Program Analysis

6. Abstract Interpretation (2): Abstract Semantics

Kihong Heo

KAIST

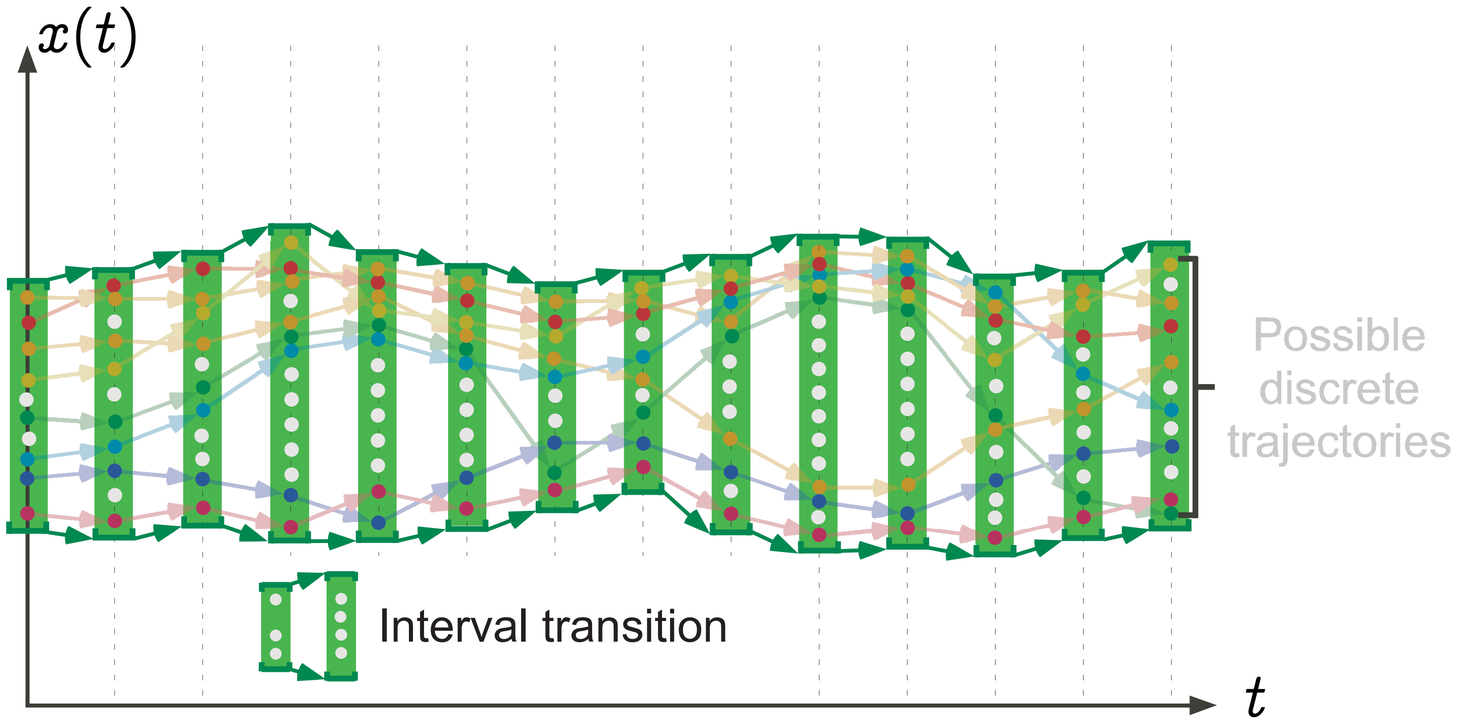
Design of Static Analysis

- Goal: conservative and terminating static analysis
- Design principles:
  - Define concrete semantics
  - Define abstract semantics (sound w.r.t the concrete semantics)
- Computation & implementation:
  - Abstract semantics of a program: the least fixed point of the semantic function
  - Static analyzer: compute the least fixed point within finite time

Step 2: Design Abstract Semantics

- Formalization of **abstract** program executions
  - Soundly subsume concrete executions
- How to subsume: different choices depending on the purposes
  - Some are more expressive than others
- Example: abstraction of {1, 3, 5, 7}
  - Integer, Positive, Odd, [1, 7], etc

Transitions of Abstract States



*from Patrick Cousot's slides

Abstract Semantics

- Define an abstract domain $\mathbb{D}^\sharp$ (CPO)
- Define an abstract semantic function $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ (monotone or extensive)

(Monotone) $\forall x^\sharp, y^\sharp \in \mathbb{D}^\sharp.\ x^\sharp \sqsubseteq y^\sharp \implies F^\sharp(x^\sharp) \sqsubseteq F^\sharp(y^\sharp)$

(Extensive) $\forall x^\sharp \in \mathbb{D}.\ x^\sharp \sqsubseteq F^\sharp(x^\sharp)$

- Static analysis is to compute an upper bound of the chain:

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp)$$

Q. How to ensure that the abstract semantics soundly subsume the concrete semantics?

Requirement 1: Galois Connection (1)

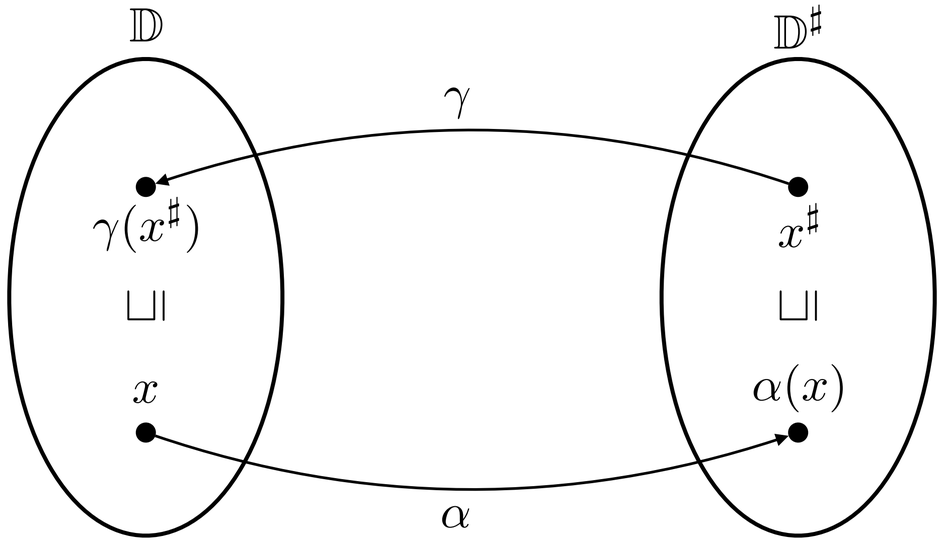
$$\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$$

- $\mathbb{D}$ and $\mathbb{D}^\sharp$ must be related with a Galois connection where
  - Abstraction function: $\alpha \in \mathbb{D} \to \mathbb{D}^\sharp$
  - Concretization function: $\gamma \in \mathbb{D}^\sharp \to \mathbb{D}$

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

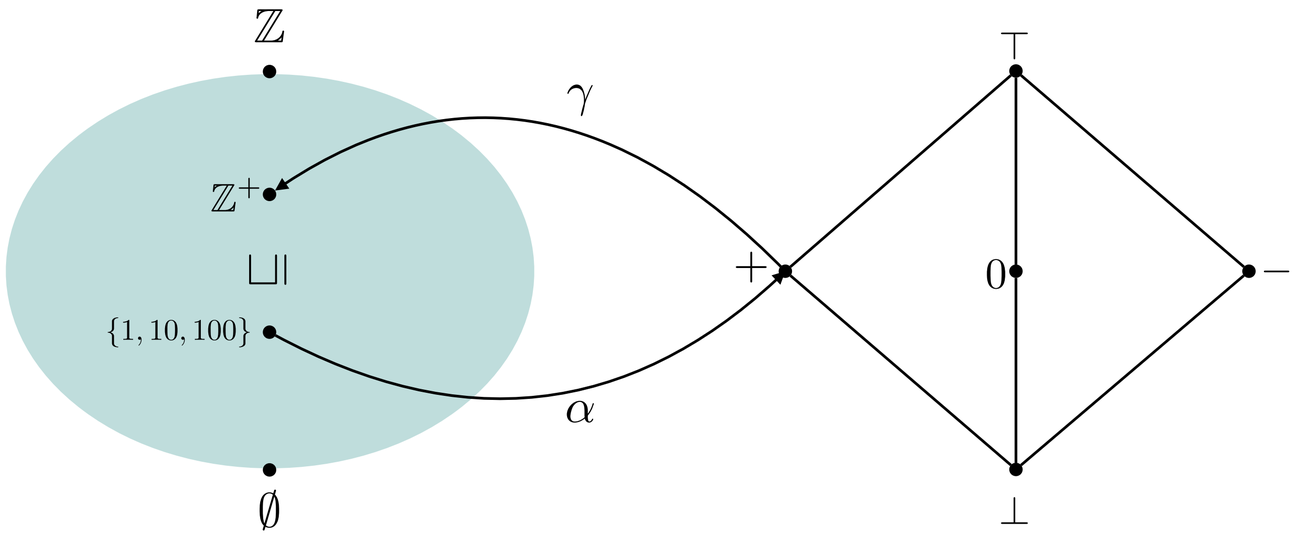
Requirement 1: Galois Connection (2)

- Intuition: order preservation between two semantic domains



Example: Sign Abstraction (1)

$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot, -, 0, +, \top\}$$



Example: Sign Abstraction (2)

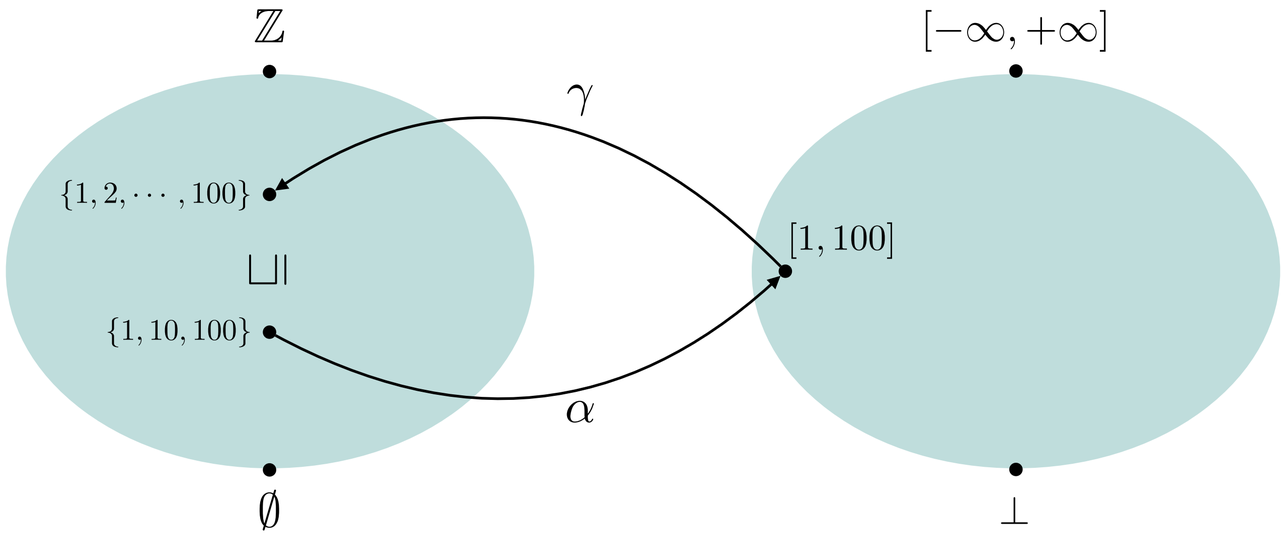
$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot, -, 0, +, \top\}$$

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

$$\gamma(\bot) = \emptyset$$
$$\gamma(+) = \{z \in \mathbb{Z} \mid z > 0\}$$
$$\gamma(0) = \{0\}$$
$$\gamma(-) = \{z \in \mathbb{Z} \mid z < 0\}$$
$$\gamma(\top) = \mathbb{Z}$$

Example: Interval Abstraction (1)

$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot\} \cup \{[a,b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$



Example: Interval Abstraction (2)

$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot\} \cup \{[a,b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$$

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

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

Properties of Galois Connection

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

- $id \sqsubseteq \gamma \circ \alpha$

$$\begin{array}{rrcll} & \alpha(x) & \sqsubseteq & \alpha(x) & \\ \iff & x & \sqsubseteq & \gamma(\alpha(x)) & \text{(by Galois connection)} \end{array}$$

- α is monotone

$$\begin{array}{rrcll} & x & \sqsubseteq & y & \\ \implies & x & \sqsubseteq & \gamma(\alpha(y)) & (id \sqsubseteq \gamma \circ \alpha) \\ \iff & \alpha(x) & \sqsubseteq & \alpha(y) & \text{(by Galois connection)} \end{array}$$

- $\alpha \circ \gamma \sqsubseteq id$

$$\begin{array}{rrcll} & \gamma(x^\sharp) & \sqsubseteq & \gamma(x^\sharp) & \\ \iff & \alpha(\gamma(x^\sharp)) & \sqsubseteq & x^\sharp & \text{(by Galois connection)} \end{array}$$

- γ is monotone

$$\begin{array}{rrcll} & x^\sharp & \sqsubseteq & y^\sharp & \\ \implies & \alpha(\gamma(x^\sharp)) & \sqsubseteq & y^\sharp & (\alpha \circ \gamma \sqsubseteq id) \\ \iff & \gamma(x^\sharp) & \sqsubseteq & \gamma(x^\sharp) & \text{(by Galois connection)} \end{array}$$

Deriving Galois Connections (1)

- Pointwise lifting:

$$\text{Given a Galois connection } \mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp \text{ and a set } \mathbb{S}$$

$$\mathbb{S} \to \mathbb{D} \underset{\alpha'}{\overset{\gamma'}{\leftrightarrows}} \mathbb{S} \to \mathbb{D}^\sharp$$

$$\text{where } \alpha'(f) = \lambda x \in \mathbb{S}.\ \alpha(f(x)) \text{ and } \gamma'(f^\sharp) = \lambda x \in \mathbb{S}.\ \gamma(f^\sharp(x))$$

- Example
  - $\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot, -, 0, +, \top\}$
  - $\mathbb{S} = \{x, y, z\}$

Deriving Galois Connections (2)

- Composition:

$$\text{Given two galois connections } \mathbb{D}_1 \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \mathbb{D}_2 \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{D}_3$$

$$\mathbb{D}_1 \underset{\alpha_2 \circ \alpha_1}{\overset{\gamma_1 \circ \gamma_2}{\leftrightarrows}} \mathbb{D}_3$$

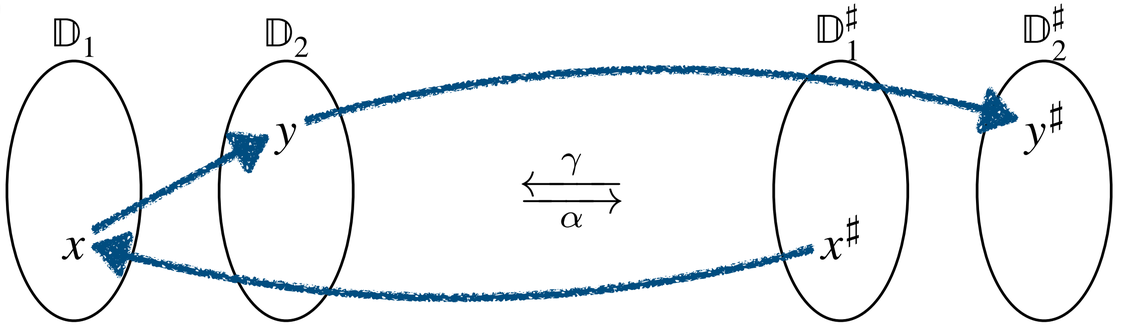
- Example
  - $(\mathbb{S} \to \wp(\mathbb{Z})) \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \wp(\mathbb{Z}) \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \{\bot, -, 0, +, \top\}$

Deriving Galois Connections (3)

Given two Galois connections $\mathbb{D}_1 \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \mathbb{D}_1^\sharp$ and $\mathbb{D}_2 \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{D}_2^\sharp$

- $\mathbb{D}_1 \times \mathbb{D}_2 \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}_1^\sharp \times \mathbb{D}_2^\sharp$ where $\alpha = \lambda\langle x, y\rangle.\langle \alpha_1(x), \alpha_2(y)\rangle$
- $\mathbb{D}_1 + \mathbb{D}_2 \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}_1^\sharp + \mathbb{D}_2^\sharp$ where $\alpha = \lambda x. \begin{cases} \alpha_1(x) & \text{if } x \in \mathbb{D}_1 \\ \alpha_2(x) & \text{if } x \in \mathbb{D}_2 \end{cases}$
- $\mathbb{D}_1 \to \mathbb{D}_2 \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}_1^\sharp \to \mathbb{D}_2^\sharp$ where $\alpha = \lambda f.\alpha_2 \circ f \circ \gamma_1$

(set of monotone functions)



Deriving Galois Connections (4)

Given two Galois connections $\wp(\mathbb{A}) \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \mathbb{D}_1^\sharp$ and $\wp(\mathbb{B}) \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{D}_2^\sharp$

- $\wp(\mathbb{A} \times \mathbb{B}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}_1^\sharp \times \mathbb{D}_2^\sharp$ where $\alpha = \lambda X.\langle \alpha_1(\{a \mid \langle a, b\rangle \in X\}), \alpha_2(\{b \mid \langle a, b\rangle \in X\})\rangle$
- $\wp(\mathbb{A} \times \mathbb{B}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{A}' \to \mathbb{D}_2^\sharp$ where $\alpha = \lambda X.\{a \mapsto \alpha_2(S) \mid \langle a, b\rangle \in X, S = \{b \mid \langle a, b\rangle \in X\}\}$ and $\mathbb{A}' \subseteq \mathbb{A}$
- $\wp(\mathbb{A} + \mathbb{B}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}_1^\sharp \times \mathbb{D}_2^\sharp$ where $\alpha = \lambda X.\langle \alpha_1(X \cap \mathbb{A}), \alpha_2(X \cap \mathbb{B})\rangle$
- $\wp(\mathbb{A}) \to \wp(\mathbb{B}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}_1^\sharp \to \mathbb{D}_2^\sharp$ where $\alpha = \lambda f.\alpha_2 \circ f \circ \gamma_1$

  (set of monotone functions)

Example

- Concrete domain: $\mathbb{D} = \wp(\mathbb{M}) \to \wp(\mathbb{M})$ where $\mathbb{M} = \mathbb{X} \to \mathbb{Z}$
- Abstract domain: $\mathbb{D}^\sharp = \mathbb{M}^\sharp \to \mathbb{M}^\sharp$ where $\mathbb{M}^\sharp = \mathbb{X} \to \mathbb{Z}^\sharp$
- Galois connection: $\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$
  - Memory abstraction: $\wp(\mathbb{M}) \underset{\alpha_{\mathbb{M}}}{\overset{\gamma_{\mathbb{M}}}{\leftrightarrows}} \mathbb{M}^\sharp$ via $\wp(\mathbb{X} \to \mathbb{Z}) \underset{\alpha_{\mathbb{M}}}{\overset{\gamma_{\mathbb{M}}}{\leftrightarrows}} \mathbb{X} \to \mathbb{Z}^\sharp$

$$\gamma_{\mathbb{M}} : \mathbb{M}^\sharp \to \wp(\mathbb{M})$$
$$\gamma_{\mathbb{M}} = \lambda m^\sharp.\{m \mid \forall x.m(x) \in \gamma_{\mathbb{Z}}(m^\sharp(x))\}$$

  - Value abstraction: $\wp(\mathbb{Z}) \underset{\alpha_{\mathbb{Z}}}{\overset{\gamma_{\mathbb{Z}}}{\leftrightarrows}} \mathbb{Z}^\sharp$

Requirement 2: F and $F^\sharp$

- $F^\sharp$ is a sound abstraction of F (option 1)

$$F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$$

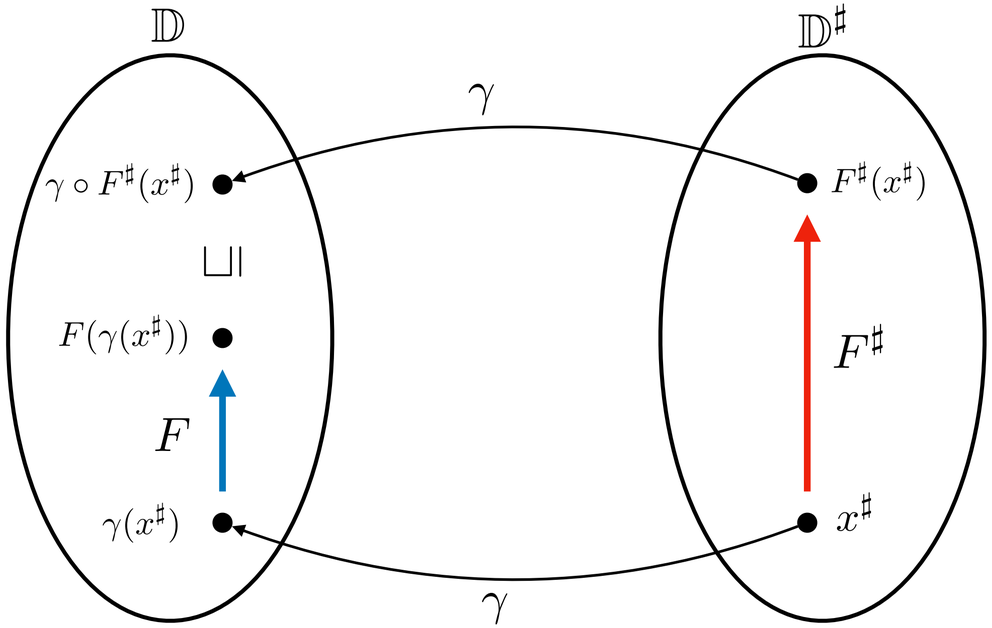
- $F^\sharp$ is a sound abstraction of F (option 2)

$$x \sqsubseteq \gamma(x^\sharp) \implies F(x) \sqsubseteq \gamma(F^\sharp(x^\sharp))$$

Intuition: the result of one-step abstract execution ($F^\sharp$) subsumes that of one-step concrete execution (F)

Sound Abstract Semantics (1)

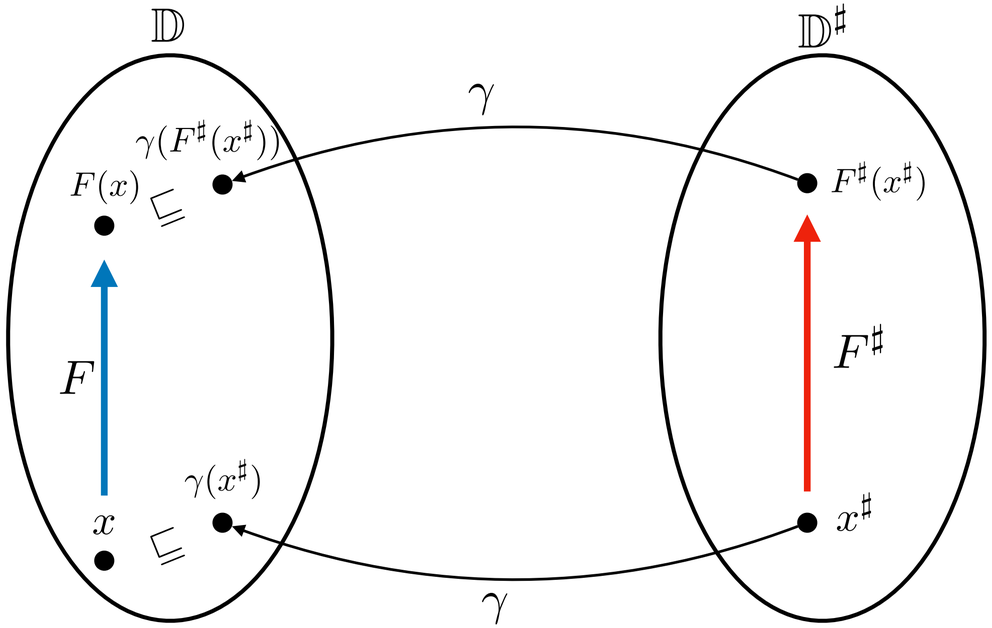
$$F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$$



Intuition: the result of one-step abstract execution ($F^\sharp$) subsumes that of one-step concrete execution (F)

Sound Abstract Semantics (2)

$$x \sqsubseteq \gamma(x^\sharp) \implies F(x) \sqsubseteq \gamma(F^\sharp(x^\sharp))$$



Intuition: the result of one-step abstract execution ($F^\sharp$) subsumes that of one-step concrete execution (F)

Soundness

- Static analysis result $\bigsqcup_{i \geq 0} F^{\sharp i}(\bot)$ soundly subsumes all possible executions

$$\mathbf{lfp} F \sqsubseteq \gamma(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot))$$

- How to guarantee the soundness?
- How to compute the sound result within finite time?

Fixpoint Transfer Theorems

- With option 1

Theorem (Fixpoint Transfer 1)**.** *Let* $\mathbb{D}$ *and* $\mathbb{D}^\sharp$ *be related by Galois connection* $\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$*. Let* $F : \mathbb{D} \to \mathbb{D}$ *be a continuous function and* $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a monotone or extensive function such that* $F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$*. Then,*

$$\mathbf{lfp} F \sqsubseteq \gamma(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp)).$$

- With option 2

Theorem (Fixpoint Transfer 2)**.** *Let* $\mathbb{D}$ *and* $\mathbb{D}^\sharp$ *be related by Galois connection* $\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$*. Let* $F : \mathbb{D} \to \mathbb{D}$ *be a continuous function and* $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ *be a monotone or extensive function such that* $x \sqsubseteq \gamma(x^\sharp) \implies F(x) \sqsubseteq \gamma(F^\sharp(x^\sharp))$*. Then,*

$$\mathbf{lfp} F \sqsubseteq \gamma(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp)).$$

Proof

Theorem (Fixpoint Transfer 1). *Let $\mathbb{D}$ and $\mathbb{D}^\sharp$ be related by Galois connection $\mathbb{D} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \mathbb{D}^\sharp$. Let $F : \mathbb{D} \to \mathbb{D}$ be a continuous function and $F^\sharp : \mathbb{D}^\sharp \to \mathbb{D}^\sharp$ be a monotone or extensive function such that $F \circ \gamma \sqsubseteq \gamma \circ F^\sharp$. Then,*

$$\mathbf{lfp} F \sqsubseteq \gamma(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp)).$$

Proof.

1. First we prove $\forall n \in \mathbb{N}.\ F^n(\bot) \sqsubseteq \gamma(F^{\sharp n}(\bot^\sharp))$ by induction. The base case is trivial. The inductive case is as follows:

$$\begin{aligned} F^{n+1}(\bot) &= F \circ F^n(\bot) \\ &\sqsubseteq F \circ \gamma(F^{\sharp n}(\bot^\sharp)) \quad \text{(by induction hypothesis and monotonicity of } F) \\ &\sqsubseteq \gamma \circ F^\sharp \circ F^{\sharp n}(\bot^\sharp) \quad \text{(by assumption } F \circ \gamma \sqsubseteq \gamma \circ F^\sharp) \\ &= \gamma(F^{\sharp n+1}(\bot^\sharp)) \end{aligned}$$

2. $\{F^i(\bot)\}_i$ is a chain because F is continuous (so monotone). Then, the least upper bound of the chain $\bigsqcup_{i \geq 0} F^i(\bot)$ exists because $\mathbb{D}$ is a CPO.

3. $\{F^{\sharp i}(\bot^\sharp)\}_i$ is a chain because $F^\sharp$ is monotone or extensive. Then, $\{\gamma(F^{\sharp i}(\bot^\sharp))\}_i$ is also a chain because γ is monotone. Therefore, the least upper bound of the chain $\bigsqcup_{i \geq 0} \{\gamma(F^{\sharp i}(\bot^\sharp))\}_i$ exists.

4. Finally,

$$\begin{aligned} \mathbf{lfp} F = \bigsqcup_{i \geq 0} F^i(\bot) &\sqsubseteq \bigsqcup_{i \geq 0} \gamma(F^{\sharp i}(\bot^\sharp)) \\ &\sqsubseteq \gamma(\bigsqcup_{i \geq 0} (F^{\sharp i}(\bot^\sharp))) \quad \text{(by monotonicity of } \gamma) \end{aligned}$$

Abstraction of Compositions

- Composition of sound semantic functions is also sound

$$
\begin{array}{ccc}
\mathbb{D}_1 & \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} & \mathbb{D}_1^\sharp \\
f \downarrow & & \downarrow f^\sharp \\
\mathbb{D}_2 & \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} & \mathbb{D}_2^\sharp \\
g \downarrow & & \downarrow g^\sharp \\
\mathbb{D}_3 & \underset{\alpha_3}{\overset{\gamma_3}{\leftrightarrows}} & \mathbb{D}_3^\sharp
\end{array}
\quad \Rightarrow \quad
g \circ f \circ \gamma_1 \sqsubseteq \gamma_3 \circ g^\sharp \circ f^\sharp
$$

- Implication: soundness proof can be compositional

Abstract Semantics of Expressions

$$
\begin{aligned}
[\![E]\!]^\sharp &: \mathbb{M}^\sharp \to \mathbb{Z}^\sharp \\
[\![n]\!]^\sharp &= \lambda m^\sharp.\alpha(\{n\}) \\
[\![x]\!]^\sharp &= \lambda m^\sharp.m^\sharp(x) \\
[\![E_1 \odot E_2]\!]^\sharp &= \lambda m^\sharp.[\![E_1]\!]^\sharp(m^\sharp) \odot^\sharp [\![E_2]\!]^\sharp(m^\sharp)
\end{aligned}
$$

- Example
  - Sign domain $\mathbb{Z}^\sharp = \{\bot, -, 0, +, \top\}$
  - Interval domain $\mathbb{Z}^\sharp = \{\bot\} \cup \{[a, b] \mid a \in \mathbb{Z} \cup \{-\infty\}, b \in \mathbb{Z} \cup \{+\infty\}\}$
- Soundness: $[\![E]\!]_\wp \circ \gamma_\mathbb{M} \subseteq \gamma_\mathbb{Z} \circ [\![E]\!]^\sharp$

Example: Binary Operator

$$\wp(\mathbb{Z}) \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \{\bot, -, 0, +, \top\}$$

- Define an abstract addition operator $+^\sharp : \mathbb{Z}^\sharp \to \mathbb{Z}^\sharp \to \mathbb{Z}^\sharp$ (as precise as possible)

	$\bot$	-	0	+	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
-	$\bot$	-	-	$\top$	$\top$
0	$\bot$	-	0	+	$\top$
+	$\bot$	$\top$	+	+	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$	$\top$

Soundness Proof

$$[\![E]\!]_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{Z}} \circ [\![E]\!]^{\sharp}$$

- $E : n$

$$\begin{aligned}[\![n]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= \{n\} \\ &= \gamma_{\mathbb{Z}} \circ [\![n]\!]^{\sharp}(m^{\sharp})\end{aligned}$$

- $E : x$

$$\begin{aligned}[\![x]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= [\![x]\!]_{\wp}\{m \mid \forall x.m(x) \in \gamma_{\mathbb{Z}}(m^{\sharp}(x))\} \\ &= \{m(x) \mid \forall x.m(x) \in \gamma_{\mathbb{Z}}(m^{\sharp}(x))\} \\ &= \gamma_{\mathbb{Z}}(m^{\sharp}(x)) \\ &= \gamma_{\mathbb{Z}} \circ [\![x]\!]^{\sharp}(m^{\sharp})\end{aligned}$$

- $E : E_1 \odot E_2$
  - Exercise!
  - For each operator, prove using induction

Abstract Semantics of Conditions

$$
\begin{aligned}
[\![B]\!]^\sharp &: \mathbb{M}^\sharp \to \mathbb{M}^\sharp \\
[\![\mathsf{true}]\!]^\sharp &= \lambda m^\sharp . m^\sharp \\
[\![\mathsf{false}]\!]^\sharp &= \lambda m^\sharp . \bot
\end{aligned}
$$

- Example
  - Sign domain $[\![x < 0]\!]^\sharp = \lambda m^\sharp . \begin{cases} \bot & \text{if } m^\sharp(x) \in \{+, 0, \bot\} \\ m^\sharp\{x \mapsto -\} & \text{o.w.} \end{cases}$
  - Interval domain $[\![x < n]\!]^\sharp = \lambda m^\sharp . \begin{cases} \bot & \text{if } m^\sharp(x) = [a, b] \ \wedge \ a > n \\ m^\sharp\{x \mapsto [a, n-1]\} & \text{if } a \leq n \leq b \\ m^\sharp & \text{if } b < n \end{cases}$
- Soundness: $[\![B]\!]_\wp \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ [\![B]\!]^\sharp$

Soundness Proof

$$[\![B]\!]_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ [\![B]\!]^{\sharp}$$

- $B : x < 0$ and $[\![x < 0]\!]^{\sharp} = \lambda m^{\sharp}. \begin{cases} \bot & \text{if } m^{\sharp}(x) \in \{+, 0, \bot\} \\ m^{\sharp}\{x \mapsto -\} & \text{o.w.} \end{cases}$

$$\begin{aligned} [\![x < 0]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= [\![x < 0]\!]_{\wp}\{m \mid \forall i. m(i) \in \gamma_{\mathbb{Z}}(m^{\sharp}(i))\} \\ &= \{m \mid \forall i. m(i) \in \gamma_{\mathbb{Z}}(m^{\sharp}(i)), m(x) < 0\} \end{aligned}$$

  - Case 1: $m^{\sharp}(x) \in \{+,0,\bot\}$

$$LHS = \emptyset = RHS$$

  - Case 2: $m^{\sharp}(x) \in \{-, \top\}$

$$\begin{aligned} \gamma_{\mathbb{M}} \circ [\![x < 0]\!]^{\sharp}(m^{\sharp}) &= \gamma_{\mathbb{M}}(m^{\sharp}\{x \mapsto -\}) \\ &= \{m \mid \forall i. m(i) \in \gamma_{\mathbb{Z}}(m^{\sharp}\{x \mapsto -\}(i)), m(x) < 0\} \\ &= LHS \end{aligned}$$

Abstract Semantics of Commands

$$
\begin{aligned}
[\![C]\!]^\sharp &: \mathbb{M}^\sharp \to \mathbb{M}^\sharp \\
[\![\texttt{skip}]\!]^\sharp &= \lambda m^\sharp . m^\sharp \\
[\![C_0 \texttt{;} C_1]\!]^\sharp &= \lambda m^\sharp . [\![C_1]\!]^\sharp \circ [\![C_0]\!]^\sharp (m^\sharp) \\
[\![x \texttt{:=} E]\!]^\sharp &= \lambda m^\sharp . m^\sharp \{x \mapsto [\![E]\!]^\sharp (m^\sharp)\} \\
[\![\texttt{input}(x)]\!]^\sharp &= \lambda m^\sharp . m^\sharp \{x \mapsto \alpha(\mathbb{Z})\} \\
[\![\texttt{if } B \texttt{ then } C_1 \texttt{ else } C_2]\!]^\sharp &= \lambda m^\sharp . [\![C_1]\!]^\sharp \circ [\![B]\!]^\sharp (m^\sharp) \sqcup [\![C_2]\!]^\sharp \circ [\![\neg B]\!]^\sharp (m^\sharp) \\
[\![\texttt{while } B \ C]\!]^\sharp &= \lambda m^\sharp . [\![\neg B]\!]^\sharp \Big(\bigsqcup_{i \geq 0} F^{\sharp i}(\bot) \Big) \\
&\qquad \text{where } F^\sharp = \lambda X . m^\sharp \sqcup [\![C]\!]^\sharp \circ [\![B]\!]^\sharp (X)
\end{aligned}
$$

- Soundness: $[\![C]\!]_\wp \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ [\![C]\!]^\sharp$ and $\cup \circ (\gamma_{\mathbb{M}}, \gamma_{\mathbb{M}}) \subseteq \gamma_{\mathbb{M}} \circ \sqcup$

Soundness Proof (1)

$$[\![C]\!]_{\wp} \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ [\![C]\!]^{\sharp}$$

- $C_1 ; C_2$

$$\begin{aligned}
[\![C_0 ; C_1]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) &= [\![C_0]\!]_{\wp} \circ [\![C_1]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \\
&\subseteq [\![C_0]\!]_{\wp} \circ \gamma_{\mathbb{M}} \circ [\![C_1]\!]^{\sharp}(m^{\sharp}) \\
&\subseteq \gamma_{\mathbb{M}} \circ [\![C_0]\!]^{\sharp} \circ [\![C_1]\!]^{\sharp}(m^{\sharp}) \\
&= \gamma_{\mathbb{M}} \circ [\![C_0 ; C_1]\!]^{\sharp}(m^{\sharp})
\end{aligned}$$

- $\texttt{if}\ B\ \texttt{then}\ C_1\ \texttt{else}\ C_2$

$$\begin{aligned}
&[\![\texttt{if}\ B\ \texttt{then}\ C_1\ \texttt{else}\ C_2]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \\
&= [\![C_1]\!]_{\wp} \circ [\![B]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \cup [\![C_2]\!]_{\wp} \circ [\![\neg B]\!]_{\wp} \circ \gamma_{\mathbb{M}}(m^{\sharp}) \\
&\subseteq [\![C_1]\!]_{\wp} \circ \gamma_{\mathbb{M}} \circ [\![B]\!]^{\sharp}(m^{\sharp}) \cup [\![C_2]\!]_{\wp} \circ \gamma_{\mathbb{M}} \circ [\![B]\!]^{\sharp}(m^{\sharp}) \\
&\subseteq \gamma_{\mathbb{M}} \circ [\![C_1]\!]^{\sharp} \circ [\![B]\!]^{\sharp}(m^{\sharp}) \cup \gamma_{\mathbb{M}} \circ [\![C_2]\!]^{\sharp} \circ [\![B]\!]^{\sharp}(m^{\sharp}) \\
&\subseteq \gamma_{\mathbb{M}}\big([\![C_1]\!]^{\sharp} \circ [\![B]\!]^{\sharp}(m^{\sharp}) \sqcup [\![C_2]\!]^{\sharp} \circ [\![B]\!]^{\sharp}(m^{\sharp})\big) \\
&= \gamma_{\mathbb{M}} \circ [\![\texttt{if}\ B\ \texttt{then}\ C_1\ \texttt{else}\ C_2]\!]^{\sharp}(m^{\sharp})
\end{aligned}$$

Soundness Proof (2)

$$[\![C]\!]_\wp \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ [\![C]\!]^\sharp$$

- `while` $B\ C$

$$[\![\texttt{while}\ B\ C]\!]_\wp \circ \gamma_{\mathbb{M}}(m^\sharp)$$
$$= [\![\neg B]\!]_\wp\big(\mathbf{lfp}\lambda X.\gamma_{\mathbb{M}}(m^\sharp) \cup [\![C]\!]_\wp \circ [\![B]\!]_\wp(X)\big)$$
$$\subseteq [\![\neg B]\!]_\wp \circ \gamma_{\mathbb{M}}\big(\bigsqcup_{i\geq 0} F^{\sharp i}(\bot)\big)$$
$$\subseteq \gamma_{\mathbb{M}} \circ [\![\neg B]\!]^\sharp\big(\bigsqcup_{i\geq 0} F^{\sharp i}(\bot)\big)$$

where $F^\sharp = \lambda X.m^\sharp \sqcup [\![C]\!]^\sharp \circ [\![B]\!]^\sharp(X)$

- $\big(\mathbf{lfp}\lambda X.\gamma_{\mathbb{M}}(m^\sharp) \cup [\![C]\!]_\wp \circ [\![B]\!]_\wp(X)\big) \subseteq \gamma_{\mathbb{M}}\big(\bigsqcup_{i\geq 0} F^{\sharp i}(\bot)\big)$

  This holds by the fixed point transfer theorem if $F \circ \gamma_{\mathbb{M}} \subseteq \gamma_{\mathbb{M}} \circ F^\sharp$

$$\big(\lambda X.\gamma_{\mathbb{M}}(m^\sharp) \cup [\![C]\!]_\wp \circ [\![B]\!]_\wp(X)\big) \circ \gamma_{\mathbb{M}}(m^\sharp)$$
$$= \gamma_{\mathbb{M}}(m^\sharp) \cup [\![C]\!]_\wp \circ [\![B]\!]_\wp(\gamma_{\mathbb{M}}(m^\sharp))$$
$$\subseteq \gamma_{\mathbb{M}}(m^\sharp) \cup [\![C]\!]_\wp \circ \gamma_{\mathbb{M}} \circ [\![B]\!]^\sharp(m^\sharp)$$
$$\subseteq \gamma_{\mathbb{M}}(m^\sharp) \cup \gamma_{\mathbb{M}} \circ [\![C]\!]^\sharp \circ [\![B]\!]^\sharp(m^\sharp)$$
$$\subseteq \gamma_{\mathbb{M}}\big(m^\sharp \sqcup [\![C]\!]^\sharp \circ [\![B]\!]^\sharp(m^\sharp)\big)$$
$$= \gamma_{\mathbb{M}} \circ \big(\lambda X.m^\sharp \sqcup [\![C]\!]^\sharp \circ [\![B]\!]^\sharp(X)\big)(m^\sharp)$$

Summary

- Abstract semantics: a **sound approximation** of the concrete semantics
- **Soundness guarantee** by Fixpoint transfer theorem
  - Galois connection, sound abstract semantic function
- Static analysis design: design of **precise and efficient** abstract semantics
- Plan: compute the abstract semantics within a **finite time**