Principles of Abstract Interpretation
MIT press

Ch. **17**, Structural fixpoint prefix and maximal trace semantics

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-17--structural-fixpoint-prefix-trace-semantics-PrAbsInt.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 16.11: 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 ($\widehat{\mathcal{S}}^*[\![\mathsf{S}]\!] = \mathsf{lfp}\, \mathcal{F}^*[\![\mathsf{S}]\!]$ 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 $\mathtt{S} ::= {}^{\ell}\ \mathtt{x = A ;}$ $(\mathrm{at}[\![\mathtt{S}]\!] = \ell)$

- $$\frac{}{\mathrm{at}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{*}[\![\mathtt{S}]\!](\pi_1\mathrm{at}[\![\mathtt{S}]\!])} \tag{6.11}$$

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

Prefix traces of an assignment statement $\mathtt{S} ::= {}^{\ell}\ \mathtt{x = E ;}$

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

Rule-based deductive versus fixpoint semantics of assignment

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

- $$\frac{}{\text{at}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{\,*}[\![\mathtt{S}]\!](\pi_1\text{at}[\![\mathtt{S}]\!])} \tag{6.11}$$

- $$\frac{\upsilon = \mathcal{A}[\![\mathtt{A}]\!]\varrho(\pi^{\ell})}{\ell \xrightarrow{\mathtt{x = A} = \upsilon} \text{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{\,*}[\![\mathtt{S}]\!](\pi^{\ell})} \tag{6.16}$$

Prefix traces of an assignment statement $\mathtt{S} ::= {}^{\ell}\ \mathtt{x = E\ ;}$

$$\begin{array}{rcl}\widehat{\mathcal{S}}^{\,*}[\![\mathtt{S}]\!](\pi^{\ell}) & = & \{\ell\} \cup \{\ell \xrightarrow{\mathtt{x = E} = \upsilon} \text{after}[\![\mathtt{S}]\!] \mid \upsilon = \mathcal{E}[\![\mathtt{E}]\!]\varrho(\pi^{\ell})\} \\ \widehat{\mathcal{S}}^{\,*}[\![\mathtt{S}]\!](\pi^{\ell'}) & = & \varnothing \qquad \text{when} \quad \ell' \neq \ell\end{array} \tag{17.2}$$

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!

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

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

Fixpoint prefix trace semantics of a statement list

Prefix traces of a statement list `Sl ::= Sl′ S`

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

Fixpoint prefix trace semantics of an iteration

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

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

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

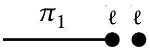
$$\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!](X)(\pi_1\ell) \quad \triangleq \quad \{\ell\} \tag{a}$$

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

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

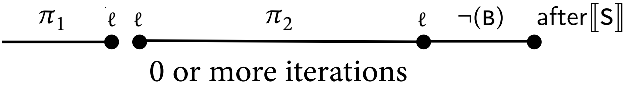
Explanation of the term (a)

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



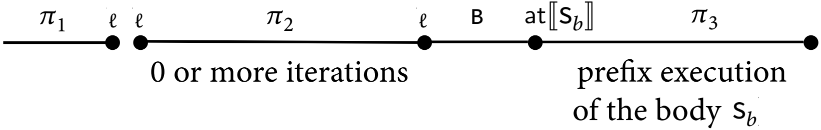
Explanation of the term (b)

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



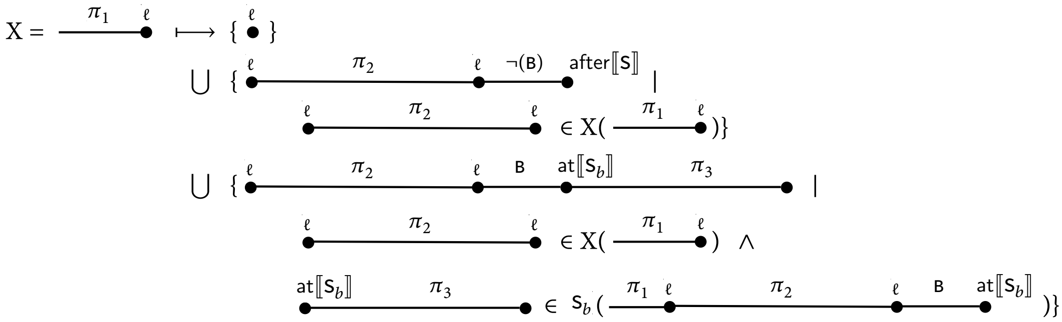
Explanation of the term (c)

$$
\begin{aligned}
\mathscr{F}^*[\![\texttt{while}\,^{\ell}\,\texttt{(B)}\;\texttt{S}_b]\!](X)(\pi_1{}^{\ell}) \quad &\triangleq \quad \ldots \\
\cup \{\ell'\pi_2\ell' \xrightarrow{\texttt{B}} \mathsf{at}[\![\texttt{S}_b]\!] \frown \pi_3 \mid \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathscr{B}[\![\texttt{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathsf{tt} \\
\wedge\, \pi_3 \in \mathscr{S}^*[\![\texttt{S}_b]\!](\pi_1\ell'\pi_2\ell' \xrightarrow{\texttt{B}} \mathsf{at}[\![\texttt{S}_b]\!]) \wedge \ell' = \ell\} \qquad \text{(c)}
\end{aligned}
$$



Explanation of the fixpoint iteration

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



Fixpoint prefix trace semantics of an iteration

Prefix traces of an iteration statement S ::= while ℓ (B) S_b

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

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

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

$$\cup \left\{\ell'\pi_2\ell' \xrightarrow{\neg(\texttt{B})} \mathsf{after}[\![\texttt{S}]\!] \;\middle|\; \ell'\pi_2\ell' \in X(\pi_1\ell') \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_1\ell'\pi_2\ell') = \mathrm{ff} \wedge \ell' = \ell\right\} \tag{b}$$

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

Home work

- Read Ch. **17** "Structural fixpoint prefix and maximal trace semantics" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you