New York University, CIMS, CS, Course CSCI-GA.3140-001, Spring 2014

"Abstract Interpretation"

Ch. 17, Structural Fixpoint Prefix and Maximal Trace Semantics

Patrick Cousot

pcousot@cs.nyu.edu   cs.nyu.edu/~pcousot

Class 3, Monday, February 5th, 2014, 4:55-6:55 PM, WWH, Room CIWW 202

These slides are available at
http://cs.nyu.edu/~pcousot/courses/spring14/CSCI-GA.3140-001/slides/03--2024-02-05-structural-fixpoint-prefix-trace-semantics/slides-17--structural-fixpoint-prefix-trace-semantics-AI.pdf

Chapter 17

Ch. 17, Structural Fixpoint Prefix and Maximal Trace Semantics

Structural deductive prefix trace semantics

- The structural rule-based deductive definition of the prefix trace semantics in chapter 6 is great to prove that a trace is a feasible execution of a program;
- Not so great to prove program properties (we must reason not on one execution trace but on all of them);
- We reformulate the prefix trace semantics as a structural fixpoint definition;
- Great for program verification and program analysis!
- A mere application of theorem 16.12: a rule-based deductive definition can be reformulated as an equivalent fixpoint definition

Structural fixpoint prefix trace semantics

- A definition by induction on the program structure ($\widehat{\mathcal{S}}^*[\![\mathsf{S}]\!]$ is defined using $\widehat{\mathcal{S}}^*[\![\mathsf{S}']\!]$ for the (immediate) components S' of S, if any)

- For a given program component S, a fixpoint definition ($\widehat{\mathcal{S}}^*[\![\mathsf{S}]\!] = \mathrm{lfp}\ \mathcal{F}^*[\![\mathsf{S}]\!]$ where $\mathcal{F}^*[\![\mathsf{S}]\!]$ can use the semantics $\widehat{\mathcal{S}}^*[\![\mathsf{S}']\!]$ of the (immediate) components S' of S)

Rule-based deductive versus fixpoint semantics of assignment

Prefix traces of an assignment statement S ::= ℓ x = A ; $(\mathrm{at}[\![\mathsf{S}]\!] = \ell)$

- $$\frac{}{\mathrm{at}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi_1 \mathrm{at}[\![\mathsf{S}]\!])} \qquad (6.11)$$
- $$\frac{v = \mathscr{A}[\![\mathsf{A}]\!]\varrho(\pi^{\ell})}{\ell \xrightarrow{\mathsf{x} = \mathsf{A} = v} \mathrm{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi^{\ell})} \qquad (6.16)$$

Prefix traces of an assignment statement S ::= ℓ x = A ;

$$\begin{aligned} \widehat{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi^{\ell}) &= \{\ell\} \cup \{\ell \xrightarrow{\mathsf{x} = \mathsf{A} = v} \mathrm{after}[\![\mathsf{S}]\!] \mid v = \mathscr{A}[\![\mathsf{A}]\!]\varrho(\pi^{\ell})\} \qquad (17.2)\\ \widehat{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi^{\ell'}) &= \varnothing \qquad \text{when} \quad \ell' \neq \ell \end{aligned}$$

Rule-based deductive versus fixpoint semantics of assignment

Prefix traces of an assignment statement S ::= $^\ell$ x = A ; $(\mathsf{at}[\![\mathsf{S}]\!] = \ell)$

- $$\frac{}{\mathsf{at}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!])} \tag{6.11}$$
- $$\frac{v = \mathscr{A}[\![\mathsf{A}]\!]\varrho(\pi^\ell)}{\ell \xrightarrow{\mathsf{x} = \mathsf{A} = v} \mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathsf{S}]\!](\pi^\ell)} \tag{6.16}$$

Prefix traces of an assignment statement S ::= $^\ell$ x = A ;

$$\begin{aligned}
\widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathsf{S}]\!](\pi^\ell) &= \{\ell\} \cup \{\ell \xrightarrow{\mathsf{x} = \mathsf{A} = v} \mathsf{after}[\![\mathsf{S}]\!] \mid v = \mathscr{A}[\![\mathsf{A}]\!]\varrho(\pi^\ell)\} \\
\widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathsf{S}]\!](\pi^{\ell'}) &= \varnothing \qquad \text{when} \quad \ell' \neq \ell
\end{aligned} \tag{17.2}$$

But where is the fixpoint???

Fixpoint semantics of assignment

- No recursion is involved in the definition of the semantics
- The fixpoint of a constant function $f(x) = c$ is that constant c!

$$\begin{array}{rcl}
\widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathsf{S}]\!](\pi^\ell) & = & \mathsf{lfp}^{\dot{\subseteq}}\, \boldsymbol{\mathcal{F}}^*[\![\mathsf{S}]\!] \\
\boldsymbol{\mathcal{F}}^*[\![\mathsf{S}]\!](X)\,\pi^\ell & = & \{\ell\} \cup \{\ell \xrightarrow{\mathsf{x} = \mathsf{A} = v} \mathsf{after}[\![\mathsf{S}]\!] \mid v = \boldsymbol{\mathcal{A}}[\![\mathsf{A}]\!]\boldsymbol{\varrho}(\pi^\ell)\}
\end{array}$$

($\dot{\subseteq}$ is $\subseteq$ pointwise)

Fixpoint prefix trace semantics of a statement list

Prefix traces of a statement list $\texttt{Sl} ::= \texttt{Sl}' \ \texttt{S}$

$$
\begin{aligned}
\widehat{\boldsymbol{\mathcal{S}}}^{*}[\![\texttt{Sl}]\!](\pi_1) \quad = \quad & \widehat{\boldsymbol{\mathcal{S}}}^{*}[\![\texttt{Sl}']\!](\pi_1) \cup \\
& \{\pi_2 \frown \pi_3 \mid \pi_2 \in \widehat{\boldsymbol{\mathcal{S}}}^{+}[\![\texttt{Sl}']\!](\pi_1) \wedge \pi_3 \in \widehat{\boldsymbol{\mathcal{S}}}^{*}[\![\texttt{S}]\!](\pi_1 \frown \pi_2)\}
\end{aligned}
\tag{17.3}
$$

Fixpoint prefix trace semantics of an iteration

Prefix traces of an iteration statement $\mathsf{S} ::= \mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b$

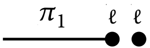
$$\mathcal{S}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] \quad = \quad \mathsf{lfp}^{\subseteq}\ \mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] \tag{17.4}$$

$$\mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1\ell') \quad \triangleq \quad \varnothing \qquad \text{when} \quad \ell' \neq \ell$$

$$\begin{array}{ll}
\mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1\ell) \quad \triangleq \quad \{\ell\} & \text{(a)}\\
\cup\ \{\ell'\pi_2\ell' \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge & \\
\qquad \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{ff} \wedge \ell' = \ell\} & \text{(b)}\\
\cup\ \{\ell'\pi_2\ell' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3 \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{tt} & \\
\qquad \wedge\ \pi_3 \in \mathcal{S}^*[\![\mathsf{S}_b]\!](\pi_1\ell'\pi_2\ell' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \ell' = \ell\} & \text{(c)}
\end{array}$$

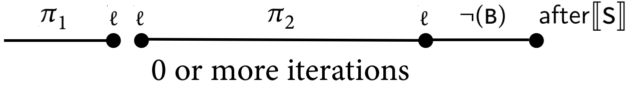
Explanation of the term (a)

$$\mathscr{F}^*[\![\mathtt{while}\ ^{\ell}\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1{}^{\ell}) \quad \triangleq \quad \{\ell\} \qquad \text{(a)}$$
$$\qquad \cup\ \ldots$$



Explanation of the term (b)

$$
\begin{aligned}
\mathscr{F}^*[\![\texttt{while}\ ^{\ell}\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1\ell) \quad &\triangleq \quad \ldots \\
\cup \ \{\ell'\pi_2\ell' \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{ff} \wedge \ell' = \ell\} \qquad & (\mathrm{b}) \\
\cup \ \ldots &
\end{aligned}
$$

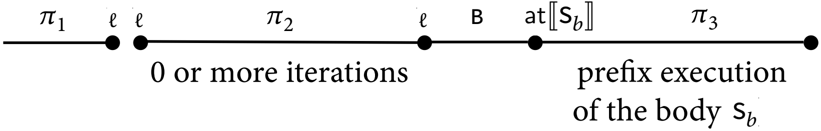


Explanation of the term (c)

$$\mathscr{F}^*[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1\ell) \triangleq \ldots$$

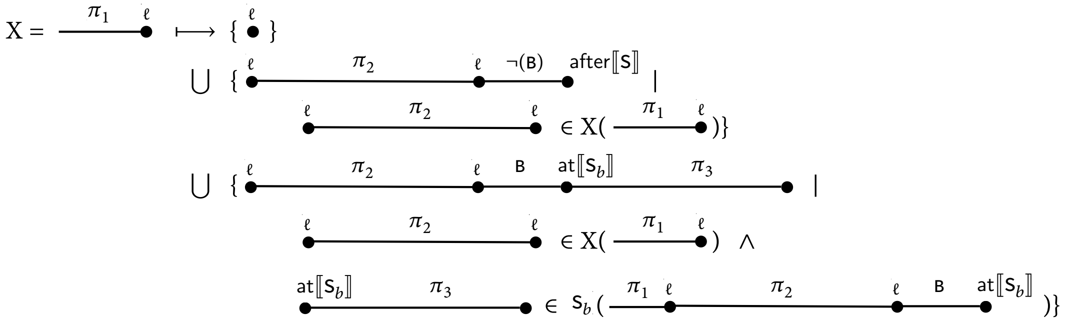
$$\cup\ \{\ell'\pi_2\ell' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3 \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{tt}$$

$$\wedge\ \pi_3 \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!](\pi_1\ell'\pi_2\ell' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \ell' = \ell\} \qquad \text{(c)}$$



Explanation of the fixpoint iteration

$$X = \mathscr{F}^*[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!](X)$$



Fixpoint prefix trace semantics of an iteration

Prefix traces of an iteration statement $\mathsf{S} ::= \mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b$

$$\mathcal{S}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] \quad = \quad \mathsf{lfp}^{\subseteq}\ \mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] \tag{17.4}$$

$$\mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1\ell') \quad \triangleq \quad \varnothing \qquad \text{when} \quad \ell' \neq \ell$$

$$\mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!](X)(\pi_1\ell) \quad \triangleq \quad \{\ell\} \tag{a}$$

$$\cup\ \{\ell'\pi_2\ell' \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{ff} \wedge \ell' = \ell\} \tag{b}$$

$$\cup\ \{\ell'\pi_2\ell' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3 \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{tt} \wedge \pi_3 \in \mathcal{S}^*[\![\mathsf{S}_b]\!](\pi_1\ell'\pi_2\ell' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \ell' = \ell\} \tag{c}$$

The End, Thank you