

Proof principles for Operational Semantics

Hanne Riis Nielson

Informatics and Mathematical Modelling
Technical University of Denmark

Natural semantics

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

$$\langle \text{skip}, s \rangle \rightarrow s$$

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

$$\frac{\langle S_1, s \rangle \rightarrow s'}{\langle \text{if } b \text{ then } S_1 \text{ else } S_2, s \rangle \rightarrow s'}$$

if $\mathcal{B}[[b]]s = \text{tt}$

$$\frac{\langle S_2, s \rangle \rightarrow s'}{\langle \text{if } b \text{ then } S_1 \text{ else } S_2, s \rangle \rightarrow s'}$$

if $\mathcal{B}[[b]]s = \text{ff}$

$$\frac{\langle S, s \rangle \rightarrow s' \quad \langle \text{while } b \text{ do } S, s' \rangle \rightarrow s''}{\langle \text{while } b \text{ do } S, s \rangle \rightarrow s''}$$

if $\mathcal{B}[[b]]s = \text{tt}$

$$\langle \text{while } b \text{ do } S, s \rangle \rightarrow s$$

if $\mathcal{B}[[b]]s = \text{ff}$

Structural operational semantics

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

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

$$\frac{\langle S_1, s \rangle \Rightarrow \langle S'_1, s' \rangle}{\langle S_1; S_2, s \rangle \Rightarrow \langle S'_1; S_2, s' \rangle}$$

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

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

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

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

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

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

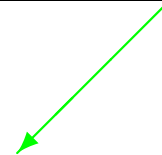
Proof obligations

if $\langle S, s \rangle \rightarrow s'$
then $\langle S, s \rangle \Rightarrow^* s'$

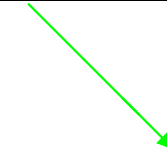


if $\langle S_1, s \rangle \Rightarrow^k s'$
then $\langle S_1; S_2, s \rangle \Rightarrow^k s'$

if $\langle S, s \rangle \Rightarrow^k s'$
then $\langle S, s \rangle \rightarrow s'$



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 $\langle \text{if } b \text{ then } (S; \text{while } b \text{ do } S) \text{ else skip}, s \rangle \rightarrow s'$
then $\langle \text{while } b \text{ do } S, s \rangle \rightarrow s'$

How robust are these results?

Extend the while language with

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

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:

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

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

- for natural semantics:

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

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

Adding parallelism

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

$$\frac{\langle S_1, s \rangle \Rightarrow \langle S'_1, s' \rangle}{\langle S_1 \text{ par } S_2, s \rangle \Rightarrow \langle S'_1 \text{ par } S_2, s' \rangle}$$

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

$$\frac{\langle S_2, s \rangle \Rightarrow \langle S'_2, s' \rangle}{\langle S_1 \text{ par } S_2, s \rangle \Rightarrow \langle S_1 \text{ par } S'_2, s' \rangle}$$

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

- for natural semantics:

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

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

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