Working example

For a while, we will work with a trivial iterative programming language:

TINY

- simple arithmetic expressions
- simple boolean expressions
- simple statements (assignment, conditional, loop)

Syntactic categories

- *numerals*

$$N \in \mathbf{Num}$$

with syntax given by:

$$N ::= 0 \mid 1 \mid 2 \mid \cdots$$

- *variables*

$$x \in \mathbf{Var}$$

with syntax given by:

$$x ::= \cdots \textit{ sequences of letters and digits beginning with a letter } \cdots$$

- *(arithmetic) expressions*

$$e \in \mathbf{Exp}$$

with syntax given by:

$$e ::= N \mid x \mid e_1 + e_2 \mid e_1 * e_2 \mid e_1 - e_2$$

- *boolean expressions*

$$\boxed{b \in \mathbf{BExp}}$$

with syntax given by:

$$b ::= \mathbf{true} \mid \mathbf{false} \mid e_1 \leq e_2 \mid \neg b' \mid b_1 \wedge b_2$$

- *statements*

$$\boxed{S \in \mathbf{Stmt}}$$

with syntax given by:

$$S ::= x := e \mid \mathbf{skip} \mid S_1; S_2 \mid \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2 \mid \mathbf{while}\ b\ \mathbf{do}\ S'$$

Before we move on

(to the semantics)

The definition of syntax, like:

- *(arithmetic) expressions*

$$e \in \mathbf{Exp}$$

with syntax given by:

$$e ::= N \mid x \mid e_1 + e_2 \mid e_1 * e_2 \mid e_1 - e_2$$

implies that each expression is of exactly one of the forms given above, all these forms are distinct, and all the expressions can be built by using the above constructs consecutively.

Things can be defined and proved by

(STRUCTURAL) INDUCTION

Structural induction

Given a property $P(\_)$ of expressions:

IF

- $P(N)$, for all $N \in \mathbf{Num}$
- $P(x)$, for all $x \in \mathbf{Var}$
- $P(e_1 + e_2)$ follows from $P(e_1)$ and $P(e_2)$, for all $e_1, e_2 \in \mathbf{Exp}$
- $P(e_1 * e_2)$ follows from $P(e_1)$ and $P(e_2)$, for all $e_1, e_2 \in \mathbf{Exp}$
- $P(e_1 - e_2)$ follows from $P(e_1)$ and $P(e_2)$, for all $e_1, e_2 \in \mathbf{Exp}$

THEN

- $P(e)$ for all $e \in \mathbf{Exp}$.

Inductive definitions

Free variables in expressions $FV(e) \subset \mathbf{Var}$:

$$
\begin{aligned}
FV(N) &= \emptyset \\
FV(x) &= \{x\} \\
FV(e_1 + e_2) &= FV(e_1) \cup FV(e_2) \\
FV(e_1 * e_2) &= FV(e_1) \cup FV(e_2) \\
FV(e_1 - e_2) &= FV(e_1) \cup FV(e_2)
\end{aligned}
$$

Fact: *For each expression $e \in \mathbf{Exp}$, the set $FV(e)$ of its free variables is finite.*

Easy proof by structural induction

Semantic categories

Easy things first:

- *boolean values*

  $$\mathbf{Bool} = \{\mathbf{tt}, \mathbf{ff}\}$$

- *integers*

  $$\mathbf{Int} = \{0, 1, -1, 2, -2, \ldots\}$$

  with the obvious semantic function:

$$\mathcal{N} : \mathbf{Num} \to \mathbf{Int}$$

$$\mathcal{N}[\![0]\!] = 0$$
$$\mathcal{N}[\![1]\!] = 1$$
$$\mathcal{N}[\![2]\!] = 2$$
$$\ldots$$

BTW: $\_[\![\_]\!]$ is just a semantic function application, with $[\![\ ]\!]$ used to separate syntactic phrases from the semantic context.

Valuations of variables

- *states* (for now: total functions from **Var** to **Int**)

  $$s \in \mathbf{State} = \mathbf{Var} \to \mathbf{Int}$$

  – lookup (of the value of a variable x in a state s) is function application

  $$s\, x$$

  $s(x)$ often written as $s\, x$

  – update a state: $s' = s[y \mapsto n]$

  $$s'\, x = \begin{cases} s\, x & \text{if } x \neq y \\ n & \text{if } x = y \end{cases}$$

Semantics of expressions

$$\mathcal{E} : \mathbf{Exp} \to (\mathbf{State} \to \mathbf{Int})$$

defined in the obvious way:

$$\begin{aligned}
\mathcal{E}[\![N]\!]\, s &= \mathcal{N}[\![N]\!] \\
\mathcal{E}[\![x]\!]\, s &= s\, x \\
\mathcal{E}[\![e_1 + e_2]\!]\, s &= \mathcal{E}[\![e_1]\!]\, s + \mathcal{E}[\![e_2]\!]\, s \\
\mathcal{E}[\![e_1 * e_2]\!]\, s &= \mathcal{E}[\![e_1]\!]\, s * \mathcal{E}[\![e_2]\!]\, s \\
\mathcal{E}[\![e_1 - e_2]\!]\, s &= \mathcal{E}[\![e_1]\!]\, s - \mathcal{E}[\![e_2]\!]\, s
\end{aligned}$$

BTW: Higher-order functions will be used very frequently!

No further warnings!

Semantics of boolean expressions

$$\mathcal{B}\colon \mathbf{BExp} \to (\mathbf{State} \to \mathbf{Bool})$$

defined in the obvious way:

$$\mathcal{B}[\![\mathbf{true}]\!]\, s = \mathbf{tt}$$

$$\mathcal{B}[\![\mathbf{false}]\!]\, s = \mathbf{ff}$$

$$\mathcal{B}[\![e_1 \leq e_2]\!]\, s = \begin{cases} \mathbf{tt} & \text{if } \mathcal{E}[\![e_1]\!]\, s \leq \mathcal{E}[\![e_2]\!]\, s \\ \mathbf{ff} & \text{if } \mathcal{E}[\![e_1]\!]\, s \not\leq \mathcal{E}[\![e_2]\!]\, s \end{cases}$$

$$\mathcal{B}[\![\neg b]\!]\, s = \begin{cases} \mathbf{ff} & \text{if } \mathcal{B}[\![b]\!]\, s = \mathbf{tt} \\ \mathbf{tt} & \text{if } \mathcal{B}[\![b]\!]\, s = \mathbf{ff} \end{cases}$$

$$\mathcal{B}[\![b_1 \wedge b_2]\!]\, s = \begin{cases} \mathbf{tt} & \text{if } \mathcal{B}[\![b_1]\!]\, s = \mathbf{tt} \text{ and } \mathcal{B}[\![b_2]\!]\, s = \mathbf{tt} \\ \mathbf{ff} & \text{if } \mathcal{B}[\![b_1]\!]\, s = \mathbf{ff} \text{ or } \mathcal{B}[\![b_2]\!]\, s = \mathbf{ff} \end{cases}$$

Before we move on

(to the semantics of statements)

Fact: *The meaning of expression depends only on the valuation of its free variables: for any* $e \in \mathbf{Exp}$ *and* $s, s' \in \mathbf{State}$, *if* $s\,x = s'\,x$ *for all* $x \in FV(e)$ *then*

$$\mathcal{E}[\![e]\!]\,s = \mathcal{E}[\![e]\!]\,s'.$$

Proof in a moment...

Exercise: *Formulate (and prove) this property for boolean expressions.*

Proof

Thesis: *if* $s\,x = s'\,x$ *for all* $x \in FV(e)$ *then* $\mathcal{E}[\![e]\!]\,s = \mathcal{E}[\![e]\!]\,s'$

By structural induction:

- for $N \in \mathbf{Num}$, $\mathcal{E}[\![N]\!]\,s = \mathcal{N}[\![N]\!]$
  $= \mathcal{E}[\![N]\!]\,s'$
- for $x \in \mathbf{Var}$, $\mathcal{E}[\![x]\!]\,s = s\,x$
  $= s'\,x$ (since $x \in FV(x)$)
  $= \mathcal{E}[\![x]\!]\,s'$
- for $e_1, e_2 \in \mathbf{Exp}$, $\mathcal{E}[\![e_1 + e_2]\!]\,s = \mathcal{E}[\![e_1]\!]\,s + \mathcal{E}[\![e_2]\!]\,s$
  $= \mathcal{E}[\![e_1]\!]\,s' + \mathcal{E}[\![e_2]\!]\,s'$ (by the inductive hypothesis, since $FV(e_1) \subseteq FV(e_1 + e_2)$, and similarly for e_2)
  $= \mathcal{E}[\![e_1 + e_2]\!]\,s'$
- ...

Referential transparency...

Substitution of e' for x in e results in $e[e'/x]$:

$$
\begin{aligned}
N[e'/x] &= N \\
x'[e'/x] &= \begin{cases} e' & \text{if } x = x' \\ x' & \text{if } x \neq x' \end{cases} \\
(e_1 + e_2)[e'/x] &= e_1[e'/x] + e_2[e'/x] \\
(e_1 * e_2)[e'/x] &= e_1[e'/x] * e_2[e'/x] \\
(e_1 - e_2)[e'/x] &= e_1[e'/x] - e_2[e'/x]
\end{aligned}
$$

Prove:

$$\mathcal{E}[\![e[e'/x]]\!]\, s = \mathcal{E}[\![e]\!]\, s[x \mapsto \mathcal{E}[\![e']\!]\, s]$$

Semantics of statements

This will be given in various styles to illustrate various approaches to formal semantics.

Consider the previous definitions as auxiliary

Operational semantics

small-step semantics

1960's abstract machines: Landin, McCarthy, VDL
1981 SOS: Plotkin

Overall idea:

- define *configurations*: $\gamma \in \Gamma$
- indicate which of them are *terminal*: $\mathrm{T} \subseteq \Gamma$
- define a *(one-step) transition relation*: $\Rightarrow \subseteq \Gamma \times \Gamma$
  - for $\gamma \in \mathrm{T}$, assume $\gamma \not\Rightarrow$
- study *computations*: (finite or infinite) sequences of configurations

$$\gamma_0, \gamma_1, \ldots, \gamma_i, \gamma_{i+1}, \ldots,$$

such that $\gamma_i \Rightarrow \gamma_{i+1}$, written as:

$$\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_i \Rightarrow \gamma_{i+1} \Rightarrow \cdots$$

Computations

Maximal computations may be:

- terminating: $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_n$, $\gamma_n \in \mathrm{T}$
- blocking: $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_n$, $\gamma_n \notin \mathrm{T}$ and $\gamma_n \not\Rightarrow$
- infinite (looping): $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots$

Moreover:

- $\gamma \Rightarrow^k \gamma'$ for $k \geq 0$, if there is a computation $\gamma = \gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_k = \gamma'$
- $\gamma \Rightarrow^* \gamma'$ if $\gamma \Rightarrow^k \gamma'$ for some $k \geq 0$

BTW: $\Rightarrow^* \subseteq \Gamma \times \Gamma$ is the least reflexive and transitive relation that contains $\Rightarrow$.

TINY: operational semantics

Configurations: $\Gamma = (\mathbf{Stmt} \times \mathbf{State}) \cup \mathbf{State}$

Terminal configurations: $\mathrm{T} = \mathbf{State}$

Transition relation contains only:

$$\langle x := e, s\rangle \Rightarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$$

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

$$\langle S_1; S_2, s\rangle \Rightarrow \langle S_1'; S_2, s'\rangle \quad \text{if } \langle S_1, s\rangle \Rightarrow \langle S_1', s'\rangle$$

$$\langle S_1; S_2, s\rangle \Rightarrow \langle S_2, s'\rangle \quad \text{if } \langle S_1, s\rangle \Rightarrow s'$$

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

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

$$\langle \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow \langle S; \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \quad \text{if } \mathcal{B}[\![b]\!]\, s = \mathbf{tt}$$

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

Rules to derive transitions

$$\frac{}{\langle x := e, s\rangle \Rightarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]} \qquad \frac{}{\langle \mathbf{skip}, s\rangle \Rightarrow s}$$

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

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

$$\frac{\mathcal{B}[\![b]\!]\, s = \mathbf{tt}}{\langle \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow \langle S; \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle} \qquad \frac{\mathcal{B}[\![b]\!]\, s = \mathbf{ff}}{\langle \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow s}$$

Notational variants:

- axioms vs. rules without premises: $\langle \mathbf{skip}, s\rangle \Rightarrow s$
- side-conditions vs. premises: $\dfrac{}{\langle \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow s}$ if $\mathcal{B}[\![b]\!]\, s = \mathbf{ff}$

Some properties

Fact: TINY *is deterministic, i.e.: for each configuration* $\langle S, s\rangle$

$$\textit{if } \langle S, s\rangle \Rightarrow \gamma_1 \textit{ and } \langle S, s\rangle \Rightarrow \gamma_2 \textit{ then } \gamma_1 = \gamma_2.$$

Proof: By structural induction on S.

Fact: *In* TINY, *for each configuration* $\langle S, s\rangle$ *there is exactly one maximal computation starting in* $\langle S, s\rangle$.

Another proof technique:

Induction on the length of computation

On nondeterminism of computations

Nondeterministic small-step semantics for arithmetic expressions: $\Gamma = \mathbf{Exp} \times \mathbf{State}$

$$\frac{}{\langle x, s\rangle \Rightarrow \langle N, s\rangle} \text{ if } \mathcal{N}[\![N]\!] = s\, x$$

$$\frac{\langle e_1, s\rangle \Rightarrow \langle e_1', s'\rangle}{\langle e_1 + e_2, s\rangle \Rightarrow \langle e_1' + e_2, s'\rangle} \qquad \frac{\langle e_2, s\rangle \Rightarrow \langle e_2', s'\rangle}{\langle e_1 + e_2, s\rangle \Rightarrow \langle e_1 + e_2', s'\rangle}$$

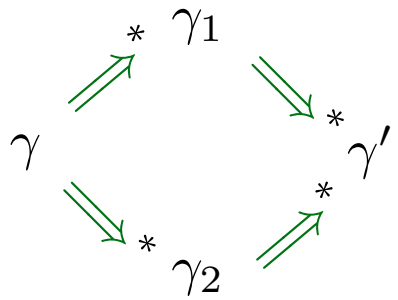
"numerals" for negative integers needed

$$\frac{}{\langle N_1 + N_2, s\rangle \Rightarrow \langle M, s\rangle} \text{ if } \mathcal{N}[\![N_1]\!] + \mathcal{N}[\![N_2]\!] = \mathcal{N}[\![M]\!]$$

BUT: $\cdots$ and similarly for $e_1 * e_2$ and $e_1 - e_2 \cdots$

Fact: *if* $\langle e, s\rangle \Rightarrow^* \langle N, s'\rangle$ *and* $\langle e, s\rangle \Rightarrow^* \langle N', s''\rangle$ *then* $\mathcal{N}[\![N]\!] = \mathcal{N}[\![N']\!]$ *(and* $s = s' = s''$*).*

Include "semantic" integers as expressions and modify the semantics above

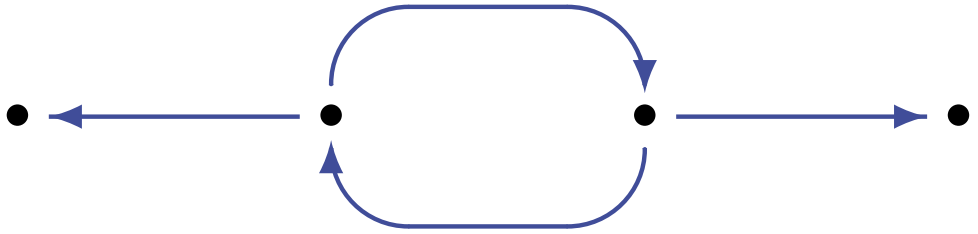


Church-Rosser property

Confluence: if $\gamma \Rightarrow^* \gamma_1$ and $\gamma \Rightarrow^* \gamma_2$ then $\gamma_1 \Rightarrow^* \gamma'$ and $\gamma_2 \Rightarrow^* \gamma'$ for some γ'

Weak confluence: if $\gamma \Rightarrow \gamma_1$ and $\gamma \Rightarrow \gamma_2$ then $\gamma_1 \Rightarrow^* \gamma'$ and $\gamma_2 \Rightarrow^* \gamma'$ for some γ'

Warning: weak confluence does not entail confluence:



Fact: *If $\Rightarrow \subseteq \Gamma \times \Gamma$ is strongly normalizing (i.e., no infinite computations) and is weakly confluent then it is confluent.*

Newman's Lemma

Two more properties

Fact: *If* $\langle S_1; S_2, s\rangle \Rightarrow^k s'$ *then* $\langle S_1, s\rangle \Rightarrow^{k_1} \hat{s}$ *and* $\langle S_2, \hat{s}\rangle \Rightarrow^{k_2} s'$, *for some* $\hat{s} \in \mathbf{State}$ *and* $k_1, k_2 > 0$ *such that* $k = k_1 + k_2$.

Proof: By induction on k:

$k = 0$: OK

$k > 0$: Then $\langle S_1; S_2, s\rangle \Rightarrow \gamma \Rightarrow^{k-1} s'$. By the definition of the transitions, two possibilities only:

- $\gamma = \langle S_2, \hat{s}\rangle$, where $\langle S_1, s\rangle \Rightarrow \hat{s}$. OK
- $\gamma = \langle S_1'; S_2, s''\rangle$, where$\langle S_1, s\rangle \Rightarrow \langle S_1', s''\rangle$. By the inductive hypothesis then, $\langle S_1', s''\rangle \Rightarrow^{k_1} \hat{s}$ and $\langle S_2, \hat{s}\rangle \Rightarrow^{k_2} s'$, for some $\hat{s} \in \mathbf{State}$ and $k_1, k_2 > 0$ such that $k - 1 = k_1 + k_2$. OK

Fact: *Further context does not influence computation:*

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

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

Some variants

- instead of the current rules for **if**:

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

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

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

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

- similarly for **while**, the first case
- instead of the current rules for **while**:

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

- ...

Natural semantics

big-step operational semantics

mid 1980's: Gilles Kahn

Overall idea:

- define *configurations*: $\gamma \in \Gamma$
- indicate which of them are *terminal*: $\mathrm{T} \subseteq \Gamma$
- instead of computations, consider (define) *transitions* directly *to final configurations* that are reached by computations: $\rightsquigarrow \subseteq \Gamma \times \mathrm{T}$

Informally:

– if $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_n$, $\gamma_n \in \mathrm{T}$, then $\gamma_0 \rightsquigarrow \gamma_n$

– if $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_n$, $\gamma_n \notin \mathrm{T}$ and $\gamma_n \not\Rightarrow$, then $\gamma_0 \not\rightsquigarrow$

– if $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \cdots$ then $\gamma_0 \not\rightsquigarrow$

TINY: natural semantics

$$\langle x := e, s\rangle \rightsquigarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$$

$$\langle \mathbf{skip}, s\rangle \rightsquigarrow s$$

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

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

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

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

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

Configurations:

$\Gamma = (\mathbf{Stmt} \times \mathbf{State}) \cup \mathbf{State}$

Terminal configurations: as before

$\mathrm{T} = \mathbf{State}$

Transitions: as given here

How to read this?

"set-theoretically"

As before:

$\rightsquigarrow \subseteq \Gamma \times \mathrm{T}$ is the least relation such that

- $\langle x := e, s\rangle \rightsquigarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$, for all $x \in \mathbf{Var}$, $e \in \mathbf{Exp}$, $s \in \mathbf{State}$
- ...
- $\langle S_1; S_2, s\rangle \rightsquigarrow s''$ if $\langle S_1, s\rangle \rightsquigarrow s'$ and $\langle S_2, s'\rangle \rightsquigarrow s''$, for all $S_1, S_2 \in \mathbf{Stmt}$, $s, s', s'' \in \mathbf{State}$
- $\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, s\rangle \rightsquigarrow s'$ if $\langle S_1, s\rangle \rightsquigarrow s'$ and $\mathcal{B}[\![b]\!]\, s = \mathbf{tt}$, for all $b \in \mathbf{BExp}$, $S_1, S_2 \in \mathbf{Stmt}$, $s, s' \in \mathbf{State}$
- ...

How to read this?

"proof-theoretically"

We give

- axioms, like $\langle x := e, s\rangle \rightsquigarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$, and
- rules, like $$\frac{\langle S_1, s\rangle \rightsquigarrow s' \qquad \langle S_2, s'\rangle \rightsquigarrow s''}{\langle S_1; S_2, s\rangle \rightsquigarrow s''}$$

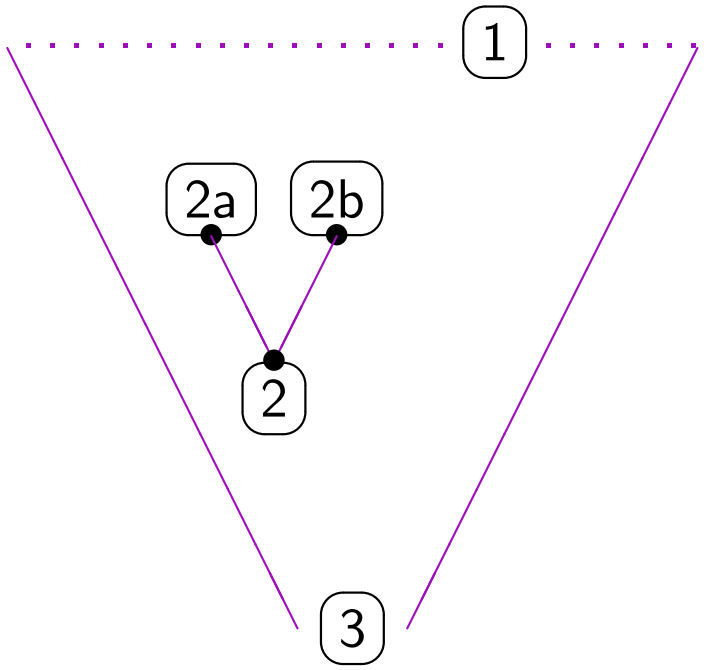
to *derive* (or better: *prove*) *judgements* of the form

$$\langle S, s\rangle \rightsquigarrow s'$$

Actually: we give axiom and rule *schemata*, which are *generic* in the choice of elements to be substituted for meta-variables used ($x \in \mathbf{Var}$, $e \in \mathbf{Exp}$, $s, s', s'' \in \mathbf{State}$, $S_1, S_2 \in \mathbf{Stmt}$, etc).

Proofs/derivations

Finite *proof tree* (or *derivation tree*):



- leaves: labelled by axioms, e.g.
  $\boxed{1}: \ \langle x := e, s\rangle \rightsquigarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$
- other nodes: labelled according to the rules, e.g.
  $$\frac{\boxed{2a}: \ \langle S_1, s\rangle \rightsquigarrow s' \qquad \boxed{2b}: \ \langle S_2, s'\rangle \rightsquigarrow s''}{\boxed{2}: \ \langle S_1; S_2, s\rangle \rightsquigarrow s''}$$
- root: judgement proved, e.g. $\boxed{3}: \ \langle S, s\rangle \rightsquigarrow s'$

We often write $\vdash \langle S, s\rangle \rightsquigarrow s'$ to indicate that there exists a proof of $\langle S, s\rangle \rightsquigarrow s'$.

Another proof technique

Induction on the structure of derivation trees

To prove if $\vdash \langle S, s\rangle \rightsquigarrow s'$ then $P(S, s, s')$ show:

- $P(x := e, s, s[x \mapsto (\mathcal{E}[\![e]\!]\, s)])$
- $P(\mathbf{skip}, s, s)$
- $P(S_1; S_2, s, s'')$ follows from $P(S_1, s, s')$ and $P(S_2, s', s'')$
- $P(\mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, s, s')$ follows from $P(S_1, s, s')$ whenever $\mathcal{B}[\![b]\!]\, s = \mathbf{tt}$
- $P(\mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, s, s')$ follows from $P(S_2, s, s')$ whenever $\mathcal{B}[\![b]\!]\, s = \mathbf{ff}$
- $P(\mathbf{while}\ b\ \mathbf{do}\ S, s, s'')$ follows from $P(S, s, s')$ and $P(\mathbf{while}\ b\ \mathbf{do}\ S, s', s'')$ whenever $\mathcal{B}[\![b]\!]\, s = \mathbf{tt}$
- $P(\mathbf{while}\ b\ \mathbf{do}\ S, s, s)$ whenever $\mathcal{B}[\![b]\!]\, s = \mathbf{ff}$

clarify quantification

Some properties

Fact: TINY *is deterministic, i.e.:*

$$\textit{for each } \vdash \langle S, s\rangle \rightsquigarrow s', \textit{ if } \vdash \langle S, s\rangle \rightsquigarrow s'' \textit{ then } s' = s''.$$

Proof: By (easy) induction on the proof of $\vdash \langle S, s\rangle \rightsquigarrow s'$.

BTW: Try also to prove this by induction on the structure of S — *is there a trouble?*

- structural induction fails here: the semantics of **while** is *not compositional*.

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

More on compositionality later

Semantic equivalence

Statements $S_1, S_2 \in \mathbf{Stmt}$ are *naturally equivalent* (equivalent w.r.t. the natural semantics)

$$S_1 \equiv_{\mathcal{NS}} S_2$$

if for all states $s, s' \in \mathbf{State}$,

$$\vdash \langle S_1, s\rangle \rightsquigarrow s' \quad \text{iff} \quad \vdash \langle S_2, s\rangle \rightsquigarrow s'$$

Fact: *For instance, the following can be proved by induction of the derivation:*

- $S; \mathbf{skip} \equiv_{\mathcal{NS}} \mathbf{skip}; S \equiv_{\mathcal{NS}} S$
- $(S_1; S_2); S_3 \equiv_{\mathcal{NS}} S_1; (S_2; S_3)$
- $\mathbf{while}\ b\ \mathbf{do}\ S \equiv_{\mathcal{NS}} \mathbf{if}\ b\ \mathbf{then}\ (S; \mathbf{while}\ b\ \mathbf{do}\ S)\ \mathbf{else}\ \mathbf{skip}$
- $\mathbf{if}\ b\ \mathbf{then}\ (\mathbf{if}\ b'\ \mathbf{then}\ S_1\ \mathbf{else}\ S_1')\ \mathbf{else}\ S_2$
  $\equiv_{\mathcal{NS}} \mathbf{if}\ b \wedge b'\ \mathbf{then}\ S_1\ \mathbf{else}\ (\mathbf{if}\ b \wedge \neg b'\ \mathbf{then}\ S_1'\ \mathbf{else}\ S_2)$

Congruence properties

Fact: *The semantic equivalence is preserved by the linguistic constructs:*

- *if* $S_1 \equiv_{\mathcal{NS}} S_1'$ *and* $S_2 \equiv_{\mathcal{NS}} S_2'$ *then*

$$S_1; S_2 \equiv_{\mathcal{NS}} S_1'; S_2'$$

- *if* $S_1 \equiv_{\mathcal{NS}} S_1'$ *and* $S_2 \equiv_{\mathcal{NS}} S_2'$ *then*

$$\textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2 \equiv_{\mathcal{NS}} \textbf{if } b \textbf{ then } S_1' \textbf{ else } S_2'$$

- *if* $S \equiv_{\mathcal{NS}} S'$ *then*

$$\textbf{while } b \textbf{ do } S \equiv_{\mathcal{NS}} \textbf{while } b \textbf{ do } S'$$

BTW: This can be extended to incorporate a similarly defined equivalence for expressions and boolean expressions.

Operational vs. natural semantics for TINY

"They are essentially the same"

Fact: *The two semantics are equivalent w.r.t. the final results described:*

$$\vdash \langle S, s\rangle \rightsquigarrow s' \quad \text{iff} \quad \langle S, s\rangle \Rightarrow^* s'$$

for all statements $S \in \mathbf{Stmt}$ *and states* $s, s' \in \mathbf{State}$.

Proof:

"$\Longrightarrow$": By induction on the structure of the derivation for $\langle S, s\rangle \rightsquigarrow s'$.

"$\Longleftarrow$": By induction on the length of the computation $\langle S, s\rangle \Rightarrow^* s'$.

"$\Longrightarrow$": By induction on the structure of the derivation for $\langle S, s\rangle \rightsquigarrow s'$.

- $\langle x := e, s\rangle \Rightarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$. OK
- $\langle \mathbf{skip}, s\rangle \Rightarrow s$. OK
- Suppose $\langle S_1, s\rangle \rightsquigarrow s'$ and $\langle S_2, s'\rangle \rightsquigarrow s''$, so that $\langle S_1, s\rangle \Rightarrow^* s'$ and $\langle S_2, s'\rangle \Rightarrow^* s''$. Then $\langle S_1; S_2, s\rangle \Rightarrow^* \langle S_2, s'\rangle \Rightarrow^* s''$. OK
- Suppose $\mathcal{B}[\![b]\!]\, s = \mathbf{tt}$ and $\langle S_1, s\rangle \rightsquigarrow s'$, so that $\langle S_1, s\rangle \Rightarrow^* s'$. Then $\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, s\rangle \Rightarrow \langle S_1, s\rangle \Rightarrow^* s'$. OK
- Suppose $\mathcal{B}[\![b]\!]\, s = \mathbf{ff}$ and $\langle S_2, s\rangle \rightsquigarrow s'$, so that $\langle S_2, s\rangle \Rightarrow^* s'$. Then $\langle \mathbf{if}\ b\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2, s\rangle \Rightarrow \langle S_2, s\rangle \Rightarrow^* s'$. OK
- Suppose $\mathcal{B}[\![b]\!]\, s = \mathbf{tt}$ and $\langle S, s\rangle \rightsquigarrow s'$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ S, s'\rangle \rightsquigarrow s''$, so that $\langle S, s\rangle \Rightarrow^* s'$ and $\langle \mathbf{while}\ b\ \mathbf{do}\ S, s'\rangle \Rightarrow^* s''$. Then $\langle \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow \langle S; \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow^* \langle \mathbf{while}\ b\ \mathbf{do}\ S, s'\rangle \Rightarrow^* s''$. OK
- If $\mathcal{B}[\![b]\!]\, s = \mathbf{ff}$ then $\langle \mathbf{while}\ b\ \mathbf{do}\ S, s\rangle \Rightarrow s$. OK

"$\Longleftarrow$": By induction on the length of the computation $\langle S, s\rangle \Rightarrow^* s'$.

$\langle S, s\rangle \Rightarrow^k s'$: Take $k > 0$ and $\boxed{\langle S, s\rangle \Rightarrow \gamma \Rightarrow^{k-1} s'}$. By cases on the first step (few sample cases only):

- $\langle x := e, s\rangle \Rightarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$. Then $s' = s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$;
  $\langle x := e, s\rangle \rightsquigarrow s[x \mapsto (\mathcal{E}[\![e]\!]\, s)]$. OK
- $\langle S_1; S_2, s\rangle \Rightarrow \langle S_1'; S_2, s''\rangle$, with $\langle S_1, s\rangle \Rightarrow \langle S_1', s''\rangle$.
  Then $\langle S_1'; S_2, s''\rangle \Rightarrow^{k-1} s'$, and so $\langle S_1', s''\rangle \Rightarrow^{k_1} \widehat{s''}$ and $\langle S_2, \widehat{s''}\rangle \Rightarrow^{k_2} s'$, for $k_1, k_2 > 0$ with $k_1 + k_2 = k - 1$. Hence also $\langle S_1, s\rangle \Rightarrow^{k_1+1} \widehat{s''}$.
  Then $\langle S_1, s\rangle \rightsquigarrow \widehat{s''}$ and $\langle S_2, \widehat{s''}\rangle \rightsquigarrow s'$, and so $\langle S_1; S_2, s\rangle \rightsquigarrow s'$. OK
- $\langle \textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2, s\rangle \Rightarrow \langle S_1, s\rangle$, with $\mathcal{B}[\![b]\!]\, s = \textbf{tt}$. Then
  $\langle S_1, s\rangle \Rightarrow^{k-1} s'$, so $\langle S_1, s\rangle \rightsquigarrow s'$ and $\langle \textbf{if } b \textbf{ then } S_1 \textbf{ else } S_2, s\rangle \rightsquigarrow s'$. OK
- $\langle \textbf{while } b \textbf{ do } S, s\rangle \Rightarrow \langle S; \textbf{while } b \textbf{ do } S, s\rangle$, with $\mathcal{B}[\![b]\!]\, s = \textbf{tt}$. Then
  $\langle S; \textbf{while } b \textbf{ do } S, s\rangle \Rightarrow^{k-1} s'$, hence $\langle S, s\rangle \Rightarrow^{k_1} \hat{s}$ and
  $\langle \textbf{while } b \textbf{ do } S, \hat{s}\rangle \Rightarrow^{k_2} s'$, for $k_1, k_2 > 0$ with $k_1 + k_2 = k - 1$. Thus
  $\langle S, s\rangle \rightsquigarrow \hat{s}$, $\langle \textbf{while } b \textbf{ do } S, \hat{s}\rangle \rightsquigarrow s'$, and so $\langle \textbf{while } b \textbf{ do } S, s\rangle \rightsquigarrow s'$. OK

"Denotational" semantics of statements

$$\mathcal{S}_{\mathcal{DO}} : \mathbf{Stmt} \to (\mathbf{State} \rightharpoonup \mathbf{State})$$

extracted from the natural or operational semantics as follows:

$$\mathcal{S}_{\mathcal{DO}}[\![S]\!]\, s = s' \;\text{ iff }\; \langle S, s\rangle \rightsquigarrow s' \quad (\text{ iff } \langle S, s\rangle \Rightarrow^* s')$$

BTW: TINY is deterministic, so this indeed defines a function

$$\mathcal{S}_{\mathcal{DO}}[\![S]\!] : \mathbf{State} \rightharpoonup \mathbf{State}$$

However, this function in general is *partial*.

So, in fact we define:

$$\mathcal{S}_{\mathcal{DO}}[\![S]\!]\, s = \begin{cases} s' & \text{if } \langle S, s\rangle \rightsquigarrow s', \text{ i.e. } \langle S, s\rangle \Rightarrow^* s' \\ \text{undefined} & \text{if } \langle S, s\rangle \not\rightsquigarrow \end{cases}$$

Operational vs. natural semantics

"They are quite different"

Natural semantics is more abstract than operational semantics

There are naturally equivalent statements with quite different sets of computations given by the operational semantics.

- Natural semantics disregards all computations that "block" or "loop".
- Natural semantics does not provide detailed view of computations.

Operational equivalence

Statements $S_1, S_2 \in \mathbf{Stmt}$ are *operationally equivalent* (equivalent w.r.t. the operational semantics)

$$S_1 \equiv_{\mathcal{OS}} S_2$$

if for all states $s \in \mathbf{State}$, $\langle S_1, s\rangle \sim \langle S_2, s\rangle$ for some relation $\sim \subseteq \Gamma \times \Gamma$ such that $s_1 \sim s_2$ iff $s_1 = s_2$, and for all $\gamma_1, \gamma_2 \in \mathbf{Stmt} \times \mathbf{State}$ such that $\gamma_1 \sim \gamma_2$

- if $\gamma_1 \Rightarrow \gamma_1'$ then $\gamma_2 \Rightarrow^* \gamma_2'$ for some γ_2' with $\gamma_1' \sim \gamma_2'$
- if $\gamma_2 \Rightarrow \gamma_2'$ then $\gamma_1 \Rightarrow^* \gamma_1'$ for some γ_1' with $\gamma_1' \sim \gamma_2'$

WEAK BISIMULATION

Fact: *If* $S_1 \equiv_{\mathcal{OS}} S_2$ *then* $S_1 \equiv_{\mathcal{NS}} S_2$

Equivalences given as examples for natural equivalence carry over here as well. In fact, for the language considered so far, natural and operational equivalence coincide.

Bisimulation in general

Consider a graph $\langle K, \rightarrow \rangle$ with "local observations" $\mathcal{O}(\kappa)$, for each $\kappa \in K$.

Definition: *$\rho \subseteq K \times K$ is a (strong) bisimulation on $\langle K, \rightarrow \rangle$ w.r.t. $\mathcal{O}(\_)$ if for all $\kappa_1, \kappa_2 \in K$ such that $\kappa_1 \; \rho \; \kappa_2$ we have $\mathcal{O}(\kappa_1) = \mathcal{O}(\kappa_2)$, and*

- *if $\kappa_1 \rightarrow \kappa_1'$ then $\kappa_2 \rightarrow \kappa_2'$ for some κ_2' with $\kappa_1' \; \rho \; \kappa_2'$*
- *if $\kappa_2 \rightarrow \kappa_2'$ then $\kappa_1 \rightarrow \kappa_1'$ for some κ_1' with $\kappa_1' \; \rho \; \kappa_2'$*

Two nodes $\kappa_1, \kappa_2 \in K$ are *(strongly) bisimilar*, written $\kappa_1 \approx \kappa_2$, if $\kappa_1 \; \rho \; \kappa_2$ for some bisimulation $\rho \subseteq K \times K$.

Fact: *$\approx \subseteq K \times K$ is an equivalence and bisimulation.*

Weak bisimilarity, as used for $\equiv_{\mathcal{OS}}$, is defined analogously

Fact: *Every bisimulation is a weak bisimulation, but not vice versa in general.*

Adding nondeterminism and blocking

Extend the (syntax for) statements $S \in \mathbf{Stmt}$ as follows:

$$S ::= \cdots \mid \mathbf{abort} \mid S_1 \ \mathbf{or} \ S_2$$

Operational semantics

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

Natural semantics

$$\frac{\langle S_1, s\rangle \rightsquigarrow s'}{\langle S_1 \ \mathbf{or} \ S_2, s\rangle \rightsquigarrow s'} \qquad \frac{\langle S_2, s\rangle \rightsquigarrow s'}{\langle S_1 \ \mathbf{or} \ S_2, s\rangle \rightsquigarrow s'}$$

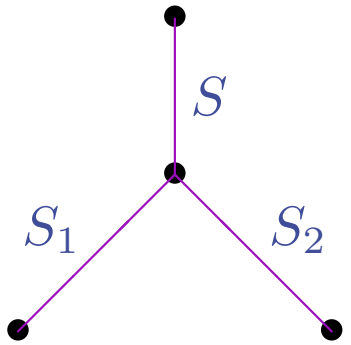
BTW: In either case, **abort** blocks (aborts?)...

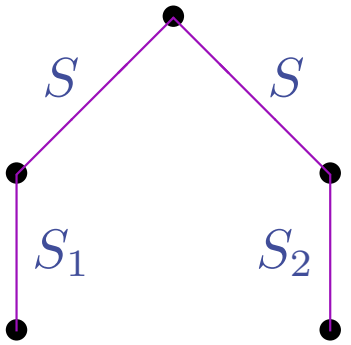
Looking at equivalences

- S_1 **or** $S_2 \equiv_{\mathcal{OS}} S_2$ **or** S_1
- **abort** $\equiv_{\mathcal{NS}}$ **while true do skip**
- **abort** $\equiv_{\mathcal{OS}}$ **while true do skip**

  BTW: this does not hold under (strong) bisimulation!
- S **or abort** $\equiv_{\mathcal{NS}} S$ (*angelic nondeterminism*)
- S **or abort** $\not\equiv_{\mathcal{OS}} S$ (unless $S \equiv_{\mathcal{OS}}$ **abort**)
- In general, the point of choice matters for operational equivalence:

  $S; (S_1$ **or** $S_2) \not\equiv_{\mathcal{OS}} (S; S_1)$ **or** $(S; S_2)$
- $S; (S_1$ **or** $S_2) \equiv_{\mathcal{NS}} (S; S_1)$ **or** $(S; S_2)$





Adding "parallelism"

Extend the statements $S \in \mathbf{Stmt}$ with a "parallel" (interleaving) construct:

$$S ::= \cdots \mid S_1 \parallel S_2$$

Operational semantics

$$\langle S_1 \parallel S_2, s\rangle \Rightarrow \langle S_1' \parallel S_2, s'\rangle \quad \text{if } \langle S_1, s\rangle \Rightarrow \langle S_1', s'\rangle$$

$$\langle S_1 \parallel S_2, s\rangle \Rightarrow \langle S_1 \parallel S_2', s'\rangle \quad \text{if } \langle S_2, s\rangle \Rightarrow \langle S_2', s'\rangle$$

Acceptable

Natural semantics

$$??? \frac{\langle S_1, s\rangle \rightsquigarrow s' \quad \langle S_2, s'\rangle \rightsquigarrow s''}{\langle S_1 \parallel S_2, s\rangle \rightsquigarrow s''} \qquad \frac{\langle S_1, s'\rangle \rightsquigarrow s'' \quad \langle S_2, s\rangle \rightsquigarrow s'}{\langle S_1 \parallel S_2, s\rangle \rightsquigarrow s''} ???$$

Makes no sense