New York University, CIMS, CS, Course CSCI-GA.3140-001, Fall 2021

"Abstract Interpretation"

Ch. 42, Stateful Prefix Trace Semantics

Patrick Cousot

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

Class 1 (preliminary), Monday, January 25th, 2021, M 9:30–11:40 AM, Online class

These slides are available at
http://cs.nyu.edu/~pcousot/courses/spring21/CSCI-GA.3140-001/slides/slides-42--stateful-trace-semantics-AI.pdf

Chapter 42

Ch. 42, Stateful Prefix Trace Semantics

Introduction

Objectives

- Our prefix/maximal trace semantics have no memory states (only a control state materialized by a program label)
- Classical trace semantics do have a memory state (often with no actions)
- This is a simple abstraction

Stateful prefix trace semantics abstraction

Stateful abstraction

- States $\sigma = \langle \ell,\ \rho \rangle \in \mathbb{S} \triangleq (\mathbb{L} \times \mathbb{E}\mathrm{v})$
- Stateful abstraction

$$
\begin{aligned}
\alpha^{\mathbb{S}}(\langle \pi_0\ell,\ \ell \rangle) &\triangleq \langle \ell,\ \boldsymbol{\varrho}(\pi_0\ell) \rangle \\
\alpha^{\mathbb{S}}(\langle \pi_0,\ \pi \xrightarrow{\mathsf{a}} \ell \rangle) &\triangleq \alpha^{\mathbb{S}}(\langle \pi_0,\ \pi \rangle) \cdot \langle \ell,\ \boldsymbol{\varrho}(\pi_0 \frown \pi \xrightarrow{\mathsf{a}} \ell) \rangle
\end{aligned}
\tag{42.1}
$$

- Actions are abstracted away, values of variables are recorded everywhere in the trace (instead of being retrieved from past computations).
- Therefore

$\alpha^{\mathbb{S}}(\langle \pi_0,\ \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ell_3 \ldots \ell_{n-1} \xrightarrow{\mathsf{a}_{n-1}} \ell_n \rangle) = \langle \ell_1,\ \boldsymbol{\varrho}(\pi_0 \frown \ell_1) \rangle \langle \ell_2,\ \boldsymbol{\varrho}(\pi_0 \frown \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2) \rangle \langle \ell_3,$ $\boldsymbol{\varrho}(\pi_0 \frown \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ell_3) \rangle \ldots \langle \ell_{n-1},\ \boldsymbol{\varrho}(\pi_0 \frown \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ell_3 \ldots \ell_{n-1}) \rangle \langle \ell_n,\ \boldsymbol{\varrho}(\pi_0 \frown \ell_1 \xrightarrow{\mathsf{a}_1}$ $\ell_2 \xrightarrow{\mathsf{a}_2} \ell_3 \ldots \ell_{n-1} \xrightarrow{\mathsf{a}_{n-1}} \ell_n) \rangle$

Stateful abstraction

- The abstraction of semantics is the homomorphic abstraction of these trace pairs.

$$\alpha^{\mathbb{S}}(\Pi) \quad \triangleq \quad \{\alpha^{\mathbb{S}}(\langle\pi_0,\ \pi\rangle) \mid \langle\pi_0,\ \pi\rangle \in \Pi\}$$

  so that, by exercise 11.6,

$$\langle\wp(\mathbb{T}^+ \times \mathbb{T}^+),\ \subseteq\rangle \xrightleftharpoons[\alpha^{\mathbb{S}}]{\gamma^{\mathbb{S}}} \langle\wp(\mathbb{S}^+),\ \subseteq\rangle$$

- We consider all possible initialization traces that is the abstraction

$$\langle\mathbb{T}^+ \rightarrow \wp(\mathbb{T}^+),\ \dot{\subseteq}\rangle \xrightleftharpoons[\alpha^{\mathbb{S}}]{\gamma^{\mathbb{S}}} \langle\wp(\mathbb{S}^+),\ \subseteq\rangle$$

  defined by

$$\alpha^{\mathbb{S}}(\boldsymbol{\mathcal{S}}) \triangleq \alpha^{\mathbb{S}}(\{\langle\pi_0,\ \pi\rangle \mid \pi_0 \in \mathbb{T}^+ \wedge \pi \in \boldsymbol{\mathcal{S}}(\pi_0)\}) = \{\alpha^{\mathbb{S}}(\langle\pi_0,\ \pi\rangle) \mid \pi_0 \in \mathbb{T}^+ \wedge \pi \in \boldsymbol{\mathcal{S}}(\pi_0)\}$$

  where $\mathbb{S}^+$ is the set of all non-empty sequences of states in $\mathbb{S}$.

Stateful prefix trace semantics

- $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!] \quad \triangleq \quad \alpha^{\mathbb{S}}(\boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!])$ (42.2)
- We now look for a structural specification $\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!] = \boldsymbol{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!]$ of the prefix state trace semantics

$$\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!] \quad = \quad f^{*}_{\mathbb{S}}[\![\mathsf{S}]\!](\prod_{\mathsf{S}' \lhd \mathsf{S}} \widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{S}}[\![\mathsf{S}']\!]) \tag{42.3}$$

- By calculational design.

Structural stateful prefix trace semantics

- A prefix trace describes the beginning of a computation
- Evaluation of an arithmetic expression

$$
\begin{aligned}
\mathscr{A}[\![1]\!]\rho &\triangleq 1 \\
\mathscr{A}[\![\mathsf{x}]\!]\rho &\triangleq \rho(\mathsf{x}) \\
\mathscr{A}[\![\mathsf{A}_1 - \mathsf{A}_2]\!]\rho &\triangleq \mathscr{A}[\![\mathsf{A}_1]\!]\rho - \mathscr{A}[\![\mathsf{A}_2]\!]\rho
\end{aligned}
\tag{3.4}
$$

- Assignment $\mathsf{S} ::= {}^{\ell}\ \mathsf{x} = \mathsf{A}\ ;$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$
\widehat{\boldsymbol{\mathcal{S}}}^{\,*}_{\mathbb{S}}[\![\mathsf{S}]\!] = \{\langle\ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \{\langle\ell,\ \rho\rangle\langle\mathsf{after}[\![\mathsf{S}]\!],\ \rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho]\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}
\tag{42.4}
$$

Proof of (42.4)

$$\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!]$$

$$\triangleq \boldsymbol{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!] \qquad \text{\textit{(def. $\widehat{\boldsymbol{\mathcal{S}}}^{*}_{\mathbb{S}}$, structural version of $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{S}}$)}}$$

$$\triangleq \alpha^{\mathbb{S}}(\boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!]) \qquad \text{(def. (42.2) of $\boldsymbol{\mathcal{S}}^{*}_{\mathbb{S}}$)}$$

$$= \alpha^{\mathbb{S}}(\widehat{\boldsymbol{\mathcal{S}}}^{*}[\![\mathsf{S}]\!]) \qquad \text{(theorem 17.7)}$$

$$= \{\alpha^{\mathbb{S}}(\langle \pi,\ \pi' \rangle) \mid \pi \in \mathbb{T}^{+} \wedge \pi' \in \widehat{\boldsymbol{\mathcal{S}}}^{*}[\![\mathsf{S}]\!](\pi)\} \qquad \text{(def. (42.1) of $\alpha^{\mathbb{S}}$)}$$

$$= \{\alpha^{\mathbb{S}}(\langle \pi\ell',\ \pi' \rangle) \mid \pi\ell' \in \mathbb{T}^{+} \wedge \pi' \in \{\ell'\} \cup \{\ell' \xrightarrow{\ \mathsf{x}\,=\,\mathsf{A}\,=\,v\ } \mathsf{after}[\![\mathsf{S}]\!] \mid v = \boldsymbol{\mathscr{A}}[\![\mathsf{A}]\!]\boldsymbol{\varrho}(\pi\ell')\} \wedge \ell' = \ell\}$$

$$\text{(def. (17.2) of $\widehat{\boldsymbol{\mathcal{S}}}^{*}[\![\mathsf{S}]\!]$ and \textit{Remark} 17.8)}$$

$$= \{\alpha^{\mathbb{S}}(\langle \pi\ell',\ \ell' \rangle) \mid \pi\ell' \in \mathbb{T}^{+} \wedge \ell' = \ell\} \cup \{\alpha^{\mathbb{S}}(\langle \pi\ell',\ \ell' \xrightarrow{\ \mathsf{x}\,=\,\mathsf{A}\,=\,v\ } \mathsf{after}[\![\mathsf{S}]\!] \rangle) \mid \pi\ell' \in \mathbb{T}^{+} \wedge v = \boldsymbol{\mathscr{A}}[\![\mathsf{A}]\!]\boldsymbol{\varrho}(\pi\ell') \wedge \ell' = \ell\} \qquad \text{(def. $\cup$)}$$

$$= \{\langle \ell,\ \boldsymbol{\varrho}(\pi\ell) \rangle \mid \pi\ell' \in \mathbb{T}^{+} \wedge \ell' = \ell\} \cup \{\langle \ell',\ \boldsymbol{\varrho}(\pi\ell') \rangle \langle \mathsf{after}[\![\mathsf{S}]\!],\ \boldsymbol{\varrho}(\pi\ell' \xrightarrow{\ \mathsf{x}\,=\,\mathsf{A}\,=\,v\ } \mathsf{after}[\![\mathsf{S}]\!]) \rangle \mid \pi\ell' \in \mathbb{T}^{+} \wedge v = \boldsymbol{\mathscr{A}}[\![\mathsf{A}]\!]\boldsymbol{\varrho}(\pi\ell') \wedge \ell' = \ell\} \qquad \text{(def. $\alpha^{\mathbb{S}}$)}$$

$$= \{\langle \ell,\ \rho \rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \{\langle \ell,\ \rho \rangle \langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho[\mathsf{x} \leftarrow v] \rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge v = \boldsymbol{\mathscr{A}}[\![\mathsf{A}]\!]\rho\}$$

$$\text{(letting $\rho = \boldsymbol{\varrho}(\pi\ell')$ and conversely, by (6.6) and exercise 6.8, $\forall \rho \in \mathbb{E}\mathbb{v}\ .\ \exists \pi\ell' \in \mathbb{T}^{+}\ .\ \rho = \boldsymbol{\varrho}(\pi\ell')$, and $\ell' = \ell = \mathsf{at}[\![\mathsf{S}]\!]$)}$$

$\square$

Structural stateful prefix trace semantics (cont'd)

- Break statement $\mathsf{S} ::= \ell\ \texttt{break}\ ;$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$\boldsymbol{\mathcal{S}}^*[\![\mathsf{S}]\!] \triangleq \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \{\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \tag{42.14}$$

Structural stateful prefix trace semantics (cont'd)

- Conditional statement $\mathsf{S} ::= \mathtt{if}\ \ell\ (\mathsf{B})\ \mathsf{S}_t$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$\begin{aligned}\widehat{\mathcal{S}}^*[\![\mathsf{S}]\!] \triangleq\ & \{\langle\ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}\\ & \cup \{\langle\ell,\ \rho\rangle\langle\mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{ff}\}\\ & \cup \{\langle\ell,\ \rho\rangle\langle\mathsf{at}[\![\mathsf{S}_t]\!],\ \rho\rangle\pi \mid \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \langle\mathsf{at}[\![\mathsf{S}_t]\!],\ \rho\rangle\pi \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!]\}\end{aligned}$$

- If the conditional statement S is inside an iteration statement, and S_t has a break, the execution goes on at the $\mathsf{break\text{-}to}[\![\mathsf{S}]\!]$ after the iteration.

Structural stateful prefix trace semantics (cont'd)

- Statement list $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$ (where $\mathsf{at}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{Sl}']\!]$)

$$
\begin{aligned}
\widehat{\mathcal{S}}^*[\![\mathtt{Sl}]\!] &\triangleq \widehat{\mathcal{S}}^*[\![\mathtt{Sl}']\!] \cup \widehat{\mathcal{S}}^*[\![\mathtt{Sl}']\!] \mathbin{\frown\!\!\!\!\cdot\;} \mathcal{S}^*[\![\mathtt{S}]\!] \\
\mathcal{S} \mathbin{\frown\!\!\!\!\cdot\;} \mathcal{S}' &\triangleq \{\pi \mathbin{\frown\!\!\!\!\cdot\;} \pi' \mid \pi \in \mathcal{S} \wedge \pi' \in \mathcal{S}' \wedge \pi \mathbin{\frown\!\!\!\!\cdot\;} \pi' \text{ is well-defined}\}
\end{aligned}
\tag{42.5}
$$

- $\pi' \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!]$ starts $\mathsf{at}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{Sl}']\!]$ so, by def. $\frown\!\!\!\!\cdot\;$, the trace $\pi \in \widehat{\mathcal{S}}^*[\![\mathtt{Sl}']\!]$ must terminate to be able to go on with $\mathtt{S}$.

Structural stateful prefix trace semantics (cont'd)

- Empty statement list $\texttt{Sl} ::= \epsilon$ (where $\mathsf{at}[\![\texttt{Sl}]\!] \triangleq \mathsf{after}[\![\texttt{Sl}]\!]$)

$$\boldsymbol{\mathcal{S}}^*[\![\texttt{Sl}]\!] \triangleq \{\langle \mathsf{at}[\![\texttt{Sl}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}$$

Structural stateful prefix trace semantics (cont'd)

- Iteration statement $\mathsf{S} ::= \texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b$ (where $\mathsf{at}[\![\mathsf{S}]\!] = \ell$)

$$\widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] \quad = \quad \mathsf{lfp}^{\subseteq}\ \mathcal{F}(prefixtag)[\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b] \tag{42.6}$$

$$\begin{aligned}
\mathcal{F}^{*}_{\mathbb{S}}[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]\ X \quad \triangleq \quad & \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} && \text{(a)}\\
& \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff} \wedge \ell' = \ell\} && \text{(b)}\\
& \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{tt} \wedge && \text{(c)}\\
& \qquad \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!] \wedge \ell' = \ell\}
\end{aligned}$$

(a) either the execution observation stop at $[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] = \ell$, or

(b) after a number of iterations, control is back to ℓ, the test is false, and the loop is exited, or

(c) after a number of iterations, control is back to ℓ, the test is true, and the loop body is executed

(This includes the termination of the loop body after$[\![\mathsf{S}_b]\!]$ = at$[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!] = \ell$)

Maximal trace semantics

- Maximal trace semantics

$$\begin{aligned}\boldsymbol{\mathcal{S}}^{+}[\![\mathsf{S}]\!] &\triangleq \{\pi\langle \ell,\ \rho\rangle \in \boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!] \mid (\ell = \mathsf{after}[\![\mathsf{S}]\!]) \vee (\mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell = \mathsf{break\text{-}to}[\![\mathsf{S}]\!])\}\\ \boldsymbol{\mathcal{S}}^{\infty}[\![\mathsf{S}]\!] &\triangleq \lim(\boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!])\end{aligned}$$

- Limit

$$\lim \mathscr{T} \triangleq \{\pi \in \mathbb{T}^{\infty} \mid \forall n \in \mathbb{N}\ .\ \pi[0..n] \in \mathscr{T}\}.$$

Conclusion

Conclusion

- We made the link between the stateless prefix trace semantics of chapter 6 and the more traditional stateful trace
- An early reference is [Wegner, 1972] stating “Implementation-dependent models may be referred to as *operational models* since they characterize functions constructively in terms of the ″observable″ sequences of state transitions by which they may be evaluated.″

Bibliography

References I

Bibliography

Wegner, Peter (Jan. 1972). "Operational Semantics of Programming Languages.". *ACM SIGPLAN Not.* 7.1, pp. 128–141.

The End, Thank you