

Exercise Sheet 2

Sample Solution

Task 1: Operational Semantics & Derivation Trees

To shorten the derivation tree we first introduce the following two abbreviations.

$c_1 = \mathbf{while} \ (x \leq y) \ \mathbf{do} \ c_2 \ \mathbf{end}$

$c_2 = y := y - x; \ x := x - 4$

Furthermore we introduce the notation σ_{ij} which defines $\sigma(x) = i$ and $\sigma(y) = j$.

$$\begin{array}{c}
 \text{(asgn)} \frac{\overline{\langle 23, \sigma \rangle \rightarrow 23}}{\langle x := 23, \sigma \rangle \rightarrow \sigma[x \mapsto 23]} \quad \text{(seq)} \frac{\text{(asgn)} \frac{\overline{\langle 42, \sigma[x \mapsto 23] \rangle \rightarrow 42}}{\langle y := 42, \sigma[x \mapsto 23] \rangle \rightarrow \sigma_{23,42}} \quad \textcircled{a} \langle c_1, \sigma_{23,42} \rangle \rightarrow \sigma_{15,0}}{\langle y := 42; c_1, \sigma[x \mapsto 23] \rangle \rightarrow \sigma_{15,0}} \\
 \text{(seq)} \frac{}{\langle c, \sigma \rangle \rightarrow \sigma_{15,0}}
 \end{array}$$

$$\textcircled{a} \frac{\overline{\langle x, \sigma_{23,42} \rangle \rightarrow 23} \quad \overline{\langle y, \sigma_{23,42} \rangle \rightarrow 42} \quad \text{(wh-t)} \frac{\langle x \leq y, \sigma_{23,42} \rangle \rightarrow \mathbf{true} \quad \textcircled{b} \langle c_2, \sigma_{23,42} \rangle \rightarrow \sigma_{19,19} \quad \textcircled{c} \langle c_1, \sigma_{19,19} \rangle \rightarrow \sigma_{15,0}}{\langle c_1, \sigma_{23,42} \rangle \rightarrow \sigma_{15,0}}$$

$$\textcircled{b} \frac{\text{(asgn)} \frac{\overline{\langle y - x, \sigma_{23,42} \rangle \rightarrow 19}}{\langle y := y - x, \sigma_{23,42} \rangle \rightarrow \sigma_{23,19}} \quad \text{(asgn)} \frac{\overline{\langle x - 4, \sigma_{23,19} \rangle \rightarrow 19}}{\langle x := x - 4, \sigma_{23,19} \rangle \rightarrow \sigma_{19,19}}}{\text{(seq)} \frac{}{\langle c_2, \sigma_{23,42} \rangle \rightarrow \sigma_{19,19}}}$$

$$\textcircled{c} \frac{\overline{\langle x, \sigma_{19,19} \rangle \rightarrow 19} \quad \overline{\langle y, \sigma_{19,19} \rangle \rightarrow 19} \quad \text{(wh-t)} \frac{\langle x \leq y, \sigma_{19,19} \rangle \rightarrow \mathbf{true} \quad \textcircled{d} \langle c_2, \sigma_{19,19} \rangle \rightarrow \sigma_{15,0} \quad \textcircled{e} \langle c_1, \sigma_{15,0} \rangle \rightarrow \sigma_{15,0}}{\langle c_1, \sigma_{19,19} \rangle \rightarrow \sigma_{15,0}}$$

$$\begin{array}{c}
\textcircled{d} \quad \frac{\frac{\frac{\langle y, \sigma_{19,19} \rangle \rightarrow 19}{\langle y - x, \sigma_{19,19} \rangle \rightarrow 0} \quad \frac{\langle x, \sigma_{19,19} \rangle \rightarrow 19}{\langle x - 4, \sigma_{19,0} \rangle \rightarrow 15}}{\langle y := y - x, \sigma_{19,19} \rangle \rightarrow \sigma_{19,0}} \quad \frac{\langle x - 4, \sigma_{19,0} \rangle \rightarrow 15}{\langle x := x - 4, \sigma_{19,0} \rangle \rightarrow \sigma_{15,0}}}{\langle c_2, \sigma_{19,19} \rangle \rightarrow \sigma_{15,0}} \\
\\
\textcircled{e} \quad \frac{\frac{\langle x, \sigma_{15,0} \rangle \rightarrow 15 \quad \langle y, \sigma_{15,0} \rangle \rightarrow 0}{\langle x \leq y, \sigma_{15,0} \rangle \rightarrow \mathbf{false}}}{\langle c_1, \sigma_{15,0} \rangle \rightarrow \sigma_{15,0}} \text{ (wh-f)}
\end{array}$$

Task 2: Operational Semantics of other Statements

For $c \in Cmd$, $\sigma, \sigma', \sigma'' \in \Sigma$ and $b \in BExp$ the **repeat until relation** $\langle \mathbf{repeat} \ c \ \mathbf{until} \ b, \sigma \rangle \rightarrow \sigma''$ is defined by:

$$\begin{array}{c}
\frac{\langle c, \sigma \rangle \rightarrow \sigma'' \quad \langle b, \sigma'' \rangle \rightarrow \mathbf{true}}{\langle \mathbf{repeat} \ c \ \mathbf{until} \ b, \sigma \rangle \rightarrow \sigma''} \text{ (repeat-true)} \\
\\
\frac{\langle c, \sigma \rangle \rightarrow \sigma' \quad \langle b, \sigma' \rangle \rightarrow \mathbf{false} \quad \langle \mathbf{repeat} \ c \ \mathbf{until} \ b, \sigma' \rangle \rightarrow \sigma''}{\langle \mathbf{repeat} \ c \ \mathbf{until} \ b, \sigma \rangle \rightarrow \sigma''} \text{ (repeat-false)}
\end{array}$$

Task 3: Termination

Prove that $\langle \mathbf{while} \ b \ \mathbf{do} \ c \ \mathbf{end}, \sigma \rangle \rightarrow \sigma'$ implies that $\langle b, \sigma' \rangle \rightarrow \mathbf{false}$.
This will be proven by induction on the height h of derivation trees.

Induction Base: (h=1)

If the derivation tree has height 1 only one derivation is possible, namely

$$\frac{\langle b, \sigma \rangle \rightarrow \mathbf{false}}{\langle \mathbf{while} \ b \ \mathbf{do} \ c \ \mathbf{end}, \sigma \rangle \rightarrow \sigma'} \text{ (while-false)}$$

Since this rule is unambiguous the induction base holds trivially.

Induction Hypothesis:

$\langle \mathbf{while\ b\ do\ c\ end}, \sigma \rangle \rightarrow \sigma'$ implies $\langle b, \sigma' \rangle \rightarrow \mathbf{false}$

holds for all derivations of an arbitrary, but fixed height h and for all states σ, σ' .

Induction Step: ($h \mapsto h + 1$)

For all derivations of height $h + 1$ ($h \geq 1$), we have

$$\frac{\langle b, \sigma \rangle \rightarrow \mathbf{true} \quad \langle c, \sigma \rangle \rightarrow \sigma' \quad \frac{\dots (\text{derivation tree of height } h)}{\langle \mathbf{while\ } b \mathbf{\ do\ } c \mathbf{\ end}, \sigma' \rangle \rightarrow \sigma''}}{\langle \mathbf{while\ } b \mathbf{\ do\ } c \mathbf{\ end}, \sigma \rangle \rightarrow \sigma''}$$

By Induction Hypothesis $\langle \mathbf{while\ b\ do\ c\ end}, \sigma' \rangle \rightarrow \sigma''$ implies $\langle b, \sigma' \rangle \rightarrow \mathbf{false}$.

Due to the propagating characteristics of the derivation trees we also know that $\langle \mathbf{while\ b\ do\ c\ end}, \sigma \rangle \rightarrow \sigma''$ implies $\langle b, \sigma'' \rangle \rightarrow \mathbf{false}$.

□

Task 4: Variables that do not matter

(a)

$\mathbf{mod} : \quad \mathbf{Cmd} \rightarrow 2^{\mathbf{Var}},$
 $\mathbf{skip} \mapsto \emptyset$
 $x := a \mapsto \{x\}$
 $c_1; c_2 \mapsto \mathbf{mod}(c_1) \cup \mathbf{mod}(c_2)$
 $\mathbf{repeat\ } c \mathbf{\ until\ } b \mapsto \mathbf{mod}(c)$

(b)

$\mathbf{dep} : \quad \mathbf{Cmd} \rightarrow 2^{\mathbf{Var}},$
 $\mathbf{skip} \mapsto \emptyset$
 $x := a \mapsto \mathbf{FV}(a)$
 $c_1; c_2 \mapsto \mathbf{dep}(c_1) \cup \mathbf{dep}(c_2)$
 $\mathbf{repeat\ } c \mathbf{\ until\ } b \mapsto \mathbf{dep}(c) \cup \mathbf{FV}(b)$

(c)

Show for every program c and states σ_1, σ_2 with

- $\sigma_1 =_{\mathbf{dep}}(c) \sigma_2$
- $\langle c, \sigma_1 \rangle \rightarrow \sigma'_1$ and
- $\langle c, \sigma_2 \rangle \rightarrow \sigma'_2$

that $\sigma'_1 =_{\mathbf{mod}(c)} \sigma'_2$.

This will be shown by induction on the height h of derivation trees.

Induction Base: (h=1)

If the derivation tree has height 1 only two derivations are possible, namely the skip and the assignment derivations.

case: $c = \text{skip}$

This case is trivial due to the definition of **mod** and that the empty set is identical in any two arbitrary but fixed states σ_1 and σ_2 .

case: $c = x := a$

Following the definitions of **dep** and **mod** we get $\mathbf{mod}(c) = \{x\}$ and $\mathbf{dep}(c) = \mathbf{FV}(a)$.

Furthermore we have

$$\frac{\langle a, \sigma_i \rangle \rightarrow z_i}{\langle x := a, \sigma_i \rangle \rightarrow \sigma_i [x \mapsto z_i]}, i \in \{1, 2\}$$

Since $\sigma_1 =_{\mathbf{FV}(a)} \sigma_2$ (assumption) it holds that $\langle a, \sigma_1 \rangle \rightarrow z \Leftrightarrow \langle a, \sigma_2 \rangle \rightarrow z$ (Lemma 2.6, Chapter 2, Slide 17). Thus $z_1 = z_2$ and moreover $\sigma'_1 =_{\mathbf{mod}(c)} \sigma'_2$.

Induction Hypothesis:

$\sigma_1 =_{\mathbf{dep}(c)} \sigma_2, \langle c, \sigma_1 \rangle \rightarrow \sigma'_1$ and $\langle c, \sigma_2 \rangle \rightarrow \sigma'_2$ imply that $\sigma'_1 =_{\mathbf{mod}(c)} \sigma'_2$

holds for all derivations of an arbitrary, but fixed height h and for all states σ, σ' .

Induction Step: ($h \mapsto h + 1$)

case: $c = c_1; c_2$

Following the definition of **dep** and **mod** we get

mod(c) = **mod**(c_1) $\cup$ **mod**(c_2) and **dep**(c) = **dep**(c_1) $\cup$ **dep**(c_2).

Furthermore we have

$$\frac{\langle c_1, \sigma_i \rangle \rightarrow \sigma_i^* \quad \langle c_2, \sigma_i^* \rangle \rightarrow \sigma_i'}{\langle c_1; c_2, \sigma_i \rangle \rightarrow \sigma_i'}, i \in \{1, 2\}$$

By induction hypothesis it holds that $\sigma_1^* =_{\mathbf{mod}(c_1)} \sigma_2^*$.

Now let $R = \mathbf{dep}(c_2) \setminus \mathbf{mod}(c_1)$. Then we get two additional coherences:

- (1) $\sigma_1 =_R \sigma_2$ (because $R \subseteq \mathbf{dep}(c)$)
- (2) $\sigma_i =_R \sigma_i^*, i \in \{1, 2\}$ (by auxiliary (a))

Thus it holds that $\sigma_1^* =_R \sigma_2^*$ and therefore $\sigma_1^* =_{\mathbf{mod}(c_1) \cup \mathbf{dep}(c_2)} \sigma_2^*$.

Applying the induction hypothesis we then get that $\sigma_1' =_{\mathbf{mod}(c_2)} \sigma_2'$.

Now we introduce another set $R' = \mathbf{mod}(c_1) \setminus \mathbf{dep}(c_2) \subseteq \mathbf{mod}(c_1)$.

As stated earlier $\sigma_1^* =_{\mathbf{mod}(c_1)} \sigma_2^*$ thus it also holds that $\sigma_1^* =_{R'} \sigma_2^*$.

Using auxiliary (a) we learn that $\sigma_1' =_{R'} \sigma_2'$ holds.

Using this information and our previously gathered knowledge we now know that $\sigma_1' =_{\mathbf{mod}(c_1) \setminus \mathbf{dep}(c_2) \cup \mathbf{mod}(c_2)} \sigma_2'$ holds.

This is equal to $\sigma_1' =_{\mathbf{mod}(c_1) \cup \mathbf{mod}(c_2)} \sigma_2'$.

case: $c = \text{repeat } c' \text{ until } b$

Following the definition of **dep** and **mod** we get **mod**(c) = **mod**(c') and **dep**(c) = **dep**(c') $\cup$ **FV**(b).

Lets assume there exist states σ_1^*, σ_2^* so that $\langle c', \sigma_i \rangle \rightarrow \sigma_i^* \quad (i \in \{1, 2\})$

By induction hypothesis and auxiliary (a) we know that

$\sigma_1^* =_{\mathbf{dep}(c) \cup \mathbf{mod}(c')} \sigma_2^*$ holds.

Lemma 2.6 (for boolean expressions) yields that

$\langle b, \sigma_1^* \rangle \rightarrow \mathbf{true}$ iff $\langle b, \sigma_2^* \rangle \rightarrow \mathbf{true}$

We now assume that $\langle b, \sigma_i^* \rangle \rightarrow \mathbf{true}$.

This leads to the following derivation tree:

$$\frac{\langle c', \sigma_i \rangle \rightarrow \sigma_i^* \quad \langle b, \sigma_i^* \rangle \rightarrow \mathbf{true}}{\langle \text{repeat } c' \text{ until } b, \sigma_i \rangle \rightarrow \sigma_i^*}$$

Since $\sigma_1^* =_{\mathbf{dep}(c) \cup \mathbf{mod}(c')} \sigma_2^*$ (By induction hypothesis and auxiliary (a)),

$\sigma_1^* =_{\mathbf{mod}(c)} \sigma_2^*$ holds as well (**mod**(c) = **mod**(c')).

Now assume that $\langle b, \sigma_i^* \rangle \rightarrow \mathbf{false}$.

This leads to the following derivation tree:

$$\frac{\langle c, \sigma_i \rangle \rightarrow \sigma_i^* \quad \langle b, \sigma_i^* \rangle \rightarrow \mathbf{false} \quad \overline{\langle \mathbf{repeat } c' \text{ until } b, \sigma_i^* \rangle \rightarrow \sigma_i'}}{\langle \mathbf{repeat } c' \text{ until } b, \sigma_i \rangle \rightarrow \sigma_i'}$$

In order to prove that $\sigma_1' =_{\mathbf{mod}(c)} \sigma_2'$ we show that $\sigma_1^* =_{\mathbf{dep}(c)} \sigma_2^*$.

The induction hypothesis can than be utilised to prove that $\sigma_1' =_{\mathbf{mod}(c)} \sigma_2'$.

By induction hypothesis and auxiliary (a) we get that $\sigma_1^* =_{\mathbf{dep}(c) \setminus \mathbf{mod}(c')} \sigma_2^*$.

Since the induction hypothesis also states that $\sigma_1^* =_{\mathbf{mod}(c')} \sigma_2^*$ we also get that $\sigma_1^* =_{\mathbf{dep}(c)} \sigma_2^*$. Therefore we get that $\sigma_1' =_{\mathbf{mod}(c)} \sigma_2'$ by induction hypothesis.

□