Principles of Abstract Interpretation

MIT press

Ch. **6**, Structural deductive stateless prefix 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-06--prefix-trace-semantics-PrAbsInt.pdf

Chapter 6

Ch. **6**, Structural deductive stateless prefix trace semantics

Trace semantics, informally

Hand computation of

$$\underbrace{\underbrace{\underbrace{(1-1)}_{a}-1}_{b} < \underbrace{(1-1)}_{a}}_{c}$$

is

$$
\begin{aligned}
a &= 1 - 1\\
a &= 0\\
b &= a - 1\\
b &= 0 - 1\\
b &= -1\\
c &= b < a\\
c &= -1 < 0\\
c &= tt
\end{aligned}
$$

read from

partial trace

maximal finite trace

Syntax and trace semantics of a language

- syntax: rules to write programs of the language;
- semantics: defines the runtime behavior of programs that is what and how they compute when executed:
  - trace: sequence of events recording the actions executed during a program execution,
  - partial trace: finite observation of an execution; this observation can stop at any time,
  - finite trace: partial trace that ends upon execution termination,
  - infinite trace: infinite observation of an execution that never terminates,
  - maximal trace: finite or infinite execution trace.

Traces

Finite traces of a program: P

- Program:

$$
\begin{array}{l}
\ell_1\ \mathtt{x = x + 1 ;} \\
\quad \mathtt{while}\ \ell_2\ (\mathrm{tt})\ \{ \\
\qquad \ell_3\ \mathtt{x = x + 1 ;} \\
\qquad \mathtt{if}\ \ell_4\ (\mathtt{x > 2})\ \ell_5\ \mathtt{break ;}\}\ell_6\mathtt{;}\ell_7
\end{array}
\tag{4.5}
$$

- Prefix traces (from ℓ_1, initially $\mathtt{x} = 0$):
  - ℓ_1
  - $\ell_1 \xrightarrow{\mathtt{x = x + 1} = 1} \ell_2 \xrightarrow{\mathrm{tt}} \ell_3 \xrightarrow{\mathtt{x = x + 1} = 2} \ell_4 \xrightarrow{\neg(\mathtt{x > 2})} \ell_2 \xrightarrow{\mathrm{tt}} \ell_3 \tag{6.2}$
- Finite (maximal) traces:
  - $\ell_1 \xrightarrow{\mathtt{x = x + 1} = 1} \ell_2 \xrightarrow{\mathrm{tt}} \ell_3 \xrightarrow{\mathtt{x = x + 1} = 2} \ell_4 \xrightarrow{\neg(\mathtt{x > 2})} \ell_2 \xrightarrow{\mathrm{tt}} \ell_3 \xrightarrow{\mathtt{x = x + 1} = 3}$
    $\ell_4 \xrightarrow{\mathtt{x > 2}} \ell_5 \xrightarrow{\mathtt{break}} \ell_6 \xrightarrow{\mathtt{skip}} \ell_7$

Infinite traces of a program: P

- Program:

$$\ell_1\ \texttt{x = 0 ; while}\ \ell_2\ (\mathtt{tt})\ \{\ \ell_3\ \texttt{x = x+1 ;}\ \}\ \ell_4$$

- Infinite trace:

$$\ell_1 \xrightarrow{\texttt{x = 0} = 0} \ell_2 \xrightarrow{\mathtt{tt}} \ell_3 \xrightarrow{\texttt{x = x + 1} = 1} \ell_2 \xrightarrow{\mathtt{tt}} \ell_3 \xrightarrow{\texttt{x = x + 1} = 2} \ell_2 \ldots \ell_2 \xrightarrow{\mathtt{tt}} \ell_3$$
$$\xrightarrow{\texttt{x = x + 1} = n} \ell_2 \xrightarrow{\mathtt{tt}} \ell_3 \xrightarrow{\texttt{x = x + 1} = n+1} \ell_2 \ldots$$

Traces

- $\mathbb{T}^+$: the set of all finite traces,
- $\mathbb{T}^\infty$: the set of all infinite traces,
- $\mathbb{T}^{+\infty}$: the set of all finite or infinite traces.
- Conventions:
  - we write $\pi = {}^{\ell}\pi'$ to make clear that the trace π is assumed to start with the program label ℓ (although π' is not itself a properly formed trace),
  - we write $\pi = \pi'{}^{\ell}$ when assuming that the trace π is finite and ends with label ℓ (although, again, π' is not itself a properly formed trace).

Trace concatenation $\frown$

- Definition:

$$
\begin{array}{rcll}
\pi_1\ell_1 \frown \ell_2\pi_2 & & & \text{undefined if } \ell_1 \neq \ell_2 \\
\pi_1\ell_1 \frown \ell_1\pi_2 & \triangleq & \pi_1\ell_1\pi_2 & \text{if } \pi_1 \text{ is finite} \\
\pi_1 \frown \pi_2 & \triangleq & \pi_1 & \text{if } \pi_1 \text{ is infinite}
\end{array}
$$

- In pattern matching, we sometimes need the empty trace $\ni$. For example $\ell\pi\ell' = \ell$ then $\pi = \ni$ and $\ell = \ell'$.

Value of variables

Values of variables on a trace

- the value $\varrho(\pi)\mathtt{x}$ of variable $\mathtt{x}$ *at the end* of trace π is the last value assigned to $\mathtt{x}$ (or 0 at initialization).

$$
\begin{aligned}
\varrho(\pi^{\ell} \xrightarrow{\;\mathtt{x = A} = \upsilon\;} \ell')\mathtt{x} &\triangleq \upsilon \\
\varrho(\pi^{\ell} \xrightarrow{\;\cdots\;} \ell')\mathtt{x} &\triangleq \varrho(\pi^{\ell}) \quad \text{otherwise} \\
\varrho(\ell)\mathtt{x} &\triangleq 0
\end{aligned}
\tag{6.6}
$$

Prefix trace semantics of a statement

Prefix trace semantics

- Let $\pi_1\mathsf{at}[\![\mathsf{S}]\!]$ be an initialization trace ending on entry $\mathsf{at}[\![\mathsf{S}]\!]$ of statement S.
- $\mathcal{S}^*[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!])$ is the set of prefix traces $\mathsf{at}[\![\mathsf{S}]\!]\pi_2\ell$ of S continuing the trace $\pi_1\mathsf{at}[\![\mathsf{S}]\!]$ and reaching some program label $\ell \in \mathsf{labx}[\![\mathsf{S}]\!]$.
- Schematically,

$$\xrightarrow{\quad\pi_1\quad} \underbrace{\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\quad\pi_2\quad} \ell}_{\in\ \mathcal{S}^*[\![\mathsf{S}]\!](\pi_1\mathsf{at}[\![\mathsf{S}]\!])}$$

- Although our language is determinist, we consider a set of possible continuations to cope *e.g.* with inputs and random number generation.
- By convention $\mathcal{S}^*[\![\mathsf{S}]\!](\pi_1\ell) = \varnothing$ when $\ell \neq \mathsf{at}[\![\mathsf{S}]\!]$.

Maximal finite trace semantics

- Let $\pi_1 \mathsf{at}[\![\mathsf{S}]\!]$ be an initialization trace ending on entry $\mathsf{at}[\![\mathsf{S}]\!]$ of statement S.
- $\mathcal{S}^+[\![\mathsf{S}]\!](\pi_1 \mathsf{at}[\![\mathsf{S}]\!])$ is the set of maximal finite traces $\mathsf{at}[\![\mathsf{S}]\!]\pi_2\mathsf{after}[\![\mathsf{S}]\!]$ of S continuing the trace $\pi_1 \mathsf{at}[\![\mathsf{S}]\!]$ and reaching $\mathsf{after}[\![\mathsf{S}]\!]$.
- Schematically,

$$\xrightarrow{\quad\quad\pi_1\quad\quad} \underbrace{\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\quad\quad\pi_2\quad\quad} \mathsf{after}[\![\mathsf{S}]\!]}_{\in\ \mathcal{S}^+[\![\mathsf{S}]\!](\pi_1 \mathsf{at}[\![\mathsf{S}]\!])}$$

- Formally,

$$\mathcal{S}^+[\![\mathsf{S}]\!](\pi_1 \mathsf{at}[\![\mathsf{S}]\!]) \quad \triangleq \quad \{\pi_2 \ell \in \mathcal{S}^*[\![\mathsf{S}]\!](\pi_1 \mathsf{at}[\![\mathsf{S}]\!]) \mid \ell = \mathsf{after}[\![\mathsf{S}]\!]\} \tag{6.9}$$

Introduction to rule-based structural definitions

Structural definitions and proofs

- Structural definitions are recursive definitions over the syntax of programs;
- Structural proofs generalize proofs by recurrence to induction on the syntax of programs;
- Structural proofs are well suited to prove properties of structural definitions (*e.g.* that a structural definition is well-defined *i.e.* the recursive definition considered as a program does terminate).

Example of rule-based structural definition

- Denotation of positive integers $\mathbb{N}^+$ by a collection of sticks:
$$\mathbb{N}^+ ::= \mathbf{I} \mid \mathbb{N}^+\mathbf{I}$$
- Example: $\mathbf{IIIIII}$ is six
- Structural definition of the set $\mathbb{O}$ of odd positive integers:
  - axiom $\dfrac{}{\mathbf{I} \in \mathbb{O}}$
  - inference rule $\dfrac{n \in \mathbb{O}}{n\mathbf{II} \in \mathbb{O}}$
- Set $s(n)$ of numbers smaller than or equal to n:
$$\frac{}{n \in s(n)} \qquad \frac{m\mathbf{I} \in s(n)}{m \in s(n)}$$

Example: $\mathbf{III} \in s(\mathbf{III})$ by the axiom so $\mathbf{II} \in s(\mathbf{III})$ by the inference rule so $\mathbf{I} \in s(\mathbf{III})$ by the inference rule proving that $s(\mathbf{III}) = \{\mathbf{III}, \mathbf{II}, \mathbf{I}\}$.

Structural prefix trace semantics

Prefix trace semantics $\widehat{\mathcal{S}}^*[\![\mathsf{S}]\!]$ of a program component S

$$\pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}]\!](\pi_1)$$

- the prologue trace π_1 terminates at $\mathsf{at}[\![\mathsf{S}]\!]$
- the continuation trace π_2 starts at $\mathsf{at}[\![\mathsf{S}]\!]$

(will be proved by structural induction on S)

Axioms

Structural prefix trace semantics at a program component

Prefix trace at a program component S

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

A prefix continuation of the traces $\pi_1\mathsf{at}[\![\mathsf{S}]\!]$ arriving at a program, statement or statement list S can be reduced to the program point $\mathsf{at}[\![\mathsf{S}]\!]$ at this program, statement or statement list S.

Structural prefix trace semantics of an empty statement list

Prefix traces of an empty statement list $\mathtt{Sl} ::= \epsilon$

- $$\frac{}{\mathsf{at}[\![\mathtt{Sl}]\!] \in \widehat{\mathcal{S}}^{*}[\![\mathtt{Sl}]\!](\pi\mathsf{at}[\![\mathtt{Sl}]\!])} \qquad (6.15)$$

- A prefix/maximal trace π of the empty statement list ϵ continuing some trace is reduced to the program label $\mathsf{at}[\![\mathtt{Sl}]\!]$ at that empty statement.
- This case is redundant and already covered by (6.11).

Structural prefix trace semantics of an assignment statement

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

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

A prefix/maximal finite trace of an assignment ℓ $\mathtt{x = E\ ;}$ continuing some trace π^{ℓ} is ℓ followed by the event $\mathtt{x} = v$ where v is the last value of $\mathtt{x}$ previously assigned to $\mathtt{x}$ on π^{ℓ} (otherwise initialized to 0) and finishing at the label $\mathsf{after}[\![\mathtt{S}]\!]$ after the assignment.

Structural prefix trace semantics of a skip statement

Prefix traces of a skip statement $\mathtt{S} ::= \ell\,\mathtt{;}$

- $$\frac{}{\ell \xrightarrow{\mathtt{skip}} \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{\,*}[\![\mathtt{S}]\!](\pi^{\ell})} \tag{6.17}$$

A prefix/maximal finite trace of a skip statement $\ell\,\mathtt{;}$ continuing an initial trace π^{ℓ} arriving at ℓ is just continuing after the skip statement.

Structural prefix trace semantics of a break statement

Prefix traces of a break statement $\mathtt{S} ::= {}^{\ell}\ \mathtt{break}\ \mathtt{;}$

- $$\frac{}{\ell \xrightarrow{\mathtt{break}} \text{break-to}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{*}[\![\mathtt{S}]\!](\pi^{\ell})} \qquad (6.29)$$

A prefix/maximal finite trace of a break ${}^{\ell}$ **break ;** continuing some initial trace π^{ℓ} is the trace ℓ followed by the **break ;** event and ending at the break label break-to$[\![\mathtt{S}]\!]$ (which is the exit label of the closest enclosing iteration loop or else the program exit).

Structural inference rules

Structural prefix trace semantics of a program

Prefix traces of a program $\texttt{P} ::= \texttt{Sl}\ ^{\ell}$

- $$\frac{\pi_2 \in \widehat{\mathcal{S}}^{\,*}[\![\texttt{Sl}]\!](\pi_1 \mathsf{at}[\![\texttt{Sl}]\!])}{\pi_2 \in \widehat{\mathcal{S}}^{\,*}[\![\texttt{P}]\!](\pi_1 \mathsf{at}[\![\texttt{P}]\!])} \tag{6.12}$$

If $\texttt{P} ::= \texttt{Sl}\ ^{\ell}$ then the prefix continuations of the traces $\pi_1 \mathsf{at}[\![\texttt{Sl}]\!]$ arriving at program entry $\mathsf{at}[\![\texttt{P}]\!] = \mathsf{at}[\![\texttt{Sl}]\!]$ are the continuations of the statement list $\texttt{Sl}$.

Structural prefix trace semantics of a compound statement

Prefix traces of a compound statement `S ::= { Sl }`

- $$\frac{\pi_2 \in \widehat{\mathcal{S}}^*[\![\mathtt{Sl}]\!](\pi_1)}{\pi_2 \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\pi_1)} \qquad (6.30)$$

A prefix trace of a compound statement `{ Sl }` is that of its statement list `Sl`.

Structural prefix trace semantics of a conditional statement

Prefix traces of a conditional statement `S ::= if` $^{\ell}$ `(B)` $\mathtt{S}_t$

- $$\frac{\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_1{}^{\ell}) = \mathrm{ff}}{\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{\,*}[\![\mathsf{S}]\!](\pi_1{}^{\ell})} \qquad (6.18)$$

- $$\frac{\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_1{}^{\ell}) = \mathrm{tt}, \quad \pi_2 \in \widehat{\mathcal{S}}^{\,*}[\![\mathsf{S}_t]\!](\pi_1{}^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])}{\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \pi_2 \in \widehat{\mathcal{S}}^{\,*}[\![\mathsf{S}]\!](\pi_1{}^{\ell})} \qquad (6.19)$$

Structural prefix trace semantics of a conditional statement

- A prefix trace of a conditional statement `if` ℓ `(B)` $\mathtt{S}_t$ continuing some initial trace $\pi_1\ell$ is
  - either ℓ (a case already covered by (6.11));
  - or, in case (6.18), ℓ followed by the event $\neg(\mathtt{B})$ when the value of this boolean expression on $\pi_1\ell$ is ff and finishing at the label after⟦S⟧ after the conditional statement;
  - or, in case case (6.19). when the value of the boolean expression B on $\pi_1\ell$ is tt, ℓ followed by the test event B followed by a prefix trace of $\mathtt{S}_t$ continuing $\pi_1\ell \xrightarrow{\mathtt{B}} \mathrm{at}[\![\mathtt{S}_t]\!]$.

Structural prefix trace semantics of a conditional statement

Prefix traces of a conditional statement $\texttt{S} ::= \texttt{if}\ \ell\ \texttt{(B)}\ \texttt{S}_t\ \texttt{else}\ \texttt{S}_f$

- $$\frac{\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell) = \mathsf{tt}, \quad \pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi_1\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])}{\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}]\!](\pi_1\ell)} \tag{6.22}$$

- $$\frac{\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell) = \mathsf{ff}, \quad \pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_f]\!](\pi_1\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{at}[\![\mathsf{S}_f]\!])}{\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{at}[\![\mathsf{S}_f]\!] \frown \pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}]\!](\pi_1\ell)} \tag{6.23}$$

A prefix finite trace of a conditional statement $\texttt{if}\ \ell\ \texttt{(B)}\ \texttt{S}_t\ \texttt{else}\ \texttt{S}_f$ continuing an initial trace $\pi_1\ell$ is the test event $\texttt{B}$ (respectively $\neg(\texttt{B})$) at ℓ followed by a prefix trace of $\texttt{S}_t$ (respectively $\texttt{S}_f$) when boolean expression $\texttt{B}$ is tt (respectively ff) on $\pi_1\ell$ in case (6.22) (respectively (6.23)).

Structural prefix trace semantics of a statement list

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

- $$\frac{\pi_2 \in \widehat{\mathcal{S}}^*[\![\texttt{Sl}']\!](\pi_1)}{\pi_2 \in \widehat{\mathcal{S}}^*[\![\texttt{Sl}]\!](\pi_1)} \tag{6.13}$$
- $$\frac{\pi_2 \in \widehat{\mathcal{S}}^+[\![\texttt{Sl}']\!](\pi_1), \quad \pi_3 \in \widehat{\mathcal{S}}^*[\![\texttt{S}]\!](\pi_1 \frown \pi_2)}{\pi_2 \frown \pi_3 \in \widehat{\mathcal{S}}^*[\![\texttt{Sl}]\!](\pi_1)} \tag{6.14}$$

In case (6.14),

$$\xrightarrow{\pi_1} \underbrace{\underbrace{\begin{matrix}\text{at}[\![\texttt{Sl}]\!]\\ \text{at}[\![\texttt{Sl}']\!]\end{matrix} \xrightarrow{\pi_2} \begin{matrix}\text{after}[\![\texttt{Sl}']\!]\\ \text{at}[\![\texttt{S}]\!]\end{matrix}}_{\in\ \widehat{\mathcal{S}}^+[\![\texttt{Sl}']\!](\pi_1\text{at}[\![\texttt{Sl}']\!])} \quad \underbrace{\xrightarrow{\pi_3} \ell}_{\in\ \widehat{\mathcal{S}}^*[\![\texttt{S}]\!](\pi_1\text{at}[\![\texttt{Sl}']\!]\pi_2\text{at}[\![\texttt{S}]\!])}}_{\in\ \widehat{\mathcal{S}}^*[\![\texttt{Sl}]\!](\pi_1\text{at}[\![\texttt{Sl}]\!])}$$

A prefix trace of $\texttt{Sl}'\ \texttt{S}$ continuing an initial trace π_1 can be a prefix trace of $\texttt{Sl}'$ or a finite maximal trace of $\texttt{Sl}'$ followed by a prefix trace of $\texttt{S}$.

Structural prefix trace semantics of an iteration statement

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

- $$\frac{}{\ell \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\pi_1\ell)} \tag{6.24}$$

- $$\frac{\ell\pi_2\ell \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\pi_1\ell), \quad \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_1\ell\pi_2\ell) = \mathrm{ff}}{\ell\pi_2\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\pi_1\ell)} \tag{6.25}$$

- $$\frac{\begin{array}{c}\ell\pi_2\ell \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\pi_1\ell), \quad \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_1\ell\pi_2\ell) = \mathrm{tt},\\ \pi_3 \in \widehat{\mathcal{S}}^*[\![\mathtt{S}_b]\!](\pi_1\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!])\end{array}}{\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!] \frown \pi_3 \in \widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\pi_1\ell)} \tag{6.26}$$

This is a forward, left recursive definition where $n+1$ iterations are n iterations followed by one more iteration.

Structural prefix trace semantics of an iteration statement: break statements

Remark 6.27 The inference rule (6.26) includes the case of an iteration ending with an exits by a break statement that would have the form

$$\blacksquare \quad \frac{\ell\pi_2\ell \in \widehat{\mathcal{S}}^*[\![\mathsf{S}]\!](\pi_1\ell), \quad \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_1\ell\pi_2\ell) = \mathrm{tt}, \\ \pi_3 \xrightarrow{\texttt{break}} \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_b]\!](\pi_1\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!])}{\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3 \xrightarrow{\texttt{break}} \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^*[\![\mathsf{S}]\!](\pi_1\ell)} \tag{6.28}$$

Structural prefix trace semantics of an iteration statement

- A prefix finite trace of an iteration statement $\texttt{while}\,^{\ell}\,\texttt{(B)}\;\texttt{S}_b$ continuing some initial trace $\pi_1{}^{\ell}$ is
  - either $^{\ell}$ (case (6.24), already covered by (6.11));
  - or, in case (6.25), the trace starting at $^{\ell}$ followed by the event $\neg(\texttt{B})$ when the value of this boolean expression on $\pi_1{}^{\ell}$ is ff and finishing at the label after$[\![\texttt{S}]\!]$ after the iteration statement;
  - or, in case (6.28), the trace starting at $^{\ell}$ followed by the event $\texttt{B}$ when the value of this boolean expression on $\pi_1{}^{\ell}$ is tt and finishing at the label at$[\![\texttt{S}_b]\!]$ followed by a prefix (indeed maximal) trace of the loop body $\texttt{S}_b$ ending up in a break;
  - or, in case (6.26), the trace starting at $^{\ell}$, followed by a prefix trace of the iteration statement $\texttt{while}\,^{\ell}\,\texttt{(B)}\;\texttt{S}_b$ representing 0 or more of iterations ending at $^{\ell}$, followed by the test event $\texttt{B}$ (where the expression $\texttt{B}$ is tt), followed by a prefix finite trace of the body $\texttt{S}_t$.

Prefix trace semantics

- The prefix trace semantics is defined structurally:
$$\mathcal{S}^*[\![\mathsf{s}]\!] \triangleq \widehat{\mathcal{S}}^*[\![\mathsf{s}]\!]$$
- The prefix traces starting from a set $\mathcal{R}_0$ of initial traces are
$$\mathcal{S}^*[\![\mathsf{s}]\!]\,\mathcal{R}_0 \triangleq \bigcup\{\mathcal{S}^*[\![\mathsf{s}]\!](\pi^\ell) \mid \pi^\ell \in \mathcal{R}_0\}\ .$$
- The prefix traces starting from a set $\mathcal{R}_0$ of initial traces and arriving at program label ℓ are
$$\begin{aligned}\mathcal{S}^{\dot{*}}[\![\mathsf{s}]\!] &\in \wp(\mathbb{T}^+) \xrightarrow{\nearrow} (\mathbb{L} \to \wp(\mathbb{T}^+)) \\ \mathcal{S}^{\dot{*}}[\![\mathsf{s}]\!]\,\mathcal{R}_0\,\ell &\triangleq \{\pi_0{\ell_0}\pi_1{\ell_1} \mid \pi_0{\ell_0} \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell_1 \in \mathcal{S}^*[\![\mathsf{s}]\!](\pi_0\ell_0) \wedge \ell_1 = \ell\}\end{aligned} \tag{6.47}$$

Example of prefix trace semantics

- $\mathtt{S} = \mathtt{while}\ ^{\ell_1}\ (\mathtt{tt})\ ^{\ell_2}\ \mathtt{x = x + 1}\ ;^{\ell_3}$.
- $\widehat{\mathcal{S}}^*[\![\mathtt{S}]\!](\ell_1) = \left\{\left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathtt{x} = i} \ell_1\right)_{i=1}^{n}, \left(\ell_1 \xrightarrow{\mathtt{tt}} \ell_2 \xrightarrow{\mathtt{x} = i} \ell_1\right)_{i=1}^{n} \xrightarrow{\mathtt{tt}} \ell_2 \;\middle|\; n \in \mathbb{N}\right\}$ (reduced to ℓ_1 for $n = 0$).

- Notation:
  - $\left({}^{\ell}\pi(i)^{\ell}\right)_{i=1}^{n}$ denotes the finite trace ${}^{\ell}\pi(1)^{\ell}\pi(2)^{\ell} \dots \pi(n)^{\ell}$. This is the trace ℓ for $n = 0$.
  - $\left({}^{\ell}\pi(i)^{\ell}\right)_{i=1}^{\infty}$ denotes the infinite trace ${}^{\ell}\pi(1)^{\ell}\pi(2)^{\ell} \dots \pi(n)^{\ell}\pi(n+1)^{\ell} \dots$.

Conclusion

Conclusion

- We have defined the structural deductive stateless prefix trace semantics of a subset of C to observe partial computations of programs, where this observation can stop at any time.
- By passing to the limit, we will define the maximal trace semantics where observations terminate with the execution of the program or last for ever in case of non-termination.

Home work

- Read Ch. **6** "Structural deductive stateless prefix trace semantics" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you