Semantics of Programming Languages

Denotational Semantics

Prof. Peter Müller

Software Component Technology

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

3. Denotational Semantics

Equivalence Theorem

Theorem:

For every statement s of IMP we have $\mathcal{S}_{SOS}[\![s]\!] = \mathcal{S}_{DS}[\![s]\!]$

- $\mathcal{S}_{SOS}[\![s]\!]$ and $\mathcal{S}_{DS}[\![s]\!]$ are elements of the partially ordered set State $\hookrightarrow$ State
- It suffices to prove
  1. $\mathcal{S}_{SOS}[\![s]\!] \sqsubseteq \mathcal{S}_{DS}[\![s]\!]$
  2. $\mathcal{S}_{DS}[\![s]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s]\!]$

Equivalence Lemma 1

Lemma:

For every statement s of IMP we have
$\mathcal{S}_{SOS}[\![s]\!] \sqsubseteq \mathcal{S}_{DS}[\![s]\!]$

- We prove this lemma in two steps
- Part 1: Individual steps in the SOS

$$\langle s, \sigma\rangle \to_1 \sigma' \quad \Rightarrow \mathcal{S}_{DS}[\![s]\!]\sigma = \sigma'$$
$$\langle s, \sigma\rangle \to_1 \langle s', \sigma'\rangle \quad \Rightarrow \mathcal{S}_{DS}[\![s]\!]\sigma = \mathcal{S}_{DS}[\![s']\!]\sigma'$$

- Part 2: Derivation sequences in the SOS

$$\langle s, \sigma\rangle \to_1^* \sigma' \Rightarrow \mathcal{S}_{DS}[\![s]\!]\sigma = \sigma'$$

Proof of Part 1—Individual Steps

- We prove the property by induction on the shape of the derivation tree for $\langle s, \sigma \rangle \rightarrow_1 \sigma'$ or $\langle s, \sigma \rangle \rightarrow_1 \langle s', \sigma' \rangle$
- Case assign-axiom: We have
  - $\langle x := e, \sigma \rangle \rightarrow_1 \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]$
  - $\mathcal{S}_{DS}[\![x := e]\!]\sigma = \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]$
- Case skip-axiom: Analogously

Proof of Part 1—Individual Steps

- Case sequence-rule 1:
  - Assume that $\langle s_1 ; s_2, \sigma\rangle \rightarrow_1 \langle s_1' ; s_2, \sigma'\rangle$ because $\langle s_1, \sigma\rangle \rightarrow_1 \langle s_1', \sigma'\rangle$
  - By the induction hypothesis, we get $\mathcal{S}_{DS}[\![s_1]\!]\sigma = \mathcal{S}_{DS}[\![s_1']\!]\sigma'$
  - We get $\mathcal{S}_{DS}[\![s_1 ; s_2]\!]\sigma = \mathcal{S}_{DS}[\![s_2]\!](\mathcal{S}_{DS}[\![s_1]\!]\sigma) = \mathcal{S}_{DS}[\![s_2]\!](\mathcal{S}_{DS}[\![s_1']\!]\sigma') = \mathcal{S}_{DS}[\![s_1' ; s_2]\!]\sigma'$

- Case sequence-rule 2:
  - Assume that $\langle s_1 ; s_2, \sigma\rangle \rightarrow_1 \langle s_2, \sigma'\rangle$ because $\langle s_1, \sigma\rangle \rightarrow_1 \sigma'$
  - By the induction hypothesis, we get $\mathcal{S}_{DS}[\![s_1]\!]\sigma = \sigma'$
  - We get $\mathcal{S}_{DS}[\![s_1 ; s_2]\!]\sigma = \mathcal{S}_{DS}[\![s_2]\!](\mathcal{S}_{DS}[\![s_1]\!]\sigma) = \mathcal{S}_{DS}[\![s_2]\!]\sigma'$

Proof of Part 1—Individual Steps

- Case if-rule, $\mathcal{B}[\![b]\!]\sigma = tt$:
  - We have $\langle \texttt{if}\ b\ \texttt{then}\ s_1\ \texttt{else}\ s_2\ \texttt{end}, \sigma\rangle \rightarrow_1 \langle s_1, \sigma\rangle$
  - We get $\mathcal{S}_{DS}[\![\texttt{if}\ b\ \texttt{then}\ s_1\ \texttt{else}\ s_2\ \texttt{end}]\!]\sigma = cond(\mathcal{B}[\![b]\!], \mathcal{S}_{DS}[\![s_1]\!], \mathcal{S}_{DS}[\![s_2]\!])\sigma = \mathcal{S}_{DS}[\![s_1]\!]\sigma$
- Case if-rule, $\mathcal{B}[\![b]\!]\sigma = ff$: Analogously

Proof of Part 1—Individual Steps

- Case while-rule:
  - We have $\langle \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma\rangle \rightarrow_1 \langle \texttt{if}\ b\ \texttt{then}\ s\texttt{;while}\ b\ \texttt{do}\ s\ \texttt{end}\ \texttt{else}\ \texttt{skip}\ \texttt{end}, \sigma\rangle$
  - We have $\mathcal{S}_{DS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!] = FIXF$ where $F(g) = cond(\mathcal{B}[\![b]\!], g \circ \mathcal{S}_{DS}[\![s]\!], id)$
  - We get

$$\mathcal{S}_{DS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!] =$$
$$FIXF =$$
$$F(FIXF) =$$
$$cond(\mathcal{B}[\![b]\!], \mathcal{S}_{DS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!] \circ \mathcal{S}_{DS}[\![s]\!], id) =$$
$$cond(\mathcal{B}[\![b]\!], \mathcal{S}_{DS}[\![s\texttt{;while}\ b\ \texttt{do}\ s\ \texttt{end}]\!], \mathcal{S}_{DS}[\![\texttt{skip}]\!]) =$$
$$\mathcal{S}_{DS}[\![\texttt{if}\ b\ \texttt{then}\ s\texttt{;while}\ b\ \texttt{do}\ s\ \texttt{end}\ \texttt{else}\ \texttt{skip}\ \texttt{end}]\!]$$

Proof of Part 2—Derivation Sequences

- We prove $\langle s, \sigma \rangle \rightarrow_1^k \sigma' \Rightarrow \mathcal{S}_{DS}[\![s]\!]\sigma = \sigma'$ by induction on k
- Induction Base: Trivial
- Induction Step: We can assume $\langle s, \sigma \rangle \rightarrow_1^{k+1} \sigma'$
- Case 1: $\langle s, \sigma \rangle \rightarrow_1 \langle s', \sigma'' \rangle$ and $\langle s', \sigma'' \rangle \rightarrow_1^k \sigma'$
  - By the lemma for individual steps, we get $\mathcal{S}_{DS}[\![s]\!]\sigma = \mathcal{S}_{DS}[\![s']\!]\sigma''$
  - By the induction hypothesis, we get $\mathcal{S}_{DS}[\![s']\!]\sigma'' = \sigma'$
- Case 2: $\langle s, \sigma \rangle \rightarrow_1 \sigma''$ and $\sigma'' \rightarrow_1^k \sigma'$
  - By the lemma for individual steps, we get $\mathcal{S}_{DS}[\![s]\!]\sigma = \sigma''$
  - $\sigma'' \rightarrow_1^k \sigma'$ implies $k = 0$ and $\sigma'' = \sigma'$

Equivalence Lemma 2

Lemma:

For every statement s of IMP we have
$\mathcal{S}_{DS}[\![s]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s]\!]$

- The proof runs by structural induction on s
- Induction base:
  - Case $x := e$: $\mathcal{S}_{DS}[\![x := e]\!]\sigma = \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma] = \mathcal{S}_{SOS}[\![x := e]\!]\sigma$
  - Case `skip`: Analogously

Induction Step: Seq. Composition

- Case $s_1 ; s_2$:
  - We have $\mathcal{S}_{DS}[\![s_1 ; s_2]\!] = \mathcal{S}_{DS}[\![s_2]\!] \circ \mathcal{S}_{DS}[\![s_1]\!]$
  - By the induction hypothesis, we get $\mathcal{S}_{DS}[\![s_1]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s_1]\!]$ and $\mathcal{S}_{DS}[\![s_2]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s_2]\!]$
  - By monotonicity of $\circ$ (Lemma 3.10 and a symmetric lemma), we get $\mathcal{S}_{DS}[\![s_2]\!] \circ \mathcal{S}_{DS}[\![s_1]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s_2]\!] \circ \mathcal{S}_{SOS}[\![s_1]\!]$
  - From Exercise 16, we know:
    $\langle s_1, \sigma\rangle \rightarrow_1^* \sigma' \Rightarrow \langle s_1 ; s_2, \sigma\rangle \rightarrow_1^* \langle s_2, \sigma'\rangle$ or
    $\mathcal{S}_{SOS}[\![s_1]\!]\sigma = \sigma' \Rightarrow \mathcal{S}_{SOS}[\![s_1 ; s_2]\!]\sigma = \mathcal{S}_{SOS}[\![s_2]\!]\sigma'$
  - Therefore, we have $(\mathcal{S}_{SOS}[\![s_2]\!] \circ \mathcal{S}_{SOS}[\![s_1]\!])\sigma =$
    $\mathcal{S}_{SOS}[\![s_2]\!](\mathcal{S}_{SOS}[\![s_1]\!]\sigma) = \mathcal{S}_{SOS}[\![s_1 ; s_2]\!]\sigma$

Induction Step: Conditional

- Case `if` b `then` s_1 `else` s_2 `end`:
  - We have $\mathcal{S}_{DS}[\![\texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}]\!] = cond(\mathcal{B}[\![b]\!], \mathcal{S}_{DS}[\![s_1]\!], \mathcal{S}_{DS}[\![s_2]\!])$
  - By the induction hypothesis, we get $\mathcal{S}_{DS}[\![s_1]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s_1]\!]$ and $\mathcal{S}_{DS}[\![s_2]\!] \sqsubseteq \mathcal{S}_{SOS}[\![s_2]\!]$
  - By monotonicity of $cond$ (Lemma 3.9 and a symmetric lemma), we get $cond(\mathcal{B}[\![b]\!], \mathcal{S}_{DS}[\![s_1]\!], \mathcal{S}_{DS}[\![s_2]\!]) \sqsubseteq cond(\mathcal{B}[\![b]\!], \mathcal{S}_{SOS}[\![s_1]\!], \mathcal{S}_{SOS}[\![s_2]\!])$
  - From the SOS rules, we know

$$\mathcal{S}_{SOS}[\![\texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}]\!]\sigma = \mathcal{S}_{SOS}[\![s_1]\!]\sigma \quad \text{if } \mathcal{B}[\![b]\!]\sigma = tt$$
$$\mathcal{S}_{SOS}[\![\texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}]\!]\sigma = \mathcal{S}_{SOS}[\![s_2]\!]\sigma \quad \text{if } \mathcal{B}[\![b]\!]\sigma = ff$$

  - Therefore, we have $cond(\mathcal{B}[\![b]\!], \mathcal{S}_{SOS}[\![s_1]\!], \mathcal{S}_{SOS}[\![s_2]\!]) = \mathcal{S}_{SOS}[\![\texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}]\!]$

Induction Step: Loop

- Auxiliary Lemma:

  Let $f : D \to D$ be a continuous function on ccpo $(D, \sqsubseteq)$ and let $d \in D$ satisfy $f(d) \sqsubseteq d$. Then $FIX\, f \sqsubseteq d$.

  - See Exercise session 8 for the proof

- Case `while` b `do` s `end`:

  - We have $\mathcal{S}_{DS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!] = FIXF$ where $F(g) = cond(\mathcal{B}[\![b]\!], g \circ \mathcal{S}_{DS}[\![s]\!], id)$

  - By the auxiliary lemma, it is sufficient to prove $F(\mathcal{S}_{SOS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!]) \sqsubseteq \mathcal{S}_{SOS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!]$

Induction Step: Loop (cont'd)

$$
\begin{aligned}
& F(\mathcal{S}_{SOS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!]) && = \\
& && \text{[Definition of } F\text{]} \\
& cond(\mathcal{B}[\![b]\!], \mathcal{S}_{SOS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!] \circ \mathcal{S}_{DS}[\![s]\!], id) && \sqsubseteq \\
& && \text{[Induction hypothesis]} \\
& cond(\mathcal{B}[\![b]\!], \mathcal{S}_{SOS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!] \circ \mathcal{S}_{SOS}[\![s]\!], id) && = \\
& && \text{[Exercise 16]} \\
& cond(\mathcal{B}[\![b]\!], \mathcal{S}_{SOS}[\![s\texttt{;while}\ b\ \texttt{do}\ s\ \texttt{end}]\!], id) && = \\
& \mathcal{S}_{SOS}[\![\texttt{if}\ b\ \texttt{then}\ s\texttt{;while}\ b\ \texttt{do}\ s\ \texttt{end else skip end}]\!] && = \\
& \mathcal{S}_{SOS}[\![\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}]\!]
\end{aligned}
$$

Equivalence: Summary

- The operational semantics and denotational semantics are equivalent

- Proof of Lemma 1
  - runs by induction on the shape of the derivation tree for each individual step in the SOS
  - runs by induction on the length of the derivation sequence for whole statements

- Proof of Lemma 2 runs by structural induction on the statements