Principles of Abstract Interpretation
MIT press

Ch. **19**, Structural forward reachability semantics

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-19--structural-forward-reachability-semantics-PrAbsInt.pdf

Design of a verification/analysis method for a programming language by abstract interpretation

- Define the syntax and operational semantics of the language
- Define program properties and the collecting semantics
- Define an abstraction of properties (preferably by a Galois connection)
- Calculate a sound (and possibly complete) abstract semantics by abstraction of the collecting semantics $\leftarrow$ this chapter
- Define an abstract inductive proof method/analysis algorithm

Chapter 17

Structural fixpoint prefix trace semantics (quick reminder from Chapter **17**)

Fixpoint prefix trace semantics of an assignment statement

Fixpoint prefix trace semantics of an assignment statement $\mathtt{S} ::= {}^{\ell}\ x = \mathtt{E}\ ;$

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

- example of basic case

Fixpoint prefix trace semantics of a statement list

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

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

- example of inductive case ($\widehat{\mathcal{S}}^{*}[\![\mathtt{Sl}]\!]$ defined in terms of $\widehat{\mathcal{S}}^{+}[\![\mathtt{Sl}']\!]$ and $\widehat{\mathcal{S}}^{*}[\![\mathtt{S}]\!]$ with $\mathtt{Sl}' \lhd \mathtt{Sl}$ and $\mathtt{S} \lhd \mathtt{Sl}$)

Fixpoint prefix trace semantics of an iteration

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

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

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

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

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

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

- example of inductive/structural fixpoint case
  - inductive/structural: $\mathcal{S}^*[\![\texttt{while}\,^{\ell}\,\texttt{(B)}\ \texttt{S}_b]\!]$ defined in terms of $\mathcal{S}^*[\![\texttt{S}_b]\!]$ with $\texttt{S}_b \lhd \texttt{while}\,^{\ell}\,\texttt{(B)}\ \texttt{S}_b$
  - fixpoint: $\mathcal{S}^*[\![\texttt{while}\,^{\ell}\,\texttt{(B)}\ \texttt{S}_b]\!]$ recursively defined in terms of itself $(n+1$ iterations are n iterations plus 1 iteration$)$

Chapter 19

Ch. **19**, Structural forward reachability semantics

Forward relational reachability semantics

- Objective: define a semantics that attaches to each program point ℓ of the program
  - the strongest predicate $/\star\ I^{\ell}(\vec{x}_0, \vec{x})\ \star/$ describing the relation between the initial values $\vec{x}_0$ of the variables $\vec{\mathtt{x}}$ and the values $\vec{x}$ of these variables $\vec{\mathtt{x}}$ whenever control reaches that program point ℓ.

  - *i.e.* the relation $\mathcal{R}^{\ell} \in \wp(\mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v})$ between the initial and current environment $\mathcal{R}^{\ell} = \{\langle\rho_0,\ \rho\rangle \mid I^{\ell}(\rho_0(\vec{\mathtt{x}}), \rho(\vec{\mathtt{x}}))\}$ with the convention that $\vec{x_0} = \rho_0(\vec{\mathtt{x}})$ denotes the initial value of $\vec{\mathtt{x}}$ in the initial environment ρ_0 while $\vec{x} = \rho(\vec{\mathtt{x}})$ denotes the current value of $\vec{\mathtt{x}}$ in the current environment ρ.

Forward assertional reachability semantics

- Similar, but forgets about the initial values $\vec{x}_0$ *i.e.* $/\star\ I^{\ell}(\vec{x})\ \star/$

  en.wikipedia.org/wiki/Reachability
  en.wikipedia.org/wiki/Reachability_problem
  en.wikipedia.org/wiki/Invariant_(mathematics)#Invariants_in_computer_science
  https://en.wikipedia.org/wiki/Loop_invariant

Examples of reachability/invariant semantics

Assertional local invariants, Example

```
/* x = 0 (initialization hypothesis) */
while ℓ1 (x < 10)  /* 0 ⩽ x ⩽ 10 (loop invariant) */
  ℓ2  /* 0 ⩽ x < 10 */
     x = x + 1 ;
ℓ3  /* x = 10  */
```

Representing such logical propositions by sets of environments, we have

ℓ	$\mathcal{S}^{\vec{r}}[\![\mathtt{S}]\!]\, \mathcal{R}_0\ \ell$ where $\mathcal{R}_0 = \{\rho \in \mathbb{E}\mathbb{v} \mid \forall \mathtt{y} \in \mathbb{V} \,.\, \rho(\mathtt{y}) = 0\}$
ℓ_1	$\{\rho \in \mathbb{E}\mathbb{v} \mid 0 \leqslant \rho(\mathtt{x}) \leqslant 10 \wedge \forall \mathtt{y} \in \mathbb{V} \setminus \{\mathtt{x}\} \,.\, \rho(\mathtt{y}) = 0\}$
ℓ_2	$\{\rho \in \mathbb{E}\mathbb{v} \mid 0 \leqslant \rho(\mathtt{x}) < 10 \wedge \forall \mathtt{y} \in \mathbb{V} \setminus \{\mathtt{x}\} \,.\, \rho(\mathtt{y}) = 0\}$
ℓ_3	$\{\rho \in \mathbb{E}\mathbb{v} \mid \rho(\mathtt{x}) = 10 \wedge \forall \mathtt{y} \in \mathbb{V} \setminus \{\mathtt{x}\} \,.\, \rho(\mathtt{y}) = 0\}$

$\square$

en.wikipedia.org/wiki/Invariant_(mathematics)#Invariants_in_computer_science
https://en.wikipedia.org/wiki/Loop_invariant

Relational local invariants, Example

```
/* x = x₀ (initialization hypothesis) */
while ℓ1 (x < 10)  /* (10 ⩽ x₀ = x) ∨ (x₀ ⩽ x ⩽ 10) (loop invariant) */
    ℓ2 /* x₀ ⩽ x < 10 */
       x = x + 1 ;
ℓ3 /* (10 ⩽ x₀ = x) ∨ (x₀ < 10 ∧ x = 10) */
```

Representing such logical propositions by a binary relation between environments, we have

ℓ	$\mathcal{S}^{\vec{R}}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell$ where $\mathcal{R}_0 = \{\langle\rho_0,\ \rho\rangle \in \mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v} \mid \rho = \rho_0\}$
ℓ_1	$\{\langle\rho_0,\ \rho\rangle \in \mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v} \mid (10 \leqslant \rho_0(\mathtt{x}) = \rho(\mathtt{x})) \vee (\rho_0(\mathtt{x}) \leqslant \rho(\mathtt{x}) \leqslant 10) \wedge \forall \mathtt{y} \in \mathbb{V} \setminus \{\mathtt{x}\} \,.\, \rho(\mathtt{y}) = \rho_0(\mathtt{y})\}$
ℓ_2	$\{\langle\rho_0,\ \rho\rangle \in \mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v} \mid \rho_0(\mathtt{x}) \leqslant \rho(\mathtt{x}) < 10 \wedge \forall \mathtt{y} \in \mathbb{V} \setminus \{\mathtt{x}\} \,.\, \rho(\mathtt{y}) = \rho_0(\mathtt{y})\}$
ℓ_3	$\{\langle\rho_0,\ \rho\rangle \in \mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v} \mid (10 \leqslant \rho_0(\mathtt{x}) = \rho(\mathtt{x})) \vee (\rho_0(\mathtt{x}) \leqslant \rho(\mathtt{x}) \leqslant 10) \wedge \forall \mathtt{y} \in \mathbb{V} \setminus \{\mathtt{x}\} \,.\, \rho(\mathtt{y}) = \rho_0(\mathtt{y})\}$

□

Reachability/invariant semantics

Notations to handle both the assertional and relational cases at once

tag	assertional	relational
$\vec{\varrho}$	$\vec{\mathsf{r}}$	$\vec{\mathsf{R}}$
$\mathcal{S}^{\vec{\varrho}}[\![\mathsf{P}]\!]$	$\mathcal{S}^{\vec{\mathsf{r}}}[\![\mathsf{P}]\!]$	$\mathcal{S}^{\vec{\mathsf{R}}}[\![\mathsf{P}]\!]$
$\mathbb{E}\mathbb{v}^{\varrho}$	$\mathbb{E}\mathbb{v}$	$\mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v}$
$\ldots$	$\ldots$	$\ldots$

$$\mathcal{S}^{\vec{\varrho}}[\![\mathsf{S}]\!] \in \underset{\substack{\uparrow \\ \text{precondition}}}{\wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}})} \rightarrow (\underset{\substack{\uparrow \\ \text{program point}}}{\mathbb{L}} \rightarrow \underset{\substack{\uparrow \\ \text{invariant}}}{\wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}})})$$

Formal definition of the assertional/relational reachability semantics

- Let $\ell_0 = \mathsf{at}[\![\mathsf{S}]\!]$.

$$\mathcal{S}^{\vec{r}}[\![\mathsf{S}]\!]\,\mathcal{R}_0\,\ell \;\triangleq\; \{\boldsymbol{\varrho}(\pi_0\ell_0\pi_1\ell') \mid \boldsymbol{\varrho}(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \exists \pi_2 \,.\, \ell_0\pi_1\ell'\pi_2 \in \mathcal{S}^*[\![\mathsf{S}]\!](\pi_0\ell_0) \wedge \ell' = \ell\}$$

$$\mathcal{S}^{\vec{R}}[\![\mathsf{S}]\!]\,\mathcal{R}_0\,\ell \;\triangleq\; \{\langle\rho_0,\, \boldsymbol{\varrho}(\pi_0\ell_0\pi_1\ell')\rangle \mid \langle\rho_0,\, \boldsymbol{\varrho}(\pi_0\ell_0)\rangle \in \mathcal{R}_0 \wedge \exists \pi_2 \,.\, \ell_0\pi_1\ell'\pi_2 \in \mathcal{S}^*[\![\mathsf{S}]\!](\pi_0\ell_0) \wedge \ell' = \ell\}$$

- (Informally, if $\mathcal{R}_0 \in \wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}})$ is a precondition and $\ell \in \mathbb{L}$ is the program label then $\mathcal{S}^{\vec{\varrho}}[\![\mathsf{S}]\!]\,\mathcal{R}_0\,\ell$ is an invariant at ℓ which holds if and when execution of the program component S started with an initial state satisfying the precondition $\mathcal{R}_0$ reaches program point ℓ.)

- This formal definition is hard to work with, so we look for an equivalent structural definition $\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{S}]\!] = \mathcal{S}^{\vec{\varrho}}[\![\mathsf{S}]\!]$.

Environment assignment

Assignment $\rho[\mathsf{x} \leftarrow \upsilon]$ of a value $\upsilon \in \mathbb{V}$ to a variable $\mathsf{x} \in \mathbb{V}$ in an environment $\rho \in \mathbb{E}\mathbb{v}$.

$$\begin{aligned} \rho[\mathsf{x} \leftarrow \upsilon](\mathsf{x}) &\triangleq \upsilon \\ \rho[\mathsf{x} \leftarrow \upsilon](\mathsf{y}) &\triangleq \rho(\mathsf{y}) \quad \text{when} \quad \mathsf{x} \neq \mathsf{y} \end{aligned} \tag{19.10}$$

Examples of environment assignment

- $ \leftarrow \rho$ encodes the values of variables *before* the assignment

  `x = 0 ;`

  $\leftarrow \rho[\mathtt{x} \leftarrow 0]$ encodes the values of variables *after* the assignment

i.e. $\rho[\mathtt{x} \leftarrow 0](\mathtt{x}) = 0$ is the value of x after the assignment while the value of the other variables is unchanged.

- $\leftarrow \rho$ encodes the values of variables *before* the assignment

  `x = x + 1 ;`

  $\leftarrow \rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1]$ encodes the values of variables *after* the assignment

The value of x after the assignment `x = x + 1 ;` is the value $\rho(\mathtt{x})$ of x before the assignment incremented by 1 that is $\rho(\mathtt{x}) + 1$. Value of all other variables unchanged.

Structural assertional/relational reachability semantics

Structural assertional/relational reachability semantics

Reachability at a statement S

$$\mathcal{S}^{\vec{\varrho}}[\![\mathtt{S}]\!](\mathcal{R}_0)\mathsf{at}[\![\mathtt{S}]\!] \quad \triangleq \quad \mathcal{R}_0$$

Reachability outside a statement S

$$\ell \notin \mathsf{labx}[\![\mathtt{S}]\!] \quad \Rightarrow \quad \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!](\mathcal{R}_0)^{\ell} = \varnothing \tag{19.30}$$

Reachability of a program $\mathtt{P} ::= \mathtt{Sl}\ \ell'$

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{P}]\!] \quad \triangleq \quad \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{Sl}]\!] \tag{19.19}$$

Structural assertional/relational reachability semantics (cont'd)

Reachability of a skip statement S ::= ;

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{S}]\!]\,\mathcal{R}_0\,\ell \quad = \quad (\!|\ \ell \in \{\mathsf{at}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]\} \ ?\ \mathcal{R}_0 \ :\ \varnothing\ |\!) \tag{19.21}$$

Reachability of an assignment statement S ::= x = E ;

$$\begin{array}{rcl}\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{S}]\!]\,\mathcal{R}_0\,\ell & = & (\!|\ \ell = \mathsf{at}[\![\mathsf{S}]\!] \ ?\ \mathcal{R}_0 \\ & & [\!]\ \ell = \mathsf{after}[\![\mathsf{S}]\!] \ ?\ \mathsf{assign}_{\vec{\varrho}}[\![\mathsf{x}, \mathsf{E}]\!]\,\mathcal{R}_0 \\ & & :\ \varnothing\ |\!) \\ \mathsf{assign}_{\vec{\mathsf{r}}}[\![\mathsf{x}, \mathsf{E}]\!]\,\mathcal{R}_0 & \triangleq & \{\rho[\mathsf{x} \leftarrow \mathcal{E}[\![\mathsf{E}]\!]\rho] \mid \rho \in \mathcal{R}_0\} \\ \mathsf{assign}_{\vec{\mathsf{R}}}[\![\mathsf{x}, \mathsf{E}]\!]\,\mathcal{R}_0 & \triangleq & \{\langle\rho_0,\ \rho[\mathsf{x} \leftarrow \mathcal{E}[\![\mathsf{E}]\!]\rho]\rangle \mid \langle\rho_0,\ \rho\rangle \in \mathcal{R}_0\}\end{array} \tag{19.12}$$

Assignment example

$$\widehat{\mathcal{S}}^{\vec{r}}[\![\ell_1\ \mathtt{x = x + 1\ ;}^{\ell_2}]\!]\ \{\rho \mid \rho(\mathtt{x}) = 0\}\ \ell_2$$

$$\triangleq\ \mathsf{assign}_{\vec{r}}[\![\mathtt{x}, \mathtt{x + 1}]\!]\ \{\rho \mid \rho(\mathtt{x}) = 0\} \qquad \text{(def. (19.12) of } \widehat{\mathcal{S}}^{\vec{r}}\text{)}$$

$$\triangleq\ \{\rho[\mathtt{x} \leftarrow \mathcal{A}[\![\mathtt{x + 1}]\!]\rho] \mid \rho \in \{\rho \mid \rho(\mathtt{x}) = 0\}\} \qquad \text{(def. (19.12) of } \mathsf{assign}_{\vec{r}}\text{)}$$

$$\triangleq\ \{\rho[\mathtt{x} \leftarrow \rho(\mathtt{x}) + 1] \mid \rho(\mathtt{x}) = 0\}$$

$$\text{(def. } \in \text{ and semantics of arithmetic expressions in Section } \mathbf{3.6}\text{)}$$

$$=\ \{\rho[\mathtt{x} \leftarrow 1] \mid \rho \in \mathbb{E}\mathbb{v}\} \qquad \text{(mathematical def. } +\text{)} \qquad \square$$

Structural assertional/relational reachability semantics (cont'd)

Reachability of a conditional statement S ::= `if (B)` $\mathtt{S}_t$

$$\widehat{\mathcal{S}}^{\vec{e}}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell \quad = \quad \big(\!\!\big|\; \ell = \mathsf{at}[\![\mathtt{S}]\!] \;?\; \mathcal{R}_0 \\ \big\|\; \ell \in \mathsf{in}[\![\mathtt{S}_t]\!] \;?\; \widehat{\mathcal{S}}^{\vec{e}}[\![\mathtt{S}_t]\!]\,(\mathsf{test}^{\vec{e}}[\![\mathtt{B}]\!]\mathcal{R}_0)\,\ell \\ \big\|\; \ell = \mathsf{after}[\![\mathtt{S}]\!] \;?\; \widehat{\mathcal{S}}^{\vec{e}}[\![\mathtt{S}_t]\!]\,(\mathsf{test}^{\vec{e}}[\![\mathtt{B}]\!]\mathcal{R}_0)\,\ell \cup (\overline{\mathsf{test}}^{\vec{e}}[\![\mathtt{B}]\!]\mathcal{R}_0) \\ \,\text{\textit{:}}\; \varnothing \;\big|\!\!\big) \tag{19.22}$$

where

$$\begin{aligned}
\mathsf{test}^{\vec{r}}[\![\mathtt{B}]\!]\mathcal{R}_0 &\triangleq \{\rho \in \mathcal{R}_0 \mid \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathrm{tt}\}\\
\mathsf{test}^{\vec{R}}[\![\mathtt{B}]\!]\mathcal{R}_0 &\triangleq \{\langle\rho_0,\ \rho\rangle \in \mathcal{R}_0 \mid \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathrm{tt}\}\\
\overline{\mathsf{test}}^{\vec{r}}[\![\mathtt{B}]\!]\mathcal{R}_0 &\triangleq \{\rho \in \mathcal{R}_0 \mid \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathrm{ff}\}\\
\overline{\mathsf{test}}^{\vec{R}}[\![\mathtt{B}]\!]\mathcal{R}_0 &\triangleq \{\langle\rho_0,\ \rho\rangle \in \mathcal{R}_0 \mid \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathrm{ff}\}
\end{aligned}$$

Structural assertional/relational reachability semantics (cont'd)

Reachability of a conditional statement `S ::= if (B) S`$_t$ `else S`$_f$

$$
\begin{aligned}
\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell \quad = \quad & (\!\![\ \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{?} \mathcal{R}_0 \\
& \|\ \ell \in \mathsf{in}[\![\mathtt{S}_t]\!] \mathrel{?} \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}_t]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\mathtt{B}]\!]\mathcal{R}_0)\,\ell \\
& \|\ \ell \in \mathsf{in}[\![\mathtt{S}_f]\!] \mathrel{?} \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}_f]\!]\,(\overline{\mathsf{test}}^{\vec{\varrho}}[\![\mathtt{B}]\!]\mathcal{R}_0)\,\ell \\
& \|\ \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} \\
& \qquad \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}_t]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\mathtt{B}]\!]\mathcal{R}_0)\,\ell \cup \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}_f]\!]\,(\overline{\mathsf{test}}^{\vec{\varrho}}[\![\mathtt{B}]\!]\mathcal{R}_0)\,\ell \\
& \mathrel{:} \varnothing\ ]\!\!)
\end{aligned}
\tag{19.23}
$$

Structural assertional/relational reachability semantics (cont'd)

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

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{Sl}]\!]\mathcal{R}_0\,\ell \;=\; (\!\!\mid \ell \in \mathsf{labs}[\![\texttt{Sl}']\!] \setminus \{\mathsf{at}[\![\texttt{S}]\!]\} \;?\; \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{Sl}']\!]\mathcal{R}_0\,\ell \;\|\; \ell \in \mathsf{labs}[\![\texttt{S}]\!] \;?\; \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}]\!](\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{Sl}']\!]\mathcal{R}_0\,\mathsf{at}[\![\texttt{S}]\!])\,\ell \;:\; \varnothing \mid\!\!) \tag{19.24}$$

Reachability of an empty statement list $\texttt{Sl} ::= \epsilon$

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{Sl}]\!]\mathcal{R}_0\,\ell \;=\; (\!\!\mid \ell = \mathsf{at}[\![\texttt{Sl}]\!] \;?\; \mathcal{R}_0 \;:\; \varnothing \mid\!\!) \tag{19.20}$$

Structural assertional/relational reachability semantics (cont'd)

Reachability of a break statement S ::= $^{\ell}$ **break ;**

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell \quad = \quad (\!|\,\ell = \mathsf{at}[\![\mathtt{S}]\!]\ ?\ \mathcal{R}_0 : \varnothing\,|\!) \tag{19.25}$$

Reachability of a compound statement S ::= { Sl }

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!] \quad = \quad \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{Sl}]\!] \tag{19.26}$$

Structural assertional/relational reachability semantics (cont'd)

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

$$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}]\!]\,\mathcal{R}_0\,\ell' \;=\; (\mathsf{lfp}^{\dot{\subseteq}}\,\mathcal{F}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0)\,\ell' \tag{19.16}$$

$$\mathcal{F}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0 \;\in\; (\mathbb{L} \rightarrow \wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}})) \xrightarrow{\nearrow} (\mathbb{L} \rightarrow \wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}}))$$

$$\begin{aligned}
&\mathcal{F}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0\,X\,\ell' \;=\\
&\quad \llparenthesis\ \ell' = \ell \ ?\ \mathcal{R}_0 \cup \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\texttt{B}]\!]X(\ell))\,\ell\\
&\quad \parallel\ \ell' \in \mathsf{in}[\![\texttt{S}_b]\!] \setminus \{\ell\}\ ?\ \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\texttt{B}]\!]X(\ell))\,\ell'\\
&\quad \parallel\ \ell' = \mathsf{after}[\![\texttt{S}]\!]\ ?\ \overline{\mathsf{test}}^{\vec{\varrho}}[\![\texttt{B}]\!](X(\ell)) \cup \bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\texttt{S}_b]\!]} \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\texttt{B}]\!]X(\ell))\,\ell''\\
&\quad :\ \varnothing\ \rrparenthesis
\end{aligned}$$

Only the *loop invariant* $X(\ell)$ is used!

Loop invariant

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

$$
\begin{array}{rcl}
 & & \overrightarrow{\mathcal{F}}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0 \quad \in \quad \wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}}) \xrightarrow{\nearrow} \wp(\mathbb{E}\mathbb{v}^{\vec{\varrho}}) \\
\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}]\!]\,\mathcal{R}_0\,\ell' & = & \text{let} \\
 & & \quad \overrightarrow{\mathcal{F}}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0\,X \;=\; \mathcal{R}_0 \cup \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\texttt{B}]\!]X)\,\ell \\
 & & \text{and } I \;=\; \mathsf{lfp}^{\subseteq}\,\overrightarrow{\mathcal{F}}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0 \text{ in} \\
 & & \quad (\!\![\; \ell' = \ell \;?\; I \\
 & & \quad \;\|\; \ell' \in \mathsf{in}[\![\texttt{S}_b]\!] \setminus \{\ell\} \;?\; \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\texttt{B}]\!]\,I)\,\ell' \\
 & & \quad \;\|\; \ell' = \mathsf{after}[\![\texttt{S}]\!] \;?\; \overline{\mathsf{test}}^{\vec{\varrho}}[\![\texttt{B}]\!]\,I \cup \displaystyle\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\texttt{S}_b]\!]} \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\vec{\varrho}}[\![\texttt{B}]\!]\,I)\,\ell'' \\
 & & \quad \;:\; \varnothing \;]\!\!)
\end{array}
\tag{19.42}
$$

$I = (\mathsf{lfp}^{\dot{\subseteq}}\,\overrightarrow{\mathcal{F}}^{\vec{\varrho}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0)\,\ell$ (see Exercise 19.18) can be mathematically calculated iteratively but not mechanizable (Rice theorem).

Reachability transformers preserve joins

Theorem (19.36) For all program components S, $\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]$ preserves arbitrary joins *i.e.* $\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,(\bigcup_i P_i)\,\ell = \bigcup_i \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,(P_i)\,\ell$.

In particular $\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,(\varnothing) = \varnothing$ and the loop transformer $\mathcal{F}^{\vec{\varrho}}[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}]\!]$ preserves arbitrary joins $\dot{\bigcup}$.

System of equations for the iteration statement

- By (19.16) for an iteration statement $\mathtt{S} ::= \mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b$, $\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,\mathcal{R}_0$ is the pointwise $\subseteq$-least solution to the system of equations

$$\begin{cases} X(\ell') &= \mathcal{F}^{\vec{\varrho}}[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\,\mathcal{R}_0\, X\, \ell' \\ \ell' \in \mathsf{labx}[\![\mathtt{S}]\!] \end{cases}$$

- Mathematically solved iteratively
- Not mechanizable, even if the loop invariant is given (Rice theorem)
- Approximations needed

Example 19.15: iteration

- $\texttt{P} = \textbf{while}\ \ell_1\ \texttt{(x < 10)}\ \ell_2\ \texttt{x = x + 1 ;}\ \ell_3$
- all variables are initially 0
- Since there is only one variable $\texttt{x}$ we don't consider properties to be sets of environments but more simply the set of value of $\texttt{x}$
- Let $R^n_{\ell_1}$ be the set of reachable values of $\texttt{x}$ at ℓ_1 after at most $n \geqslant 0$ iterations
- The initial value $\texttt{x} = 0$ is reachable at ℓ_1 on iteration entry, that is at iteration 0. So $R^0_{\ell_1} = \mathcal{R}_0 = \{0\}$
- After at most 1 iteration, the reachable values $R^1_{\ell_1}$ of x at ℓ_1 are those $\mathcal{R}_0$ reachable at iteration 0 plus those of iteration 0 which pass the test and have been incremented in the loop body. So $R^1_{\ell_1} \quad = \quad \mathcal{R}^0 \cup \{x + 1 \mid x \in R^0_{\ell_1} \wedge x < 10\} \quad = \quad \{0, 1\}$
- ...

- Similarly, $R^{9}_{\ell_1} \;=\; \{0, 1, \ldots, 9\}$.
- Then, after at most 10 iterations, the reachable values $R^{10}_{\ell_1}$ of x at ℓ_1 are those $\mathcal{R}_0$ reachable at iteration 0 plus those $R^{9}_{\ell_1}$ of previous iterations which pass the test and have been incremented in the loop body. So

$$
\begin{aligned}
R^{10}_{\ell_1} &= \mathcal{R}^0 \cup \{x + 1 \mid x \in R^{9}_{\ell_1} \wedge x < 10\} \\
&= \{0\} \cup \{1, \ldots, 10\} \;=\; \{0, 1, \ldots, 10\};
\end{aligned}
$$

- After at most 11 iterations, the reachable values $R^{11}_{\ell_1}$ of x at ℓ_1 are those $\mathcal{R}_0$ reachable at iteration 0 plus those $R^{10}_{\ell_1}$ of previous iterations which pass the test and have been incremented in the loop body. So

$$
\begin{aligned}
R^{11}_{\ell_1} &= \mathcal{R}^0_{\ell_1} \cup \{x + 1 \mid x \in R^{10}_{\ell_1} \wedge x < 10\} \\
&= \{0\} \cup \{1, \ldots, 10\} \;=\; \{0, 1, \ldots, 10\} \;=\; R^{10}_{\ell_1};
\end{aligned}
$$

- Similarly, after at most $n > 10$ iterations, $R^n_{\ell_1} = R^{10}_{\ell_1}$.
- Therefore we have

$$\begin{array}{rcl} R^0_{\ell_1} & = & \mathcal{R}^0 \\ R^{n+1}_{\ell_1} & = & \mathcal{R}^0 \cup \{x+1 \mid x \in R^n_{\ell_1} \wedge x < 10\} \end{array}$$

with $R^0_{\ell_1} \subseteq R^1_{\ell_1} \subseteq \ldots R^n_{\ell_1} \subseteq R^{n+1}_{\ell_1} \subseteq \ldots$.

- Letting $R'^0_{\ell_1} = \varnothing$ and $R'^{n+1}_{\ell_1} = R^n_{\ell_1}$, this is the same as

$$\begin{array}{rcl} R'^0_{\ell_1} & = & \varnothing \\ R'^{n+1}_{\ell_1} & = & \mathcal{R}^0 \cup \{x+1 \mid x \in R'^n_{\ell_1} \wedge x < 10\} \end{array}$$

with $R'^0_{\ell_1} \subseteq R'^1_{\ell_1} \subseteq \ldots R'^n_{\ell_1} \subseteq R'^{n+1}_{\ell_1} \subseteq \ldots$

- This limit is the set of reachable values $\bigcup R'^n_{\ell_1} = \{0, 1, \ldots, 10\}$ of x at ℓ_1.

- Obviously, the function $\mathsf{F}(R') \triangleq \mathcal{R}^{0}_{\ell_1} \cup \{x+1 \mid x \in R' \wedge x < 10\}$ preserves arbitrary joins $\bigcup$
- So, by Theorem 15.26, the reachable values of $\mathtt{x}$ at ℓ_1 are $\widehat{\mathcal{S}}^{\vec{\mathsf{r}}}[\![\mathsf{P}]\!]\,\mathcal{R}^{0}\,\ell_1 \quad = \quad \mathsf{lfp}^{\subseteq}\,\mathsf{F}$.
- The reachable values of $\mathtt{x}$ at ℓ_3 on loop exit are those reachable at ℓ_1 that do not pass the test, that is

$$\widehat{\mathcal{S}}^{\vec{\mathsf{r}}}[\![\mathsf{P}]\!]\,\mathcal{R}^{0}\,\ell_3 \quad = \quad \{x \in \widehat{\mathcal{S}}^{\vec{\mathsf{r}}}[\![\mathsf{P}]\!]\,\mathcal{R}^{0}\,\ell_1 \mid x \geqslant 10\} \quad = \quad \{10\}.$$

Chapter 19

Sound, complete, and exact structural abstract semantics (Section **19.6**)

Concrete semantics

- Let $\langle \mathcal{S}[\![\mathsf{s}]\!] \in \mathcal{D}[\![\mathsf{s}]\!],\ \mathsf{s} \in \mathbb{P}\mathbb{c}\rangle$ be a structural semantics defined as

$$\begin{cases}\mathcal{S}[\![\mathsf{s}]\!] & \triangleq \quad \mathcal{F}[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \triangleleft \mathsf{s}} \mathcal{S}[\![\mathsf{s}']\!])\\ \mathsf{s} \in \mathbb{P}\mathbb{c}\end{cases} \tag{19.38}$$

  where $\langle \mathsf{s}',\ \mathsf{s}' \triangleleft \mathsf{s}\rangle$ is the finite vector of immediate subcomponents of program components $\mathsf{s} \in \mathbb{P}\mathbb{c}$.
- The map $\mathcal{F}[\![\mathsf{s}]\!] \in \prod_{\mathsf{s}' \triangleleft \mathsf{s}} \mathcal{D}[\![\mathsf{s}']\!] \to \mathcal{D}[\![\mathsf{s}]\!]$ has no parameters in the basic cases (assignment, skip, *etc*.).
- It is defined has the fixpoint for iteration statements.

Abstract semantics

- Let $\alpha[\![\mathsf{S}]\!] \in \wp(\mathcal{D}[\![\mathsf{S}]\!]) \rightarrow \langle \mathbb{D}[\![\mathsf{S}]\!], \sqsubseteq\rangle$ be an abstraction of the properties of the semantics $\mathcal{S}[\![\mathsf{S}]\!] \in \mathcal{D}[\![\mathsf{S}]\!]$.
- The abstract semantics of interest is the abstraction of the collecting semantics.

$$\mathcal{S}^{¤}[\![\mathsf{S}]\!] \quad \triangleq \quad \alpha[\![\mathsf{S}]\!](\{\mathcal{S}[\![\mathsf{S}]\!]\}) \tag{19.39}$$

- The definition of a structural abstract semantics has the form

$$\begin{cases}\widehat{\mathcal{S}}^{¤}[\![\mathsf{S}]\!] & \triangleq \quad \mathcal{F}^{¤}[\![\mathsf{S}]\!](\prod_{\mathsf{S}' \triangleleft \mathsf{S}} \widehat{\mathcal{S}}^{¤}[\![\mathsf{S}']\!]) \\ \mathsf{S} \in \mathbb{P}\mathrm{c} & \end{cases} \tag{19.40}$$

where $\mathcal{F}^{¤}[\![\mathsf{S}]\!] \in \prod_{\mathsf{S}' \triangleleft \mathsf{S}} \mathbb{D}[\![\mathsf{S}']\!] \rightarrow \mathbb{D}[\![\mathsf{S}]\!]$.

- So the calculation of the structural abstract semantics $\widehat{\mathcal{S}}^{¤}[\![\mathsf{S}]\!]$ is purely in the abstract domains $\langle \mathbb{D}[\![\mathsf{S}]\!], \mathsf{S} \in \mathbb{P}\mathrm{c}\rangle$ as opposed to abstract semantics $\mathcal{S}^{¤}[\![\mathsf{S}]\!]$ involving calculations in the more complicated concrete domains $\langle \mathcal{D}[\![\mathsf{S}]\!], \mathsf{S} \in \mathbb{P}\mathrm{c}\rangle$.

Structural soundness, completeness, exactness

- The structural abstract semantics is
  - *sound* when $\forall \mathtt{S} \in \mathbb{P}\mathtt{c}\ .\ \mathcal{S}^{\sharp}[\![\mathtt{S}]\!] \sqsubseteq \widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!]$,
  - *complete* when $\forall \mathtt{S} \in \mathbb{P}\mathtt{c}\ .\ \mathcal{S}^{\sharp}[\![\mathtt{S}]\!] \sqsupseteq \widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!]$, and
  - *sound and complete* or *exact* when $\forall \mathtt{S} \in \mathbb{P}\mathtt{c}\ .\ \mathcal{S}^{\sharp}[\![\mathtt{S}]\!] = \widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!]$.
- Examples:
  - The structural reachability semantics $\widehat{\mathcal{S}}^{\vec{\varrho}}$ is exact.
  - The structural sign semantics $\widehat{\mathcal{S}}^{\pm}$ of Section **3.13** is sound but not exact. For example, $\mathcal{S}^{\pm}[\![2 - 1]\!] = \alpha_{\pm}(\{\mathcal{S}[\![2 - 1]\!]\}) = \alpha_{\pm}(\{1\}) = (>0)$ while $\widehat{\mathcal{S}}^{\pm}[\![2 - 1]\!] = \widehat{\mathcal{S}}^{\pm}[\![2]\!] -_{\pm} \widehat{\mathcal{S}}^{\pm}[\![1]\!] = (>0) -_{\pm} (>0) = \top_{\pm}$.

How to prove the exactness of a structural abstract semantics?

- We first prove the commutation property

$$\forall \mathsf{s} \in \mathbb{P}\mathbb{c} \;.\; \alpha[\![\mathsf{s}]\!](\{\mathscr{F}[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \vartriangleleft \mathsf{s}} X_{\mathsf{s}'})\}) \;=\; \mathscr{F}^{¤}[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \vartriangleleft \mathsf{s}} \alpha[\![\mathsf{s}']\!](\{X_{\mathsf{s}'}\})) \qquad (19.48)$$

  for all $\mathsf{s} \in \mathbb{P}\mathbb{c}$ and $X_{\mathsf{s}'} \in \mathscr{D}[\![\mathsf{s}']\!]$, $\mathsf{s}' \vartriangleleft \mathsf{s}$.

- For iteration statements, $\mathscr{F}[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \vartriangleleft \mathsf{s}} X_{\mathsf{s}'})$ is a fixpoint, and this proof involves *e.g.* Theorems 18.21 and 18.24, Corollaries 18.31 and 18.32, or similar results.
- This allows us to derive the abstract transformer $\mathscr{F}^{¤}[\![\mathsf{s}]\!]$, knowing the concrete transformer $\mathscr{F}[\![\mathsf{s}]\!]$ and the abstraction $\alpha[\![\mathsf{s}]\!]$.

- Then the proof proceed by structural induction on $\langle \mathbb{P}c, \lhd \rangle$.
- Assuming, by structural induction hypothesis, that $\forall s' \lhd s \,.\, \mathcal{S}^{¤}[\![s']\!] = \widehat{\mathcal{S}}^{¤}[\![s']\!]$, we have

$$
\begin{aligned}
& \mathcal{S}^{¤}[\![s]\!] \\
= {} & \alpha[\![s]\!](\{\mathcal{S}[\![s]\!]\}) && \wr(19.39)\int \\
= {} & \alpha[\![s]\!](\{\mathcal{F}[\![s]\!](\prod_{s' \lhd s} \mathcal{S}[\![s']\!])\}) && \wr(19.38)\int \\
= {} & \mathcal{F}^{¤}[\![s]\!](\prod_{s' \lhd s} \alpha[\![s']\!](\{\mathcal{S}[\![s']\!]\})) && \wr\text{commutation property } (19.48)\int \\
= {} & \mathcal{F}^{¤}[\![s]\!](\prod_{s' \lhd s} \mathcal{S}^{¤}[\![s']\!]) && \wr(19.39)\int \\
= {} & \mathcal{F}^{¤}[\![s]\!](\prod_{s' \lhd s} \widehat{\mathcal{S}}^{¤}[\![s']\!]) && \wr\text{structural ind. hyp.}\int \\
= {} & \widehat{\mathcal{S}}^{¤}[\![s]\!] && \wr(19.40)\int \quad \square
\end{aligned}
$$

Home work

- Read Ch. **19** "Structural forward reachability semantics" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you