AAA616: Program Analysis

Lecture 6 — Abstract Interpretation Example

Hakjoo Oh
2022 Fall

Concrete Semantics

- Program representation:
  - P is represented by control flow graph $(\mathbb{C}, \to, c_0)$
  - Each program point c is associated with a command **cmd**(c)

$$
\begin{array}{rcl}
cmd & \to & skip \mid x := e \\
e & \to & n \mid x \mid e + e \mid e - e.
\end{array}
$$

- Concrete memory states: $\mathbb{M} = \textbf{Var} \to \mathbb{Z}$
- Concrete semantics:

$$
\begin{array}{rcl}
[\![c]\!] & : & \mathbb{M} \to \mathbb{M} \\
\\
[\![skip]\!](m) & = & m \\
[\![x := e]\!](m) & = & m[x \mapsto [\![e]\!](s)]
\end{array}
$$

$$
\begin{array}{rcl}
[\![e]\!] & : & \mathbb{M} \to \mathbb{Z} \\
\\
[\![n]\!](m) & = & n \\
[\![x]\!](m) & = & m(x) \\
[\![e_1 + e_2]\!](m) & = & [\![e_1]\!](m) + [\![e_2]\!](m) \\
[\![e_1 - e_2]\!](m) & = & [\![e_1]\!](m) + [\![e_2]\!](m)
\end{array}
$$

Concrete Semantics

- Program states: $\mathbb{S} = \mathbb{C} \times \mathbb{M}$
- A trace $\boldsymbol{\sigma} \in \mathbb{S}^+$ is a (partial) execution sequence of the program:

$$\boldsymbol{\sigma_0} \in \boldsymbol{I} \ \wedge \ \forall \boldsymbol{k}.\boldsymbol{\sigma_k} \rightsquigarrow \boldsymbol{\sigma_{k+1}}$$

where $\boldsymbol{I} \subseteq \mathbb{S}$ is the initial program states

$$\boldsymbol{I} = \{(\boldsymbol{c_0}, \boldsymbol{m_0}) \mid \boldsymbol{m_0} \in \mathbb{M}\}$$

and $(\rightsquigarrow) \subseteq \mathbb{S} \times \mathbb{S}$ is the relation for the one-step execution:

$$(\boldsymbol{c_i}, \boldsymbol{s_i}) \rightsquigarrow (\boldsymbol{c_j}, \boldsymbol{s_j}) \iff \boldsymbol{c_i} \rightarrow \boldsymbol{c_j} \ \wedge \ \boldsymbol{s_j} = [\![\textbf{cmd}(\boldsymbol{c_j})]\!](\boldsymbol{s_i})$$

Concrete Semantics

The collecting semantics of program P is defined as the set of all finite traces of the program:

$$[\![P]\!] = \{\sigma \in \mathbb{S}^+ \mid \sigma_0 \in I \ \wedge \ \forall k.\sigma_k \rightsquigarrow \sigma_{k+1}\}$$

The semantic domain:

$$D = \wp(\mathbb{S}^+)$$

The semantic function:

$$\begin{array}{rcl} F & : & \wp(\mathbb{S}^+) \rightarrow \wp(\mathbb{S}^+) \\ F(\Sigma) & = & I \cup \{\sigma \cdot (c, m) \mid \sigma \in \Sigma \ \wedge \ \sigma_{\dashv} \rightsquigarrow (c, m)\} \end{array}$$

Lemma

$[\![P]\!] = \mathit{fix} F$.

Partitioning Abstraction

Galois-connection: $\wp(\mathbb{S}^+) \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \mathbb{C} \to \wp(\mathbb{M})$

$$\alpha_1(\Sigma) \;=\; \lambda c.\{m \in \mathbb{M} \mid \exists \sigma \in \Sigma \;\wedge\; \exists i.\sigma_i = (c, m)\}$$

Semantic function:

$$\hat{F}_1 : (\mathbb{C} \to \wp(\mathbb{M})) \to (\mathbb{C} \to \wp(\mathbb{M}))$$

$$\hat{F}_1(X) = \alpha_1(I) \sqcup \lambda c \in \mathbb{C}.\; f_c(\bigcup_{c' \to c} X(c'))$$

where $f_c : \wp(\mathbb{M}) \to \wp(\mathbb{M})$ is a *transfer function* at program point c:

$$f_c(M) \;=\; \{m' \mid m \in M \;\wedge\; m' = [\![\mathbf{cmd}(c)]\!](m)\}$$

Lemma (Soundness of Partitioning Abstraction)

$\alpha_1(\mathit{fix}F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}_1^i(\bot)$.

Memory State Abstraction

Galois-connection:

$$\mathbb{C} \to \wp(\mathbb{M}) \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{C} \to \hat{\mathbb{M}}$$

$$\begin{array}{rcl} \alpha_2(f) & = & \lambda c.\ \alpha_m(f(c)) \\ \gamma_1(\hat{f}) & = & \lambda c.\ \gamma_m(\hat{f}(c)) \end{array}$$

where we assume

$$\wp(\mathbb{M}) \underset{\alpha_m}{\overset{\gamma_m}{\leftrightarrows}} \hat{\mathbb{M}}$$

Semantic function $\hat{F} : (\mathbb{C} \to \hat{\mathbb{M}}) \to (\mathbb{C} \to \hat{\mathbb{M}})$:

$$\hat{F}(X) = (\alpha_2 \circ \alpha_1)(I) \sqcup \lambda c \in \mathbb{C}.\ \hat{f}_c(\bigsqcup_{c' \to c} X(c'))$$

where *abstract transfer function* $\hat{f}_c : \hat{\mathbb{M}} \to \hat{\mathbb{M}}$ is given such that

$$\alpha_m \circ f_c \sqsubseteq \hat{f}_c \circ \alpha_m \tag{1}$$

Theorem (Soundness)

$\alpha(\mathit{fix} F) \sqsubseteq \bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\bot)$ *where* $\alpha = \alpha_2 \circ \alpha_1$.

Sign Analysis

Memory state abstraction:

$$\wp(\mathbb{M}) \underset{\alpha_m}{\overset{\gamma_m}{\leftrightarrows}} \hat{\mathbb{M}}$$

$$\alpha_m(M) \quad = \quad \lambda x \in \textbf{Var}.\ \alpha_s(\{m(x) \mid m \in M\})$$

where α_s is the sign abstraction:

$$\wp(\mathbb{Z}) \underset{\alpha_s}{\overset{\gamma_s}{\leftrightarrows}} \hat{\mathbb{Z}}$$

The transfer function $\hat{f}_c : \hat{\mathbb{M}} \to \hat{\mathbb{M}}$:

$$\begin{array}{rcll} \hat{f}_c(\hat{m}) & = & \hat{m} & c = skip \\ \hat{f}_c(\hat{m}) & = & \hat{m}[x \mapsto \hat{\mathcal{V}}(e)(\hat{m})] & c = x := e \end{array}$$

$$\begin{array}{rcl} \hat{\mathcal{V}}(n)(\hat{m}) & = & \alpha_s(\{n\}) \\ \hat{\mathcal{V}}(x)(\hat{m}) & = & \hat{m}(x) \\ \hat{\mathcal{V}}(e_1 + e_2) & = & \hat{\mathcal{V}}(e_1)(\hat{m}) \mathbin{\hat{+}} \hat{\mathcal{V}}(e_2)(\hat{m}) \\ \hat{\mathcal{V}}(e_1 - e_2) & = & \hat{\mathcal{V}}(e_1)(\hat{m}) \mathbin{\hat{-}} \hat{\mathcal{V}}(e_2)(\hat{m}) \end{array}$$

Lemma

$\alpha_m \circ f_c \sqsubseteq \hat{f}_c \circ \alpha_m$

Interval Analysis

Memory state abstraction:

$$\alpha_m(M) \quad = \quad \lambda x \in \textbf{Var}.\ \alpha_n(\{m(x) \mid m \in M\})$$

where α_n is the interval abstraction:

$$\wp(\mathbb{Z}) \underset{\alpha_n}{\overset{\gamma_n}{\leftrightarrows}} \hat{\mathbb{Z}}$$

$$\hat{\mathbb{Z}} = \{\bot\} \cup \{[l,u] \mid l,u \in \mathbb{Z} \cup \{-\infty,+\infty\} \land l \leq u\}$$

The transfer function $\hat{f}_c : \hat{\mathbb{M}} \to \hat{\mathbb{M}}$:

$$\begin{array}{rcll} \hat{f}_c(\hat{m}) & = & \hat{m} & c = skip \\ \hat{f}_c(\hat{m}) & = & \hat{m}[x \mapsto \hat{\mathcal{V}}(e)(\hat{m})] & c = x := e \end{array}$$

$$\begin{array}{rcl} \hat{\mathcal{V}}(n)(\hat{m}) & = & \alpha_s(\{n\}) \\ \hat{\mathcal{V}}(x)(\hat{m}) & = & \hat{m}(x) \\ \hat{\mathcal{V}}(e_1 + e_2) & = & \hat{\mathcal{V}}(e_1)(\hat{m}) \mathbin{\hat{+}} \hat{\mathcal{V}}(e_2)(\hat{m}) \\ \hat{\mathcal{V}}(e_1 - e_2) & = & \hat{\mathcal{V}}(e_1)(\hat{m}) \mathbin{\hat{-}} \hat{\mathcal{V}}(e_2)(\hat{m}) \end{array}$$

Lemma

$\alpha_m \circ f_c \sqsubseteq \hat{f}_c \circ \alpha_m$

Widening/Narrowing Example

```
i = 0;
while (i<10)
  i++;
```

- Abstract equation ($\hat{F}$):

$$
\begin{array}{rcl}
X_1 & = & [0,0] \\
X_2 & = & (X_1 \sqcup X_3] \sqcap [-\infty, 9] \\
X_3 & = & X_2 \mathbin{\hat{+}} [1,1] \\
X_4 & = & (X_1 \sqcup X_3) \sqcap [10, +\infty]
\end{array}
$$

- Abstract domain $\hat{D} = \text{Interval} \times \text{Interval} \times \text{Interval} \times \text{Interval}$
- Semantic function $\hat{F} : \hat{D} \to \hat{D}$ such that

$$(X_1, X_2, X_3, X_4) = \hat{F}(X_1, X_2, X_3, X_4)$$

Widening/Narrowing Example

$$
\begin{array}{rcl}
X_1 & = & [0,0] \\
X_2 & = & (X_1 \sqcup X_3] \sqcap [-\infty, 9] \\
X_3 & = & X_2 \hat{+} [1,1] \\
X_4 & = & (X_1 \sqcup X_3) \sqcap [10, +\infty]
\end{array}
$$

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

	0	1	2	3	4	5	6	...	
X_1	$\hat{\bot}$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$		$[0,0]$
X_2	$\hat{\bot}$	$\hat{\bot}$	$[0,0]$	$[0,0]$	$[0,1]$	$[0,1]$	$[0,2]$		$[0,9]$
X_3	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$[1,1]$	$[1,1]$	$[1,2]$	$[1,2]$		$[1,10]$
X_4	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$		$[10,10]$

Widening/Narrowing Example

A simple widening operator for the Interval domain:

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

A simple narrowing operator:

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

Widening/Narrowing Example

Widening iteration:

	0	1	2	3	4	5	6	7
X_1	$\hat{\bot}$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$
X_2	$\hat{\bot}$	$\hat{\bot}$	$[0,0]$	$[0,0]$	$[0,+\infty]$	$[0,+\infty]$	$[0,+\infty]$	$[0,+\infty]$
X_3	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$[1,1]$	$[1,1]$	$[1,+\infty]$	$[1,+\infty]$	$[1,+\infty]$
X_4	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$\hat{\bot}$	$[10,+\infty]$	$[10,+\infty]$

Narrowing iteration:

	0	1	2	3	4
X_1	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$	$[0,0]$
X_2	$[0,+\infty]$	$[0,9]$	$[0,9]$	$[0,9]$	$[0,9]$
X_3	$[1,+\infty]$	$[1,+\infty]$	$[1,10]$	$[1,10]$	$[1,10]$
X_4	$[10,+\infty]$	$[10,+\infty]$	$[10,+\infty]$	$[10,10]$	$[10,10]$