Operational Semantics

Operational semantics provides a way of understanding what a program means by mimicking, at a high level, the operation of a computer executing the program. Operational semantics falls under two broad classes: *big-step* operational semantics, which specifies the entire operation of a given expression or statement; and *small-step* operational semantics, which specifies the operation of the program one step at a time. Both are powerful tools for verifying the correctness and other desired properties of programs.

Exercises

1. Use the big-step operational semantics rules for the WHILE language to write a well-formed derivation with $\langle E, y := 3; \texttt{if}\ y > 1\ \texttt{then}\ z := y\ \texttt{else}\ z := 2\rangle \Downarrow E[y \mapsto 3; z \mapsto 3]$ as its conclusion. Make sure to indicate which rule you used to prove each premise or conclusion.

$$\dfrac{\dfrac{\dfrac{}{\langle E, 3\rangle \Downarrow_a 3}\ \textit{int}}{\langle E, y := 3\rangle \Downarrow E[y \mapsto 3]}\ \textit{assign} \qquad \dfrac{\dfrac{\dfrac{}{\langle E[y \mapsto 3], y\rangle \Downarrow_a 3}\ \textit{var} \quad \dfrac{}{\langle E[y \mapsto 3], 1\rangle \Downarrow_a 1}\ \textit{int}}{\langle E[y \mapsto 3], y > 1\rangle \Downarrow_b \texttt{true}}\ \textit{boolop} \quad \dfrac{\dfrac{}{\langle E[y \mapsto 3], y\rangle \Downarrow_a 3}\ \textit{var}}{\langle E[y \mapsto 3], z := y\rangle \Downarrow E[y \mapsto 3; z \mapsto 3]}\ \textit{assign}}{\langle E[y \mapsto 3], \texttt{if}\ y > 1\ \texttt{then}\ z := y\ \texttt{else}\ z := 2\rangle \Downarrow E[y \mapsto 3; z \mapsto 3]}\ \textit{if-true}}{\langle E, y := 3; \texttt{if}\ y > 1\ \texttt{then}\ z := y\ \texttt{else}\ z := 2\rangle \Downarrow E[y \mapsto 3; z \mapsto 3]}\ \textit{seq}$$

2. For homework 2, you will be partially proving that if a statement terminates, then the big- and small-step semantics for WHILE will obtain equivalent results; i.e.,

$$\forall S \in \texttt{Stmt}.\forall E, E' \in \texttt{Var} \mapsto \mathbb{Z}.\langle E, S\rangle \to^* \langle E', \texttt{skip}\rangle \iff \langle E, S\rangle \Downarrow E'$$

You will prove this by induction on the structure of derivations for each direction of $\iff$.

For your homework proof, you are only required to show

- The base case(s).
- The inductive case for `let` using the semantics developed in question 1 of the homework.
- Two more representative inductive cases.

You may assume that this property holds for arithmetic and boolean expressions, i.e., you may assume the following hold:

$$\forall a \in \texttt{AExp}.\forall n \in \mathbb{Z}.\langle E, a\rangle \to_a^* n \iff \langle E, a\rangle \Downarrow_a n \tag{1}$$

$$\forall P \in \texttt{BExp}.\forall b \in \{\texttt{true}, \texttt{false}\}.\langle E, P\rangle \to_b^* b \iff \langle E, P\rangle \Downarrow_b b \tag{2}$$

You may also assume the small-step if congruence of $\langle E, S\rangle \to^* \langle E', S'\rangle$:

$$\frac{\langle E, P\rangle \to_b^* P'}{\langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \to^* \langle E, \texttt{if } P' \texttt{ then } S_1 \texttt{ else } S_2\rangle} \tag{3}$$

For this exercise, you will prove the following representative inductive case:

$$\forall S \in \texttt{Stmt}.\forall E, E' \in \texttt{Var} \mapsto \mathbb{Z}.\langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \Downarrow E' \iff \langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \to^* \langle E', \texttt{skip}\rangle$$

Proof: We proceed by induction on the structure of the derivations D, D', defined as $D :: \langle E, S\rangle \Downarrow E'$ and $D' :: \langle E, S\rangle \to^* \langle E'', \texttt{skip}\rangle$

Base Case (`skip`): Let $D :: \langle E, \texttt{skip}\rangle \Downarrow E'$ and $D' :: \langle E, \texttt{skip}\rangle \to^* \langle E'', \texttt{skip}\rangle$. By the big-step rule for `skip` we have that $E = E'$, and by the small-step rule for `skip`, we have that $E = E''$, therefore $E' = E''$ and $D \iff D'$.

Inductive Hypothesis: Our inductive hypothesis is $\langle E, S\rangle \Downarrow E' \iff \langle E, S\rangle \to^* \langle E', \texttt{skip}\rangle$

Inductive Case (`if`): Let $D :: \langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \Downarrow E'$ and $D' :: \langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \to^* \langle E'', \texttt{skip}\rangle$. By inversion there are two cases for the previous rule applied to D, *big-if-true* and *big-if-false*.

Case 1 *big-if-true*: We have:

$$D :: \frac{\langle E, P\rangle \Downarrow \texttt{true} \quad \langle E, S_1\rangle \Downarrow E'}{\langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \Downarrow E'} \textit{ big-if-true}$$

By (2) we have that $\langle E, P\rangle \Downarrow_b \texttt{true} \iff \langle E, P\rangle \to_b^* \texttt{true}$, and by (3) we have:

$$\frac{\langle E, P\rangle \to_b^* \texttt{true}}{\langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \to^* \langle E, \texttt{if true then } S_1 \texttt{ else } S_2\rangle}$$

By inversion, we know that the previous rule applied to D' must have been *small-if-true*:

$$D' :: \frac{\langle E, P\rangle \to_b^* \texttt{true} \quad \langle E, S_1\rangle \to^* \langle E'', \texttt{skip}\rangle}{\langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \to^* \langle E'', \texttt{skip}\rangle} \textit{ small-if-true}$$

By the inductive hypothesis, we have that $\langle E, S_1\rangle \Downarrow E' \iff \langle E, S_1\rangle \to^* \langle E', \texttt{skip}\rangle$, therefore $E' = E''$ and $D \iff D'$. $\square$