P. Müller and C. Sprenger

Formal Methods and Functional Programming

Solutions of Exercise Sheet 12: Small Step Semantics

Assignment 1 (Applying Small-Step Semantics)

Let s' be the body of the loop.

$$
\begin{aligned}
\langle \texttt{s}, \sigma\rangle &\rightarrow_1^1 \langle \texttt{if n \# 0 then s'; s else skip end}, \sigma\rangle\\
&\rightarrow_1^1 \langle \texttt{(a := a+n; (b := b*n; n := n-1)); s}, \sigma\rangle\\
&\rightarrow_1^1 \langle \texttt{(b := b*n; n := n-1); s}, \sigma[\texttt{a} \mapsto 2]\rangle\\
&\rightarrow_1^1 \langle \texttt{n := n-1; s}, \sigma[\texttt{a}, \texttt{b} \mapsto 2, 2]\rangle\\
&\rightarrow_1^1 \langle \texttt{s}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 2, 2, 1]\rangle\\
&\rightarrow_1^1 \langle \texttt{if n \# 0 then s'; s else skip end}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 2, 2, 1]\rangle\\
&\rightarrow_1^1 \langle \texttt{(a := a+n; (b := b*n; n := n-1)); s}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 2, 2, 1]\rangle\\
&\rightarrow_1^1 \langle \texttt{(b := b*n; n := n-1); s}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 3, 2, 1]\rangle\\
&\rightarrow_1^1 \langle \texttt{n := n-1; s}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 3, 2, 1]\rangle\\
&\rightarrow_1^1 \langle \texttt{s}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 3, 2, 0]\rangle\\
&\rightarrow_1^1 \langle \texttt{if n \# 0 then s'; s else skip end}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 3, 2, 0]\rangle\\
&\rightarrow_1^1 \langle \texttt{skip}, \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 3, 2, 0]\rangle\\
&\rightarrow_1^1 \sigma[\texttt{a}, \texttt{b}, \texttt{n} \mapsto 3, 2, 0]
\end{aligned}
$$

The first three single-step transitions are justified by the following three derivation trees:

$$
\frac{}{\langle \texttt{s}, \sigma\rangle \rightarrow_1 \langle \texttt{if n \# 0 then s';s else skip end}, \sigma\rangle}\ (\textsc{While}_{SOS})
$$

$$
\frac{}{\langle \texttt{if n \# 0 then s';s else skip end}, \sigma\rangle \rightarrow_1 \langle (\texttt{a} := \texttt{a} + \texttt{n};(\texttt{b} := \texttt{b} * \texttt{n};\texttt{n} := \texttt{n} - 1));\texttt{s}, \sigma\rangle}\ (\textsc{IfT}_{SOS})
$$

Where the side condition for IFT_{SOS} namely $\mathcal{B}[\![\texttt{n \# 0}]\!]\sigma = tt$ holds.

$$\dfrac{\dfrac{\overline{\langle \texttt{a} := \texttt{a} + \texttt{n}, \sigma\rangle \rightarrow_1 \sigma[\texttt{a} \mapsto 2]}\ (\text{Ass}_{SOS})}{\langle \texttt{a} := \texttt{a} + \texttt{n}; (\texttt{b} := \texttt{b} * \texttt{n}; \texttt{n} := \texttt{n} - 1), \sigma\rangle \rightarrow_1 \langle (\texttt{b} := \texttt{b} * \texttt{n}; \texttt{n} := \texttt{n} - 1), \sigma[\texttt{a} \mapsto 2]\rangle}\ (\text{Seq1}_{SOS})}{\langle (\texttt{a} := \texttt{a} + \texttt{n}; (\texttt{b} := \texttt{b} * \texttt{n}; \texttt{n} := \texttt{n} - 1)); \texttt{s}, \sigma\rangle \rightarrow_1 \langle (\texttt{b} := \texttt{b} * \texttt{n}; \texttt{n} := \texttt{n} - 1); \texttt{s}, \sigma[\texttt{a} \mapsto 2]\rangle}\ (\text{Seq2}_{SOS})$$

Assignment 2 (Proof of Equivalence Lemmas)

Task 2.1 We define

$$P(T) \equiv \forall \sigma, \sigma', s \cdot \big(\mathit{root}(T) \equiv (\langle s, \sigma\rangle \rightarrow \sigma') \implies \langle s, \sigma\rangle \rightarrow_1^* \sigma'\big)$$

and prove $\forall T \cdot P(T)$ by strong induction on the shape of the derivation tree T. Thus, for some arbitrary T, we get as induction hypothesis $\forall T' \sqsubset T \cdot P(T')$, and need to prove $P(T)$.

Let σ, σ', s be arbitrary. We assume $\mathit{root}(T) \equiv (\langle s, \sigma\rangle \rightarrow \sigma')$ and prove $\langle s, \sigma\rangle \rightarrow_1^* \sigma'$. The proof proceeds by case splitting on the last rule applied in T.

- **Case** Ass_{NS}: Then T is of the form:

  $$\overline{\langle x \ \texttt{:=}\ e, \sigma\rangle \rightarrow \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]}\ (\text{Ass}_{NS})$$

  for some x, e such that $s \equiv x \ \texttt{:=}\ e$ and $\sigma' = \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]$. Now we can construct a derivation tree to justify $\langle s, \sigma\rangle \rightarrow_1^1 \sigma'$:

  $$\overline{\langle x \ \texttt{:=}\ e, \sigma\rangle \rightarrow_1 \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]}\ (\text{Ass}_{SOS})$$

- **Case** Skip_{NS}: Analogous to Ass_{NS}.
- **Case** WhF_{NS}: Then T is of the form

  $$\overline{\langle \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}, \sigma\rangle \rightarrow \sigma}\ (\text{WhF}_{NS})$$

  for some b, s' such that $s \equiv \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}$, $\sigma' = \sigma$ and $\mathcal{B}[\![b]\!]\sigma = \mathit{ff}$.

  We conclude with the following derivation sequence:

  $$\begin{array}{ll} & \langle \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}, \sigma\rangle \\ \rightarrow_1^1 & \langle \texttt{if}\ b\ \texttt{then}\ s'\texttt{;while}\ b\ \texttt{do}\ s'\ \texttt{end else skip end}, \sigma\rangle \\ \rightarrow_1^1 & \langle \texttt{skip}, \sigma\rangle \\ \rightarrow_1^1 & \sigma \end{array}$$

  The second transition is justified by IfF_{SOS}, since $\mathcal{B}[\![b]\!]\sigma = \mathit{ff}$.

- **Case** $\textsc{Seq}_{\text{NS}}$: Then T is of the form

$$\frac{\dfrac{T_1}{\langle s_1, \sigma\rangle \to \sigma''} \qquad \dfrac{T_2}{\langle s_2, \sigma''\rangle \to \sigma'}}{\langle s_1; s_2, \sigma\rangle \to \sigma'} \; (\textsc{Seq}_{NS})$$

for some $s_1, s_2, \sigma'', T_1, T_2$, such that $s \equiv s_1; s_2$.

We apply the IH twice. From $P(T_1)$ we learn $\langle s_1, \sigma\rangle \to_1^* \sigma''$ and from $P(T_2)$ we learn $\langle s_2, \sigma''\rangle \to_1^* \sigma'$. $\langle s_1, \sigma\rangle \to_1^* \sigma''$ gives us $\langle s_1, \sigma\rangle \to_1^k \sigma''$ for some k. We can apply the results from Assignment 3 (optional exercises) on $\langle s_1, \sigma\rangle \to_1^k \sigma''$ to get $\langle s_1; s_2, \sigma\rangle \to_1^k \langle s_2, \sigma''\rangle$.

We conclude this case with the following derivation sequence:

$$\langle s_1; s_2, \sigma\rangle \to_1^* \langle s_2, \sigma''\rangle \to_1^* \sigma'$$

- **Case** $\textsc{IfT}_{\text{NS}}$: Then T is of the form

$$\frac{\dfrac{T_3}{\langle s_1, \sigma\rangle \to \sigma'}}{\langle \texttt{if}\ b\ \texttt{then}\ s_1\ \texttt{else}\ s_2\ \texttt{end}, \sigma\rangle \to \sigma'} \; (\textsc{IfT}_{NS})$$

for some b, s_1, s_2, T_3, such that $s \equiv \texttt{if}\ b\ \texttt{then}\ s_1\ \texttt{else}\ s_2\ \texttt{end}$ and $\mathcal{B}[\![b]\!]\sigma = tt$.

From $P(T_3)$ we learn $\langle s_1, \sigma\rangle \to_1^* \sigma'$.

We conclude this case with the following derivation sequence:

$$\langle \texttt{if}\ b\ \texttt{then}\ s_1\ \texttt{else}\ s_2\ \texttt{end}, \sigma\rangle \to_1^1 \langle s_1, \sigma\rangle \to_1^* \sigma'$$

The first transition is justified by $\textsc{IfT}_{SOS}$, since $\mathcal{B}[\![b]\!]\sigma = tt$.

- **Case** $\textsc{IfF}_{\text{NS}}$: Analogous to $\textsc{IfT}_{\text{NS}}$.
- **Case** $\textsc{WhT}_{\text{NS}}$: Then T is of the form

$$\frac{\dfrac{T_4}{\langle s', \sigma\rangle \to \sigma''} \qquad \dfrac{T_5}{\langle \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}, \sigma''\rangle \to \sigma'}}{\langle \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}, \sigma\rangle \to \sigma'} \; (\textsc{WhT}_{NS})$$

for some $b, s', \sigma'', T_4, T_5$, such that $s \equiv \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}$ and $\mathcal{B}[\![b]\!]\sigma = tt$.

We apply (IH) twice. From $P(T_4)$ we learn $\langle s', \sigma\rangle \to_1^* \sigma''$. From $P(T_5)$ we learn $\langle \texttt{while}\ b\ \texttt{do}\ s'\ \texttt{end}, \sigma''\rangle \to_1^* \sigma'$. $\langle s', \sigma\rangle \to_1^* \sigma''$ gives us $\langle s', \sigma\rangle \to_1^k \sigma''$ for some k.

We can apply the result of Assignment 3 (optional exercises) on it to get $\langle (s'; \texttt{while } b \texttt{ do } s' \texttt{ end}), \sigma\rangle \rightarrow_1^k \langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma''\rangle$.

We conclude this case with the following derivation sequence:

$$\begin{array}{ll} & \langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma\rangle \\ \rightarrow_1^1 & \langle \texttt{if } b \texttt{ then } (s'; \texttt{while } b \texttt{ do } s' \texttt{ end}) \texttt{ else skip}, \sigma\rangle \\ \rightarrow_1^1 & \langle (s'; \texttt{while } b \texttt{ do } s' \texttt{ end}), \sigma\rangle \\ \rightarrow_1^* & \langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma''\rangle \\ \rightarrow_1^* & \sigma' \end{array}$$

The second transition is justified by IfT_{SOS}, since $\mathcal{B}[\![b]\!]\sigma = tt$.

Task 2.2 We define

$$Q(k) \equiv \forall \sigma, \sigma', s \cdot \langle s, \sigma\rangle \rightarrow_1^k \sigma' \implies \vdash \langle s, \sigma\rangle \rightarrow \sigma'$$

and prove $\forall k \cdot Q(k)$ by strong mathematical induction on k.

For arbitrary k assume $\forall k' < k \cdot Q(k')$ and prove $Q(k)$. Let σ, σ', s be arbitrary. Case splitting on the condition $k > 0$ immediately proves the case for $k = 0$ (the assumptions lead to $\langle s, \sigma\rangle \rightarrow_1^0 \sigma'$, which is a contradiction). So we are left with case $k > 0$. Assume $\langle s, \sigma\rangle \rightarrow_1^k \sigma'$ and prove $\vdash \langle s, \sigma\rangle \rightarrow \sigma'$.

We unroll the derivation sequence once to $\langle s, \sigma\rangle \rightarrow_1^1 \gamma \rightarrow_1^{k-1} \sigma'$. Let T be the derivation tree which justifies the first transition. We inspect the last rule applied to T.

- **Case** Ass_{SOS}: Then T is of the form

  $$\frac{}{\langle x \texttt{ := } e, \sigma\rangle \rightarrow_1 \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]}\ (\text{Ass}_{SOS})$$

  for some x, e such that $s \equiv x \texttt{ := } e$ and $\gamma = \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]$. Since γ is a final state there is no further derivation sequence ($k = 1$), and hence $\sigma' = \gamma = \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]$. Now we can construct a derivation tree for $\langle x \texttt{ := } e, \sigma\rangle \rightarrow \sigma'$:

  $$\frac{}{\langle x \texttt{ := } e, \sigma\rangle \rightarrow \sigma[x \mapsto \mathcal{A}[\![e]\!]\sigma]}\ (\text{Ass}_{NS})$$

- **Case** Skip_{SOS}: Similar to Ass_{SOS}, we apply the corresponding NS rule and are done.

- **Case** Seq1_{SOS}, Seq2_{SOS}: Then we must have *root*$(T) \equiv \langle s_1; s_2, \sigma\rangle \rightarrow_1 \gamma$ and hence $\vdash \langle s_1; s_2, \sigma\rangle \rightarrow_1 \gamma$ for some statements s_1, s_2, such that $s \equiv s_1; s_2$.

  Returning to our original assumption, we apply the lemma proven on the lecture slides on $\langle s_1; s_2, \sigma\rangle \rightarrow_1^k \sigma'$. We get $\langle s_1, \sigma\rangle \rightarrow_1^{k_1} \sigma''$ and $\langle s_2, \sigma''\rangle \rightarrow_1^{k_2} \sigma'$, for some σ'', k_1, k_2, such that $k_1 + k_2 = k$.

  Note that $k_1 \neq 0$ and $k_2 \neq 0$ (otherwise, by the definition of $\rightarrow_1^0$ we would have to have a non-final configuration equal to a state, e.g. $\langle s_1, \sigma\rangle \equiv \sigma''$, which is impossible). Therefore, we must have $k_1 < k$ and $k_2 < k$.

Since $k_1, k_2 < k$ we can apply the IH twice. From $Q(k_1)$ we learn $\vdash \langle s_1, \sigma \rangle \to \sigma''$ and from $Q(k_2)$ we learn $\vdash \langle s_2, \sigma'' \rangle \to \sigma'$. Let T_1, T_2 be the corresponding derivation trees, such that *root*$(T_1) \equiv \langle s_1, \sigma \rangle \to \sigma''$ and *root*$(T_2) \equiv \langle s_2, \sigma'' \rangle \to \sigma'$

Now we can construct the derivation tree for $\vdash \langle s_1; s_2, \sigma \rangle \to \sigma'$ as follows:

$$\dfrac{\begin{array}{c} T_1 \\ \langle s_1, \sigma \rangle \to \sigma'' \end{array} \qquad \begin{array}{c} T_2 \\ \langle s_2, \sigma'' \rangle \to \sigma' \end{array}}{\langle s_1 ; s_2, \sigma \rangle \to \sigma'} \ (\textsc{Seq}_{NS})$$

- **Case** $\textsc{IfT}_{\textsc{sos}}$: Then T is of the form

$$\dfrac{}{\langle \texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}, \sigma \rangle \to_1 \langle s_1, \sigma \rangle} \ (\textsc{IfT}_{SOS})$$

for some b, s_1, s_2, such that $s \equiv \texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}$ and $\mathcal{B}[\![b]\!]\sigma = tt$. Therefore the unrolled derivation sequence is of the form:

$$\langle \texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}, \sigma \rangle \to_1^1 \langle s_1, \sigma \rangle \to_1^{k-1} \sigma'$$

We apply the IH to the tail sequence, and get *root*$(T_3) \equiv \langle s_1, \sigma \rangle \to \sigma'$ for some derivation tree T_3, which enables us to conclude this case by constructing the derivation tree:

$$\dfrac{\begin{array}{c} T_3 \\ \langle s_1, \sigma \rangle \to \sigma' \end{array}}{\langle \texttt{if } b \texttt{ then } s_1 \texttt{ else } s_2 \texttt{ end}, \sigma \rangle \to \sigma'} \ (\textsc{IfT}_{NS})$$

The side condition is fulfilled since we know $\mathcal{B}[\![b]\!]\sigma = tt$.

- **Case** $\textsc{IfF}_{\textsc{sos}}$: Analogous to $\textsc{IfT}_{\textsc{sos}}$.
- **Case** $\textsc{While}_{\textsc{sos}}$: Then T is of the form

$$\dfrac{}{\langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma \rangle \to_1 \gamma} \ (\textsc{While}_{SOS})$$

for some b, s', γ, such that $\gamma = \langle \texttt{if } b \texttt{ then } s' ; \texttt{while } b \texttt{ do } s' \texttt{ end else skip end}, \sigma \rangle$ and $s \equiv \texttt{while } b \texttt{ do } s' \texttt{ end}$. Therefore the unrolled derivation sequence is of the form:

$$\begin{array}{ll} & \langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma \rangle \\ \to_1^1 & \langle \texttt{if } b \texttt{ then } s' ; \texttt{while } b \texttt{ do } s' \texttt{ end else skip end}, \sigma \rangle \\ \to_1^{k-1} & \sigma' \end{array}$$

We apply the IH to the tail sequence, and get

$$\vdash \langle \texttt{if } b \texttt{ then } s'; \texttt{while } b \texttt{ do } s' \texttt{ end else skip end}, \sigma\rangle \rightarrow \sigma'.$$

From the semantic equivalence shown in the lecture (Slide Deck 3, section 3.1.2), we get $\vdash \langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma\rangle \rightarrow \sigma'$, which concludes this case.

Note: We can also "manually" conclude this case, i.e. not use the semantic equivalence. This requires a case split on which branch of the if-statement is taken, and some decomposing and recomposing of the resulting derivation tree.