Exersice Sheet 2

Sample Solution

Task 1: Operational Semantics & Derivation Trees

To shorten the derivation tree we first introduce the following two abbreviations.
$c_1 = \textbf{while } (x \leq y) \textbf{ do } c_2 \textbf{ end}$
$c_2 = y \ := \ y \ - \ x; \ x \ := \ x \ - \ 4$

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

$$\text{(seq)}\ \dfrac{\text{(asgn)}\ \dfrac{\dfrac{}{\langle 23, \sigma\rangle \to 23}}{\langle x := 23, \sigma\rangle \to \sigma[x \mapsto 23]} \qquad \text{(seq)}\ \dfrac{\text{(asgn)}\ \dfrac{\dfrac{}{\langle 42, \sigma[x \mapsto 23]\rangle \to 42}}{\langle y := 42, \sigma[x \mapsto 23]\rangle \to \sigma_{23,42}} \qquad \text{ⓐ}\langle c_1, \sigma_{23,42}\rangle \to \sigma_{15,0}}{\langle y := 42; c_1, \sigma[x \mapsto 23]\rangle \to \sigma_{15,0}}}{\langle c, \sigma\rangle \to \sigma_{15,0}}$$

$$\text{ⓐ} \qquad \text{(wh-t)}\ \dfrac{\dfrac{\dfrac{}{\langle x, \sigma_{23,42}\rangle \to 23} \qquad \dfrac{}{\langle y, \sigma_{23,42}\rangle \to 42}}{\langle x \leq y, \sigma_{23,42}\rangle \to \textbf{true}} \qquad \text{ⓑ}\langle c_2, \sigma_{23,42}\rangle \to \sigma_{19,19} \qquad \text{ⓒ}\langle c_1, \sigma_{19,19}\rangle \to \sigma_{15,0}}{\langle c_1, \sigma_{23,42}\rangle \to \sigma_{15,0}}$$

ⓑ

$$\dfrac{\dfrac{\dfrac{\overline{\langle y, \sigma_{23,42}\rangle \to 42} \quad \overline{\langle x, \sigma_{23,42}\rangle \to 23}}{\langle y - x, \sigma_{23,42}\rangle \to 19}}{\langle y := y - x, \sigma_{23,42}\rangle \to \sigma_{23,19}}\,\text{(asgn)} \qquad \dfrac{\dfrac{\overline{\langle x, \sigma_{23,19}\rangle \to 23} \quad \overline{\langle 4, \sigma_{23,19}\rangle \to 4}}{\langle x - 4, \sigma_{23,19}\rangle \to 19}}{\langle x := x - 4, \sigma_{23,19}\rangle \to \sigma_{19,19}}\,\text{(asgn)}}{\langle c_2, \sigma_{23,42}\rangle \to \sigma_{19,19}}\,\text{(seq)}$$

ⓒ

$$\dfrac{\dfrac{\overline{\langle x, \sigma_{19,19}\rangle \to 19} \quad \overline{\langle y, \sigma_{19,19}\rangle \to 19}}{\langle x \leq y, \sigma_{19,19}\rangle \to \textbf{true}} \qquad ⓓ\langle c_2, \sigma_{19,19}\rangle \to \sigma_{15,0} \qquad ⓔ\langle c_1, \sigma_{15,0}\rangle \to \sigma_{15,0}}{\langle c_1, \sigma_{19,19}\rangle \to \sigma_{15,0}}\,\text{(wh-t)}$$

ⓓ

$$\dfrac{\dfrac{\dfrac{\overline{\langle y, \sigma_{19,19}\rangle \to 19} \quad \overline{\langle x, \sigma_{19,19}\rangle \to 19}}{\langle y - x, \sigma_{19,19}\rangle \to 0}}{\langle y := y - x, \sigma_{19,19}\rangle \to \sigma_{19,0}}\,\text{(asgn)} \qquad \dfrac{\dfrac{\overline{\langle x, \sigma_{19,0}\rangle \to 19} \quad \overline{\langle 4, \sigma_{19,0}\rangle \to 4}}{\langle x - 4, \sigma_{19,0}\rangle \to 15}}{\langle x := x - 4, \sigma_{19,0}\rangle \to \sigma_{15,0}}\,\text{(asgn)}}{\langle c_2, \sigma_{19,19}\rangle \to \sigma_{15,0}}\,\text{(seq)}$$

ⓔ

$$\dfrac{\dfrac{\overline{\langle x, \sigma_{15,0}\rangle \to 15} \quad \overline{\langle y, \sigma_{15,0}\rangle \to 0}}{\langle x \leq y, \sigma_{15,0}\rangle \to \textbf{false}}}{\langle c_1, \sigma_{15,0}\rangle \to \sigma_{15,0}}\,\text{(wh-f)}$$

Task 2: Operational Semantics of other Statements

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

$$\frac{\langle \mathrm{c},\ \sigma\rangle \to \sigma^{''} \qquad \left\langle \mathrm{b},\ \sigma^{''}\right\rangle \to \textbf{true}}{\langle \textbf{repeat}\ \mathrm{c}\ \textbf{until}\ \mathrm{b},\ \sigma\rangle \to \sigma^{''}}\ (\textbf{repeat-true})$$

$$\frac{\langle \mathrm{c},\ \sigma\rangle \to \sigma^{'} \qquad \left\langle \mathrm{b},\ \sigma^{'}\right\rangle \to \textbf{false} \qquad \left\langle \textbf{repeat}\ \mathrm{c}\ \textbf{until}\ \mathrm{b},\ \sigma^{'}\right\rangle \to \sigma^{''}}{\langle \textbf{repeat}\ \mathrm{c}\ \textbf{until}\ \mathrm{b},\ \sigma\rangle \to \sigma^{''}}\ (\textbf{repeat-false})$$

Task 3: Termination

Prove that $\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma\rangle \to \sigma^{'}$ implies that $\left\langle \mathrm{b},\ \sigma^{'}\right\rangle \to \textbf{false}$.
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

$$\frac{\langle \mathrm{b},\ \sigma\rangle \to \mathrm{false}}{\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma\rangle \to \sigma^{'}}(\textbf{while}\text{-false})$$

Since this rule is unambiguous the induction base holds trivially.

Induction Hypothesis:

$$\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma\rangle \to \sigma^{'} \text{ implies } \left\langle \mathrm{b},\ \sigma^{'}\right\rangle \to \textbf{false}$$

holds for all derivations of an arbitrary, but fixed height h and for all states $\sigma,\ \sigma^{'}$.

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

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

$$\frac{\langle \mathrm{b},\ \sigma\rangle \to \textbf{true} \qquad \langle \mathrm{c},\ \sigma\rangle \to \sigma^{'} \qquad \dfrac{\cdots\ \text{(derivation tree of height h)}}{\left\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma^{'}\right\rangle \to \sigma^{''}}}{\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma\rangle \to \sigma^{''}}$$

By Induction Hypothesis $\left\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma^{'}\right\rangle \to \sigma^{''}$ implies $\left\langle \mathrm{b},\ \sigma^{'}\right\rangle \to \textbf{false}$.
Due to the propagating characteristics of the derivation trees we also know that $\langle \textbf{while}\ \mathrm{b}\ \textbf{do}\ \mathrm{c}\ \textbf{end},\ \sigma\rangle \to \sigma^{''}$ implies $\left\langle \mathrm{b},\ \sigma^{''}\right\rangle \to \mathrm{false}$. ■

Task 4: Variables that do not matter

(a)

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

(b)

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

(c)

Show for every program c and states $\sigma_1,\ \sigma_2$ with

- $\sigma_1 =_{\mathbf{dep}} (c)\sigma_2$
- $\langle c,\ \sigma_1\rangle \to \sigma_1^{'}$ and
- $\langle c,\ \sigma_2\rangle \to \sigma_2^{'}$

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: $c = \mathbf{skip}$

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: $c = \boldsymbol{x := a}$

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

Furthermore we have

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

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

Induction Hypothesis:

$$\sigma_1 =_{\mathbf{dep}} (c)\sigma_2,\ \langle c,\ \sigma_1\rangle \to \sigma_1^{'} \text{ and } \langle c,\ \sigma_2\rangle \to \sigma_2^{'} \text{ imply that } \sigma_1^{'} =_{\mathbf{mod}} (c)\sigma_2^{'}$$

holds for all derivations of an arbitrary, but fixed height h and for all states $\sigma,\ \sigma^{'}$.

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

case: $c = \boldsymbol{c_1; c_2}$

Following the definition of **dep** and **mod** we get
$\mathbf{mod}(c) = \mathbf{mod}(c_1) \cup \mathbf{mod}(c_2)$ and $\mathbf{dep}(c) = \mathbf{dep}(c_1) \cup \mathbf{dep}(c_2)$.

Furthermore we have

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

By induction hypothesis it holds that $\sigma_1^{*} =_{\mathbf{mod}(c_1)} \sigma_2^{*}$.
Now let $R = \mathbf{dep}(c_2)\backslash\mathbf{mod}(c_1)$. 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 $R^{'} = \mathbf{mod}(c_1)\backslash\mathbf{dep}(c_2) \subseteq \mathbf{mod}(c_1)$.
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 $\sigma_1^{'} =_{\mathbf{mod}(c_1)\backslash\mathbf{dep}(c_2)\cup\mathbf{mod}(c_2)} \sigma_2^{'}$ holds.
This is equal to $\sigma_1^{'} =_{\mathbf{mod}(c_1)\cup\mathbf{mod}(c_2)} \sigma_2^{'}$.

case: $c =$ **repeat** $\boldsymbol{c^{'}}$ **until** $\boldsymbol{b}$

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

Lets assume there exist states $\sigma_1^{*},\ \sigma_2^{*}$ so that $\left\langle c^{'},\ \sigma_i\right\rangle \to \sigma_i^{*}$ $(i \in \{1,\ 2\})$
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
$\langle b,\ \sigma_1^{*}\rangle \to$ **true** iff $\langle b,\ \sigma_2^{*}\rangle \to$ **true**

We now assume that $\langle b,\ \sigma_i^{*}\rangle \to$ **true**.
This leads to the following derivation tree:

$$\frac{\left\langle c^{'}, \sigma_i\right\rangle \to \sigma_i^{*} \qquad \langle b, \sigma_i^{*}\rangle \to \mathbf{true}}{\left\langle \mathbf{repeat}\ c^{'}\ \mathbf{until}\ b, \sigma_i\right\rangle \to \sigma_i^{*}}$$