# Principles of Abstract Interpretation
# MIT press

# Ch. **20**, Calculational design of the 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-20--calculational-design-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 c.) ← this chapter
- Calculate a sound (and possibly complete) abstract semantics by abstraction of the collecting semantics ← this chapter

  We formally design the reachability semantics (*postulated* in Chapter **19** for pedagogical reasons), by calculus
- Define an abstract inductive proof method/analysis algorithm

Chapter 20

# Ch. **20**, Calculational design of the forward reachability semantics

# Reachability abstraction

# Assertional abstraction

$$\mathsf{post}^{\vec{r}}(\mathcal{S})\,\mathcal{R}_0\;\ell \;\triangleq\; \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \mathcal{S}(\pi_0\ell_0) \wedge \ell' = \ell\} \tag{20.1}$$

$$\xrightarrow{\quad\pi_0\quad}\ \overset{\ell_0}{|}\ \overbrace{\xrightarrow{\quad\pi_1\quad}\ \overset{\ell}{|}}^{\in\,\mathcal{S}(\pi_0\ell_0)}\ \overset{\pi_2}{\cdots\cdots\cdots\rightarrow}$$

$$\varrho(\pi_0\ell_0) \in \mathcal{R}_0 \quad \varrho(\pi_0\ell_0\pi_1\ell) \in \mathsf{post}^{\vec{r}}(\mathcal{S})\,\mathcal{R}_0\;\ell$$

$$\langle \mathbb{T}^+ \to \wp(\mathbb{T}^+),\ \dot{\subseteq}\rangle \underset{\mathsf{post}^{\vec{r}}}{\overset{\gamma^{\vec{r}}}{\leftrightarrows}} \langle \wp(\mathbb{E}\mathbb{v}) \to \mathbb{L} \mapsto \wp(\mathbb{E}\mathbb{v}),\ \ddot{\subseteq}\rangle$$

# Assertional abstraction, Example

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

We assume that all variables are initialized to $0$. Maximal trace semantics

$$\mathcal{S}(\pi\ell_1) \triangleq \{\ell_1 \xrightarrow{\texttt{x} = 1} \ell_2 \xrightarrow{\mathtt{tt}} \ell_3 \xrightarrow{\texttt{x} = 2} \ell_4 \xrightarrow{\neg(\texttt{x} > 2)} \ell_2 \xrightarrow{\mathtt{tt}} \ell_3 \xrightarrow{\texttt{x} = 3} \ell_4 \xrightarrow{\texttt{x} > 2} \ell_5 \xrightarrow{\texttt{break}} \ell_6 \xrightarrow{\texttt{skip}} \ell_7\} \tag{6.2}$$

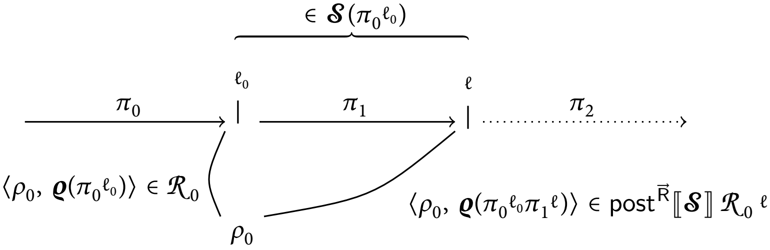
The reachable states are

| $\ell$ | $\mathsf{post}^{\vec{r}}(\mathcal{S})\,\mathcal{R}_0\,\ell$ |
|---|---|
| $\ell_1$ | $\mathcal{R}_0 \quad = \quad \{\rho \in \mathbb{E}\mathbf{v} \mid \forall \texttt{y} \in \mathbb{V} \,.\, \rho(\texttt{y}) = 0\}$ |
| $\ell_2, \ell_3$ | $\{\rho[\texttt{x} \leftarrow i] \mid \rho \in \mathcal{R}_0 \wedge i \in [1,2]\}$ |
| $\ell_4$ | $\{\rho[\texttt{x} \leftarrow i] \mid \rho \in \mathcal{R}_0 \wedge i \in [2,3]\}$ |
| $\ell_5, \ell_6, \ell_7$ | $\{\rho[\texttt{x} \leftarrow 3] \mid \rho \in \mathcal{R}_0\}$ |

$\square$

# Relational abstraction

$$\mathsf{post}^{\vec{\mathsf{R}}}[\![\mathcal{S}]\!]\,\mathcal{R}_0\,\ell \quad \triangleq \quad \{\langle \rho_0,\ \varrho(\pi_0{}^{\ell_0}\pi_1{}^{\ell'})\rangle \mid \langle \rho_0,\ \varrho(\pi_0{}^{\ell_0})\rangle \in \mathcal{R}_0 \wedge \ell_0\pi_1{}^{\ell'} \in \mathcal{S}(\pi_0{}^{\ell_0}) \wedge \ell' = \ell\} \tag{20.9}$$




$$\langle \wp(\mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v}),\ \subseteq\rangle \xleftarrow[\alpha^2]{\gamma^2} \langle \wp(\mathbb{E}\mathbb{v}),\ \subseteq\rangle$$

# Relational abstraction, Example

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

```
ℓ1 x = x + 1 ;
  while ℓ2 (tt) {
    ℓ3 x = x + 1 ;
    if ℓ4 (x > 2) ℓ5 break ;}ℓ6;ℓ7
```

We assume that all variables are initialized to 0. Maximal trace semantics

$$\mathcal{S}(\pi\ell_1) \triangleq \{\ell_1 \xrightarrow{\mathtt{x} = 1} \ell_2 \xrightarrow{\mathrm{tt}} \ell_3 \xrightarrow{\mathtt{x} = 2} \ell_4 \xrightarrow{\neg(\mathtt{x} > 2)} \ell_2 \xrightarrow{\mathrm{tt}} \ell_3 \xrightarrow{\mathtt{x} = 3} \ell_4 \xrightarrow{\mathtt{x} > 2} \ell_5 \xrightarrow{\mathtt{break}} \ell_6 \xrightarrow{\mathtt{skip}} \ell_7\} \tag{6.2}$$

The reachable states are

| $\ell$ | $\mathrm{post}^{\vec{R}}(\mathcal{S})\,\mathcal{R}_0\,\ell$ |
|---|---|
| $\ell_1$ | $\mathcal{R}_0 \quad = \quad \{\langle\rho_0,\ \rho\rangle \mid \forall \mathtt{y} \in \mathbb{V}\ .\ \rho_0(\mathtt{y}) = 0 \wedge \rho = \rho_0\}$ |
| $\ell_2, \ell_3$ | $\{\langle\rho_0,\ \rho[\mathtt{x} \leftarrow i]\rangle \mid \langle\rho_0,\ \rho\rangle \in \mathcal{R}_0 \wedge i \in [1, 2]\}$ |
| $\ell_4$ | $\{\langle\rho_0,\ \rho[\mathtt{x} \leftarrow i]\rangle \mid \langle\rho_0,\ \rho\rangle \in \mathcal{R}_0 \wedge i \in [2, 3]\}$ |
| $\ell_5, \ell_6, \ell_7$ | $\{\langle\rho_0,\ \rho[\mathtt{x} \leftarrow 3]\rangle \mid \langle\rho_0,\ \rho\rangle \in \mathcal{R}_0\}$ |

$\square$

# Formal definition of the assertional/relational reachability semantics

- We write $\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{P}]\!]$, $\mathsf{post}^{\vec{\varrho}}$, $\mathsf{post}^{\vec{\varrho}*}$, $\mathbb{E}\mathbb{v}^{\varrho}$, … to mean either $\widehat{\mathcal{S}}^{\vec{\mathsf{r}}}[\![\mathsf{P}]\!]$, $\mathsf{post}^{\vec{\mathsf{r}}}$, $\mathsf{post}^{\vec{\mathsf{r}}*}$, $\mathbb{E}\mathbb{v}$, … for $\vec{\varrho} = \vec{\mathsf{r}}$ or $\widehat{\mathcal{S}}^{\vec{\mathsf{R}}}[\![\mathsf{P}]\!]$, $\mathsf{post}^{\vec{\mathsf{R}}}$, $\mathsf{post}^{\vec{\mathsf{R}}*}$, $\mathbb{E}\mathbb{v} \times \mathbb{E}\mathbb{v}$, … for $\vec{\varrho} = \vec{\mathsf{R}}$.

- Formal definition of the assertional/relational reachability semantics:

$$\mathcal{S}^{\vec{\varrho}}[\![\mathsf{P}]\!] \quad \triangleq \quad \mathsf{post}^{\vec{\varrho}}[\![\mathcal{S}^{*}[\![\mathsf{S}]\!]]\!] \quad = \quad \mathsf{post}^{\vec{\varrho}*}[\![\mathcal{S}^{+\infty}[\![\mathsf{S}]\!]]\!] \tag{20.15}$$

- Calculational design by structural induction on the program abstract syntax.
- For an iteration statement $\mathtt{S} ::= \mathtt{while}\ ^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$,
  - we consider the prefix trace semantics in fixpoint form of Section **17.1**, and
  - apply the exact iterates abstraction Corollary 18.31.

# Calculational design strategy

# Calculational design strategy

$$
\begin{aligned}
& \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{s}]\!]\,\mathcal{R}_0\,\ell && \text{(case } \ell \in \mathsf{labs}[\![\mathsf{s}]\!]\text{)}\\
= \;& \mathsf{post}^{\vec{\varrho}}(\mathcal{S}^*[\![\mathsf{s}]\!])\,\mathcal{R}_0\,\ell && \text{(ensuring that } \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{s}]\!] = \mathcal{S}^{\vec{\varrho}}[\![\mathsf{s}]\!] \text{ by (20.15))}\\
= \;& \mathsf{post}^{\vec{\varrho}}(\widehat{\mathcal{S}}^*[\![\mathsf{s}]\!])\,\mathcal{R}_0\,\ell && \text{(} \mathcal{S}^*[\![\mathsf{s}]\!] \triangleq \widehat{\mathcal{S}}^*[\![\mathsf{s}]\!] \text{ in Section } \mathbf{6.6}\text{)}\\
= \;& \mathsf{post}^{\vec{\varrho}}(\mathcal{F}^*[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \triangleleft \mathsf{s}} \widehat{\mathcal{S}}^*[\![\mathsf{s}']\!]))\,\mathcal{R}_0\,\ell
\end{aligned}
$$

(fixpoint def. $\widehat{\mathcal{S}}^*[\![\mathsf{s}]\!] = \mathcal{F}^*[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \triangleleft \mathsf{s}} \widehat{\mathcal{S}}^*[\![\mathsf{s}']\!])$ from Chapter **17** equivalent to the inductive definition of Chapter **6**)

$$
\begin{aligned}
= \;& \ldots && \text{(calculational design)}\\
= \;& \mathcal{F}^{\vec{\varrho}}[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \triangleleft \mathsf{s}} \mathsf{post}^{\vec{\varrho}}(\mathcal{S}^*[\![\mathsf{s}']\!]))\,\mathcal{R}_0\,\ell && \text{(exhibiting the commutation property (19.48))}\\
= \;& \mathcal{F}^{\vec{\varrho}}[\![\mathsf{s}]\!](\prod_{\mathsf{s}' \triangleleft \mathsf{s}} \widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathsf{s}']\!])\,\mathcal{R}_0\,\ell && \text{(ind. hyp.)}
\end{aligned}
$$

# Calculational design by structural induction, basic cases

# Example of calculational design: skip statement

*Reachability of a skip statement* S ::= ;

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

*Proof of* (19.21)

$\widehat{\mathcal{S}}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell$

$= \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \widehat{\mathcal{S}}^{*}[\![\mathtt{S}]\!](\pi_0\ell_0) \wedge \ell' = \ell\}$

(by def. (20.15) and (20.1), similar for (20.9))

$= \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \{\mathsf{at}[\![\mathtt{S}]\!], \mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{skip}} \mathsf{after}[\![\mathtt{S}]\!]\} \wedge \ell' = \ell\}$

( def. prefix semantics same as (6.17))

$= (\![\, \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{?} \mathcal{R}_0 \;\|\; \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \{\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{skip}} \mathsf{after}[\![\mathtt{S}]\!]\} \wedge \ell' = \ell\} \mathrel{:} \varnothing \,]\!)$

( cases $\ell = \ell_0 = \mathsf{at}[\![\mathtt{S}]\!]$ or $\ell_0 = \mathsf{at}[\![\mathtt{S}]\!]$ and $\ell = \ell' = \mathsf{after}[\![\mathtt{S}]\!]$)

$$\llparenthesis\, \ell = \mathsf{at}[\![\mathsf{S}]\!] \;?\; \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathsf{S}]\!] \;?\; \{\boldsymbol{\varrho}(\pi_0\ell_0\pi_1\ell') \mid \boldsymbol{\varrho}(\pi_0\ell_0) \in \mathcal{R}_0 \land \ell_0\pi_1\ell' \in \{\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathtt{skip}} \mathsf{after}[\![\mathsf{S}]\!]\} \land \ell' = \ell\} \;:\; \varnothing \,\rrparenthesis$$

$$= \llparenthesis\, \ell = \mathsf{at}[\![\mathsf{S}]\!] \;?\; \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathsf{S}]\!] \;?\; \{\boldsymbol{\varrho}(\pi_0\ell_0) \mid \boldsymbol{\varrho}(\pi_0\ell_0) \in \mathcal{R}_0\} \;:\; \varnothing \,\rrparenthesis$$

$$\text{\{since } \boldsymbol{\varrho}(\pi_0\ell_0 \xrightarrow{\mathtt{skip}} \ell) = \boldsymbol{\varrho}(\pi_0\ell_0)\text{\}}$$

$$= \llparenthesis\, \ell \in \{\mathsf{at}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]\} \;?\; \mathcal{R}_0 \;:\; \varnothing \,\rrparenthesis \qquad \text{\{grouping cases\}} \quad \square$$

# Example of calculational design: assignment statement I

*Reachability of an assignment statement* $\mathsf{S} ::= x = \mathsf{E}\ ;$

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

**Proof of** (19.12)

# Example of calculational design: assignment statement II

$$\widehat{\mathcal{S}}^{\vec{r}}[\![\mathsf{S}]\!]\, \mathcal{R}_0\, \ell \qquad \text{(similar for } \widehat{\mathcal{S}}^{\vec{R}}\text{)}$$

$$= \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \widehat{\mathcal{S}}^{*}[\![\mathsf{S}]\!](\pi_0\ell_0) \wedge \ell' = \ell \in \mathsf{labs}[\![\mathsf{S}]\!]\}$$

(by def. (20.15) and (20.1), similar for (20.9))

$$= \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \{\mathsf{at}[\![\mathsf{S}]\!]\} \cup \{\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{x} = v} \mathsf{after}[\![\mathsf{S}]\!] \mid v = \mathcal{A}[\![\mathsf{A}]\!]\varrho(\pi_0\ell_0)\} \wedge \ell' = \ell \in \mathsf{labs}[\![\mathsf{S}]\!]\}$$

(def. prefix semantics same as (6.11) and (6.16))

$$= (\!\!|\, \ell = \mathsf{at}[\![\mathsf{S}]\!] \mathrel{?} \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \{\varrho(\pi_0\ell_0\pi_1\ell') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_1\ell' \in \{\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{x} = \mathcal{A}[\![\mathsf{A}]\!]\varrho(\pi_0\ell_0)} \mathsf{after}[\![\mathsf{S}]\!]\} \wedge \ell' = \ell \in \mathsf{labs}[\![\mathsf{S}]\!]\} : \varnothing \,|\!\!)$$

($\mathsf{labs}[\![\mathsf{S}]\!] = \{\mathsf{at}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]\}$ in Section **4.2.7**)

$$= (\!\!|\, \ell = \mathsf{at}[\![\mathsf{S}]\!] \mathrel{?} \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \{\rho[\mathsf{x} \leftarrow \mathcal{A}[\![\mathsf{A}]\!]\rho] \mid \rho \in \mathcal{R}_0\} : \varnothing \,|\!\!)$$

(letting $\rho = \varrho(\pi_0\ell_0)$ by Exercise 6.8 and def. (6.6) of $\varrho$)

# Example of calculational design: assignment statement III

$$\llparenthesis\ \ell = \mathsf{at}[\![\mathsf{S}]\!]\ ?\ \mathcal{R}_0\ \|\ \ell = \mathsf{after}[\![\mathsf{S}]\!]\ ?\ \{\rho[\mathsf{x} \leftarrow \mathscr{A}[\![\mathsf{A}]\!]\rho] \mid \rho \in \mathcal{R}_0\} \mathbin{⁏} \varnothing\ \rrparenthesis$$

$$= \llparenthesis\ \ell = \mathsf{at}[\![\mathsf{S}]\!]\ ?\ \mathcal{R}_0\ \|\ \ell = \mathsf{after}[\![\mathsf{S}]\!]\ ?\ \mathsf{assign}^{\vec{\mathsf{r}}}[\![\mathsf{x}, \mathsf{A}]\!]\ \mathcal{R}_0 \mathbin{⁏} \varnothing\ \rrparenthesis$$

$\wr$def. $\mathsf{assign}^{\vec{\mathsf{r}}}[\![\mathsf{x}, \mathsf{A}]\!]\ \mathcal{R}_0 = \{\rho[\mathsf{x} \leftarrow \mathscr{E}[\![\mathsf{E}]\!]\rho] \mid \rho \in \mathcal{R}_0\}$, similar for (20.9)$\wr$ $\square$

# Calculational design by structural induction, inductive case of iteration

# Example of calculational design: iteration statement

We abstract the prefix trace semantics:

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

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

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

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

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

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

# Structural assertional/relational reachability semantics

into the reachability semantics, exactly, by calculational design

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

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

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

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

# fixpoint abstraction

**Corollary (18.31, exact iterates abstraction)** Assume $\langle C, \sqsubseteq\rangle$ and $\langle \mathcal{A}, \preccurlyeq\rangle$ are posets, $\perp$ is the infimum of $\langle C, \sqsubseteq\rangle$, $f \in C \to C$, the lub $\bigsqcup_{n\in\mathbb{N}} f^n(\perp)$ exists in $\langle C, \sqsubseteq\rangle$ such that $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcup_{n\in\mathbb{N}} f^n(\perp)$, $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$, $\overline{f} \in \mathcal{A} \to \mathcal{A}$, and $\forall n \in \mathbb{N}\ .\ \alpha(f^{n+1}(\perp)) = \overline{f}(\alpha(f^n(\perp)))$ (*commutation hypothesis*).
Then the lub $\displaystyle\curlyvee_{n\in\mathbb{N}} \overline{f}^n(\alpha(\perp))$ exists in $\langle \mathcal{A}, \preccurlyeq\rangle$ such that $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \displaystyle\curlyvee_{n\in\mathbb{N}} \overline{f}^n(\alpha(\perp))$.

- We just have to prove the *commutation hypothesis*
- It is essential to prove it only for the iterates $X$ of $\mathscr{F}^*[\![\texttt{while}\,^\ell\ \texttt{(B)}\ \texttt{S}_b]\!]$
- For example, in (17.4), we know that $X(\pi_1\ell') = \varnothing$ when $\ell' \notin \mathsf{labx}[\![\texttt{S}]\!]$ which would not be true for arbitrary parameters

# Proof sketch of (19.16) — I

Let $X$ be an iterate of $\mathscr{F}^{\vec{\varrho}}[\![\mathtt{S}]\!]\,\mathcal{R}_0$ where $\mathtt{S} \triangleq \mathtt{while}\,\ell\,\mathtt{(B)}\;\mathtt{S}_b$.

The calculational design strategy is :

(a) expand the definitions

$$
\begin{aligned}
& \mathrm{post}^{\vec{\varrho}}(\mathscr{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\;\mathtt{S}_b]\!](X))\,\mathcal{R}_0\,\ell' \\
= \ & \{\varrho(\pi_0\ell_0\pi_1\ell'') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0 = \ell \wedge \ell_0\pi_1\ell'' \in \mathscr{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\;\mathtt{S}_b]\!](X)(\pi_0\ell_0) \wedge \ell'' = \ell' \in \mathrm{labs}[\![\mathtt{S}]\!]\} \\
& \qquad \text{\textlbrackdbl def. (20.1) of } \mathrm{post}^{\vec{\mathsf{r}}}\text{, similar with (20.9) for } \mathrm{post}^{\vec{\mathsf{R}}}\text{, and def. } \mathscr{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\;\mathtt{S}_b]\!] = \varnothing \text{ when } \ell_0 \neq \ell \text{\textrbrackdbl} \\
= \ & \{\varrho(\pi_0\ell\pi_1\ell'') \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \ell\pi_1\ell'' \in \mathscr{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\;\mathtt{S}_b]\!](X)(\pi_0\ell) \wedge \ell'' = \ell' \in \mathrm{labs}[\![\mathtt{S}]\!]\} \\
& \qquad \text{\textlbrackdbl since } \ell_0 = \ell \text{\textrbrackdbl}
\end{aligned}
$$

# Proof sketch of (19.16) — II

## (b) case analysis

By definition (17.4) of $\mathscr{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!](X)(\pi_0\ell)$, we have to consider the union of three cases.

**(1)** $\{\varrho(\pi_0\ell\pi_1\ell'') \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \ell\pi_1\ell'' \in \{\ell\} \wedge \ell'' = \ell' \in \text{labs}[\![\texttt{S}]\!]\}$

$= \quad \{\varrho(\pi_0\ell) \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \ell = \ell'\}$ $\quad$ ⟨since $\ell\pi_1\ell'' = \ell = \ell'' = \ell' \in \text{labs}[\![\texttt{S}]\!]$⟩

$= \quad (\![\, \ell' = \ell \ ?\ \mathcal{R}_0 \ \text{:}\ \varnothing \,]\!)$ $\quad$ ⟨by Exercise 6.8⟩

# Proof sketch of (19.16) — III

**(2)** $\{\varrho(\pi_0\ell\pi_1\ell'') \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \ell\pi_1\ell'' \in \{\ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \text{after}[\![\mathsf{S}]\!] \mid \ell\pi_2\ell \in X(\pi_0\ell) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \text{ff}\} \wedge \ell'' = \ell' \in \text{labs}[\![\mathsf{S}]\!]\}$

$= \{\varrho(\pi_0\ell\pi_1\ell'') \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \exists\pi_2 \,.\, \ell\pi_1\ell'' = \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \text{after}[\![\mathsf{S}]\!] \wedge \ell\pi_2\ell \in X(\pi_0\ell) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \text{ff} \wedge \ell'' = \ell' \in \text{labs}[\![\mathsf{S}]\!]\}$ $\wr$def. $\in\wr$

$= \{\varrho(\pi_0\ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \text{after}[\![\mathsf{S}]\!]) \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \ell\pi_2\ell \in X(\pi_0\ell) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \text{ff} \wedge \text{after}[\![\mathsf{S}]\!] = \ell'\}$

$\wr$since $\ell\pi_1\ell'' = \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \text{after}[\![\mathsf{S}]\!]$ so $\ell'' = \text{after}[\![\mathsf{S}]\!] \in \text{labs}[\![\mathsf{S}]\!]\wr$

$= \{\varrho(\pi_0\ell_0\pi_2\ell'') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_2\ell'' \in X(\pi_0\ell_0) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell_0\pi_2\ell'') = \text{ff} \wedge \text{after}[\![\mathsf{S}]\!] = \ell' \wedge \ell_0 = \ell'' = \ell\}$

$\wr$since $\varrho(\pi_0\ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \text{after}[\![\mathsf{S}]\!]) = \varrho(\pi_0\ell\pi_2\ell)$ by (6.6) and renaming $\ell_0 = \ell'' = \ell\wr$

# Proof sketch of (19.16) — IV

$= \quad \{\varrho(\pi_0\ell_0\pi_2\ell'') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_2\ell'' \in X(\pi_0\ell_0) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell_0\pi_2\ell'') = \mathsf{ff} \wedge \mathsf{after}[\![\mathsf{S}]\!] = \ell' \wedge \ell_0 = \ell'' = \ell\}$

$= \quad (\!| \ell' = \mathsf{after}[\![\mathsf{S}]\!] \,?\, \overline{\mathsf{test}}^{\vec{\varrho}}[\![\mathsf{B}]\!](\{\varrho(\pi_0\ell_0\pi_2\ell'') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_2\ell'' \in X(\pi_0\ell_0) \wedge \ell = \ell_0 = \ell''\}) \,\mathbin{⸪}\, \varnothing \,|\!)$

$\wr$by def. $\overline{\mathsf{test}}^{\vec{r}}[\![\mathsf{B}]\!]\mathcal{R}_0 \quad \triangleq \quad \{\rho \in \mathcal{R}_0 \mid \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{ff}\}$$\wr$

$= \quad (\!| \ell' = \mathsf{after}[\![\mathsf{S}]\!] \,?\, \overline{\mathsf{test}}^{\vec{\varrho}}[\![\mathsf{B}]\!](\{\varrho(\pi_0\ell_0\pi_2\ell'') \mid \varrho(\pi_0\ell_0) \in \mathcal{R}_0 \wedge \ell_0\pi_2\ell'' \in X(\pi_0\ell_0) \wedge \ell'' = \ell\}) \,\mathbin{⸪}\, \varnothing \,|\!)$

$\wr$by Exercise 17.11 since $X$ is an iterate of $\mathcal{F}^{\vec{\varrho}}[\![\texttt{while}\;\ell\;\texttt{(B)}\;\mathsf{S}_b]\!]\,\mathcal{R}_0$ so $\ell_0 = \ell$$\wr$

$= \quad (\!| \ell' = \mathsf{after}[\![\mathsf{S}]\!] \,?\, \overline{\mathsf{test}}^{\vec{\varrho}}[\![\mathsf{B}]\!](\mathsf{post}^{\vec{\varrho}}(X)\,\mathcal{R}_0\;\ell) \,\mathbin{⸪}\, \varnothing \,|\!)$ $\quad\wr$def. (20.1) of $\mathsf{post}^{\vec{r}}$ or (20.9) of $\mathsf{post}^{\vec{\mathsf{R}}}$$\wr$

# Proof sketch of (19.16) — V

**(3)** (a) expand the definitions

$$\{\varrho(\pi_0\ell\pi_1\ell'') \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \ell\pi_1\ell'' \in \{\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3\ell'' \mid \ell\pi_2\ell \in X(\pi_0\ell) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \pi_3\ell'' \in \mathcal{S}^*[\![\mathsf{S}_b]\!](\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!])\} \wedge \ell'' = \ell' \in \mathsf{labs}[\![\mathsf{S}]\!]\}$$

(where $\ell$ of `while` $\ell$ `(B)` $\mathsf{S}_b$ is global)

$$= \{\varrho(\pi_0\ell\pi_1\ell'') \mid \varrho(\pi_0\ell) \in \mathcal{R}_0 \wedge \exists \pi_2, \pi_2 \,.\, \ell\pi_1\ell'' = \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3\ell'' \wedge \ell\pi_2\ell \in X(\pi_0\ell) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \pi_3\ell'' \in \mathcal{S}^*[\![\mathsf{S}_b]\!](\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]) \wedge \ell'' = \ell' \in \mathsf{labs}[\![\mathsf{S}]\!]\}$$

$\wr$def. $\in\wr$

$= \ldots$

(c) rewrite and simplify the formulæ

$= \ldots$

# Proof sketch of (19.16) — VI

$= \quad \{\varrho(\pi_0 \ell_0 \pi_2 \ell'' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3 \ell') \mid \varrho(\pi_0 \ell_0) \in \mathcal{R}_0 \wedge \ell \pi_2 \ell'' \in X(\pi_0 \ell_0) \wedge \ell'' = \ell \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0 \ell_0 \pi_2 \ell'') = \mathsf{tt} \wedge \pi_3 \ell' \in \mathcal{S}^*[\![\mathsf{S}_b]\!](\pi_0 \ell_0 \pi_2 \ell'' \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!])\}$ $\wr \ldots \int$

(d) to make the definitions and abstraction appear in the formula

$= \quad \{\varrho(\pi_0 \ell_0 \pi_2 \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!] \frown \pi_3 \ell') \mid \varrho(\pi_0 \ell_0 \pi_2 \ell) \in \mathsf{test}^{\vec{\varrho}}[\![\mathsf{B}]\!](\mathsf{post}^{\vec{\varrho}}(X)\ \mathcal{R}_0\ \ell) \wedge \pi_3 \ell' \in \mathcal{S}^*[\![\mathsf{S}_b]\!](\pi_0 \ell_0 \pi_2 \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!])\}$

$\wr$by def. $\mathsf{test}^{\vec{r}}[\![\mathsf{B}]\!]\mathcal{R}_0 \triangleq \{\rho \in \mathcal{R}_0 \mid \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt}\}$ and def. (20.1) of $\mathsf{post}^{\vec{r}}(X)\mathcal{R}_0\ell \triangleq \{\varrho(\pi_0 \ell_0 \pi_2 \ell'') \mid \varrho(\pi_0 \ell_0) \in \mathcal{R}_0 \wedge \ell_0 \pi_2 \ell'' \in X(\pi_0 \ell_0) \wedge \ell'' = \ell\}$ or (20.9) of $\mathsf{post}^{\vec{\mathsf{R}}}$ $\int$

$= \quad \ldots$

# Proof sketch of (19.16) — VII

$= \quad \ldots$

$= \{\varrho(\pi_0\ell_0\pi_1\ell'') \mid \varrho(\pi_0\ell_0) \in \mathsf{test}^{\vec{\varrho}}[\![\mathsf{B}]\!](\mathsf{post}^{\vec{\varrho}}(X)\ \mathcal{R}_0\ \ell) \wedge \ell_0\pi_1\ell'' \in \widehat{\mathcal{S}}^{\,*}[\![\mathsf{S}_b]\!](\pi_0\ell_0) \wedge \ell'' = \ell' \in \mathsf{labs}[\![\mathsf{S}]\!]\}$

$= \mathsf{post}^{\vec{\varrho}}(\widehat{\mathcal{S}}^{\,*}[\![\mathsf{S}_b]\!])\ (\mathsf{test}^{\vec{\varrho}}[\![\mathsf{B}]\!](\mathsf{post}^{\vec{\varrho}}(X)\ \mathcal{R}_0\ \ell))\ \ell', \quad \ell' \in \mathsf{labs}[\![\mathsf{S}]\!]$ (by def. (20.1) or (20.9))

$= \widehat{\mathcal{S}}^{\,\vec{\varrho}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\vec{\varrho}}[\![\mathsf{B}]\!](\mathsf{post}^{\vec{\varrho}}(X)\ \mathcal{R}_0\ \ell))\ \ell', \quad \ell' \in \mathsf{labs}[\![\mathsf{S}]\!]$ (by def. (20.15))

# Proof sketch of (19.16) — VIII

(e) regroup terms to simplify

By Section **4.2.7**, $\mathsf{labs}[\![\mathsf{S}]\!] = \{\ell\} \cup \mathsf{in}[\![\mathsf{S}_b]\!] \cup \{\mathsf{after}[\![\mathsf{S}]\!]\}$ and by Section **4.2.4**, $\mathsf{break\text{-}to}[\![\mathsf{S}_b]\!] \triangleq \mathsf{after}[\![\mathsf{S}]\!]$ so we can group the various terms as follows

(a) for $\ell' = \ell$ we have the term (1) and the case $\ell' = \ell$ of (3);

(b) for $\ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\}$ we have the terms (3);

(c) for $\ell' = \mathsf{after}[\![\mathsf{S}]\!]$, we have the term (2) and the terms (3) such that $\ell' = \mathsf{after}[\![\mathsf{S}]\!] = \mathsf{break\text{-}to}[\![\mathsf{S}_b]\!]$ that is, by Section **4.2.5**, belong to $\mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]$.

This regrouping of cases yield (19.16).

By commutation, we conclude for the fixpoint by Corollary 18.31 $\square$

# Proofs

- All proofs are given *in extenso* in the book
- Read them, at least for the iteration, to see the application of the exact fixpoint iterates abstraction Corollary 18.31
- The take away is that the reachability semantics $\mathcal{S}^{\vec{\varrho}}$ is entirely determined by
  - The prefix trace semantics $\mathcal{S}^*$
  - The reachability abstraction $\mathsf{post}^{\vec{\varrho}}$

  so that it is exact (sound and complete)

$$\mathcal{S}^{\vec{\varrho}}[\![\mathtt{S}]\!] \quad = \quad \mathsf{post}^{\vec{\varrho}}(\mathcal{S}^*[\![\mathtt{S}]\!])$$

# Home work

- Read Ch. **20** "Calculational design of the forward reachability semantics" of

*Principles of Abstract Interpretation*
Patrick Cousot
MIT Press

# The End, Thank you