Proof principles for Operational Semantics

Hanne Riis Nielson

Informatics and Mathematical Modelling
Technical University of Denmark

Natural semantics

$$\langle x := a\ ,\ s\rangle \to s[x \mapsto \mathcal{A}[\![a]\!]s]$$

$$\langle \texttt{skip}\ ,\ s\rangle \to s$$

$$\frac{\langle S_1\ ,\ s\rangle \to s' \quad \langle S_2\ ,\ s'\rangle \to s''}{\langle S_1; S_2\ ,\ s\rangle \to s''}$$

$$\frac{\langle S_1\ ,\ s\rangle \to s'}{\langle \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ ,\ s\rangle \to s'} \qquad \text{if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$\frac{\langle S_2\ ,\ s\rangle \to s'}{\langle \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ ,\ s\rangle \to s'} \qquad \text{if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

$$\frac{\langle S\ ,\ s\rangle \to s' \quad \langle \texttt{while}\ b\ \texttt{do}\ S\ ,\ s'\rangle \to s''}{\langle \texttt{while}\ b\ \texttt{do}\ S\ ,\ s\rangle \to s''} \qquad \text{if } \mathcal{B}[\![b]\!]s = \mathbf{tt}$$

$$\langle \texttt{while}\ b\ \texttt{do}\ S\ ,\ s\rangle \to s \qquad \text{if } \mathcal{B}[\![b]\!]s = \mathbf{ff}$$

Structural operational semantics

$$\langle x := a \,,\, s\rangle \Rightarrow s[x \mapsto \mathcal{A}[\![a]\!]s]$$

$$\langle \texttt{skip} \,,\, s\rangle \Rightarrow s$$

$$\frac{\langle S_1 \,,\, s\rangle \Rightarrow \langle S_1' \,,\, s'\rangle}{\langle S_1; S_2 \,,\, s\rangle \Rightarrow \langle S_1'; S_2 \,,\, s'\rangle}$$

$$\frac{\langle S_1 \,,\, s\rangle \Rightarrow s'}{\langle S_1; S_2 \,,\, s\rangle \Rightarrow \langle S_2 \,,\, s'\rangle}$$

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

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

$$\langle \texttt{while } b \texttt{ do } S \,,\, s\rangle \Rightarrow \langle \texttt{if } b \texttt{ then } (S;\ \texttt{while } b \texttt{ do } S) \texttt{ else skip} \,,\, s\rangle$$

Proof principle: structural induction

To prove a property of all the elements of the syntactic category do the following:

- Prove that the property holds for all the basis elements of the syntactic category.
- Prove that the property holds for all the composite elements of the syntactic category: Assume that the property holds for all the immediate constituents of the element — this is called the induction hypothesis — and prove that it also holds for the element itself.

Proof principle:
induction on shape of derivation trees

To prove a property of all the derivation trees of a natural semantics do the following:

- Prove that the property holds for all the simple derivation trees by showing that it holds for the axioms of the transition system.
- Prove that the property holds for all composite derivation trees: For each rule assume that the property holds for its premises — this is called the induction hypothesis — and prove that it also holds for the conclusion of the rule provided that the conditions of the rule are satisfied.

Proof principle:
induction on length of derivation sequences

To prove a property of all the derivation sequences of a structural operational semantics do the following:

- Prove that the property holds for all derivation sequences of length 0.
- Prove that the property holds for all other derivation sequences: Assume that the property holds for all derivation sequences of length at most k — this is called the induction hypothesis — and show that it holds for derivation sequences of length $k + 1$.

Theorem

$$\langle S\,,\, s\rangle \to s' \quad \text{if and only if} \quad \langle S\,,\, s\rangle \Rightarrow^{*} s'$$

Proof obligations

if $\langle S\,,\, s\rangle \to s'$
then $\langle S\,,\, s\rangle \Rightarrow^{*} s'$

if $\langle S_1\,,\, s\rangle \Rightarrow^{k} s'$
then $\langle S_1; S_2\,,\, s\rangle \Rightarrow^{k} s'$

if $\langle S\,,\, s\rangle \Rightarrow^{k} s'$
then $\langle S\,,\, s\rangle \to s'$

if $\langle S_1; S_2\,,\, s\rangle \Rightarrow^{k} s''$
then $\langle S_1\,,\, s\rangle \Rightarrow^{k_1} s'$
$\langle S_2\,,\, s'\rangle \Rightarrow^{k_2} s''$
and $k = k_1 + k_2$

if $\langle$if b then (S; while b do S)
else skip, s$\rangle \to$ s$'$
then $\langle$while b do S $,\, s\rangle \to s'$

How robust are these results?

Extend the while language with

- abortion: $S ::= \cdots \mid \texttt{abort}$
- non-determinism: $S ::= \cdots \mid S_1 \texttt{ or } S_2$
- parallelism: $S ::= \cdots \mid S_1 \texttt{ par } S_2$

Questions:

- how are the semantics modified?
- are both kinds of semantics "equally powerful"?

Adding abortion

- Configurations: extended to include the abort statement
- Terminal configurations: unchanged
- Transitions:
  - for structural operational semantics: unchanged
  - for natural semantics: unchanged

Adding nondeterminism

- Configurations: extended to include the or statement
- Terminal configurations: unchanged
- Transitions:
  - for structural operational semantics:

$$\langle S_1 \text{ or } S_2\,,\, s\rangle \Rightarrow \langle S_1\,,\, s\rangle \qquad \langle S_1 \text{ or } S_2\,,\, s\rangle \Rightarrow \langle S_2\,,\, s\rangle$$

  - for natural semantics:

$$\frac{\langle S_1\,,\, s\rangle \to s'}{\langle S_1 \text{ or } S_2\,,\, s\rangle \to s'} \qquad \frac{\langle S_2\,,\, s\rangle \to s'}{\langle S_1 \text{ or } S_2\,,\, s\rangle \to s'}$$

Adding parallelism

- Configurations: extended to include the par statement
- Terminal configurations: unchanged
- Transitions:
  - for structural operational semantics:

$$\frac{\langle S_1\ ,\ s\rangle \Rightarrow \langle S_1'\ ,\ s'\rangle}{\langle S_1 \ \textsf{par}\ S_2\ ,\ s\rangle \Rightarrow \langle S_1' \ \textsf{par}\ S_2\ ,\ s'\rangle} \qquad \frac{\langle S_1\ ,\ s\rangle \Rightarrow s'}{\langle S_1 \ \textsf{par}\ S_2\ ,\ s\rangle \Rightarrow \langle S_2\ ,\ s'\rangle}$$

$$\frac{\langle S_2\ ,\ s\rangle \Rightarrow \langle S_2'\ ,\ s'\rangle}{\langle S_1 \ \textsf{par}\ S_2\ ,\ s\rangle \Rightarrow \langle S_1 \ \textsf{par}\ S_2'\ ,\ s'\rangle} \qquad \frac{\langle S_2\ ,\ s\rangle \Rightarrow s'}{\langle S_1 \ \textsf{par}\ S_2\ ,\ s\rangle \Rightarrow \langle S_1\ ,\ s'\rangle}$$

  - for natural semantics:

$$\frac{\langle S_1, s\rangle \rightarrow s' \quad \langle S_2, s'\rangle \rightarrow s''}{\langle S_1 \ \textsf{par}\ S_2, s\rangle \rightarrow s''} \qquad \frac{\langle S_2, s\rangle \rightarrow s' \quad \langle S_1, s'\rangle \rightarrow s''}{\langle S_1 \ \textsf{par}\ S_2, s\rangle \rightarrow s''}$$

Summary

Natural semantics

- cannot distinguish between looping and abnormal termination
- non-determinism suppresses looping
- cannot express interleaving of computations

Structural operational semantics

- distinguishes between looping and abnormal termination
- non-determinism does not suppress looping
- can express interleaving of computations