

Introduction to Program Analysis

7. Abstract Interpretation (3): Widening and Narrowing

Kihong Heo



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**

Computing Abstract Semantics

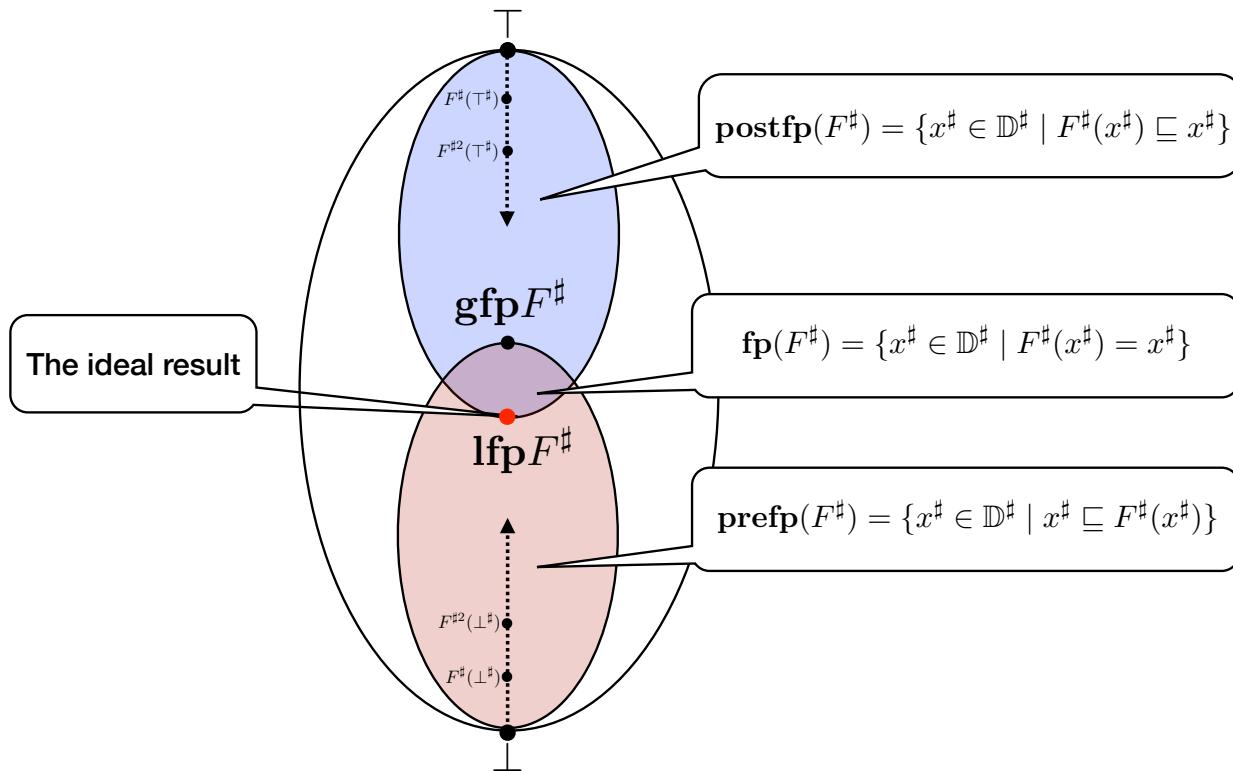
- If the abstract domain \mathbb{D}^\sharp has **finite** height (i.e., all chains are finite)

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

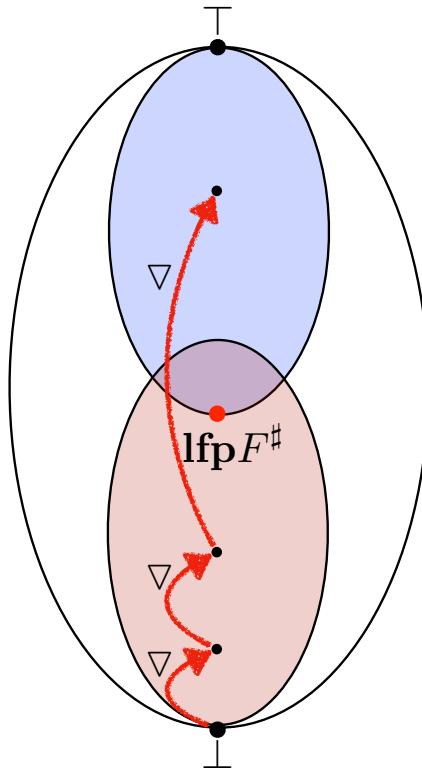
- If the abstract domain \mathbb{D}^\sharp has **infinite** height, we compute a finite chain $X_0^\sharp \sqsubseteq X_1^\sharp \sqsubseteq X_2^\sharp \sqsubseteq \dots \sqsubseteq X_{\text{lim}}^\sharp$ such that

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq X_{\text{lim}}^\sharp$$

Fixed Points



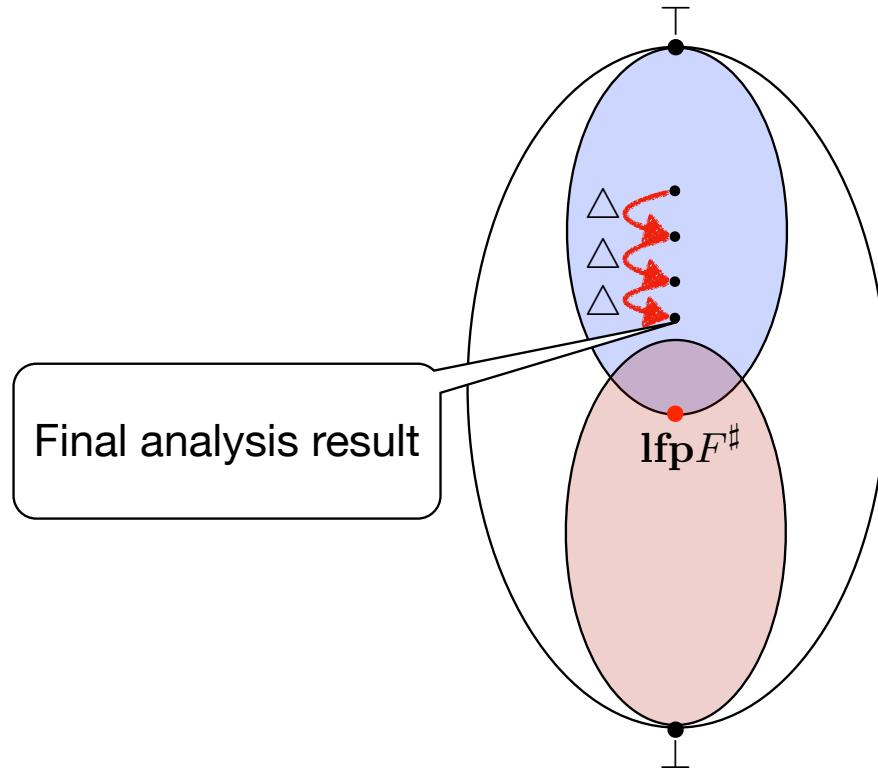
Widening



$$\nabla : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$$

Widening: enforcing the convergence of fix point iterations

Narrowing



$$\triangle : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$$

Narrowing: refining the analysis results
with widening

Overshooting by Widening

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^{\sharp}) \sqsubseteq Y_{\lim}^{\sharp}$$

- Define finite chain $\{Y_i\}_i$ by an widening operator $\nabla \in \mathbb{D}^{\sharp} \times \mathbb{D}^{\sharp} \rightarrow \mathbb{D}^{\sharp}$:

$$\begin{aligned} Y_0^{\sharp} &= \perp^{\sharp} \\ Y_{i+1}^{\sharp} &= \begin{cases} Y_i^{\sharp} & \text{if } F^{\sharp}(Y_i^{\sharp}) \sqsubseteq Y_i^{\sharp} \\ Y_i^{\sharp} \nabla F^{\sharp}(Y_i^{\sharp}) & \text{otherwise} \end{cases} \end{aligned}$$

Finite Increasing Chain with Widening

$$\begin{array}{c} \vdots \\ | \\ F^{\sharp 2}(\perp^{\sharp}) \\ | \\ F^{\sharp}(\perp^{\sharp}) \\ | \\ \perp^{\sharp} \end{array}$$

Original Chain

$$\begin{array}{c} Y_{N+1}^{\sharp} = Y_N^{\sharp} \\ | \\ Y_N^{\sharp} = Y_{N-1}^{\sharp} \vee F^{\sharp}(Y_{N-1}^{\sharp}) \\ \vdots \\ Y_2^{\sharp} = Y_1^{\sharp} \vee F^{\sharp}(Y_1^{\sharp}) \\ | \\ Y_1^{\sharp} = Y_0^{\sharp} \vee F^{\sharp}(Y_0^{\sharp}) \\ | \\ Y_0^{\sharp} = \perp^{\sharp} \end{array}$$

New Chain with Widening

Q. What conditions are required to ensure

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^{\sharp}) \sqsubseteq Y_{\lim}^{\sharp}$$

Example

- A simple widening operator for the interval domain

$$\begin{array}{lll} [a, b] \quad \nabla \quad \perp & = & [a, b] \\ \perp \quad \nabla \quad [c, d] & = & [c, d] \\ [a, b] \quad \nabla \quad [c, d] & = & [(c < a? -\infty : a), (b < d? +\infty : b)] \end{array}$$

Safety of Widening Operator

- Conditions on widening operator:
 - $\forall a, b \in \mathbb{D}^\sharp. (a \sqsubseteq a \vee b) \wedge (b \sqsubseteq a \vee b)$
 - \forall increasing chain $\{x_i\}_i$, the following increasing chain $\{y_i\}_i$ is finite:

$$y_0 = x_0$$

$$y_{i+1} = y_i \vee x_{i+1}$$

- Then,

- Chain $\{Y_i^\sharp\}_i$ is finite
- $\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq Y_{\lim}^\sharp$

Proof

Theorem (Widening's Safety). *Let \mathbb{D}^\sharp be a CPO, $F^\sharp : \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$ be a monotone function, and $\nabla : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$ be a widening operator. Then, chain $\{Y_i^\sharp\}_i$ eventually stabilizes and*

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq Y_{\lim}^\sharp$$

where Y_{\lim}^\sharp is the greatest element of the chain.

Proof. First we prove chain $\{Y_i^\sharp\}_i$ is finite. According to the second condition on widening operator, it is enough to show that chain $\{F^\sharp(Y_i^\sharp)\}_i$ is increasing. The chain is increasing because 1) $F^\sharp(Y_{i+1}^\sharp)$ is either $F^\sharp(Y_i^\sharp)$ or $F^\sharp(Y_i^\sharp \nabla F^\sharp(Y_i^\sharp))$, 2) $Y_i^\sharp \sqsubseteq Y_i^\sharp \nabla F^\sharp(Y_i^\sharp)$ according to the first condition on widening, and 3) F^\sharp is monotone.

Second, we prove $\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq Y_{\lim}^\sharp$. It is enough to show that $\forall i \in \mathbb{N}. F^{\sharp i}(\perp^\sharp) \sqsubseteq Y_i^\sharp$ that can be proven by induction. The base case is trivial. The inductive case is as follows:

$$\begin{aligned} F^{\sharp i+1}(\perp^\sharp) &= F^\sharp(F^{\sharp i}(\perp^\sharp)) \\ &\sqsubseteq F^\sharp(Y_i^\sharp) \quad (\text{by induction hypothesis and monotonicity of } F^\sharp) \end{aligned}$$

If $F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp$, then $Y_{i+1}^\sharp = Y_i^\sharp$ by definition. Therefore, $F^{\sharp i+1}(\perp^\sharp) \sqsubseteq Y_{i+1}^\sharp$.

If $F^\sharp(Y_i^\sharp) \supsetneq Y_i^\sharp$, then $Y_{i+1}^\sharp = Y_i^\sharp \nabla F^\sharp(Y_i^\sharp)$ by definition. According to the first condition on widening, $F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp \nabla F^\sharp(Y_i^\sharp)$. Therefore, $F^{\sharp i+1}(\perp^\sharp) \sqsubseteq Y_{i+1}^\sharp$.

Example (Revisited)

- A simple widening operator for the interval domain

$$\begin{array}{lcl} [a, b] \quad \nabla \quad \perp & = & [a, b] \\ \perp \quad \nabla \quad [c, d] & = & [c, d] \\ [a, b] \quad \nabla \quad [c, d] & = & [(c < a? - \infty : a), (b < d? + \infty : b)] \end{array}$$

Check: Safety conditions
for widening

Refinement by Narrowing

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^{\sharp}) \sqsubseteq Z_{\text{lim}}^{\sharp}$$

- Define finite chain $\{Z_i^{\sharp}\}_i$ by an narrowing operator $\triangle \in \mathbb{D}^{\sharp} \times \mathbb{D}^{\sharp} \rightarrow \mathbb{D}^{\sharp}$:

$$\begin{aligned} Z_0^{\sharp} &= Y_{\text{lim}}^{\sharp} \\ Z_{i+1}^{\sharp} &= Z_i^{\sharp} \triangle F^{\sharp}(Z_i^{\sharp}) \end{aligned}$$

Finite Decreasing Chain with Narrowing

$$\begin{array}{c} Y_{\lim}^{\sharp} \\ | \\ F^{\sharp}(Y_{\lim}^{\sharp}) \\ | \\ F^{\sharp 2}(Y_{\lim}^{\sharp}) \\ \vdots \end{array}$$

Original Chain

$$\begin{array}{c} Z_0^{\sharp} = Y_{\lim}^{\sharp} \\ | \\ Z_1^{\sharp} = Z_0^{\sharp} \triangle F^{\sharp}(Z_0^{\sharp}) \\ | \\ Z_2^{\sharp} = Z_1^{\sharp} \triangle F^{\sharp}(Z_1^{\sharp}) \\ \vdots \\ Z_N^{\sharp} = Z_{N-1}^{\sharp} \triangle F^{\sharp}(Z_{N-1}^{\sharp}) \\ | \\ Z_{N+1}^{\sharp} = Z_N^{\sharp} \end{array}$$

New Chain with Narrowing

Q. What conditions are required to ensure

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^{\sharp}) \sqsubseteq Z_{\lim}^{\sharp}$$

Example

- A simple narrowing operator for the interval domain

$$\begin{array}{lcl} [a, b] \triangle \perp & = & \perp \\ \perp \triangle [c, d] & = & \perp \\ [a, b] \triangle [c, d] & = & [(a = -\infty ? c : a), (b = +\infty ? d : b)] \end{array}$$

Safety of Narrowing Operator

- Conditions on narrowing operator:
 - $\forall a, b \in \mathbb{D}^\sharp. a \sqsupseteq b \implies a \sqsupseteq (a \triangle b) \sqsupseteq b$
 - For all decreasing chain $\{y_i\}_i$, the following decreasing chain $\{z_i\}_i$ is finite

$$z_0 = y_0$$

$$z_{i+1} = z_i \triangle y_{i+1}$$

- Then,
 - Decreasing chain $\{Z_i^\sharp\}_i$ is finite
 - $\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq Z_{\lim}$

Proof

Theorem (Narrowing's Safety). Let \mathbb{D}^\sharp be a CPO, $F^\sharp : \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$ be a monotone function, and $\Delta : \mathbb{D}^\sharp \times \mathbb{D}^\sharp \rightarrow \mathbb{D}^\sharp$ be a narrowing operator. Then, chain $\{Z_i^\sharp\}_i$ eventually stabilizes and

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq Z_{\lim}^\sharp$$

where Z_{\lim}^\sharp is the least element of the chain.

Proof. First we prove chain $\{Z_i^\sharp\}_i$ is finite. According to the condition on narrowing operator, it is enough to show that chain $\{F^\sharp(Z_i^\sharp)\}_i$ is decreasing. The chain is decreasing if $\forall i \in \mathbb{N}. Z_i^\sharp \sqsupseteq F^\sharp(Z_i^\sharp)$ because $Z_i^\sharp \sqsupseteq Z_i^\sharp \Delta F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_i^\sharp)$ and $F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_i^\sharp \Delta F^\sharp(Z_i^\sharp)) = F^\sharp(Z_{i+1}^\sharp)$. We prove $\forall i \in \mathbb{N}. Z_i^\sharp \sqsupseteq F^\sharp(Z_i^\sharp)$ by induction. The base case is true by definition of Z_{\lim}^\sharp from the increasing chain by widening. The inductive case is as follows:

$$\begin{aligned} Z_i^\sharp &\sqsupseteq F^\sharp(Z_i^\sharp) && \text{(by induction hypothesis)} \\ \implies Z_i^\sharp &\sqsupseteq Z_i^\sharp \Delta F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_i^\sharp) && \text{(by the first condition on narrowing)} \\ \implies Z_i^\sharp &\sqsupseteq Z_{i+1}^\sharp \sqsupseteq F^\sharp(Z_i^\sharp) && \text{(by definition)} \\ \implies F^\sharp(Z_i^\sharp) &\sqsupseteq F^\sharp(Z_{i+1}^\sharp) && \text{(by monotonicity of } F^\sharp \text{ and } Z_i^\sharp \sqsupseteq Z_{i+1}^\sharp) \\ \implies Z_{i+1}^\sharp &\sqsupseteq F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_{i+1}^\sharp) \end{aligned}$$

Second we prove chain $\bigsqcup_{i \geq 0} F^{\sharp i}(\perp^\sharp) \sqsubseteq Z_{\lim}^\sharp$. It is enough to show that $\forall i \in \mathbb{N}. F^{\sharp i}(\perp^\sharp) \sqsubseteq Z_i^\sharp$ that can be proven by induction. The base case is trivial. The inductive case is as follows:

$$\begin{aligned} F^{\sharp i+1}(\perp^\sharp) &= F^\sharp \circ F^{\sharp i}(\perp^\sharp) \\ &\sqsubseteq F^\sharp(Z_i^\sharp) && \text{(by induction hypothesis and monotonicity of } F^\sharp) \\ &\sqsubseteq Z_i^\sharp \Delta F^\sharp(Z_i^\sharp) && \text{(by condition } \forall i \in \mathbb{N}. Z_i^\sharp \sqsupseteq F^\sharp(Z_i^\sharp)) \\ &= Z_{i+1}^\sharp && \text{(by definition)} \end{aligned}$$

Example

- A simple narrowing operator for the interval domain

$$\begin{array}{lllll} [a, b] & \triangle & \perp & = & \perp \\ \perp & \triangle & [c, d] & = & \perp \\ [a, b] & \triangle & [c, d] & = & [(a = -\infty ? c : a), (b = +\infty ? d : b)] \end{array}$$

Check: Safety conditions
for narrowing

Computable Abstract Semantics

$$\llbracket C \rrbracket^\sharp : \mathbb{M}^\sharp \rightarrow \mathbb{M}^\sharp$$

$$\llbracket \text{skip} \rrbracket^\sharp = \lambda m^\sharp. m^\sharp$$

$$\llbracket C_0 ; C_1 \rrbracket^\sharp = \lambda m^\sharp. \llbracket C_1 \rrbracket^\sharp \circ \llbracket C_0 \rrbracket^\sharp(m^\sharp)$$

$$\llbracket x := E \rrbracket^\sharp = \lambda m^\sharp. m^\sharp \{x \mapsto \llbracket E \rrbracket^\sharp(m^\sharp)\}$$

$$\llbracket \text{input}(x) \rrbracket^\sharp = \lambda m^\sharp. m^\sharp \{x \mapsto \alpha(\mathbb{Z})\}$$

$$\llbracket \text{if } B \text{ then } C_1 \text{ else } C_2 \rrbracket^\sharp = \lambda m^\sharp. \llbracket C_1 \rrbracket^\sharp \circ \llbracket B \rrbracket^\sharp(m^\sharp) \sqcup \llbracket C_2 \rrbracket^\sharp \circ \llbracket \neg B \rrbracket^\sharp(m^\sharp)$$

$$\llbracket \text{while } B \text{ } C \rrbracket^\sharp = \lambda m^\sharp. \llbracket \neg B \rrbracket^\sharp \circ \text{Narrow} \circ \text{Widen} \circ (\lambda X. m^\sharp \sqcup \llbracket C \rrbracket^\sharp \circ \llbracket B \rrbracket^\sharp(X))$$

$$Widen(F^\sharp) = \lim_{i \in \mathbb{N}} \begin{cases} Y_0^\sharp = \perp \\ Y_{i+1}^\sharp = \begin{cases} Y_i^\sharp & \text{if } F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp \\ Y_i^\sharp \bigtriangledown F^\sharp(Y_i^\sharp) & \text{o.w.} \end{cases} \end{cases} \quad \text{Narrow}(m^\sharp) = \lim_{i \in \mathbb{N}} \begin{cases} Z_0^\sharp = m^\sharp \\ Z_{i+1}^\sharp = Z_i^\sharp \triangle F^\sharp(Z_i^\sharp) \end{cases}$$

Summary

- **Computing** a sound approximation of the concrete semantics
 - Finite height: directly compute the fixed point by iteration
 - Infinite height: fixpoint iteration with widening and narrowing
- Widening: **termination** guarantee
- Narrowing: **refinement** of widening results