Software-Modellierung und Verifikation
Informatik 2
Prof. J.-P. Katoen
RWTH Aachen

Priv.-Doz. T. Noll noll@cs.rwth-aachen.de
T. Han tingting.han@cs.rwth-aachen.de
A. Mereacre mereacre@cs.rwth-aachen.de

8. Exercise sheet *Semantics and Verification of Software 2008*

Due to Mon., 15 December 2008, *before* the exercise course begins.

Exercise 8.1:

Consider Example 12.3 from the lecture:

$c_0 \equiv$ **begin**
  var x; **var** y;
  proc P **is** $y := x$;
  $x := 1$;
  begin
    var x;
    $x := 2$;
    call P
  end
end

Choose initial variable environment ρ_0 such that with static scope semantics, for all π_0 and σ_0:

$$\rho_0, \pi_0 \vdash \langle c_0, \sigma_0 \rangle \to \sigma_0[0 \mapsto 1, 1 \mapsto 1, 2 \mapsto 2]$$

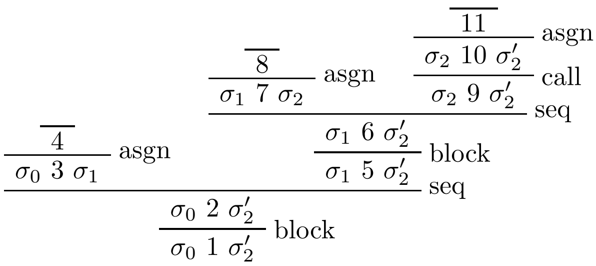
Give a formal proof, using the operational semantics in Definition 12.4.

Solution

$\sigma : \mathbf{Loc} \dashrightarrow \mathbb{Z}$ is representing the memory
$\rho : \mathbf{Var} \dashrightarrow \mathbf{Loc}$ is mapping variables to memory cells
π is mapping procedure names to code and declaration environment

Starting with $\rho_0 := \rho_\emptyset[y/0] \in \mathbf{VEnv}$, else y would not be declared. Initially the value of the memory is undefined. Also we have $\sigma_0(0) = 0$.

The proof structure:



[1] $(\rho_0, \pi_0) \vdash \langle c_0, \sigma_0 \rangle \to \sigma_2'$

block-rule updates the environment only:

[2] $(\rho_1, \pi_1) \vdash \langle c_1, \sigma_0[1 \mapsto 0] \rangle \to \sigma_2'$

where $\rho_1 := \rho_0[x \mapsto 1]$ and $\pi_1 := \pi_0[P \mapsto (y := x, \rho_1, \pi_0)]$ $\overset{\rho_1}{\sigma_0}$: $[\ \overset{y}{\cdot} \mid \overset{x}{\cdot} \mid \ldots$
and $c_1 \equiv x := 1;$ **begin** ... **end**:

[3] $(\rho_1, \pi_1) \vdash \langle x := 1, \sigma_0[1 \mapsto 0] \rangle \to \sigma_1$ where $\sigma_1 = \sigma_0[1 \mapsto 1]$ since **[4]** $\langle 1, \sigma_0[1 \mapsto 0] \circ \rho_1 \rangle \to 1$ $\overset{\rho_1}{\sigma_1}$: $[\ \overset{y}{\cdot} \mid \overset{x}{1} \mid \ldots$

[5] $(\rho_1, \pi_1) \vdash \langle$**begin** ... **end**$, \sigma_1 \rangle \to \sigma_2'$

block-rule updates the environment only:

[6] $(\rho_2, \pi_2) \vdash \langle c_2, \sigma_1[2 \mapsto 0] \rangle \to \sigma_2'$

where $\rho_2 := \rho_1[x \mapsto 2]$ and $\pi_2 := \pi_1$ $\overset{\rho_2}{\sigma_1}$: $[\ \overset{y}{\cdot} \mid 1 \mid \overset{x}{\cdot} \mid \ldots$
and $c_2 \equiv x := 2;$ **call** P:

[7] $(\rho_2, \pi_2) \vdash \langle x := 2, \sigma_1[2 \mapsto 0] \rangle \to \sigma_2$ where $\sigma_2 = \sigma_1[2 \mapsto 2]$ since **[8]** $\langle 2, \sigma_1[2 \mapsto 0] \circ \rho_2 \rangle \to 2$ $\overset{\rho_2}{\sigma_2}$: $[\ \overset{y}{\cdot} \mid 1 \mid \overset{x}{2} \mid \ldots$

[9] $(\rho_2, \pi_2) \vdash \langle$**call** $P, \sigma_2 \rangle \to \sigma_2'$

call-rule evaluates σ_2 to σ_2', if the procedure does so in its declaration environment (here ρ_1 and π_0):

[10] $(\rho_2, \overbrace{\pi_2'[P \mapsto (y := x, \rho_2, \pi_2')]}^{\pi_2'}) \vdash \langle y := x, \sigma_2 \rangle \to \sigma_2'$
. where $\sigma_2' = \sigma_2[0/1]$, $\pi_2(P) = (y := x, \rho_2, \pi_2')$ since **[11]** $\langle x, \sigma_2 \circ \rho_1 \rangle \to 1$ $\overset{\rho_1}{\sigma_2'}$: $[\ \overset{y}{1} \mid \overset{x}{1} \mid 2 \mid \ldots$

We get that $\sigma_2' = \sigma_0[0 \mapsto 1, 1 \mapsto 1, 2 \mapsto 2]$.

$\square$

Exercise 8.2:

Consider the following modification to our *WHILE* language, where procedures have (exactly) two *call-by-value* parameters:

$$\begin{array}{rcl} p & ::= & \textsf{proc}\ P(x_1, x_2)\ \textsf{is}\ c;\ p \mid \varepsilon \in \mathbf{PDec} \\ c & ::= & \ldots \mid \textsf{call}\ p(a_1, a_2) \in \mathbf{Cmd} \end{array}$$

(a) Define new *call* and *block* rules.

(b) Evaluate $\langle c_0, \sigma_\emptyset \rangle$ for environment $\rho_\emptyset, \pi_\emptyset$ and

$$\begin{array}{rcl} c_0 & \equiv & \textsf{begin} \\ & & \quad \textsf{var}\ y; \\ & & \quad \textsf{proc}\ MAX(x_1, x_2)\ \textsf{is if}\ x_1 > x_2\ \textsf{then}\ y := x_1\ \textsf{else}\ y := x_2; \\ & & \quad \textsf{call}\ MAX(1, 2); \\ & & \textsf{end} \end{array}$$

Solution

(a) Effect of procedure call now dependent on parameters:

$$\mathbf{PEnv} = \{\pi \mid \pi : \mathbf{PVar} \longrightarrow \mathbf{Var} \times \mathbf{Var} \times \mathbf{Cmd} \times \mathbf{VEnv} \times \mathbf{PEnv}\}$$

block-rule with new update function (effect of declaration):

$$\mathbf{upd}_p[\![\textsf{proc}\ P(x_1, x_2)\ \textsf{is}\ c;\ p]\!](\rho, \pi) = \mathbf{upd}_p[\![p]\!](\rho, \pi[P/(x_1, x_2, c, \rho, \pi)])$$

$$\frac{\mathbf{upd}_v[\![v]\!](\rho, \sigma) = (\rho', \sigma') \qquad (\rho', \mathbf{upd}_p[\![p]\!](\rho', \pi)) \vdash \langle c, \sigma' \rangle \to \sigma''}{(\rho, \pi) \vdash \langle \textsf{begin}\ v, p, c\ \textsf{end}, \sigma \rangle \to \sigma''}$$

call-rule:

$$\frac{\langle a_1, \sigma \circ \rho \rangle \to z_1 \qquad \langle a_2, \sigma \circ \rho \rangle \to z_2 \qquad (\rho', \pi'[P \mapsto (x_1, x_2, c, \rho', \pi')]) \vdash \langle c, \sigma[\rho'(x_1)/z_1, \rho'(x_2)/z_2] \rangle \to \sigma'}{(\rho, \pi) \vdash \langle \textsf{call}\ P(a_1, a_2), \sigma \rangle \to \sigma'}$$

if $\pi(P) = (x_1, x_2, c, \rho', \pi')$
and $(\rho', \sigma') = \mathbf{upd}_v[\![\textsf{var}\ x_1; \textsf{var}\ x_2;]\!](\rho, \sigma)$

(b)

$$\frac{\dfrac{}{\langle 1, \sigma_\emptyset[0 \mapsto 0] \circ \rho_1 \rangle \to 1} \qquad \dfrac{}{\langle 2, \sigma_\emptyset[0 \mapsto 0] \circ \rho_1 \rangle \to 2} \qquad \dfrac{\dfrac{}{\langle x_1 > x_2, \sigma_2 \circ \rho_2 \rangle \to \textsf{false}} \qquad \dfrac{\dfrac{}{\langle x_2, \sigma_2 \circ \rho_2 \rangle \to 2}}{(\rho_2, \pi_1) \vdash \langle y := x_2, \sigma_2 \rangle \to \sigma_1}}{(\rho_2, \pi_1) \vdash \langle \textsf{if}\ x_1 > x_2 \ldots, \sigma_2 \rangle \to \sigma_1}}{\dfrac{(\rho_1, \pi_1) \vdash \langle \textsf{call}\ P(1, 2), \sigma_\emptyset[0 \mapsto 0] \rangle \to \sigma_1}{(\rho_\emptyset, \pi_\emptyset) \vdash \langle c_0, \sigma_\emptyset \rangle \to \sigma_1}}$$

where $\rho_1 = \rho_\emptyset[y \mapsto 0]$, $\pi_1 = \pi_\emptyset[P \mapsto (x_1, x_2, \textsf{if} \ldots, \rho, \pi)]$
and $\rho_2 = \rho_1[x_1 \mapsto 1, x_2 \mapsto 2]$, $\sigma_2 = \sigma_\emptyset[0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 2]$
and $\sigma_1 = \sigma_2[0 \mapsto 2]$