Concepts in Programming Languages

Recitation 4: Structural Operational Semantics

Yotam Feldman

Reference:

Semantics with Applications by H. Nielson and F. Nielson – Ch. 2

http://www.cs.kun.nl/~hubbers/courses/sc_1718/materiaal/wiley.pdf

Operational Semantics

- Formal definition of program semantics
- The meaning of the program is described "operationally"
- Natural Operational Semantics - NOS
- Structural Operational Semantics - SOS

- We can go **systematically** from operational semantics (NOS or SOS) to an **interpreter**

Structural Operational Semantics

- Emphasizes the individual execution steps
- **<S, *s*>** $\Rightarrow \gamma$
  - the **"first"** step of executing **S** on state ***s*** leads to γ
- Two possibilities for γ
  - γ **= <S', s'>**
    The execution of S is not completed and, S' is the remaining computation to be performed on s'
  - γ **= s'**
    The execution of S has terminated with a final state s'
- γ is a **stuck** configuration when there are no transitions

Formally defining $\Rightarrow$

- $\Rightarrow$ is defined **inductively** using **inference rules**, with both **syntactic** conditions on S and **semantic** conditions on s

$$[\text{ass}_{\text{sos}}] \qquad \langle x := a,\ s\rangle \Rightarrow s[x \mapsto \mathcal{A}[\![a]\!]s]$$

$$[\text{skip}_{\text{sos}}] \qquad \langle \texttt{skip},\ s\rangle \Rightarrow s$$

$$[\text{comp}^1_{\text{sos}}] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow \langle S_1',\ s'\rangle}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S_1';S_2,\ s'\rangle}$$

$$[\text{comp}^2_{\text{sos}}] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow s'}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S_2,\ s'\rangle}$$

$$[\text{if}^{\text{tt}}_{\text{sos}}] \qquad \langle \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2,\ s\rangle \Rightarrow \langle S_1,\ s\rangle \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$[\text{if}^{\text{ff}}_{\text{sos}}] \qquad \langle \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2,\ s\rangle \Rightarrow \langle S_2,\ s\rangle \text{ if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

$$[\text{while}_{\text{sos}}] \qquad \langle \texttt{while}\ b\ \texttt{do}\ S,\ s\rangle \Rightarrow \langle \texttt{if}\ b\ \texttt{then}\ (S;\ \texttt{while}\ b\ \texttt{do}\ S)\ \texttt{else skip},\ s\rangle$$

SOS Example

$\langle y := 1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 3] \rangle \Rightarrow$

$\langle \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 3, y \mapsto 1] \rangle \Rightarrow$

$\langle \text{if } x \neq 1 \text{ then } (y := y*x; x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1)) \text{ else skip}, s_0[x \mapsto 3, y \mapsto 1] \rangle \Rightarrow$

$\langle y := y*x; x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 3, y \mapsto 1] \rangle \Rightarrow$

$\langle x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 3, y \mapsto 3] \rangle \Rightarrow$

$\langle \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 2, y \mapsto 3] \rangle \Rightarrow$

$\langle \text{if } x \neq 1 \text{ then } (y := y*x; x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1)) \text{ else skip}, s_0[x \mapsto 2, y \mapsto 3] \rangle \Rightarrow$

$\langle y := y*x; x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 2, y \mapsto 3] \rangle \Rightarrow$

$\langle x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 2, y \mapsto 6] \rangle \Rightarrow$

$\langle \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1), s_0[x \mapsto 1, y \mapsto 6] \rangle \Rightarrow$

$\langle \text{if } x \neq 1 \text{ then } (y := y*x; x := x-1; \text{while } x \neq 1 \text{ do } (y := y*x; x := x-1)) \text{ else skip}, s_0[x \mapsto 1, y \mapsto 6] \rangle \Rightarrow$

$\langle \text{skip}, s_0[x \mapsto 1, y \mapsto 6] \rangle \Rightarrow$

$s_0[x \mapsto 1, y \mapsto 6]$

Semantic Equivalence in SOS

- S_1 and S_2 are semantically equivalent if the following two conditions hold:
  - For all s and γ which is either final or stuck $\langle S_1, s\rangle \Rightarrow^* \gamma$ if and only if $\langle S_2, s\rangle \Rightarrow^* \gamma$
  - For all s, there is an infinite derivation sequence starting at $\langle S_1, s\rangle$ if and only if there is an infinite derivation sequence starting at $\langle S_2, s\rangle$

Example: S; skip ≈ S

From rhs to lhs:

- Assume <S, s> $\Rightarrow^*$ γ where γ is final or stuck.
  Show that <S; skip, s> $\Rightarrow^*$ γ.
  - In the basic While language there are no stuck configurations, so we can consider just γ=s'.
  - ?

- (Also nonterminating computations)

Proving properties of SOS

- Many properties are proved by induction on the length of derivation sequence
- Prove that the property holds for all derivation sequences of length 0
- Prove that the property holds for all other derivation sequences:
  - Assume the property holds for all sequences of length k or less (induction hypothesis)
  - Show that the property holds for sequences of length k+1

Sequential Composition – Property 1

- Claim: $\langle S_1, s\rangle \Rightarrow^k s'$ implies $\langle S_1; S_2, s\rangle \Rightarrow^k \langle S_2, s'\rangle$
- Proof: By induction over k.
  - Base case, k=0: holds vacuously

$$[\text{comp}^1_{\text{sos}}] \quad \frac{\langle S_1, s\rangle \Rightarrow \langle S_1', s'\rangle}{\langle S_1;S_2, s\rangle \Rightarrow \langle S_1';S_2, s'\rangle}$$

$$[\text{comp}^2_{\text{sos}}] \quad \frac{\langle S_1, s\rangle \Rightarrow s'}{\langle S_1;S_2, s\rangle \Rightarrow \langle S_2, s'\rangle}$$

Inductive Step

- **Assume for all $j \leq k$**: if $\langle S_1, s\rangle \Rightarrow^j s'$ then $\langle S_1; S_2, s\rangle \Rightarrow^j \langle S_2, s'\rangle$. Prove for k+1.
- Assume $\langle S_1, s\rangle \Rightarrow^{k+1} s''$, then, by definition of deriv. seq. :
  - $\langle S_1, s\rangle \Rightarrow \gamma \Rightarrow^k s''$
  - $\gamma = \langle S'_1, s'\rangle$ is not a final or stuck configuration.
- By the induction hypothesis, $\langle S'_1; S_2, s'\rangle \Rightarrow^k \langle S_2, s''\rangle$
- $\langle S_1, s\rangle \Rightarrow \langle S'_1, s'\rangle$, so by [comp^1] we get $\langle S_1; S_2, s\rangle \Rightarrow \langle S'_1; S_2, s'\rangle$
- Together we get $\langle S_1; S_2, s\rangle \Rightarrow^{k+1} \langle S_2, s''\rangle$

$$[\mathrm{comp}^1_{\mathrm{sos}}] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow \langle S'_1,\ s'\rangle}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S'_1;S_2,\ s'\rangle}$$

$$[\mathrm{comp}^2_{\mathrm{sos}}] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow s'}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S_2,\ s'\rangle}$$

S; skip ≈ S

From rhs to lhs:

- **Final:** Assume <S, s> $\Rightarrow^*$ s'.
  From the previous claim, <S; skip, s> $\Rightarrow^*$ <skip, s'>.
  <skip, s'> $\Rightarrow$ s', so overall <S; skip, s> $\Rightarrow^*$s'.
- **Non-terminating:**

  <S, s> $\Rightarrow$ <S', s'> $\Rightarrow$ <S'', s''> $\Rightarrow$ …

  similarly to the proof of the previous claim,
  <S; skip, s> $\Rightarrow$ <S'; skip, s'> $\Rightarrow$ <S''; skip, s''> $\Rightarrow$ …
  (by induction on the length of the prefix)

S; skip ≈ S

From lhs to rhs:

- Assume <S; skip, s> $\Rightarrow^*$ γ where γ is final or stuck. Show that <S, s> $\Rightarrow^*$ γ.
  - In the basic While language there are no stuck configurations, so we can consider just γ=s'.
  - ?

- (Also nonterminating computations)

Sequential Composition – Property 2

- If $\langle S_1; S_2, s\rangle \Rightarrow^k s''$ then there exists a state s' and numbers k_1 and k_2 such that:
  - $\langle S_1, s\rangle \Rightarrow^{k1} s'$
  - $\langle S_2, s'\rangle \Rightarrow^{k2} s''$
  - $k = k_1 + k_2$

Proof

- If **$\langle S_1; S_2, s\rangle \Rightarrow^k s''$** then there exists a state **s'** and numbers **k_1** and **k_2** such that: $\langle S_1, s\rangle \Rightarrow^{k1} s'$, $\langle S_2, s'\rangle \Rightarrow^{k2} s''$ and $k = k_1 + k_2$

- Base case: k=0, holds vacuously

Inductive Step

- **Assume for all $j \leq k$**: if $\langle S_{1;}\ S_2, s\rangle \Rightarrow^j s''$ then there exists a state s' and numbers j_1 and j_2 such that: $\langle S_1, s\rangle \Rightarrow^{j1} s'$, $\langle S_2, s'\rangle \Rightarrow^{j2} s''$ and $j = j_1 + j_2$
- Assume $\langle S_{1;}\ S_2, s\rangle \Rightarrow^{k+1} s''$. By the definition of deriv. seq :
  - $\langle S_{1;}\ S_2, s\rangle \Rightarrow \gamma$
  - $\gamma \Rightarrow^k s''$
  - γ is not a final or stuck configuration (unless k=0)
- Split according to two cases of $\langle S_{1;}\ S_2, s\rangle \Rightarrow \gamma$

$$[\mathrm{comp}^1_{\mathrm{sos}}] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow \langle S_1',\ s'\rangle}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S_1';S_2,\ s'\rangle}$$

$$[\mathrm{comp}^2_{\mathrm{sos}}] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow s'}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S_2,\ s'\rangle}$$

Case $\mathbf{comp}_{\mathbf{sos}}^{\mathbf{2}}$

- $\gamma = \langle S_2, s' \rangle$
- $\langle S_{1;}\ S_2, s \rangle \Rightarrow \langle S_2, s' \rangle$
- $\langle S_2, s' \rangle \Rightarrow^k s''$

$$[\mathrm{comp}_{\mathrm{sos}}^2] \qquad \frac{\langle S_1,\ s\rangle \Rightarrow s'}{\langle S_1;S_2,\ s\rangle \Rightarrow \langle S_2,\ s'\rangle}$$

- Set $k_1 = 1$, $k_2 = k$ and get:
  - $k+1 = k_1 + k_2$
  - $\langle S_1, s \rangle \Rightarrow^{k1} s'$
  - $\langle S_2, s' \rangle \Rightarrow^{k2} s''$

Case $\mathbf{comp}_{\mathbf{sos}}^{\mathbf{1}}$

- $\gamma = \langle S'_1; S_2, s' \rangle$
- $\langle S_1; S_2, s \rangle \Rightarrow \langle S'_1; S_2, s' \rangle$
- $\langle S'_1; S_2, s' \rangle \Rightarrow^k s''$

$$[\mathrm{comp}^1_{\mathrm{sos}}] \qquad \frac{\langle S_1, s \rangle \Rightarrow \langle S'_1, s' \rangle}{\langle S_1; S_2, s \rangle \Rightarrow \langle S'_1; S_2, s' \rangle}$$

- By induction hypothesis on $\langle S'_1; S_2, s' \rangle \Rightarrow^k s''$ we get j_1, j_2 and state $\hat{s}$ such that:
  - $k = j_1 + j_2$
  - $\langle S'_1, s' \rangle \Rightarrow^{j1} \hat{s}$
  - $\langle S_2, \hat{s} \rangle \Rightarrow^{j2} s''$
- Set $k_1 = j_1 + 1$, $k_2 = j_2$ and get:
  - $k+1 = k_1 + k_2$
  - $\langle S_1, s \rangle \Rightarrow^{k1} \hat{s}$ since $\langle S_1, s \rangle \Rightarrow \langle S'_1, s' \rangle \Rightarrow^{j1} \hat{s}$
  - $\langle S_2, \hat{s} \rangle \Rightarrow^{k2} s''$

Example: S; skip ≈ S

From lhs to rhs:

- **Final:** Assume <S; skip, s> $\Rightarrow^*$ s'.
  From property 2 of composition, exists ŝ such that <S, s> $\Rightarrow^*$ ŝ and <skip, ŝ> $\Rightarrow^*$ s'.

  Only possible derivation is <skip, ŝ> $\Rightarrow$ ŝ which is final,
  so ŝ=s'

- **Non-terminating:**
  In an infinite derivation sequence for <S; skip, s>,
  - By induction on the length, the sequence is of the form
    <S; skip, s> $\Rightarrow$ <S'; skip, s'> $\Rightarrow$ <S''; skip, s''> $\Rightarrow$ γ $\Rightarrow$…
    since they can use only [comp^1]; [comp^2] gives <skip, ŝ> and termination
  - So necessarily there are derivations <S, s> $\Rightarrow$ <S', s'> $\Rightarrow$ <S'', s''> $\Rightarrow$…