Principles of Abstract Interpretation

MIT press

Ch. **27**, Abstraction

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-27--abstraction-PrAbsInt.pdf

Chapter 27

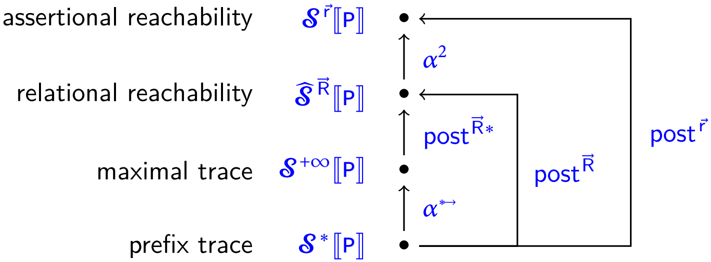
Ch. **27**, Abstraction

Definition of a Static Analyzer

- Given an abstract domain $\mathbb{D}^{\text{¤}}$, a static analyzer must, for any program P of a language $\mathbb{P}$, find an abstract inductive invariant $\mathcal{I} \in \mathsf{labs}[\![\mathsf{P}]\!] \to \mathbb{D}^{\text{¤}}$ satisfying the verification conditions $\widehat{\mathscr{V}}^{\text{¤}}[\![\mathsf{P}]\!]\mathcal{I}$ of Chapter **25** (Abstract reachability/invariance/safety verification semantics) and strong enough to imply a correctness specification $\mathcal{S}^{\text{¤}}[\![\mathsf{P}]\!] \in \mathsf{labs}[\![\mathsf{P}]\!] \to \mathbb{D}^{\text{¤}}$.

- The most difficult part is “find an abstract inductive invariant $\mathcal{I} \in \mathsf{labs}[\![\mathsf{P}]\!] \to \mathbb{D}^{\text{¤}}$” (*i.e.* find the inductive argument in an inductive proof)

Hierarchy of semantics


assertional reachability $\mathcal{S}^{\vec{r}}[\![\mathsf{P}]\!]$
relational reachability $\widehat{\mathcal{S}}^{\vec{R}}[\![\mathsf{P}]\!]$
maximal trace $\mathcal{S}^{+\infty}[\![\mathsf{P}]\!]$
prefix trace $\mathcal{S}^{*}[\![\mathsf{P}]\!]$
α^2
$\mathsf{post}^{\vec{R}*}$
$\alpha^{*\longrightarrow}$
$\mathsf{post}^{\vec{R}}$
$\mathsf{post}^{\vec{r}}$

- The assertional reachability semantics $\mathcal{S}^{\vec{r}}[\![\mathsf{P}]\!]$ of Chapter **19** is an abstraction of the relational reachability semantics $\widehat{\mathcal{S}}^{\vec{R}}[\![\mathsf{P}]\!]$ of Chapter **19** by α^2 (Exercise 20.13)
- This relational reachability semantics $\widehat{\mathcal{S}}^{\vec{R}}[\![\mathsf{P}]\!]$ of Chapter **19** is an abstraction of the maximal trace semantics $\mathcal{S}^{+\infty}[\![\mathsf{P}]\!]$ of Chapter **7** by $\mathsf{post}^{\vec{R}*}$ (20.14)
- This maximal trace semantics $\mathcal{S}^{+\infty}[\![\mathsf{P}]\!]$ of Chapter **7** is an abstraction of the prefix trace semantics $\mathcal{S}^{*}[\![\mathsf{P}]\!]$ by $\alpha^{*\longrightarrow}$ (Exercise 7.12).

Abstraction preserves the structure of semantics

- These semantics have the same structure
- These semantics are all instances of the generic abstract semantics of Chapter **21**
- These semantics are all implemented as an abstract interpreter parameterized by an abstract domain representing the information collected about program executions and the basic operations involved in this collection.
- This preservation of structure follows from the fact that *the abstraction of an instance of the abstract interpreter is an instance of the abstract interpreter*, as shown in this Chapter **27**.

Domain abstraction

Approximate domain abstraction

Definition 27.1 I — (Approximate domain abstraction)
We say that an abstract domain

$$\mathbb{D}^{\sharp} \quad \triangleq \quad \langle \mathbb{P}^{\sharp},\ \sqsubseteq^{\sharp},\ \bot^{\sharp},\ \sqcup^{\sharp},\ \mathsf{assign}^{\sharp}[\![\mathsf{x},\mathsf{A}]\!],\ \mathsf{test}^{\sharp}[\![\mathsf{B}]\!],\ \overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!]\rangle$$

is a sound *approximate abstraction* of a concrete domain

$$\mathbb{D}^{¤} \quad \triangleq \quad \langle \mathbb{P}^{¤},\ \sqsubseteq^{¤},\ \bot^{¤},\ \sqcup^{¤},\ \mathsf{assign}^{¤}[\![\mathsf{x},\mathsf{A}]\!],\ \mathsf{test}^{¤}[\![\mathsf{B}]\!],\ \overline{\mathsf{test}}^{¤}[\![\mathsf{B}]\!]\rangle$$

for concretization γ whenever

1. $\gamma \in \mathbb{P}^{\sharp} \xrightarrow{\nearrow} \mathbb{P}^{¤}$
2. $\mathsf{assign}^{¤}[\![\mathsf{x},\mathsf{A}]\!] \circ \gamma \ \dot{\sqsubseteq}^{¤}\ \gamma \circ \mathsf{assign}^{\sharp}[\![\mathsf{x},\mathsf{A}]\!]$
3. $\mathsf{test}^{¤}[\![\mathsf{B}]\!] \circ \gamma \ \dot{\sqsubseteq}^{¤}\ \gamma \circ \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]$ and $\overline{\mathsf{test}}^{¤}[\![\mathsf{B}]\!] \circ \gamma \ \dot{\sqsubseteq}^{¤}\ \gamma \circ \overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!]$.

- The hypothesis that γ is increasing in Definition 27.1-I.1 is sufficient to ensure soundness 27.8).

- It states that a logical implication in the abstract is valid in the concrete, *i.e.* reasonings in the abstract are preserved in the concrete.

- We have $\bot^{\text{¤}} \sqsubseteq^{\text{¤}} \gamma(\bot^{\sharp})$ since $\bot^{\text{¤}}$ is the infimum of $\mathbb{P}^{\text{¤}}$ and, for all $A, A' \in \mathbb{P}^{\sharp}$, $\gamma(A) \sqcup^{\text{¤}} \gamma(A') \sqsubseteq^{\text{¤}} \gamma(A \sqcup^{\sharp} A')$ since γ is increasing.

An alternative to Definition 27.1-I would be

1. $\langle \mathbb{P}^{¤}, \sqsubseteq^{¤} \rangle \mathrel{\substack{\xleftarrow{\;\gamma\;} \\ \xrightarrow[\;\alpha\;]{}}} \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp} \rangle$
2. $\alpha \circ \mathsf{assign}^{¤}[\![\mathsf{x}, \mathsf{A}]\!] \mathrel{\dot{\sqsubseteq}^{\sharp}} \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!] \circ \alpha$
3. $\alpha \circ \mathsf{test}^{¤}[\![\mathsf{B}]\!] \mathrel{\dot{\sqsubseteq}^{\sharp}} \mathsf{test}^{\sharp}[\![\mathsf{B}]\!] \circ \alpha$ and $\alpha \circ \overline{\mathsf{test}}^{¤}[\![\mathsf{B}]\!] \mathrel{\dot{\sqsubseteq}^{\sharp}} \overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!] \circ \alpha$.

Then $\gamma \in \mathbb{P}^{\sharp} \xrightarrow{\nearrow} \mathbb{P}^{¤}$ and for all $A \in \mathbb{P}^{¤}$,

$$\alpha \circ \mathsf{assign}^{¤}[\![\mathsf{x}, \mathsf{A}]\!]\, \gamma(A) \sqsubseteq^{\sharp} \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!] \circ \alpha(\gamma(A))$$

$$\Leftrightarrow \quad \alpha \circ \mathsf{assign}^{¤}[\![\mathsf{x}, \mathsf{A}]\!]\, \gamma(A) \sqsubseteq^{\sharp} \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!]\, A$$

$\wr(\Rightarrow)$ $\alpha \circ \gamma$ reductive and $\mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!]$ increasing
$(\Leftarrow)$ for $A' = \alpha(\gamma(A))$ and $\gamma(\alpha(\gamma(A'))) = \gamma(A')$ by the dual of Exercise 11.33$\int$

$$\Leftrightarrow \quad \mathsf{assign}^{¤}[\![\mathsf{x}, \mathsf{A}]\!] \circ \gamma(A) \sqsubseteq^{¤} \gamma \circ \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!]\,(A) \qquad \wr\text{def. Galois connection}\int$$

$$\Leftrightarrow \quad \mathsf{assign}^{¤}[\![\mathsf{x}, \mathsf{A}]\!] \circ \gamma \mathrel{\dot{\sqsubseteq}^{¤}} \gamma \circ \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!] \qquad \wr\text{pointwise } \textit{i.e.}\text{Definition 27.1-I.2}\int$$

and similarly for tests.

So semi-commutation hypotheses for α are equivalent to Definition 27.1-I.

Exact domain abstraction

Definition 27.1-II — (Exact domain abstraction)

We say that an abstract domain $\mathbb{D}^{\sharp}$ is an *exact abstraction* of a concrete domain $\mathbb{D}^{\text{¤}}$ for an abstraction $\langle\alpha,\ \gamma\rangle$ whenever

1. $\langle\mathbb{P}^{\text{¤}},\ \sqsubseteq^{\text{¤}}\rangle \mathrel{\underset{\alpha}{\overset{\gamma}{\leftarrows\!\!\!\twoheadrightarrow}}} \langle\mathbb{P}^{\sharp},\ \sqsubseteq^{\sharp}\rangle$
2. $\alpha \circ \mathsf{assign}^{\text{¤}}[\![\mathsf{x}, \mathsf{A}]\!] = \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!] \circ \alpha$
3. $\alpha \circ \mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!] = \mathsf{test}^{\sharp}[\![\mathsf{B}]\!] \circ \alpha$ and $\alpha \circ \overline{\mathsf{test}}^{\text{¤}}[\![\mathsf{B}]\!] = \overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!] \circ \alpha$. □

- The stronger hypotheses in Definition 27.1-II yields more precise results because there is a best abstraction, a Galois retraction, and commutation (instead of semi-commutation).

- This ensures completeness (see 27.8 below).

- Examples:
  - *Remark* 20.8 and the design of transformers in Chapter **20** show that the reachability semantics $\widehat{\mathcal{S}}^{\vec{r}}$ is the best abstraction of the pointwise prefix trace semantics $\widehat{\mathcal{S}}^{\dot{*}}$ by $\langle \ddot{\alpha}_{\varrho}, \ddot{\gamma}_{\varrho} \rangle$.
  - The assertional reachability domain is an exact abstraction of the relational reachability domain.

Concrete and abstract semantics

Objective

Given an concrete semantics

$$\widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{s}]\!] \quad \in \quad \mathbb{P}^{\text{¤}} \to \mathbb{L} \to \mathbb{P}^{\text{¤}}$$

on a concrete domain $\mathbb{D}^{\text{¤}} = \langle \mathbb{P}^{\text{¤}}, \sqsubseteq^{\text{¤}}, \perp^{\text{¤}}, \sqcup^{\text{¤}}, \mathsf{assign}^{\text{¤}}[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!], \overline{\mathsf{test}}^{\text{¤}}[\![\mathsf{B}]\!]\rangle$, the objective is to design an abstract semantics

$$\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{s}]\!] \quad \in \quad \mathbb{P}^{\sharp} \to \mathbb{L} \to \mathbb{P}^{\sharp}$$

on an abstract domain $\mathbb{D}^{\sharp} = \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp}, \perp^{\sharp}, \sqcup^{\sharp}, \mathsf{assign}^{\sharp}[\![\mathsf{x}, \mathsf{A}]\!], \mathsf{test}^{\sharp}[\![\mathsf{B}]\!], \overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!]\rangle$ which is sound (and sometimes complete) for an abstraction $\gamma \in \mathbb{P}^{\text{¤}} \xrightarrow{\nearrow} \mathbb{P}^{\sharp}$ (or $\langle \mathbb{P}^{\text{¤}}, \sqsubseteq\rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp}\rangle$) expressing the meaning of abstract properties in terms of concrete properties.

Method for an approximate abstraction

- Extend γ pointwise to $\dot{\gamma} \in (\mathbb{L} \to \mathbb{P}^{\sharp}) \xrightarrow{\nearrow} (\mathbb{L} \to \mathbb{P}^{\text{¤}})$ by $\dot{\gamma}(\overline{\mathcal{I}})\,\ell \triangleq \gamma(\overline{\mathcal{I}}(\ell))$
- Given $\mathcal{R}_0 \in \mathbb{P}^{\sharp}$, the global soundness condition is

$$\mathcal{S}^{\text{¤}}[\![\mathsf{s}]\!](\gamma(\mathcal{R}_0)) \quad \dot{\sqsubseteq}^{\text{¤}} \quad \dot{\gamma}(\mathcal{S}^{\sharp}[\![\mathsf{s}]\!](\mathcal{R}_0))$$

- Theorem 27.4 below shows that this global soundness condition on the semantics directly follows from the local soundness conditions on abstract domains stated in Definition 27.1-I.
- Note: we chose an abstract precondition $\mathcal{R}_0 \in \mathbb{P}^{\sharp}$ not a concrete one $\mathcal{R}_0' \in \mathbb{P}^{\text{¤}}$ since with $\gamma \in \mathbb{P}^{\text{¤}} \xrightarrow{\nearrow} \mathbb{P}^{\sharp}$ only, we cannot abstract $\mathcal{R}_0'$ into the abstract domain $\mathbb{P}^{\sharp}$.

Method for an exact abstraction

- In case $\langle \mathbb{P}^{\text{¤}}, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp}\rangle$, extend pointwise to $\ddot{\alpha} \in (\mathbb{P}^{\text{¤}} \to \mathbb{L} \to \mathbb{P}^{\text{¤}}) \xrightarrow{\nearrow} (\mathbb{P}^{\sharp} \to \mathbb{L} \to \mathbb{P}^{\sharp})$ by $\ddot{\alpha}(\mathcal{S}^{\text{¤}})\,\mathcal{R}_0\,\ell \triangleq \alpha(\mathcal{S}^{\text{¤}}\,\gamma(\mathcal{R}_0)\,\ell)$.

- Then $\langle \mathbb{P}^{\text{¤}} \to \mathbb{L} \to \mathbb{P}^{\text{¤}}, \ddot{\sqsubseteq}^{\text{¤}}\rangle \underset{\ddot{\alpha}}{\overset{\ddot{\gamma}}{\leftrightarrows}} \langle \mathbb{P}^{\sharp} \to \mathbb{L} \to \mathbb{P}^{\sharp}, \ddot{\sqsubseteq}^{\sharp}\rangle$ where $\ddot{\gamma}(\mathcal{S}^{\sharp})\,\mathcal{R}_0\,\ell \triangleq \gamma(\mathcal{S}^{\sharp}\,(\alpha(\mathcal{R}_0))\,\ell)$ (Note: $\mathcal{R}_0 \in \mathbb{P}^{\text{¤}}$ since we can abstract it)

- By 27.8 below, the exact abstractions hypotheses of Definition 27.1-II ensure both soundness and completeness.

$$\ddot{\alpha}(\widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{s}]\!]) \quad = \quad \widehat{\mathcal{S}}^{\sharp}[\![\mathsf{s}]\!].$$

- The semantics all have the same structure because this structure is preserved by structural abstraction.

Approximate abstraction of the abstract interpreter

Soundness of approximate abstractions

Theorem (27.4, Soundness of the abstract interpreter)
Let $\widehat{\mathcal{S}}^{\text{¤}}$ and $\widehat{\mathcal{S}}^{\sharp}$ be structural abstract interpreters for well-defined concrete $\mathbb{D}^{\text{¤}}$ and abstract domains $\mathbb{D}^{\sharp}$ by Definition 21.1 such that $\mathbb{D}^{\sharp}$ is an approximate abstraction of $\mathbb{D}^{\text{¤}}$ by Definition 27.1-I).

Then for all $\mathcal{R}_0 \in \mathbb{P}^{\sharp}$,

$$\mathcal{S}^{\text{¤}}[\![\mathsf{s}]\!](\gamma(\mathcal{R}_0)) \quad \dot{\sqsubseteq}^{\text{¤}} \quad \dot{\gamma}(\mathcal{S}^{\sharp}[\![\mathsf{s}]\!](\mathcal{R}_0))$$ □

- Note that the soundness of the abstract interpreter only depends on the soundness of the abstract domain

Proof I

Proof of Theorem 27.4 The proof is by structural induction, using Definition 27.1-I for basic cases and Exercise 18.18 for fixpoint abstraction.

- The abstract semantics $\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}]\!]\,\mathcal{R}_0\,\ell = \bot^{\sharp}$of a statement S at a label $\ell \notin \mathsf{labs}[\![\mathsf{S}]\!]$ not of that statement is empty.

Proof Assume that $\ell \notin \mathsf{labs}[\![\mathsf{S}]\!]$.

$$\begin{array}{lll}
 & \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}]\!](\gamma(\mathcal{R}_0))\ell & \wr\text{hyp. Theorem 27.4}\int \\
= & \bot^{\text{¤}} & \wr(21.3)\int \\
\sqsubseteq^{\text{¤}} & \gamma(\bot^{\sharp}) & \wr\text{def. infimum in Definition 21.1}\int
\end{array}$$

proving Theorem 27.4 by defining $\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}]\!](\mathcal{R}_0)\ell \triangleq \bot^{\sharp}$, which is (21.3) for $\mathbb{D}^{\sharp}$. □

Proof II

- Reminder: *Abstract semantics of a program* $\texttt{P} ::= \texttt{Sl}\ \ell'$

$$\widehat{\mathcal{S}}^{\,¤}[\![\texttt{P}]\!] \quad \triangleq \quad \widehat{\mathcal{S}}^{\,¤}[\![\texttt{Sl}]\!] \tag{21.4}$$

- The abstract semantics $\widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{P}]\!] \triangleq \widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{Sl}]\!]$ of a program $\texttt{P} ::= \texttt{Sl}\ \ell'$ is that of its statement list $\texttt{Sl}$.

Proof

$$\begin{array}{lll}
 & \widehat{\mathcal{S}}^{\,¤}[\![\texttt{P}]\!](\gamma(\mathcal{R}_0))\ell & \wr\text{hyp. Theorem 27.4}\int \\
= & \widehat{\mathcal{S}}^{\,¤}[\![\texttt{Sl}]\!](\gamma(\mathcal{R}_0))\ell & \wr\text{(21.4)}\int \\
\sqsubseteq^{¤} & \gamma(\widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{Sl}]\!](\mathcal{R}_0)\ell) & \wr\text{structural ind. hyp. for Theorem 27.4}\int \\
= & \gamma(\widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{P}]\!](\mathcal{R}_0)\ell) & \wr\text{by defining } \widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{P}]\!] \ \triangleq\ \widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{Sl}]\!] \text{ of the form (21.4)}\int \\
= & \dot{\gamma}(\widehat{\mathcal{S}}^{\,\sharp}[\![\texttt{P}]\!](\mathcal{R}_0))\ell & \wr\text{pointwise}\int \quad \square
\end{array}$$

Proof III

- The abstract semantics of a statement list $\texttt{Sl} ::= \texttt{Sl}'\ \texttt{S}$ collects the values of variables reachable in $\texttt{Sl}'$ and those reachable in $\texttt{S}$ after executing $\texttt{Sl}'$.

$$\begin{aligned}\widehat{\mathcal{S}}^{\sharp}[\![\texttt{Sl}]\!]\mathcal{R}_0\,\ell \quad &\triangleq \quad \llparenthesis\, \ell \in \mathsf{labs}[\![\texttt{Sl}']\!] \setminus \{\mathsf{at}[\![\texttt{S}]\!]\} \mathrel{?} \widehat{\mathcal{S}}^{\sharp}[\![\texttt{Sl}']\!]\,\mathcal{R}_0\,\ell \\ &\quad\ \ \|\ \ell \in \mathsf{labs}[\![\texttt{S}]\!] \mathrel{?} \widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!](\widehat{\mathcal{S}}^{\sharp}[\![\texttt{Sl}']\!]\,\mathcal{R}_0\,\mathsf{at}[\![\texttt{S}]\!])\,\ell \\ &\quad\ \ \mathrel{:} \bot^{\sharp}\,\rrparenthesis\end{aligned}$$

- For the empty statement list $\texttt{Sl} ::= \epsilon$,

$$\widehat{\mathcal{S}}^{\sharp}[\![\texttt{Sl}]\!]\,\mathcal{R}_0\,\ell \triangleq \llparenthesis\, \ell = \mathsf{at}[\![\texttt{Sl}]\!] \mathrel{?} \mathcal{R}_0 \mathrel{:} \bot^{\sharp}\,\rrparenthesis$$

- The abstract semantics of a skip statement $\texttt{S} ::= \texttt{;}$ is

$$\widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!]\,\mathcal{R}_0\,\ell = \llparenthesis\, \ell \in \{\mathsf{at}[\![\texttt{S}]\!], \mathsf{after}[\![\texttt{S}]\!]\} \mathrel{?} \mathcal{R}_0 \mathrel{:} \bot^{\sharp}\,\rrparenthesis$$

Proof IV

- Reminder: *Abstract semantics of an assignment statement* `S ::= x = A ;`

$$\widehat{\mathcal{S}}^{\text{¤}}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell \quad = \quad \llparenthesis\, \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{?} \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} \mathsf{assign}^{\text{¤}}[\![\mathtt{x}, \mathtt{A}]\!]\,\mathcal{R}_0 \mathrel{⦂} \bot^{\text{¤}} \,\rrparenthesis \quad (21.7)$$

- The abstract semantics of an assignment statement `S ::= x = A ;` is

$$\widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell \quad = \quad \llparenthesis\, \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{?} \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} \mathsf{assign}^{\sharp}[\![\mathtt{x}, \mathtt{A}]\!]\,\mathcal{R}_0 \mathrel{⦂} \bot^{\sharp} \,\rrparenthesis$$

Proof

$$\begin{aligned}
&\widehat{\mathcal{S}}^{\text{¤}}[\![\mathtt{S}]\!]\,(\gamma(\mathcal{R}_0))\ell && \text{≀hyp. Theorem 27.4≀}\\
=\ &\llparenthesis\, \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{?} \gamma(\mathcal{R}_0) \parallel \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} \mathsf{assign}^{\text{¤}}[\![\mathtt{x}, \mathtt{A}]\!]\,\gamma(\mathcal{R}_0) \mathrel{⦂} \top^{\text{¤}} \,\rrparenthesis && \text{≀(21.7)≀}\\
\sqsubseteq^{\text{¤}}\ &\gamma(\llparenthesis\, \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{?} \mathcal{R}_0 \parallel \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} \mathsf{assign}^{\sharp}[\![\mathtt{x}, \mathtt{A}]\!]\,\mathcal{R}_0 \mathrel{⦂} \bot^{\sharp} \,\rrparenthesis)\\
& && \text{≀}\bot^{\text{¤}} \sqsubseteq^{\text{¤}} \gamma(\bot^{\sharp})\text{, Definition 27.1.2, and factoring } \gamma \text{ over the conditional≀}\\
=\ &\dot{\gamma}(\widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!](\mathcal{R}_0))\ell && \text{≀by def. } \widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!]\mathcal{R}_0\,\ell \text{ above, of the form (21.7)≀} \quad \square
\end{aligned}$$

Proof V

- The abstract semantics of a conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t$ is

$$\begin{array}{rcl}
\widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}]\!]\,\mathcal{R}_0\,\ell & = & \llparenthesis\ \ell = \mathsf{at}[\![\mathtt{S}]\!] \mathrel{⸮} \mathcal{R}_0 \\
 & & \parallel\ \ell \in \mathsf{in}[\![\mathtt{S}_t]\!] \mathrel{⸮} \widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}_t]\!]\,(\mathsf{test}^{\sharp}[\![\mathtt{B}]\!]\,\mathcal{R}_0)\,\ell \\
 & & \parallel\ \ell = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{⸮} \widehat{\mathcal{S}}^{\sharp}[\![\mathtt{S}_t]\!]\,(\mathsf{test}^{\sharp}[\![\mathtt{B}]\!]\,\mathcal{R}_0)\,\ell \sqcup^{¤} \overline{\mathsf{test}}^{\sharp}[\![\mathtt{B}]\!]\,\mathcal{R}_0 \\
 & & ⦂\ \bot^{¤}\ \rrparenthesis
\end{array}$$

- The conditional statement $\mathtt{S} ::= \mathtt{if\ (B)\ S}_t\ \mathtt{else\ S}_f$ is similar

- See the proofs in the book

Proof VI

- Reminder: *Abstract semantics of an iteration statement* $\texttt{S} ::= \texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b$

$$\widehat{\mathcal{S}}^{\text{¤}}[\![\texttt{S}]\!]\,\mathcal{R}_0\,\ell' \quad=\quad \mathsf{lfp}^{\dot{\sqsubseteq}^{\text{¤}}}\,(\mathcal{F}^{\text{¤}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0)\,\ell' \tag{21.11}$$

$$\mathcal{F}^{\text{¤}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!] \quad\in\quad \mathbb{P}^{\text{¤}} \rightarrow ((\mathbb{L} \rightarrow \mathbb{P}^{\text{¤}}) \rightarrow (\mathbb{L} \rightarrow \mathbb{P}^{\text{¤}}))$$

$$\begin{aligned}
&\mathcal{F}^{\text{¤}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\,\mathcal{R}_0\,X\,\ell' \quad= \\
&\quad (\!|\ \ell' = \ell \mathrel{?} \mathcal{R}_0 \sqcup^{\text{¤}} \widehat{\mathcal{S}}^{\text{¤}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\text{¤}}[\![\texttt{B}]\!]X(\ell))\,\ell \\
&\quad\ \ \|\ \ell' \in \mathsf{in}[\![\texttt{S}_b]\!] \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^{\text{¤}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\text{¤}}[\![\texttt{B}]\!]X(\ell))\,\ell' \\
&\quad\ \ \|\ \ell' = \mathsf{after}[\![\texttt{S}]\!] \mathrel{?} \overline{\mathsf{test}}^{\text{¤}}[\![\texttt{B}]\!]X(\ell) \sqcup^{\text{¤}} \bigsqcup^{\text{¤}}_{\ell'' \in \mathsf{breaks\text{-}of}[\![\texttt{S}_b]\!]} \widehat{\mathcal{S}}^{\text{¤}}[\![\texttt{S}_b]\!]\,(\mathsf{test}^{\text{¤}}[\![\texttt{B}]\!]X(\ell))\,\ell'' \\
&\quad \mathrel{:} \bot^{\text{¤}}\ |\!)
\end{aligned}$$

Proof VII

- For the iteration $\texttt{S} ::= \texttt{while}\,^{\ell}\,\texttt{(B)}\;\texttt{S}_b$, we have

$$\widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!]\,\mathcal{R}_0 \quad = \quad \mathsf{lfp}^{\dot{\sqsubseteq}}\,(\mathcal{F}^{\sharp}[\![\texttt{while}\,^{\ell}\,\texttt{(B)}\;\texttt{S}_b]\!]\,\mathcal{R}_0)$$

where the transformer $\mathcal{F}^{\sharp}[\![\texttt{while}\,^{\ell}\,\texttt{(B)}\;\texttt{S}_b]\!]$ is given by (21.11).

Proof VIII

Reminder on fixpoint approximation (Exercise 18.18)

Assume that $\langle \mathcal{C}, \sqsubseteq, \bot, \sqcup \rangle$ is a cpo, $f \in \mathcal{C} \xrightarrow{\nearrow} \mathcal{C}$ is upper-continuous, $\langle \mathcal{A}, \preccurlyeq \rangle$ is a poset, $\overline{f} \in \mathcal{A} \to \mathcal{A}$, $f \circ \gamma \mathrel{\dot{\sqsubseteq}} \gamma \circ \overline{f}$, and $\gamma \in \mathcal{A} \xrightarrow{\nearrow} \mathcal{C}$ is increasing.
Then $\forall y \in \mathcal{A}, \overline{f}(y) \preccurlyeq y$ implies $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(y)$ (in particular when $y = \mathsf{lfp}^{\preccurlyeq} \overline{f}$).

The semi-commutation hypothesis provides a design method of $\overline{f}$ from the formal definition of f

Proof IX

Proof We want to prove that

$$\widehat{\mathcal{S}}^{¤}[\![\texttt{S}]\!]\,\gamma(\mathcal{R}_0) \mathrel{\dot{\sqsubseteq}^{¤}} \gamma(\widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!]\,\mathcal{R}_0)$$

that is

$$\forall \ell' \in \mathsf{labs}[\![\texttt{S}]\!] \mathrel{.} \widehat{\mathcal{S}}^{¤}[\![\texttt{S}]\!]\,\gamma(\mathcal{R}_0)\,\ell' \mathrel{\sqsubseteq^{¤}} \gamma(\widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!]\,\mathcal{R}_0)\,\ell'$$

pointwise using the concretization $\gamma \in \mathbb{P}^{\sharp} \xrightarrow{\nearrow} \mathbb{P}^{¤}$.

We look, by calculational design, for an iteration transformer $\mathscr{F}^{\sharp}[\![\texttt{while}\,\ell\,\texttt{(B)}\,\texttt{S}_b]\!]$ such that for all $\ell' \in \mathsf{labs}[\![\texttt{S}]\!]$, iterates X of $\mathscr{F}^{¤}[\![\texttt{while}\,\ell\,\texttt{(B)}\,\texttt{S}_b]\!]\,\gamma(\mathcal{R}_0)$, we have

$$\mathscr{F}^{¤}[\![\texttt{while}\,\ell\,\texttt{(B)}\,\texttt{S}_b]\!]\,\gamma(\mathcal{R}_0)\,\dot{\gamma}(X) \quad \dot{\sqsubseteq}^{¤} \quad \dot{\gamma}(\mathscr{F}^{\sharp}[\![\texttt{while}\,\ell\,\texttt{(B)}\,\texttt{S}_b]\!]\,\mathcal{R}_0\,X)$$

We conclude by Exercise 18.18 for $\ddot{\sqsubseteq}^{\sharp}$.

The semi-commutation calculational design is as follows.

Proof X

$$
\begin{aligned}
& \mathscr{F}^{\text{¤}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\ \gamma(\mathcal{R}_0)\ \dot{\gamma}(X)\ \ell' \\
= \ & \llparenthesis\ \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0) \sqcup^{\text{¤}} \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!]\dot{\gamma}(X)(\ell))\ \ell \\
& \parallel\ \ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!]\dot{\gamma}(X)(\ell))\ \ell' \\
& \parallel\ \ell' = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \overline{\mathsf{test}}^{\text{¤}}[\![\mathsf{B}]\!]\dot{\gamma}(X)(\ell) \sqcup^{\text{¤}} \bigsqcup^{\text{¤}}_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!]\dot{\gamma}(X)(\ell))\ \ell'' \\
& ⁏\ \bot^{\text{¤}}\ \rrparenthesis \qquad\qquad \wr(21.11)\wr \\
= \ & \llparenthesis\ \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0) \sqcup^{\text{¤}} \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!]\gamma(X(\ell)))\ \ell \\
& \parallel\ \ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!]\gamma(X(\ell)))\ \ell' \\
& \parallel\ \ell' = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \overline{\mathsf{test}}^{\text{¤}}[\![\mathsf{B}]\!]\gamma(X(\ell)) \sqcup^{\text{¤}} \bigsqcup^{\text{¤}}_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\mathcal{S}}^{\text{¤}}[\![\mathsf{S}_b]\!]\ (\mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!]\gamma(X(\ell)))\ \ell'' \\
& ⁏\ \bot^{\text{¤}}\ \rrparenthesis \qquad\qquad \wr\text{pointwise def. } \dot{\gamma}\wr
\end{aligned}
$$

Proof XI

$$
\begin{array}{l}
\quad\llparenthesis\, \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0) \sqcup^{\text{¤}} \widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_b\rrbracket\,(\mathsf{test}^{\text{¤}}\llbracket \mathsf{B}\rrbracket\gamma(X(\ell)))\,\ell \\
\quad\parallel \ell' \in \mathsf{in}\llbracket \mathsf{S}_b\rrbracket \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_b\rrbracket\,(\mathsf{test}^{\text{¤}}\llbracket \mathsf{B}\rrbracket\gamma(X(\ell)))\,\ell' \\
\quad\parallel \ell' = \mathsf{after}\llbracket \mathsf{S}\rrbracket \mathrel{?} \overline{\mathsf{test}}^{\text{¤}}\llbracket \mathsf{B}\rrbracket\gamma(X(\ell)) \sqcup^{\text{¤}} \displaystyle\bigsqcup^{\text{¤}}_{\ell''\in\mathsf{breaks\text{-}of}\llbracket \mathsf{S}_b\rrbracket} \widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_b\rrbracket\,(\mathsf{test}^{\text{¤}}\llbracket \mathsf{B}\rrbracket\gamma(X(\ell)))\,\ell'' \\
\quad\fatsemi \bot^{\text{¤}}\,\rrparenthesis \\
\sqsubseteq^{\text{¤}} \llparenthesis\, \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0) \sqcup^{\text{¤}} \widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_b\rrbracket\,\gamma(\mathsf{test}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell))\,\ell \\
\quad\parallel \ell' \in \mathsf{in}\llbracket \mathsf{S}_b\rrbracket \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_b\rrbracket\,\gamma(\mathsf{test}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell))\,\ell' \\
\quad\parallel \ell' = \mathsf{after}\llbracket \mathsf{S}\rrbracket \mathrel{?} \gamma(\overline{\mathsf{test}}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell)) \sqcup^{\text{¤}} \displaystyle\bigsqcup^{\text{¤}}_{\ell''\in\mathsf{breaks\text{-}of}\llbracket \mathsf{S}_b\rrbracket} \widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_b\rrbracket\,\gamma(\mathsf{test}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell))\,\ell'' \\
\quad\fatsemi \gamma(\bot^{\sharp})\,\rrparenthesis
\end{array}
$$

$\wr$Definition 27.1-I.3, $\widehat{\mathcal{S}}^{\text{¤}}\llbracket \mathsf{S}_t\rrbracket$ and $\sqcup^{\text{¤}}$ are increasing, and $\bot^{\text{¤}} \sqsubseteq^{\text{¤}} \gamma(\bot^{\sharp})$ $\int$

$$
\begin{array}{l}
\sqsubseteq^{\text{¤}} \llparenthesis\, \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0) \sqcup^{\text{¤}} \gamma(\widehat{\mathcal{S}}^{\sharp}\llbracket \mathsf{S}_b\rrbracket\,\mathsf{test}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell)\,\ell) \\
\quad\parallel \ell' \in \mathsf{in}\llbracket \mathsf{S}_b\rrbracket \setminus \{\ell\} \mathrel{?} \gamma(\widehat{\mathcal{S}}^{\sharp}\llbracket \mathsf{S}_b\rrbracket\,\mathsf{test}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell)\,\ell') \\
\quad\parallel \ell' = \mathsf{after}\llbracket \mathsf{S}\rrbracket \mathrel{?} \gamma(\overline{\mathsf{test}}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell)) \sqcup^{\text{¤}} \displaystyle\bigsqcup^{\text{¤}}_{\ell''\in\mathsf{breaks\text{-}of}\llbracket \mathsf{S}_b\rrbracket} \gamma(\widehat{\mathcal{S}}^{\sharp}\llbracket \mathsf{S}_b\rrbracket\,\mathsf{test}^{\sharp}\llbracket \mathsf{B}\rrbracket X(\ell)\,\ell'') \\
\quad\fatsemi \gamma(\bot^{\sharp})\,\rrparenthesis
\end{array}
$$

$\wr$structural ind. hyp. of Theorem 28.44$\int$

Proof XII

$$
\begin{aligned}
&\llparenthesis\, \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0) \sqcup^{\text{¤}} \gamma(\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell) \\
&\;\| \;\ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\} \mathrel{?} \gamma(\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell') \\
&\;\| \;\ell' = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \gamma(\overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!]X(\ell)) \sqcup^{\text{¤}} \bigsqcup^{\text{¤}}_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \gamma(\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell'') \\
&\;\mathrel{:} \gamma(\bot^{\sharp})\, \rrparenthesis \\
\sqsubseteq^{\text{¤}} &\llparenthesis\, \ell' = \ell \mathrel{?} \gamma(\mathcal{R}_0 \sqcup^{\sharp} \widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell) \\
&\;\| \;\ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\} \mathrel{?} \gamma(\widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell') \\
&\;\| \;\ell' = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \gamma(\overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!]X(\ell) \sqcup^{\sharp} \bigsqcup^{\sharp}_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell'') \\
&\;\mathrel{:} \gamma(\bot^{\sharp})\, \rrparenthesis \\
&\hfill \text{⟅}\gamma \text{ is increasing so } \bigsqcup^{\text{¤}}_{i\in\Delta} \gamma(x_i) \sqsubseteq^{\text{¤}} \gamma(\bigsqcup^{\sharp}_{i\in\Delta} x_i)\text{⟆} \\
= \;&\gamma(\llparenthesis\, \ell' = \ell \mathrel{?} \mathcal{R}_0 \sqcup^{\sharp} \widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell \\
&\;\| \;\ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell' \\
&\;\| \;\ell' = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \overline{\mathsf{test}}^{\sharp}[\![\mathsf{B}]\!]X(\ell) \sqcup^{\sharp} \bigsqcup^{\sharp}_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\mathcal{S}}^{\sharp}[\![\mathsf{S}_b]\!]\, \mathsf{test}^{\sharp}[\![\mathsf{B}]\!]X(\ell)\; \ell'' \\
&\;\mathrel{:} \bot^{\sharp}\, \rrparenthesis) \\
&\hfill \text{⟅factoring } \gamma \text{ over the conditional⟆}
\end{aligned}
$$

Proof XIII

$$
\begin{aligned}
&\gamma(\llparenthesis\, \ell' = \ell \mathrel{?} \mathcal{R}_0 \sqcup^\sharp \widehat{\mathcal{S}}^\sharp[\![\mathsf{S}_b]\!]\, \mathsf{test}^\sharp[\![\mathsf{B}]\!]X(\ell)\ \ell \\
&\ \ \|\ \ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus \{\ell\} \mathrel{?} \widehat{\mathcal{S}}^\sharp[\![\mathsf{S}_b]\!]\, \mathsf{test}^\sharp[\![\mathsf{B}]\!]X(\ell)\ \ell' \\
&\ \ \|\ \ell' = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} \overline{\mathsf{test}}^\sharp[\![\mathsf{B}]\!]X(\ell) \sqcup^\sharp \bigsqcup^\sharp_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\mathcal{S}}^\sharp[\![\mathsf{S}_b]\!]\, \mathsf{test}^\sharp[\![\mathsf{B}]\!]X(\ell)\ \ell'' \\
&\ \ \mathrel{:} \bot^\sharp\, \rrparenthesis) \\
= {}&\gamma(\mathscr{F}^\sharp[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]\, \mathcal{R}_0\ X\ \ell') \qquad \text{⟅by def. (21.11) of } \mathscr{F}^\sharp[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]\text{⟆} \quad \square
\end{aligned}
$$

Proof XIV

- The abstract semantics $\widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!]\,\mathcal{R}_0\,\ell = (\!|\,\ell = \mathsf{at}[\![\texttt{S}]\!]\ ?\ \mathcal{R}_0\ ⨾\ \bot^{\sharp}\,|\!)$ of a break statement $\texttt{S} ::= {}^{\ell}\ \texttt{break ;}$ is that of its entry point.
- The abstract semantics $\widehat{\mathcal{S}}^{\sharp}[\![\texttt{S}]\!] = \widehat{\mathcal{S}}^{\sharp}[\![\texttt{Sl}]\!]$ of a compound statement $\texttt{S} ::= \texttt{\{ Sl \}}$ is that of the statement list $\texttt{Sl}$.

Proof similar to that of an empty statement and that of a program. □ □

Remark: Soundness of reachability analyses

- The soundness of reachability analyses $\widehat{\mathcal{S}}^{\sharp}$ follows from Theorem 27.4 where the concrete semantics is $\mathbb{P}^{\text{¤}} = \mathcal{S}^{\vec{\varrho}}[\![\mathsf{s}]\!]$.

- To prove this it is sufficient to check the soundness conditions of Definition 27.1 for the abstract domain.

Remark: Increasingness of the abstract semantics

- The proof of Theorem 27.4 relies on the hypothesis that $\mathcal{S}^{\text{¤}}[\![\mathsf{s}]\!]$ is increasing but this hypothesis is never used for $\mathcal{S}^{\sharp}[\![\mathsf{s}]\!]$.

- So the proof remains valid when replacing $\mathcal{S}^{\sharp}[\![\mathsf{s}]\!]$ by any possibly non-increasing over-approximation.

- This is an essential remark for proving the soundness of widening in Chapter **34**.

Exact abstraction of the abstract interpreter

Soundness and completeness of exact abstractions

Theorem (27.8, Soundness and completeness of the abstract interpreter)

Let $\widehat{\mathcal{S}}^{¤}$ and $\widehat{\mathcal{S}}^{\sharp}$ be structural abstract interpreters for well-defined concrete $\mathbb{D}^{¤}$ and abstract domains $\mathbb{D}^{\sharp}$ by Definition 21.1 such that $\mathbb{D}^{\sharp}$ is an abstraction of $\mathbb{D}^{¤}$ by Definition 27.1-II.

Then for all $\mathcal{R}_0 \in \mathbb{P}^{\sharp}$,

$$\ddot{\alpha}(\widehat{\mathcal{S}}^{¤}[\![\mathsf{s}]\!])\,\mathcal{R}_0 \quad = \quad \dot{\alpha}(\mathcal{S}^{¤}[\![\mathsf{s}]\!]\,\gamma(\mathcal{R}_0)\,) \quad = \quad \mathcal{S}^{\sharp}[\![\mathsf{s}]\!]\,\mathcal{R}_0$$

Proof

Proof of 27.8 The proof is by structural induction, using

- Definition 27.1-I for basic and inductive non-recursive cases, and
- the fixpoint abstraction Theorem 18.21 for the iteration. □

Theorem (18.21, exact fixpoint abstraction in a complete lattice)

Assume that $\langle \mathcal{C}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ and $\langle \mathcal{A}, \preccurlyeq, 0, 1, \curlyvee, \curlywedge \rangle$ are complete lattices, $f \in \mathcal{C} \xrightarrow{\nearrow} \mathcal{C}$ is increasing, $\langle \mathcal{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq \rangle$, $\overline{f} \in \mathcal{A} \xrightarrow{\nearrow} \mathcal{A}$ is increasing, and $\alpha \circ f = \overline{f} \circ \alpha$ (*commutation property*).

Then $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$.

Best abstraction (continuing Section **11.12**)

Best abstraction

- Given a domain abstraction of Definition 27.1, a concrete property $P \in \mathbb{P}^{¤}$ can be over-approximated by any abstract property $\overline{P} \in \mathbb{P}^{\sharp}$ such that $P \sqsubseteq^{¤} \gamma(\overline{P})$.

- If the set of abstract over-approximations $\{\overline{P} \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{¤} \gamma(\overline{P})\}$ of concrete property P has a greatest lower bound then we call it "the best abstraction of the property P in the abstract domain $\mathbb{P}^{\sharp}$".

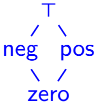
Signs

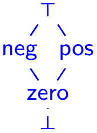
- For signs the property $P = \{0\}$ (to be zero) can be overapproximated by 0 (to be zero), $\geqslant 0$ (to be positive or zero), $\leqslant 0$ (to be negative or zero), or $\top_{\pm}$ (to be integer). <0 would be unsound.

- 0 (to be zero) is the most precise abstraction (and $\top_{\pm}$ (to be integer), the less precise one).

Truncated signs

- Consider the poset of signs $\begin{array}{ccc} & \top & \\ / & & \backslash \\ \text{neg} & & \text{pos} \end{array}$ of Exercise 3.2 from [Sintzoff, 1972] where we have added $\top$ to express that the rule of signs is inconclusive like “$\text{neg} - \text{neg} = \top$”.
- [Sintzoff, 1972] informally defined $\gamma(\text{pos}) \triangleq \{z \in \mathbb{Z} \mid z \geqslant 0\}$ and $\gamma(\text{neq}) \triangleq \{z \in \mathbb{Z} \mid z < 0\}$
- Then
  - $P = \emptyset$ (false) has no best abstraction
  - the classical rule of signs is incorrect.
- It is correct with $\gamma(\text{neq}) \triangleq \{z \in \mathbb{Z} \mid z \leqslant 0\}$ but then $P = \{0\}$ (to be zero) has no best abstraction.
- In $(0 - 1) - 0$ is should be “neg” for the first instance and “pos” for the second to get $(\text{neg}-\text{pos})\text{-pos}{=}\text{neg-pos}{=}\text{neg}$.

- Trying all possibilities would yield a combinatorial explosion which is avoided by adding "zero" to the lattice 

.
- Then the best abstraction of $P = \emptyset$ (false) and $P = \{0\}$ (to be zero), both have "zero" as best abstraction.
- Of course adding $\perp$ in 

such that $\gamma(\perp) = \emptyset$ is more precise since one can express that an expression is never evaluated *e.g.* in dead code.

Best abstractions and Galois connections (I)

Best abstractions correspond to Galois connections between the concrete and abstract domains.

Theorem (27.12) Let $\langle \mathbb{P}^{\text{¤}}, \sqsubseteq^{\text{¤}} \rangle$ be a concrete domain, $\langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp} \rangle$ be an abstract domain, and $\langle \mathbb{P}^{\text{¤}}, \sqsubseteq^{\text{¤}} \rangle \overset{\gamma}{\underset{\alpha}{\leftrightarrows}} \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp} \rangle$. Then $\alpha(P)$ is the best abstraction of P in $\mathbb{P}^{\sharp}$.

Proof By Lemma 11.41 so that $\alpha(P) = \sqcap^{\sharp}\{\overline{P} \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{\text{¤}} \gamma(\overline{P})\}$. □

Best abstractions and Galois connections (II)

Best abstractions correspond to Galois connections between the concrete and abstract

Theorem (27.13) Let $\langle\mathbb{P}^{¤}, \sqsubseteq^{¤}\rangle$ be a concrete complete lattice domain and $\langle\mathbb{P}^{\sharp}, \sqsubseteq^{\sharp}\rangle$ be an abstract complete lattice domain with meet-preserving concretization $\gamma \in \mathbb{P}^{\sharp} \xrightarrow{\nearrow} \mathbb{P}^{¤}$.

Assume that any concrete property $P \in \mathbb{P}^{¤}$ has a best abstraction in $\mathbb{P}^{\sharp}$ (*i.e.* $\sqcap^{\sharp}\{\overline{P} \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{¤} \gamma(\overline{P})\}$ exists in $\mathbb{P}^{\sharp}$).

Define $\alpha(P) \triangleq \sqcap^{\sharp}\{\overline{P} \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{¤} \gamma(\overline{P})\}$. Then $\langle\mathbb{P}^{¤}, \sqsubseteq^{¤}\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle\mathbb{P}^{\sharp}, \sqsubseteq^{\sharp}\rangle$.

It is possible to reformulate best abstractions in abstract interpretation using Moore families, closure operators, *etc*. instead of Galois connections.

Proof

$$\begin{array}{ll@{\qquad}r}
 & P \sqsubseteq^{\text{¤}} \gamma(\overline{P}) & \\
\Rightarrow & \overline{P} \in \{\overline{P}' \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{\text{¤}} \gamma(\overline{P}')\} & \wr\text{def. } \in\int \\
\Rightarrow & \sqcap^{\sharp}\{\overline{P}' \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{\text{¤}} \gamma(\overline{P}')\} \sqsubseteq^{\sharp} \overline{P} & \wr\text{def. glb } \sqcap^{\sharp}\int \\
\Rightarrow & \alpha(P) \sqsubseteq^{\sharp} \overline{P} & \wr\text{def. } \alpha\int
\end{array}$$

$$\begin{array}{ll@{\qquad}r}
 & \alpha(P) \sqsubseteq^{\sharp} \overline{P} & \\
\Rightarrow & \gamma(\alpha(P)) \sqsubseteq^{\text{¤}} \gamma(\overline{P}) & \wr\gamma\text{ preserves meets so is increasing}\int \\
\Rightarrow & \gamma(\sqcap^{\sharp}\{\overline{P}' \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{\text{¤}} \gamma(\overline{P}')\}) \sqsubseteq^{\text{¤}} \gamma(\overline{P}) & \wr\text{def. } \alpha\int \\
\Rightarrow & \sqcap^{\text{¤}}\{\gamma(\overline{P}') \in \mathbb{P}^{\sharp} \mid P \sqsubseteq^{\text{¤}} \gamma(\overline{P}')\}) \sqsubseteq^{\text{¤}} \gamma(\overline{P}) & \wr\gamma\text{ preserves meets }\int \\
\Rightarrow & P \sqsubseteq^{\text{¤}} \gamma(\overline{P}) & \wr\text{def. glb}\int \quad \square
\end{array}$$

Best sound (and complete) abstract interpreter

Best abstractions and transformers I

In case of existence of best abstraction, there is a best way of choosing the approximate transformers of an abstract domain.

Theorem (27.18) If $\langle \mathbb{P}^{\text{¤}}, \sqsubseteq^{\text{¤}} \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp} \rangle$ then $F^{\sharp} \triangleq \alpha \circ F \circ \gamma$ is the best abstraction of F satisfying the *semi-commutation condition* $F \circ \gamma \sqsubseteq^{\text{¤}} \gamma \circ F^{\sharp}$.

Proof of Theorem 27.18 By the Galois connection $\gamma \circ \alpha$ is extensive so $F \circ \gamma \mathrel{\dot{\sqsubseteq}}^{\text{¤}} \gamma \circ \alpha \circ F \circ \gamma = \gamma \circ F^{\sharp}$ proving that $F^{\sharp} \triangleq \alpha \circ F \circ \gamma$ satisfies the semi-commutation condition.

If $F^{\sharp}$ satisfies the semi-commutation condition then $F \circ \gamma \sqsubseteq^{\text{¤}} \gamma \circ F^{\sharp}$ so, by def. of a Galois connection, $\alpha \circ F \circ \gamma \sqsubseteq^{\sharp} F^{\sharp}$ proving that $\alpha \circ F \circ \gamma$ is the best abstract transformer satisfying the the semi-commutation condition. □

Best abstractions and transformers II

Moreover, in case of existence of best abstraction, the choice of the best abstraction of an abstract domain is unique.

Theorem (27.19) If $\langle \mathbb{P}^{¤}, \sqsubseteq^{¤} \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathbb{P}^{\sharp}, \sqsubseteq^{\sharp} \rangle$ and $\alpha \circ F = F^{\sharp} \circ \alpha$ then $F^{\sharp} \triangleq \alpha \circ F \circ \gamma$.

Proof of Theorem 27.19 If $\alpha \circ F = F^{\sharp} \circ \alpha$ then $\alpha \circ F \circ \gamma = F^{\sharp} \circ \alpha \circ \gamma = F^{\sharp}$ since $\alpha \circ \gamma$ is the identity for Galois retractions. □

Corollary (27.20, Best sound abstract interpreter)

Let $\widehat{\mathscr{S}}^{¤}$ and $\widehat{\mathscr{S}}^{\sharp}$ be structural abstract interpreters for well-defined concrete $\mathbb{D}^{¤}$ and abstract domains $\mathbb{D}^{\sharp}$ by Definition 21.1 such that $\mathbb{D}^{\sharp}$ is an abstraction of $\mathbb{D}^{¤}$ by Definition 27.1-I where Definition 27.1-I.1 is strengthened to $\langle \mathbb{P}^{¤},\ \sqsubseteq^{¤}\rangle \mathrel{\underset{\alpha}{\overset{\gamma}{\leftrightarrows}}} \langle \mathbb{P}^{\sharp},\ \sqsubseteq^{\sharp}\rangle$.

If $\alpha \circ \mathsf{assign}^{¤}[\![\mathsf{x}, \mathsf{A}]\!] \circ \gamma$ satisfies Definition 27.1-I.2 and $\alpha \circ \mathsf{test}^{¤}[\![\mathsf{B}]\!] \circ \gamma$ as well as $\alpha \circ \overline{\mathsf{test}}^{¤}[\![\mathsf{B}]\!] \circ \gamma$ satisfy Definition 27.1-I.3 then $\ddot{\alpha} \circ \mathscr{S}^{¤}[\![\mathsf{S}]\!] \circ \gamma$ is the best sound abstract interpreter, in that,

$$\ddot{\alpha} \circ \mathscr{S}^{¤}[\![\mathsf{S}]\!] \circ \gamma \quad \ddot{\sqsubseteq}^{¤} \quad \mathscr{S}^{\sharp}[\![\mathsf{S}]\!].$$

Proof of Corollary 27.20 By Theorem 27.4 and Theorem 27.18. □

Corollary (27.21, Best sound and complete abstract interpreter)

Let $\widehat{\mathcal{S}}^{\text{¤}}$ and $\widehat{\mathcal{S}}^{\sharp}$ be structural abstract interpreters for well-defined concrete $\mathbb{D}^{\text{¤}}$ and abstract domains $\mathbb{D}^{\sharp}$ by Definition 21.1 such that $\mathbb{D}^{\sharp}$ is an exact abstraction of $\mathbb{D}^{\text{¤}}$ by Definition 27.1-II.
If $\alpha \circ \mathsf{assign}^{\text{¤}}[\![\mathsf{x}, \mathsf{A}]\!] \circ \gamma$ satisfies Definition 27.1-II.2 and $\alpha \circ \mathsf{test}^{\text{¤}}[\![\mathsf{B}]\!] \circ \gamma$ as well as $\alpha \circ \overline{\mathsf{test}}^{\text{¤}}[\![\mathsf{B}]\!] \circ \gamma$ satisfy Definition 27.1-II.3 then

$$\mathcal{S}^{\sharp}[\![\mathsf{S}]\!] \quad = \quad \ddot{\alpha} \circ \mathcal{S}^{\text{¤}}[\![\mathsf{S}]\!] \circ \gamma$$

is the best sound and complete abstract interpreter.

Proof of Corollary 27.21 By 27.8 and Theorem 27.19 □

- Note that the soundness and completeness of the abstract interpreter only depends on the soundness of the abstract domain

Conclusion

Abstraction

- An abstraction of an abstract structural semantics (specified as an instance of the abstract interpreter) is an abstract structural semantics (specified as another instance of the abstract interpreter), obtained by abstraction of the abstract domain.
- So the abstract interpretation problem is reduced to the abstract interpretation of the primitives of an abstract domain
- Therefore the abstract interpreter can be reused without needing any other change.

Bibliography I

Sintzoff, Michel (1972). “Calculating Properties of Programs by Valuations on Specific Models”. In: *Proceedings of ACM Conference on Proving Assertions About Programs*. ACM, pp. 203–207.

Home work

Read Ch. **27** “Abstraction” of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you