}{\underset{\alpha}{\rightleftarrows}} \hat{D}$. Let $F : D \rightarrow D$ be a continuous function and $\hat{F} : \hat{D} \rightarrow \hat{D}$ be a monotone function such that $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$. Then,

$$\alpha(\text{fix } F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}).$$

Theorem (Fixpoint Transfer2)

Let D and \hat{D} be related by Galois-connection $D \stackrel{\gamma}{\underset{\alpha}{\rightleftarrows}} \hat{D}$. Let $F : D \rightarrow D$ be a continuous function and $\hat{F} : \hat{D} \rightarrow \hat{D}$ be a monotone function such that $\alpha(x) \sqsubseteq \hat{x} \implies \alpha(F(x)) \sqsubseteq \hat{F}(\hat{x})$. Then,

$$\alpha(\text{fix } F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}).$$

Proof of Fixpoint Transfer

- From $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$, we can derive

$$\forall n \in \mathbb{N}. \alpha \circ F^n \sqsubseteq \hat{F}^n \circ \alpha \quad (\forall n \in \mathbb{N}. \alpha(F^n(\perp)) \sqsubseteq \hat{F}^n(\hat{\perp}))$$

by induction as follows:

$$\begin{aligned} \alpha \circ F^{n+1} &= \alpha \circ F \circ F^n \\ &\sqsubseteq \alpha \circ F \circ \gamma \circ \alpha \circ F^n \quad \dots \alpha \circ F \text{ is mono. and } \lambda x.x \sqsubseteq \gamma \circ \alpha \\ &\sqsubseteq \alpha \circ F \circ \gamma \circ \hat{F}^n \circ \alpha \quad \dots \alpha \circ F \circ \gamma \text{ is mono. and by I.H.} \\ &\sqsubseteq \hat{F} \circ \hat{F}^n \circ \alpha \quad \dots \alpha \circ F \circ \gamma \sqsubseteq \hat{F} \end{aligned}$$

- Since α, F, \hat{F} are monotone, $\{\alpha(F^i(\perp))\}_i$ and $\{\hat{F}^i(\hat{\perp})\}_i$ are chains, and

$$\bigsqcup_{i \in \mathbb{N}} \alpha(F^i(\perp)) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}) \quad (1)$$

- Since α and F are continuous,

$$\bigsqcup_{i \in \mathbb{N}} \alpha(F^i(\perp)) = \alpha(\bigsqcup_{i \in \mathbb{N}} (F^i(\perp))) = \alpha(\text{fix } F)$$

By replacing the left-hand side of (1), we have

$$\alpha(\text{fix } F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp})$$

Computing $\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp})$

- If the abstract domain \hat{D} has finite height (i.e., all chains are finite), we can directly calculate

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}).$$

- If the domain \hat{D} has infinite height, the computation may not terminate. In this case, we find a finite chain $\hat{X}_0 \sqsubseteq \hat{X}_1 \sqsubseteq \hat{X}_2 \sqsubseteq \dots$ such that

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}) \sqsubseteq \lim_{i \in \mathbb{N}} \hat{X}_i$$

Fixpoint Accerlation with Widening

Define finite chain \hat{X}_i by an widening operator $\nabla : \hat{D} \times \hat{D} \rightarrow \hat{D}$:

$$\begin{aligned}\hat{X}_0 &= \perp \\ \hat{X}_i &= \hat{X}_{i-1} && \text{if } \hat{F}(\hat{X}_{i-1}) \sqsubseteq \hat{X}_{i-1} \\ &= \hat{X}_{i-1} \nabla \hat{F}(\hat{X}_{i-1}) && \text{otherwise}\end{aligned} \quad (2)$$

Conditions on ∇ :

- $\forall a, b \in \hat{D}. (a \sqsubseteq a \nabla b) \wedge (b \sqsubseteq a \nabla b)$
- For all increasing chains $(x_i)_i$, the increasing chain $(y_i)_i$ defined as

$$y_i = \begin{cases} x_0 & \text{if } i = 0 \\ y_{i-1} \nabla x_i & \text{if } i > 0 \end{cases}$$

eventually stabilizes (i.e., the chain is finite).

Decreasing Iterations with Narrowing

- We can refine the widening result $\lim_{i \in \mathbb{N}} \hat{X}_i$ by a narrowing operator $\Delta : \hat{D} \times \hat{D} \rightarrow \hat{D}$.
- Compute chain $(\hat{Y}_i)_i$

$$\hat{Y}_i = \begin{cases} \lim_{i \in \mathbb{N}} \hat{X}_i & \text{if } i = 0 \\ \hat{Y}_{i-1} \Delta \hat{F}(\hat{Y}_{i-1}) & \text{if } i > 0 \end{cases} \quad (3)$$

- Conditions on Δ
 - ▶ $\forall a, b \in \hat{D}. a \sqsubseteq b \implies a \sqsubseteq a \Delta b \sqsubseteq b$
 - ▶ For all decreasing chain $(x_i)_i$, the decreasing chain $(y_i)_i$ defined as

$$y_i = \begin{cases} x_i & \text{if } i = 0 \\ y_{i-1} \Delta x_i & \text{if } i > 0 \end{cases}$$

eventually stabilizes.

Safety of Widening and Narrowing

Theorem (Widening's Safety)

Let \hat{D} be a CPO, $\hat{F} : \hat{D} \rightarrow \hat{D}$ a monotone function, $\nabla : \hat{D} \times \hat{D} \rightarrow \hat{D}$ a widening operator. Then, chain $(\hat{X}_i)_i$ defined as (2) eventually stabilizes and

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}) \sqsubseteq \lim_{i \in \mathbb{N}} \hat{X}_i.$$

Theorem (Narrowing's Safety)

Let \hat{D} be a CPO, $\hat{F} : \hat{D} \rightarrow \hat{D}$ a monotone function, $\Delta : \hat{D} \times \hat{D} \rightarrow \hat{D}$ a narrowing operator. Then, chain $(\hat{Y}_i)_i$ defined as (3) eventually stabilizes and

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\hat{\perp}) \sqsubseteq \lim_{i \in \mathbb{N}} \hat{Y}_i.$$

Proof of Widening's Safety

- We first show that $\{\hat{F}(\hat{X}_i)\}_i$ is an increasing chain (if so, by the second condition of widening, the widening sequence $\{\hat{X}_i\}_i$ eventually stabilizes). Note that, by (2), $\hat{F}(\hat{X}_{i+1})$ is either $\hat{F}(\hat{X}_i)$ or $\hat{F}(\hat{X}_i \nabla \hat{F}(\hat{X}_i))$. Since $\hat{X}_i \sqsubseteq \hat{X}_i \nabla \hat{F}(\hat{X}_i)$ and \hat{F} is monotone, for all i we have

$$\hat{F}(\hat{X}_i) \sqsubseteq \hat{F}(\hat{X}_{i+1})$$

- We next show that $\forall i \in \mathbb{N}. \hat{F}^i(\hat{\perp}) \sqsubseteq \hat{X}_i$.
 - ▶ Base case. $\hat{F}^0(\hat{\perp}) = \hat{\perp} \sqsubseteq \hat{X}_0$.
 - ▶ Inductive case. From the induction hypothesis (I.H.), i.e., $\hat{F}^i(\hat{\perp}) \sqsubseteq \hat{X}_i$, and the monotonicity of \hat{F} , we have

$$\hat{F}^{i+1}(\hat{\perp}) \sqsubseteq \hat{F}(\hat{X}_i) \tag{4}$$

There are two cases to consider:

- ① When $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i$ and $\hat{X}_{i+1} = \hat{X}_i$: we have $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$ and therefore $\hat{F}^{i+1}(\hat{\perp}) \sqsubseteq \hat{X}_{i+1}$.
- ② When $\hat{F}(\hat{X}_i) \not\sqsubseteq \hat{X}_i$ and $\hat{X}_{i+1} = \hat{X}_i \nabla \hat{F}(\hat{X}_i)$: by the condition of ∇ , $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_i \nabla \hat{F}(\hat{X}_i) = \hat{X}_{i+1}$. Thus, $\hat{F}(\hat{X}_i) \sqsubseteq \hat{X}_{i+1}$ for all $i \in \mathbb{N}$. By (4), we have $\hat{F}^{i+1}(\hat{\perp}) \sqsubseteq \hat{X}_{i+1}$.

Proof of Narrowing's Safety

- We first show that $\{\hat{F}(\hat{Y}_i)\}_i$ is a decreasing chain (if so, by the second condition of narrowing, the narrowing sequence $\{\hat{Y}_i\}_i$ eventually stabilizes). We can show that $\{\hat{F}(\hat{Y}_i)\}_i$ is a decreasing chain by showing the following

$$\forall i \in \mathbb{N}. \hat{Y}_i \sqsupseteq \hat{F}(\hat{Y}_i). \quad (5)$$

This is because, from (5), we have $\hat{Y}_i \sqsupseteq \hat{Y}_i \triangle \hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i)$ and by the mono. of \hat{F} , we have

$$\hat{F}(\hat{Y}_i) \sqsupseteq \hat{F}(\hat{Y}_i \triangle \hat{F}(\hat{Y}_i)) = \hat{F}(\hat{Y}_{i+1})$$

Proof of (5): exercise.

- We next show that $\forall i \in \mathbb{N}. \hat{F}^i(\hat{\perp}) \sqsubseteq \hat{Y}_i$ by induction (exercise).