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:

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

We prove each direction of $\Leftrightarrow$ separately. We proceed by induction on derivations of program evaluation. We define a partial order over derivations $D_1 \prec D_2$ if D_1 is a sub-derivation of D_2 (that is D_1 is a premise of D_2).

Proof obligation for $\Rightarrow$: We will first prove that $\langle E, S\rangle \Downarrow E' \Rightarrow \langle E, S\rangle \to^* \langle E', \texttt{skip}\rangle$. In other words, if there exists a derivation $D :: \langle E, S\rangle \Downarrow E'$, we want to show that there exists a derivation of $\langle E, S\rangle \to^* \langle E', \texttt{skip}\rangle$.

Inductive Hypothesis: Our inductive hypothesis is that if $D' :: \langle E_1, S'\rangle \Downarrow E_2$ (for aribtrary D', S', E_1, E_2) is a sub-derivation of D, then there also exists a derivation of $\langle E_1, S'\rangle \to^* \langle E_2, \texttt{skip}\rangle$. In other words, given D' exists, we can assume that $\langle E_1, S'\rangle \Downarrow E_2 \Rightarrow \langle E_1, S'\rangle \to^* \langle E_2, \texttt{skip}\rangle$.

Base Case (`skip`): Let $D :: \langle E, \texttt{skip}\rangle \Downarrow E'$. By inversion, we know that D must end with the *big-skip* rule, which gives us $E = E'$. And, by the *multi-reflexive* rule for $\to^*$, we have that $\langle E, \texttt{skip}\rangle \to^* \langle E, \texttt{skip}\rangle$. Since E and E' are equal, we have proved that $\langle E, \texttt{skip}\rangle \Downarrow E' \Rightarrow \langle E, \texttt{skip}\rangle \to^* \langle E', \texttt{skip}\rangle$ as required.

Inductive Case (`if`): In this case, we have $D :: \langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \Downarrow E'$. We want to show that there exists a derivation for $\langle E, \texttt{if P then } S_1 \texttt{ else } S_2\rangle \to^* \langle E', \texttt{skip}\rangle$. 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:

$$D ::= \frac{\langle E, P\rangle \Downarrow \texttt{true} \quad D' :: \langle E, S_1\rangle \Downarrow E'}{\langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \Downarrow E'} \textit{ big-if-true} \tag{4}$$

Using the induction hypothesis on sub-derivation D', we also have:

$$\langle E, S_1\rangle \to^* \langle E', \texttt{skip}\rangle \tag{5}$$

By (2) we have that $\langle E, P\rangle \Downarrow_b \texttt{true} \Rightarrow \langle E, P\rangle \rightarrow_b^* \texttt{true}$, and using this result with (3) we have:

$$\frac{\langle E, P\rangle \rightarrow_b^* \texttt{true}}{\langle E, \texttt{if}\ P\ \texttt{then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E, \texttt{if true then}\ S_1\ \texttt{else}\ S_2\rangle} \tag{6}$$

By the *small-if-true* rule, we also have:

$$\langle E, \texttt{if true then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow \langle E, S_1\rangle \tag{7}$$

By (5), (7), and the *multi-inductive* rule of $\rightarrow^*$, we can then derive:

$$\frac{\langle E, \texttt{if true then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow \langle E, S_1\rangle \quad \langle E, S_1\rangle \rightarrow^* \langle E', \texttt{skip}\rangle}{\langle E, \texttt{if true then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E', \texttt{skip}\rangle} \tag{8}$$

By (6), (8), and the *transitive* property of $\rightarrow^*$, we are finally able to derive:

$$\langle E, \texttt{if P then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E', \texttt{skip}\rangle$$

Case 2 *big-if-false*: Similar to above, using corresponding rules for the `false` case.
Thus, we have shown that $\langle E, \texttt{if}\ P\ \texttt{then}\ S_1\ \texttt{else}\ S_2\rangle \Downarrow E' \Rightarrow \langle E, \texttt{if P then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E', \texttt{skip}\rangle$.

Proof obligation for $\Leftarrow$: We will now prove that $\langle E, S\rangle \Downarrow E' \Leftarrow \langle E, S\rangle \rightarrow^* \langle E', \texttt{skip}\rangle$. In other words, if there exists a derivation $D :: \langle E, S\rangle \rightarrow^* \langle E', \texttt{skip}\rangle$, we want to show that there exists a derivation of $\langle E, S\rangle \Downarrow E'$.

Inductive Hypothesis: Our inductive hypothesis is that if $D' :: \langle E_1, S'\rangle \rightarrow^* \langle E_2, \texttt{skip}\rangle$ (for aribtrary D', S', E_1, E_2) is a sub-derivation of D, then there also exists a derivation of $\langle E_1, S'\rangle \Downarrow E_2$. In other words, given D' exists, we can assume that $\langle E_1, S'\rangle \rightarrow^* \langle E_2, \texttt{skip}\rangle \Rightarrow \langle E_1, S'\rangle \Downarrow E_2$.

Base Case (`skip`): Let $D :: \langle E, \texttt{skip}\rangle \rightarrow^* \langle E', \texttt{skip}\rangle$. By inversion, we know that no small-step rule for `skip` exists. This derivation is only possible using the *multi-reflexive* rule for $\rightarrow^*$, which gives us $E = E'$. And, by the *big-step* rule, we have that $\langle E, \texttt{skip}\rangle \Downarrow E$. Since E and E' are equal, we have proved that $\langle E, \texttt{skip}\rangle \rightarrow^* \langle E', \texttt{skip}\rangle \Rightarrow \langle E, \texttt{skip}\rangle \Downarrow E'$ as required.

Inductive Case (`if`): In this case, we have $D :: \langle E, \texttt{if P then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E', \texttt{skip}\rangle$. We want to show that there exists a derivation for $\langle E, \texttt{if}\ P\ \texttt{then}\ S_1\ \texttt{else}\ S_2\rangle \Downarrow E'$ By inversion of rules we know that this derivation must use transitive applications of the *multi-inductive* rule, eq. (3), and either the *small-if-true* or *small-if-false* rules. We can discuss the *true* and *false* cases separately.

Case 1: By inversion and use of transitive applications of $\rightarrow^*$, the derivation for the *true* case will be of the form:

$$\frac{\dfrac{D_P :: \langle E, P\rangle \rightarrow_b^* \texttt{true}}{\langle \texttt{if}\ P\ \texttt{then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E, \texttt{if true then}\ S_1\ \texttt{else}\ S_2\rangle} \quad \dfrac{D_{S_1} :: \langle E, S_1\rangle \rightarrow^* \langle E', \texttt{skip}\rangle}{\langle E, \texttt{if true then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E', \texttt{skip}\rangle}}{\langle E, \texttt{if}\ P\ \texttt{then}\ S_1\ \texttt{else}\ S_2\rangle \rightarrow^* \langle E', \texttt{skip}\rangle} \tag{9}$$

Using D_P from (9) and the result from (2), we have that:

$$\langle E, P\rangle \Downarrow_b \texttt{true} \tag{10}$$

Using D_{S_1} from (9) and the induction hypothesis, we have that:

$$\langle E, S_1\rangle \Downarrow E' \tag{11}$$

Using (10), (11), and the *big-step* rule, we have the required derivation:

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

Case 2: The *false* case is similar to above, substituting S_2 for S_1.
Thus, we have shown that $\langle E, \texttt{if P then } S_1 \texttt{ else } S_2\rangle \to^* \langle E', \texttt{skip}\rangle \Rightarrow \langle E, \texttt{if } P \texttt{ then } S_1 \texttt{ else } S_2\rangle \Downarrow E'$.