Introduction to Program Analysis

7. Abstract Interpretation (3): Widening and Narrowing

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

Computing Abstract Semantics

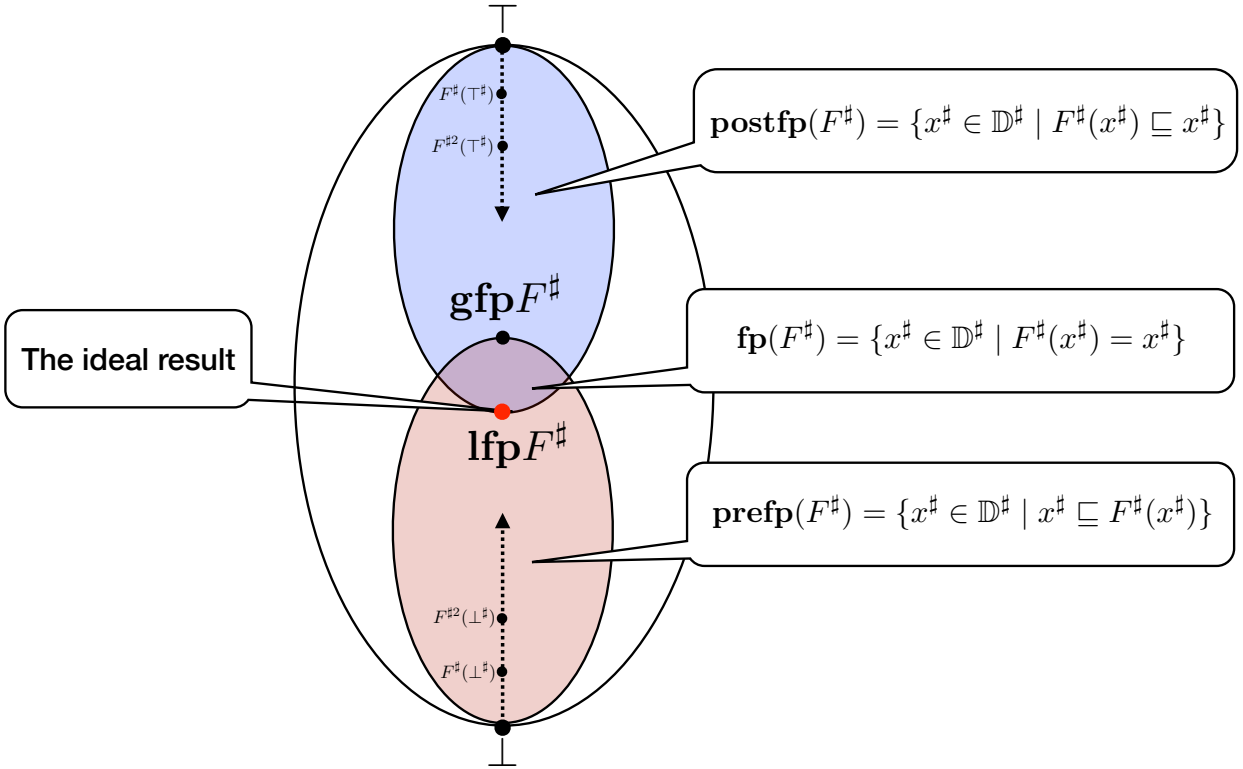
- If the abstract domain $\mathbb{D}^\sharp$ has **finite** height (i.e., all chains are finite)

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

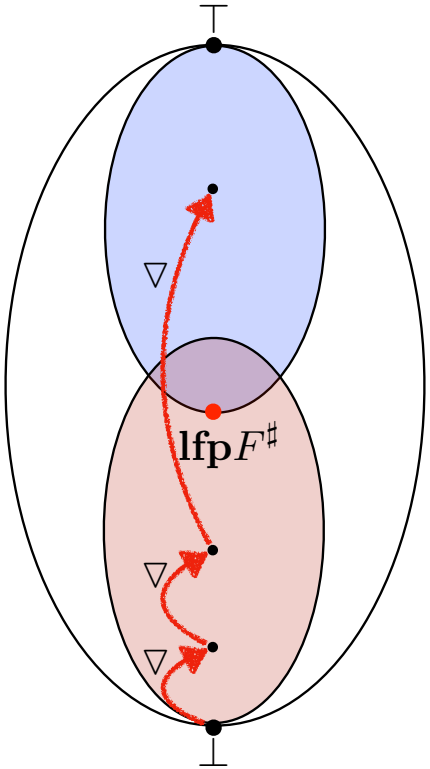
- If the abstract domain $\mathbb{D}^\sharp$ has **infinite** height, we compute a finite chain $X_0^\sharp \sqsubseteq X_1^\sharp \sqsubseteq X_2^\sharp \sqsubseteq \ldots \sqsubseteq X_{\text{lim}}^\sharp$ such that

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

Fixed Points



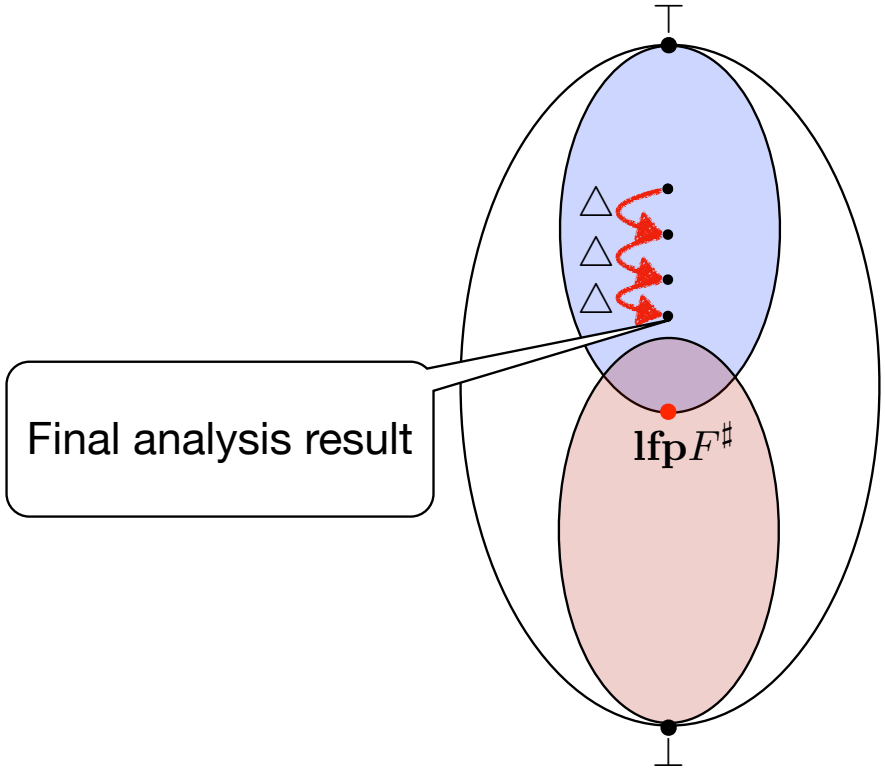
Widening



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

Widening: enforcing the convergence of fix point iterations

Narrowing



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

Narrowing: refining the analysis results with widening

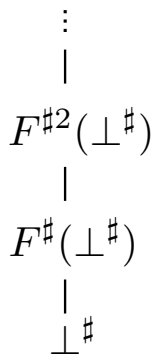
Overshooting by Widening

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y^\sharp_{\text{lim}}$$

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

$$\begin{array}{rcl} Y_0^\sharp & = & \bot^\sharp \\ Y_{i+1}^\sharp & = & \begin{cases} Y_i^\sharp & \text{if } F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp \\ Y_i^\sharp \ \triangledown \ F^\sharp(Y_i^\sharp) & \text{otherwise} \end{cases} \end{array}$$

Finite Increasing Chain with Widening



Original Chain

$$
\begin{array}{l}
Y^\sharp_{N+1} = Y^\sharp_N \\
| \\
Y^\sharp_N = Y^\sharp_{N-1} \triangledown F^\sharp(Y^\sharp_{N-1}) \\
\vdots \\
Y^\sharp_2 = Y^\sharp_1 \triangledown F^\sharp(Y^\sharp_1) \\
| \\
Y^\sharp_1 = Y^\sharp_0 \triangledown F^\sharp(Y^\sharp_0) \\
| \\
Y^\sharp_0 = \bot^\sharp
\end{array}
$$

New Chain with Widening

Q. What conditions are required to ensure

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y^\sharp_{\text{lim}}$$

Example

- A simple widening operator for the interval domain

$$
\begin{array}{rcll}
[a,b] & \triangledown & \bot & = [a,b] \\
\bot & \triangledown & [c,d] & = [c,d] \\
[a,b] & \triangledown & [c,d] & = [(c < a ? -\infty : a), (b < d ? +\infty : b)]
\end{array}
$$

Safety of Widening Operator

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

$$y_0 = x_0$$
$$y_{i+1} = y_i \ \triangledown\ x_{i+1}$$

- Then,
  - Chain $\{Y_i^\sharp\}_i$ is finite
  - $\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y^\sharp_{\text{lim}}$

Proof

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

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Y^\sharp_{\text{lim}}$$

where $Y^\sharp_{\text{lim}}$ 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 $F^\sharp(Y_i^\sharp \triangledown F^\sharp(Y_i^\sharp))$, 2) $Y_i^\sharp \sqsubseteq Y_i^\sharp \triangledown F^\sharp(Y_i^\sharp)$ according to the first condition on widening, and 3) $F^\sharp$ is monotone.

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

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

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

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

Example (Revisited)

- A simple widening operator for the interval domain

$$
\begin{array}{rcll}
[a,b] & \triangledown & \bot & = [a,b] \\
\bot & \triangledown & [c,d] & = [c,d] \\
[a,b] & \triangledown & [c,d] & = [(c < a ? -\infty : a), (b < d ? +\infty : b)]
\end{array}
$$

Check: Safety conditions for widening

Refinement by Narrowing

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Z^\sharp_{\text{lim}}$$

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

$$\begin{array}{rcl} Z^\sharp_0 & = & Y^\sharp_{\text{lim}} \\ Z^\sharp_{i+1} & = & Z^\sharp_i \ \triangle \ F^\sharp(Z^\sharp_i) \end{array}$$

Finite Decreasing Chain with Narrowing

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

Original Chain

$$
\begin{array}{l}
Z^\sharp_0 = Y^\sharp_{\text{lim}} \\
| \\
Z^\sharp_1 = Z^\sharp_0 \mathbin{\triangle} F^\sharp(Z^\sharp_0) \\
| \\
Z^\sharp_2 = Z^\sharp_1 \mathbin{\triangle} F^\sharp(Z^\sharp_1) \\
\vdots \\
Z^\sharp_N = Z^\sharp_{N-1} \mathbin{\triangle} F^\sharp(Z^\sharp_{N-1}) \\
| \\
Z^\sharp_{N+1} = Z^\sharp_N
\end{array}
$$

New Chain with Narrowing

Q. What conditions are required to ensure

$$\bigsqcup_{i \geq 0} F^{\sharp i}(\bot^\sharp) \sqsubseteq Z^\sharp_{\text{lim}}$$

Example

- A simple narrowing operator for the interval domain

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

Safety of Narrowing Operator

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

$$z_0 = y_0$$
$$z_{i+1} = z_i \mathbin{\triangle} y_{i+1}$$

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

Proof

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

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

where $Z_{\text{lim}}^\sharp$ 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 $Z_i^\sharp \sqsupseteq Z_i^\sharp \triangle F^\sharp(Z^\sharp) \sqsupseteq F^\sharp(Z^\sharp)$ and $F^\sharp(Z_i^\sharp) \sqsupseteq F^\sharp(Z_i^\sharp \triangle F^\sharp(Z^\sharp)) = F^\sharp(Z_{i+1}^\sharp)$. 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 $Y_{\text{lim}}^\sharp$ from the increasing chain by widening. The inductive case is as follows:

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

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

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

Example

- A simple narrowing operator for the interval domain

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

Check: Safety conditions for narrowing

Computable Abstract Semantics

$$[\![C]\!]^\sharp \ : \ \mathbb{M}^\sharp \to \ \mathbb{M}^\sharp$$

$$\begin{aligned}
[\![\texttt{skip}]\!]^\sharp &= \lambda m^\sharp.m^\sharp \\
[\![C_0\,;C_1]\!]^\sharp &= \lambda m^\sharp.[\![C_1]\!]^\sharp \circ [\![C_0]\!]^\sharp(m^\sharp) \\
[\![x := E]\!]^\sharp &= \lambda m^\sharp.m^\sharp\{x \mapsto [\![E]\!]^\sharp(m^\sharp)\} \\
[\![\texttt{input}(x)]\!]^\sharp &= \lambda m^\sharp.m^\sharp\{x \mapsto \alpha(\mathbb{Z})\} \\
[\![\texttt{if } B \texttt{ then } C_1 \texttt{ else } C_2]\!]^\sharp &= \lambda m^\sharp.[\![C_1]\!]^\sharp \circ [\![B]\!]^\sharp(m^\sharp) \sqcup [\![C_2]\!]^\sharp \circ [\![\neg B]\!]^\sharp(m^\sharp) \\
[\![\texttt{while } B \ C]\!]^\sharp &= \lambda m^\sharp.[\![\neg B]\!]^\sharp \circ \mathit{Narrow} \circ \mathit{Widen} \circ \left(\lambda X.m^\sharp \sqcup [\![C]\!]^\sharp \circ [\![B]\!]^\sharp(X)\right)
\end{aligned}$$

$$\mathit{Widen}(F^\sharp) = \lim_{i\in\mathbb{N}} \begin{cases} Y_0^\sharp = \bot \\ Y_{i+1}^\sharp = \begin{cases} Y_i^\sharp & \text{if } F^\sharp(Y_i^\sharp) \sqsubseteq Y_i^\sharp \\ Y_i^\sharp \bigtriangledown F^\sharp(Y_i^\sharp) & \text{o.w.} \end{cases} \end{cases}$$

$$\mathit{Narrow}(m^\sharp) = \lim_{i\in\mathbb{N}} \begin{cases} Z_0^\sharp = m^\sharp \\ Z_{i+1}^\sharp = Z_i^\sharp \bigtriangleup F^\sharp(Z_i^\sharp) \end{cases}$$

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