ETH zürich

P. Müller and D. Basin

Formal Methods and Functional Programming

Solutions of Exercise Sheet 11: Big-Step Semantics

Assignment 1 (Reversing Loop-Unrolling)

The proof is direct, that is we do not need induction here. Let σ, σ', b, s be arbitrary. To prove the implication, we assume $\vdash \langle \texttt{if}\ b\ \texttt{then}\ s;\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end else skip end}, \sigma\rangle \rightarrow \sigma'$ and we just need to prove $\vdash \langle \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma\rangle \rightarrow \sigma'$, which we will do by providing a suitable derivation tree.

From our assumption, it follows that there is some derivation tree T such that

$$\textit{root}(T) \equiv \langle \texttt{if}\ b\ \texttt{then}\ s;\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end else skip end}, \sigma\rangle \rightarrow \sigma'.$$

We consider two cases with respect to the last rule applied in the derivation tree T:

- **Case** IfT_{NS}: Then T has the form:

$$\dfrac{\dfrac{T'}{\langle s;\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma\rangle \rightarrow \sigma'}}{\langle \texttt{if}\ b\ \texttt{then}\ s;\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end else skip end}, \sigma\rangle \rightarrow \sigma'}\ (\text{IfT}_{NS})$$

  for some derivation tree T'. From the side condition we learn $\mathcal{B}[\![b]\!]\sigma = tt$. In the sub-derivation T', the last rule applied must be the rule for sequential composition. Thus, we learn further that T has the form:

$$\dfrac{\dfrac{\dfrac{T_1}{\langle s, \sigma\rangle \rightarrow \sigma''} \quad \dfrac{T_2}{\langle \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma''\rangle \rightarrow \sigma'}}{\langle s;\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma\rangle \rightarrow \sigma'}\ (\text{Seq}_{NS})}{\langle \texttt{if}\ b\ \texttt{then}\ s;\texttt{while}\ b\ \texttt{do}\ s\ \texttt{end else skip end}, \sigma\rangle \rightarrow \sigma'}\ (\text{IfT}_{NS})$$

for some derivation trees T_1, T_2 and state σ''. Using this information, including the fact that $\mathcal{B}[\![b]\!]\sigma = tt$, we can construct the following derivation tree (with the desired root):

$$\frac{\begin{array}{cc} T_1 & T_2 \\ \langle s, \sigma\rangle \to \sigma'' & \langle \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma''\rangle \to \sigma' \end{array}}{\langle \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma\rangle \to \sigma'}\ (\textsc{WhT}_{\textsf{\textit{NS}}})$$

- **Case** $\textsc{IfF}_{\textsf{\textit{NS}}}$: Then T has the form:

$$\frac{\begin{array}{c} T' \\ \langle \texttt{skip}, \sigma\rangle \to \sigma' \end{array}}{\langle \texttt{if}\ b\ \texttt{then}\ s;\ \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}\ \texttt{else}\ \texttt{skip}\ \texttt{end}, \sigma\rangle \to \sigma'}\ (\textsc{IfF}_{\textsf{\textit{NS}}})$$

for some derivation tree T'. From the side condition we learn $\mathcal{B}[\![b]\!]\sigma = \mathit{ff}$. Since the last rule applied in T' must be $\textsc{Skip}_{\textsf{\textit{NS}}}$, we conclude that in fact $\sigma = \sigma'$. Thus the following derivation tree actually has the desired root:

$$\frac{}{\langle \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}, \sigma\rangle \to \sigma}\ (\textsc{WhF}_{\textsf{\textit{NS}}})$$

Assignment 2 (Execution only Affects Free Variables)

Define $P(T)$ to be the statement:

$$\forall s, \sigma, \sigma', x \cdot \big(\mathit{root}(T) \equiv \langle s, \sigma\rangle \to \sigma') \wedge x \notin FV(s) \implies \sigma'(x) = \sigma(x)\big)$$

We prove $\forall T \cdot P(T)$ (which is equivalent to the statement to be proved) by induction on the shape of the derivation tree T. Thus, for an arbitrary tree T, we get as the induction hypothesis $\forall T' \sqsubset T \cdot P(T')$, and need to prove $P(T)$.

Let s, σ, σ', x be arbitrary, and assume $\mathit{root}(T) \equiv \langle s, \sigma\rangle \to \sigma'$ and $x \notin FV(s)$. Then, we need to prove $\sigma'(x) = \sigma(x)$. We consider all the cases with respect to the last rule applied in the derivation tree T:

- **Case** $\textsc{Skip}_{\textsf{\textit{NS}}}$: Then T must be of the form:

$$\frac{}{\langle \texttt{skip}, \sigma\rangle \to \sigma}\ (\textsc{Skip}_{\textsf{\textit{NS}}})$$

i.e., we must have $s \equiv \texttt{skip}$ and $\sigma' = \sigma$. Thus, $\sigma'(x) = \sigma(x)$ trivially follows.

- **Case** $\textsc{Ass}_{\textsf{\textit{NS}}}$: Then T must be of the form:

$$\frac{}{\langle y\ \texttt{:=}\ e, \sigma\rangle \to \sigma[y \mapsto \mathcal{A}[\![e]\!]\sigma]}\ (\textsc{Ass}_{\textsf{\textit{NS}}})$$

for some y and e, and thus we must have $s \equiv y$:= e and $\sigma' = \sigma[y \mapsto \mathcal{A}[\![e]\!]\sigma]$. Since $FV(s) = \{y\} \cup FV(e)$ and we assumed $x \notin FV(s)$, we must have $x \not\equiv y$. Thus, by the definition of state update, $\sigma'(x) = \sigma[y \mapsto \mathcal{A}[\![e]\!]\sigma](x) = \sigma(x)$ as required.

- **Case** IfT_{NS}: Then T must be of the form:

$$\frac{\begin{array}{c} T_1 \\ \langle s', \sigma \rangle \to \sigma' \end{array}}{\langle \texttt{if } b \texttt{ then } s' \texttt{ else } s'' \texttt{ end}, \sigma \rangle \to \sigma'} \ (\text{IfT}_{NS})$$

for some derivation tree T_1 and some b, s', s'' such that $s \equiv \texttt{if } b \texttt{ then } s' \texttt{ else } s'' \texttt{ end}$. Since $T_1 \sqsubset T$, we can obtain $P(T_1)$ from our I.H., i.e., we know (renaming quantified variables to avoid confusion):

$$\forall s_1, \sigma_1, \sigma_1', x_1 \cdot \big((\mathit{root}(T_1) \equiv \langle s_1, \sigma_1 \rangle \to \sigma_1') \wedge x_1 \notin FV(s_1) \implies \sigma_1'(x_1) = \sigma_1(x_1)\big)$$

To get something useful from this statement, we need to instantiate the quantified variables so that the left-hand side of the implication is true. Given that we know the root of T_1 already, we instantiate s_1 to be s', and σ_1 to be σ, and σ_1' to be σ'. Additionally, we instantiate x_1 to be x, since this is the only variable about which we have useful information (in particular, from our assumption $x \notin FV(s)$, we can obtain $x \notin FV(s')$, since $FV(s') \subseteq FV(s)$). From these instantiations, we obtain

$$(\mathit{root}(T_1) \equiv \langle s', \sigma \rangle \to \sigma') \wedge x \notin FV(s') \implies \sigma'(x) = \sigma(x))$$

Since the left-hand side of the implication holds, we conclude that $\sigma'(x) = \sigma(x)$, which is what we needed to prove.

- **Case** IfF_{NS}: Analogous to the case IfT_{NS}.

- **Case** WhT_{NS}: Then T must be of the form:

$$\frac{\begin{array}{c} T_1 \\ \langle s', \sigma \rangle \to \sigma'' \end{array} \qquad \begin{array}{c} T_2 \\ \langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma'' \rangle \to \sigma' \end{array}}{\langle \texttt{while } b \texttt{ do } s' \texttt{ end}, \sigma \rangle \to \sigma'} \ (\text{WhT}_{NS})$$

for some derivation trees T_1, T_2, some b, s', σ'', and we must have $s \equiv \texttt{while } b \texttt{ do } s' \texttt{ end}$.

From our I.H. (since $T_1 \sqsubset T$), instantiating the quantified variables to match the known root of T_1, we can obtain $(\mathit{root}(T_1) \equiv \langle s', \sigma \rangle \to \sigma'') \wedge x \notin FV(s') \implies \sigma''(x) = \sigma(x)$. The left-hand side of this implication holds (in particular, we have $x \notin FV(s')$ since $FV(s') \subseteq FV(s)$), and thus we conclude the right-hand side $\sigma''(x) = \sigma(x)$.

Next, we can similarly apply the induction hypothesis to the derivation tree T_2 in order to obtain that $(\mathit{root}(T_2) \equiv \langle s'', \sigma'' \rangle \to \sigma') \wedge x \notin FV(s'') \implies \sigma'(x) = \sigma''(x)$, where $s'' \equiv \texttt{while } b \texttt{ do } s' \texttt{ end}$, and thus (since the left-hand side of the implication holds), we conclude $\sigma'(x) = \sigma''(x)$. Combining the two equalities, we have $\sigma'(x) = \sigma(x)$, as required.

- **Case** $\textsc{WhF}_{NS}$: Analogous to the case $\textsc{Skip}_{NS}$.
- **Case** $\textsc{Seq}_{NS}$: Analogous to the case $\textsc{WhT}_{NS}$.