CONVENTIONAL SEMANTIC APPROACHES

Grigore Rosu
CS522 – Programming Language Semantics
A language designer should understand the existing design approaches, techniques and tools, to know what is possible and how, or to come up with better ones. This part of the course will cover the major PL semantic approaches, such as:

- Big-step structural operational semantics (Big-step SOS)
- Small-step structural operational semantics (Small-step SOS)
- Denotational semantics
- Modular structural operational semantics (Modular SOS)
- Reduction semantics with evaluation contexts
- Abstract Machines
- The chemical abstract machine
- Axiomatic semantics
A simple imperative language
IMP – A Simple Imperative Language

We will exemplify the conventional semantic approaches by means of IMP, a very simple non-procedural imperative language, with

- Arithmetic expressions
- Boolean expressions
- Assignment statements
- Conditional statements
- While loop statements
- Blocks
IMP Syntax

\[
\begin{align*}
\text{Int} & ::= \text{the domain of (unbounded) integer numbers, with usual operations on them} \\
\text{Bool} & ::= \text{the domain of Booleans} \\
\text{Id} & ::= \text{standard identifiers} \\
\text{AExp} & ::= \text{Int} \\
& \quad | \quad \text{Id} \\
& \quad | \quad \text{AExp} + \text{AExp} \\
& \quad | \quad \text{AExp} / \text{AExp} \\
\text{BExp} & ::= \text{Bool} \\
& \quad | \quad \text{AExp} \leq \text{AExp} \\
& \quad | \quad ! \text{BExp} \\
& \quad | \quad \text{BExp} \&\& \text{BExp} \\
\text{Block} & ::= \{ \} \\
& \quad | \quad \{ \text{Stmt} \} \\
\text{Stmt} & ::= \text{Block} \\
& \quad | \quad \text{Id} = \text{AExp} ; \\
& \quad | \quad \text{Stmt} \text{Stmt} \\
& \quad | \quad \text{if}(\text{BExp}) \text{Block} \text{else} \text{Block} \\
& \quad | \quad \text{while}(\text{BExp}) \text{Block} \\
\text{Pgm} & ::= \text{int List}\{\text{Id}\} ; \text{Stmt}
\end{align*}
\]

Suppose that, for demonstration purposes, we want “+” and “/” to be non-deterministically strict, “\leq” to be sequentially strict, and “\&\&” to be short-circuited.
mod IMP-SYNTAX is including PL-INT + PL-BOOL + PL-ID .

--- AE

sort AE . subsorts Int Id < AE .
op _+_ : AE AE --> AE [prec 33 gather (E e) format (d b o d)] .
op _/- : AE AE --> AE [prec 31 gather (E e) format (d b o d)] .

--- BE

sort BE . subsort Bool < BE .
op _<__ : AE BE --> BE [prec 37 format (d b o d)] .
op !_ : BE --> BE [prec 53 format (b o d)] .
op _&__ : BE BE --> BE [prec 55 gather (E e) format (d b o d)] .

--- Block and Stmt

sorts Block Stmt . subsort Block < Stmt .
op { } -> Block [format (b b o)] .
op { _} : Stmt --> Block [format (d n+i n--i d)] .
op _-_ : Id AE --> Stmt [prec 40 format (d b o b o)] .
op _-_ : Stmt Stmt --> Stmt [prec 60 gather (e E) format (d ni d)] .
op if(_)_else_ : BE BE Block Block --> Stmt [prec 59 format (b so d d s nib o d)] .
op while(_)_ : BE Block --> Stmt [prec 59 format (b so d d s d)] .

--- Pgm

sort Pgm .
op int_:_ : List{Id} Stmt --> Pgm [prec 70 format (nb o d ni d)] .
endm
Most semantics need some notion of state. A state holds all the semantic ingredients to fully define the meaning of a given program or fragment of program.

For IMP, a state is a partial finite-domain function from identifiers to integers (i.e., a function defined only on a finite subset of identifiers and undefined on the rest), written using a half-arrow:

$$\sigma : Id \rightarrow \mathbb{Int}$$

We let State denote the set of such functions, and may write it

$$\left[ Id \rightarrow \mathbb{Int}\right]_{\text{finite}}$$

or

$$\text{Map}\left\{ Id \mapsto \mathbb{Int}\right\}$$
We may write states by enumerating each identifier binding. For example, the following state binds $x$ to 8 and $y$ to 0:

$$\sigma = x \mapsto 8, y \mapsto 0$$

Typical state operations are lookup, update and initialization.

- **Lookup**
  $$-(_): State \times Id \to Int$$

- **Update**
  $$-_[/-]: State \times Int \times Id \to State$$

- **Initialization**
  $$-_\mapsto -: List\{Id\} \times Int \to State$$
mod STATE is including PL-INT + PL-ID.
  sort State .

  op _|->_ : List{Id} Int -> State [prec 0] .
  op .State : -> State .
  op _&_ : State State -> State [assoc comm id: .State format(d s s d)] .

  op _(_) : State Id -> Int [prec 0] . --- lookup
  op _[_/_] : State Int Id -> State [prec 0] . --- update

var Sigma : State . var I I’ : Int . var X X’ : Id . var XL : List{Id} .

eq X |-> undefined = .State . --- "undefine" a state in a variable

eq (Sigma & X |-> I)(X) = I .
eq Sigma(X) = undefined [owise] .

  eq (Sigma & X |-> I)[I’ / X ] = (Sigma & X |-> I’) .
eq Sigma[I / X] = (Sigma & X |-> I) [owise] .

  eq (X,X’,XL) |-> I = X |-> I & X’ |-> I & XL |-> I .
eq .List{Id} |-> I = .State .
endm
BIG-STEP SOS
Big-Step Structural Operational Semantics (Big-Step SOS)

- Gilles Kahn (1987), under the name natural semantics. Also known as relational semantics, or evaluation semantics. We can regard a big-step SOS as a recursive interpreter, telling for a fragment of code and state what it evaluates to.

- **Configuration**: tuple containing code and semantic ingredients
  - E.g., \( \langle a_1, \sigma \rangle \), \( \langle a_1 + a_2, \sigma \rangle \), \( \langle i_1 \rangle \), \( \langle i_1 + \text{Int } i_2 \rangle \), \( \langle \sigma \rangle \)

- **Sequent**: Pair of configurations, to be derived or proved
  - E.g., \( \langle a_1, \sigma \rangle \Downarrow \langle i_1 \rangle \), \( \langle a_1 + a_2, \sigma \rangle \Downarrow \langle i_1 + \text{Int } i_2 \rangle \)

- **Rule**: Tells how to derive a sequent from others
  - E.g.,

\[
\frac{\langle a_1, \sigma \rangle \Downarrow \langle i_1 \rangle \quad \langle a_2, \sigma \rangle \Downarrow \langle i_2 \rangle}{\langle a_1 + a_2, \sigma \rangle \Downarrow \langle i_1 + \text{Int } i_2 \rangle}
\]

Read “evaluates to”
Big-Step SOS of IMP - Arithmetic

\[
\begin{align*}
\langle i, \sigma \rangle \downarrow \langle i \rangle \\
\langle x, \sigma \rangle \downarrow \langle \sigma(x) \rangle & \text{ if } \sigma(x) \neq \bot \\
\langle a_1, \sigma \rangle \downarrow \langle i_1 \rangle & \quad \langle a_2, \sigma \rangle \downarrow \langle i_2 \rangle \\
\langle a_1 + a_2, \sigma \rangle \downarrow \langle i_1 + \text{Int } i_2 \rangle \\
\langle a_1, \sigma \rangle \downarrow \langle i_1 \rangle & \quad \langle a_2, \sigma \rangle \downarrow \langle i_2 \rangle \\
\langle a_1 / a_2, \sigma \rangle \downarrow \langle i_1 / \text{Int } i_2 \rangle & \text{ if } i_2 \neq 0
\end{align*}
\]

State lookup

Read: “provided that \( a_1 \) evaluates to \( i_1 \) in \( \sigma \) and \( a_2 \) evaluates to \( i_2 \) in \( \sigma \), then \( a_1 + a_2 \) evaluates to the integer sum of \( i_1 \) and \( i_2 \) in \( \sigma \)”

Side condition ensures rule will never apply when \( a_2 \) evaluates to 0
Big-Step SOS of IMP - Boolean

\[
\begin{align*}
\langle t, \sigma \rangle &\downarrow \langle t \rangle \\
\langle a_1, \sigma \rangle &\downarrow \langle i_1 \rangle \quad \langle a_2, \sigma \rangle &\downarrow \langle i_2 \rangle \\
\langle a_1 \leq a_2, \sigma \rangle &\downarrow \langle i_1 \leq_{\text{Int}} i_2 \rangle \\
\langle b, \sigma \rangle &\downarrow \langle \text{true} \rangle \\
\langle \lnot b, \sigma \rangle &\downarrow \langle \text{false} \rangle \\
\langle b, \sigma \rangle &\downarrow \langle \text{false} \rangle \\
\langle \lnot b, \sigma \rangle &\downarrow \langle \text{true} \rangle \\
\langle b_1, \sigma \rangle &\downarrow \langle \text{false} \rangle \\
\langle b_1 \land b_2, \sigma \rangle &\downarrow \langle \text{false} \rangle \\
\langle b_1, \sigma \rangle &\downarrow \langle \text{true} \rangle \quad \langle b_2, \sigma \rangle &\downarrow \langle t \rangle \\
\langle b_1 \land b_2, \sigma \rangle &\downarrow \langle t \rangle
\end{align*}
\]
Big-Step SOS of IMP - Statements

\[
\begin{align*}
\langle \{\}, \sigma \rangle & \downarrow \langle \sigma \rangle & & (\text{BigStep-Empty-Block}) \\
\langle s, \sigma \rangle & \downarrow \langle \sigma' \rangle & \langle \{ s \}, \sigma \rangle & \downarrow \langle \sigma' \rangle & & (\text{BigStep-Block}) \\
\langle a, \sigma \rangle & \downarrow \langle i \rangle & \langle x = a; , \sigma \rangle & \downarrow \langle \sigma[i/x] \rangle & \text{if } \sigma(x) \neq \bot & (\text{BigStep-Asgn}) \\
\langle s_1, \sigma \rangle & \downarrow \langle \sigma_1 \rangle & \langle s_2, \sigma_1 \rangle & \downarrow \langle \sigma_2 \rangle & \langle s_1 \; s_2, \sigma \rangle & \downarrow \langle \sigma_2 \rangle & (\text{BigStep-Seq}) \\
\langle b, \sigma \rangle & \downarrow \langle \text{true} \rangle & \langle s_1, \sigma \rangle & \downarrow \langle \sigma_1 \rangle & \langle \text{if} \; (b) \; s_1 \; \text{else} \; s_2, \sigma \rangle & \downarrow \langle \sigma_1 \rangle & (\text{BigStep-If-True}) \\
\langle b, \sigma \rangle & \downarrow \langle \text{false} \rangle & \langle s_2, \sigma \rangle & \downarrow \langle \sigma_2 \rangle & \langle \text{if} \; (b) \; s_1 \; \text{else} \; s_2, \sigma \rangle & \downarrow \langle \sigma_2 \rangle & (\text{BigStep-If-False}) \\
\langle b, \sigma \rangle & \downarrow \langle \text{false} \rangle & \langle \text{while} \; (b) \; s, \sigma \rangle & \downarrow \langle \sigma \rangle & & (\text{BigStep-While-False}) \\
\langle b, \sigma \rangle & \downarrow \langle \text{true} \rangle & \langle s \; \text{while} \; (b) \; s, \sigma \rangle & \downarrow \langle \sigma' \rangle & \langle \text{while} \; (b) \; s, \sigma \rangle & \downarrow \langle \sigma' \rangle & (\text{BigStep-While-True})
\end{align*}
\]
Big-Step SOS of IMP - Programs

State initialization

\[
\frac{\langle s, x_l \leftarrow 0 \rangle \Downarrow \langle \sigma \rangle}{\langle \text{int } x_l; \ s \rangle \Downarrow \langle \sigma \rangle}
\]

\((\text{BigStep-Var})\)
Rules are schemas, allowing recursively enumerable many instances; side conditions filter out instances.

E.g., these are correct instances of the rule for division:

\[
\frac{\langle x, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 8 \rangle \quad \langle 2, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 2 \rangle}{\langle x/2, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 4 \rangle}
\]

\[
\frac{\langle x, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 8 \rangle \quad \langle 2, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 4 \rangle}{\langle x/2, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 2 \rangle}
\]

The second may look suspicious, but it is not. Normally, one should never be able to apply it, because one cannot prove its hypotheses.

However, the following is not a correct instance (no matter what \(?\) is):

\[
\frac{\langle x, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 8 \rangle \quad \langle y, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle 0 \rangle}{\langle x/y, (x \mapsto 8, y \mapsto 0) \rangle \downarrow \langle ? \rangle}
\]
The following is a valid proof derivation, or proof tree, using the big-step SOS proof system of IMP above. Suppose that \( x \) and \( y \) are identifiers and \( \sigma(x) = 8 \) and \( \sigma(y) = 0 \).
Big-Step SOS for Type Systems

- Big-Step SOS is routinely used to define type systems for programming languages.
- The idea is that a fragment of code $c$, in a given type environment $\Gamma$, can be assigned a certain type $\tau$. We typically write $\Gamma \vdash c : \tau$ instead of $\langle c, \Gamma \rangle \downarrow \langle \tau \rangle$.
- Since all variables in IMP have integer type, $\Gamma$ can be replaced by a list of untyped variables in our case. In general, however, a type environment $\Gamma$ contains typed variables, that is, pairs "$x : \tau$".
Typing Arithmetic Expressions

\[
\begin{align*}
xl & \leftarrow i : \text{int} \\
xl & \leftarrow x : \text{int} \quad \text{if } x \in xl \\
xl & \leftarrow a_1 : \text{int} \quad xl \leftarrow a_2 : \text{int} \\
xl & \leftarrow a_1 + a_2 : \text{int} \\
xl & \leftarrow a_1 : \text{int} \quad xl \leftarrow a_2 : \text{int} \\
xl & \leftarrow a_1 / a_2 : \text{int} \\
xl & \leftarrow t : \text{bool} \quad \text{if } t \in \{\text{true, false}\}
\end{align*}
\]

\begin{align*}
(\text{BigStepTypeSystem-Int}) \\
(\text{BigStepTypeSystem-Lookup}) \\
(\text{BigStepTypeSystem-Add}) \\
(\text{BigStepTypeSystem-Div}) \\
(\text{BigStepTypeSystem-Bool})
\end{align*}
Typing Boolean Expressions

\[
x l \leftarrow a_1 : \text{int} \quad \quad \quad x l \leftarrow a_2 : \text{int} \\
\frac{}{x l \leftarrow a_1 \leq a_2 : \text{bool}}
\]

\[
x l \leftarrow b : \text{bool} \\
\frac{}{x l \leftarrow \neg b : \text{bool}}
\]

\[
x l \leftarrow b_1 : \text{bool} \quad x l \leftarrow b_2 : \text{bool} \\
\frac{}{x l \leftarrow b_1 \&\& b_2 : \text{bool}}
\]

\[
x l \leftarrow \{\} : \text{block}
\]

(BigStepTypeSystem-Leq)

(BigStepTypeSystem-Not)

(BigStepTypeSystem-And)

(BigStepTypeSystem-Empty-Block)
Typing Statements

The type of $s$ can be either block or stmt

\[
\frac{x_l \leftarrow s \colon \tau}{x_l \leftarrow \{ s \} : \text{block}} \quad \text{if } \tau \in \{ \text{block}, \text{stmt} \}
\]

\[
\frac{x_l \leftarrow a : \text{int}}{x_l \leftarrow x = a : \text{stmt}} \quad \text{if } x \in x_l
\]

\[
\frac{x_l \leftarrow s_1 : \tau_1 \quad x_l \leftarrow s_2 : \tau_2}{x_l \leftarrow s_1 \ s_2 : \text{stmt}} \quad \text{if } \tau_1, \tau_2 \in \{ \text{block}, \text{stmt} \}
\]

\[
\frac{x_l \leftarrow b : \text{bool} \quad x_l \leftarrow s_1 : \text{block} \quad x_l \leftarrow s_2 : \text{block}}{x_l \leftarrow \text{if } (b) \ s_1 \text{ else } s_2 : \text{stmt}}
\]

\[
\frac{x_l \leftarrow b : \text{bool} \quad x_l \leftarrow s : \text{block}}{x_l \leftarrow \text{while } (b) \ s : \text{stmt}}
\]

(\text{BigStepTypeSystem-Block})

(\text{BigStepTypeSystem-Asgn})

(\text{BigStepTypeSystem-Seq})

(\text{BigStepTypeSystem-If})

(\text{BigStepTypeSystem-While})
Typing Programs

\[
\frac{x_l \leftarrow s : \tau}{\text{int } x_l; s : \text{pgm}} \quad \text{if } \tau \in \{\text{block, stmt}\}
\]
Big-Step SOS Type Derivation

Like the big-step rules for the concrete semantics of IMP, the ones for its type system are also rule schemas. We next show a proof derivation for the well-typed-ness of an IMP program that adds all the numbers from 1 to 100:

\[
\begin{align*}
\text{tree}_1 &\vdash (n, s \leftarrow (\text{while } (! (n \leq 0)) \{s = s + n; n = n + -1;\});) : \text{stmt} \\
&\vdash (n, s \leftarrow (n = 100; s = 0; \text{while } (! (n \leq 0)) \{s = s + n; n = n + -1;\});) : \text{stmt} \\
&\vdash (\text{int } n, s; n = 100; s = 0; \text{while } (! (n \leq 0)) \{s = s + n; n = n + -1;\});) : \text{pgm}
\end{align*}
\]

where
Big-Step SOS Type Derivation

\[
\begin{align*}
tree_1 &= \\
&= \left\{ \\
&\quad \frac{n, s \vdash 100 : \text{int}}{n, s \vdash (n = 100 ;) : \text{stmt}} \\
&\quad \frac{n, s \vdash 0 : \text{int}}{n, s \vdash (s = 0 ;) : \text{stmt}} \\
&\quad \frac{n, s \vdash (n = 100 ; s = 0 ;) : \text{stmt}}{n, s \vdash (n = 100 ; s = 0 ;) : \text{stmt}}
\right. \\

tree_2 &= \\
&= \left\{ \\
&\quad \frac{n, s \vdash n : \text{int}}{n, s \vdash 0 : \text{int}} \\
&\quad \frac{n, s \vdash (n \leq 0) : \text{bool}}{n, s \vdash (! (n \leq 0)) : \text{bool}}
\right. \\
\end{align*}
\]
Big-Step SOS Type Derivation

\[
\text{tree}_3 = \begin{cases}
\begin{array}{c}
\text{n, s} \vdash \text{s} : \text{int} \\
\text{n, s} \vdash \text{n} : \text{int} \\
\text{n, s} \vdash (\text{s} + \text{n}) : \text{int} \\
\text{n, s} \vdash (\text{s} = \text{s} + \text{n};) : \text{stmt} \\
\text{n, s} \vdash (\text{s} = \text{s} + \text{n}; \text{n} = \text{n} + -1;) : \text{stmt} \\
\text{n, s} \vdash \{ \text{s} = \text{s} + \text{n}; \text{n} = \text{n} + -1; \} : \text{block}
\end{array}
\end{cases}
\]
Any big-step SOS can be associated a rewrite logic theory (or, equivalently, a Maude module)

The idea is to associate to each big-step SOS rule

\[
\begin{array}{cccc}
C_1 & \Downarrow & R_1 \\
C_2 & \Downarrow & R_2 \\
\vdots & \vdots & \vdots \\
C_n & \Downarrow & R_n \\
\hline
C & \Downarrow & R
\end{array}
\]

[if condition]

a rewrite rule

\[
\overline{C} \rightarrow \overline{R} \text{ if } \overline{C_1} \rightarrow \overline{R_1} \land \overline{C_2} \rightarrow \overline{R_2} \land \ldots \land \overline{C_n} \rightarrow \overline{R_n} \text{ [\land condition]}
\]

(over-lining means “algebraization”)

Big-Step SOS in Rewriting Logic
SMALL-STEP SOS

Small-step structural operational semantics
Small-Step Structural Operational Semantics (Small-Step SOS)

- Gordon Plotkin (1981), under the name natural semantics
- Also known as transitional semantics, or reduction semantics
- One can regard a small-step SOS as a device capable of executing a program step-by-step

- **Configuration**: tuple containing code and semantic ingredients
  - E.g., \( \langle a, \sigma \rangle \quad \langle b, \sigma \rangle \quad \langle s, \sigma \rangle \quad \langle p \rangle \)

- **Sequent (transition)**: Pair of configurations, to be derived (proved)
  - E.g., \( \langle a_1, \sigma \rangle \rightarrow \langle a'_1, \sigma \rangle \quad \langle a_1 + a_2, \sigma \rangle \rightarrow \langle a'_1 + a_2, \sigma \rangle \)

- **Rule**: Tells how to derive a sequent from others
  - E.g.,

\[
\frac{\langle a_1, \sigma \rangle \rightarrow \langle a'_1, \sigma \rangle}{\langle a_1 + a_2, \sigma \rangle \rightarrow \langle a'_1 + a_2, \sigma \rangle}
\]
Small-Step SOS of IMP - Arithmetic

\[
\langle x, \sigma \rangle \rightarrow \langle \sigma(x), \sigma \rangle \quad \text{if } \sigma(x) \neq \bot
\]  

\[
\langle a_1, \sigma \rangle \rightarrow \langle a'_1, \sigma \rangle
\]

\[
\frac{\langle a_1 + a_2, \sigma \rangle \rightarrow \langle a'_1 + a_2, \sigma \rangle}{(\text{SmallStep-Add-Arg1})}
\]

\[
\langle a_2, \sigma \rangle \rightarrow \langle a'_2, \sigma \rangle
\]

\[
\frac{\langle a_1 + a_2, \sigma \rangle \rightarrow \langle a'_1 + a'_2, \sigma \rangle}{(\text{SmallStep-Add-Arg2})}
\]

\[
\langle i_1 + i_2, \sigma \rangle \rightarrow \langle i_1 + \text{Int } i_2, \sigma \rangle
\]

\[
(\text{SmallStep-Add})
\]

+ is non-deterministic (its arguments can evaluate in any order, and interleaved)
Side condition ensures rule will never apply when denominator is 0

/ is also non-deterministic
Small-Step SOS of IMP - Boolean

\[
\begin{align*}
\langle a_1, \sigma \rangle & \to \langle a'_1, \sigma \rangle \\
\langle a_1 \leq a_2, \sigma \rangle & \to \langle a'_1 \leq a_2, \sigma \rangle \\
\langle a_2, \sigma \rangle & \to \langle a'_2, \sigma \rangle \\
\langle i_1 \leq a_2, \sigma \rangle & \to \langle i_1 \leq a'_2, \sigma \rangle \\
\langle i_1 \leq i_2, \sigma \rangle & \to \langle i_1 \leq_{\text{Int}} i_2, \sigma \rangle
\end{align*}
\]

(SMALLSTEP-LEQ-ARG1)

(SMALLSTEP-LEQ-ARG2)

(SMALLSTEP-LEQ)

Ensures sequential strictness
Small-Step SOS of IMP - Boolean

\[
\begin{align*}
\langle b, \sigma \rangle &\rightarrow \langle b', \sigma \rangle \\
\langle \neg b, \sigma \rangle &\rightarrow \langle \neg b', \sigma \rangle & (\text{SMALLSTEP-NOT-ARG}) \\
\langle \neg \text{true}, \sigma \rangle &\rightarrow \langle \text{false}, \sigma \rangle & (\text{SMALLSTEP-NOT-TRUE}) \\
\langle \neg \text{false}, \sigma \rangle &\rightarrow \langle \text{true}, \sigma \rangle & (\text{SMALLSTEP-NOT-FALSE}) \\
\langle b_1, \sigma \rangle &\rightarrow \langle b'_1, \sigma \rangle \\
\langle b_1 \&\& b_2, \sigma \rangle &\rightarrow \langle b'_1 \&\& b_2, \sigma \rangle & (\text{SMALLSTEP-AND-ARG1}) \\
\langle \text{false} \&\& b_2, \sigma \rangle &\rightarrow \langle \text{false}, \sigma \rangle & (\text{SMALLSTEP-AND-FALSE}) \\
\langle \text{true} \&\& b_2, \sigma \rangle &\rightarrow \langle b_2, \sigma \rangle & (\text{SMALLSTEP-AND-TRUE})
\end{align*}
\]

Short-circuit semantics
Small-Step SOS Derivation

The following is a valid proof derivation, or proof tree, using the small-step SOS proof system for expressions of IMP above. Suppose that $x$ and $y$ are identifiers and $\sigma(x) = 1$. 

$\frac{\langle x, \sigma \rangle \rightarrow \langle 1, \sigma \rangle}{\langle y / x, \sigma \rangle \rightarrow \langle y / 1, \sigma \rangle}$

$\frac{\langle x + (y / x), \sigma \rangle \rightarrow \langle x + (y / 1), \sigma \rangle}{\langle (x + (y / x)) \leq x, \sigma \rangle \rightarrow \langle (x + (y / 1)) \leq x, \sigma \rangle}$
Small-Step SOS of IMP - Statements

\[\langle \{ s \}, \sigma \rangle \rightarrow \langle s, \sigma \rangle\]

\[\langle a, \sigma \rangle \rightarrow \langle a', \sigma \rangle\]

\[\langle x = a; , \sigma \rangle \rightarrow \langle x = a'; , \sigma \rangle\]

\[\langle x = i; , \sigma \rangle \rightarrow \langle \{ \}, \sigma'[i/x] \rangle \text{ if } \sigma(x) \neq \bot\]

\[\langle s_1, \sigma \rangle \rightarrow \langle s_1', \sigma' \rangle\]

\[\langle s_1 \ s_2, \sigma \rangle \rightarrow \langle s_1', s_2, \sigma' \rangle\]

\[\langle \{ \} \ s_2, \sigma \rangle \rightarrow \langle s_2, \sigma \rangle\]

(SMALLSTEP-BLOCK)

(SMALLSTEP-ASGN-ARG2)

(SMALLSTEP-ASGN)

(SMALLSTEP-SEQ-ARG1)

(SMALLSTEP-SEQ-EMPTY-BLOCK)
Small-Step SOS of IMP - Statements

\[
\begin{align*}
\langle b, \sigma \rangle & \rightarrow \langle b', \sigma \rangle \\
\langle \text{if} \ (b) \ s_1 \ \text{else} \ s_2, \sigma \rangle & \rightarrow \langle \text{if} \ (b') \ s_1 \ \text{else} \ s_2, \sigma \rangle \\
\langle \text{if} \ (\text{true}) \ s_1 \ \text{else} \ s_2, \sigma \rangle & \rightarrow \langle s_1, \sigma \rangle \\
\langle \text{if} \ (\text{false}) \ s_1 \ \text{else} \ s_2, \sigma \rangle & \rightarrow \langle s_2, \sigma \rangle \\
\langle \text{while} \ (b) \ s, \sigma \rangle & \rightarrow \langle \text{if} \ (b) \ \{ s \ \text{while} \ (b) \ s \} \ \text{else} \ \{ \}, \sigma \rangle \\
\langle \text{int} \ xl; \ s \rangle & \rightarrow \langle s, xl \leftarrow 0 \rangle
\end{align*}
\]

(SMALLSTEP-IF-ARG1)  (SMALLSTEP-IF-TRUE)  (SMALLSTEP-IF-FALSE)  (SMALLSTEP-WHILE)  (SMALLSTEP-VAR)
Small-Step SOS in Rewriting Logic

- Any small-step SOS can be associated with a rewrite logic theory (or, equivalently, a Maude module).
- The idea is to associate to each small-step SOS rule a rewrite rule:

\[
\begin{align*}
C_1 & \rightarrow C'_1 \\
C_2 & \rightarrow C'_2 \\
\vdots & \\
C_n & \rightarrow C'_n
\end{align*}
\]

\[
\overline{C} \rightarrow \overline{C}' \text{ if } \overline{C_1} \rightarrow \overline{C'_1} \land \overline{C_2} \rightarrow \overline{C'_2} \land \ldots \land \overline{C_n} \rightarrow \overline{C'_n} \quad [\land \text{ condition}]
\]

(the circle means “ready for one step”)
DENOTATIONAL

Denotational or fixed-point semantics
Denotational Semantics

- Christopher Strachey and Dana Scott (1970)
- Associate *denotation*, or meaning, to (fragments of) programs into *mathematical domains*; for example,
  - The denotation of an arithmetic expression in IMP is a *partial function from states to integer numbers*
    \[
    [\_]: \text{AExp} \rightarrow (\text{State} \rightarrow \text{Int})
    \]
  - The denotation of a statement in IMP is a *partial function from states to states*
    \[
    [\_]: \text{Stmt} \rightarrow (\text{State} \rightarrow \text{State})
    \]
Denotational Semantics

Christopher Strachey and Dana Scott (1970)

Denotation, or meaning, to (fragments of programs into) mathematical domains; for example,

- The denotation of an arithmetic expression in IMP is a partial function from states to integer numbers:
  \[ [-] : \text{AExp} \rightarrow (\text{State} \rightarrow \text{Int}) \]

- The denotation of a statement in IMP is a partial function from states to states:
  \[ [-] : \text{Stmt} \rightarrow (\text{State} \rightarrow \text{State}) \]

Partial because some expressions may be undefined in some states (e.g., division by zero)

Partial because some statements in some states may use undefined expressions, or may not terminate
Denotational Semantics - Terminology

- **Denotation (function)**
  - AExp $\rightarrow (State \rightarrow Int)$
  - Stmt $\rightarrow (State \rightarrow State)$

- **Fragment of program**
  - Mathematical domain
Once the right mathematical domains are chosen, giving a denotational semantics to a language should be a straightforward and compositional process; e.g.

\[
[a_1 + a_2]_\sigma = [a_1]_\sigma +_{\text{Int}} [a_2]_\sigma
\]

\[
[a_1 / a_2]_\sigma = \begin{cases} [a_1]_\sigma /_{\text{Int}} [a_2]_\sigma & \text{if } [a_2]_\sigma \neq 0 \\ \bot & \text{if } [a_2]_\sigma = 0 \end{cases}
\]

The hardest part is to give semantics to recursion. This is done using fixed-points.
Mathematical Domains

- Mathematical domains can be anything; it is common though that they are organized as complete partial orders with bottom element.
- The partial order structure captures the intuition of informativeness: \( a \leq b \) means \( a \) is less informative than \( b \). E.g., as a loop is executed, we get more and more information about its semantics.
- Completeness means that chains of more and more informative elements have a limit.
- The bottom element, written \( \bot \), stands for undefined, or no information at all.
Partial Orders

- Partial order \((D, \leq)\) is set \(D\) and binary rel. \(\leq\) which is
  - Reflexive: \(x \leq x\)
  - Transitive: \(x \leq y\) and \(y \leq z\) imply \(x \leq z\)
  - Anti-symmetric: \(x \leq y\) and \(y \leq x\) imply \(x = y\)

- Total order = partial order with \(x \leq y\) or \(y \leq x\)

- Important example: domains of partial functions

\[
(A \rightarrow B, \leq)
\]

\(f \leq g\) iff \(g\) defined everywhere \(f\) is defined and
\[
f(a) = g(a) \text{ whenever } f(a) \text{ is defined}
\]
(Least) Upper Bounds

- An upper bound (u.b.) of $X \subseteq D$ is any element $p \in D$ such that $x \leq p$ for any $x \in X$.

- The least upper bound (l.u.b.) of $X \subseteq D$, written $\sqcup X$, is an upper bound with $\sqcup X \leq q$ for any u.b. $q$.
  - When they exist, least upper bounds are unique.

- The domains of partial functions, $(A \rightarrow B, \leq)$, admit upper bounds and least upper bounds if and only if all the partial functions in the considered set are compatible: any two agree on any element in which both are defined.
Complete Partial Orders (CPO)

- A chain in $(D, \sqsubseteq)$ is an infinite sequence
  \[ d_0 \sqsubseteq d_1 \sqsubseteq d_2 \sqsubseteq \cdots \sqsubseteq d_n \sqsubseteq \cdots \]
  also written
  \[ \{ d_n \mid n \in \mathbb{N} \} \]

- Partial order $(D, \sqsubseteq)$ is a complete partial order (CPO) iff any of its chains admits a least upper bound

- $(D, \sqsubseteq, \bot)$ is a bottomed CPO (BCPO) iff $\bot$ is a minimal element of $D$, also called its bottom

- The domain of partial functions $(A \rightarrow B, \leq, \bot)$ is a BCPO, where $\bot$ is the partial function undefined everywhere
Monotone and Continuous Functions

- \( \mathcal{F} : (D, \sqsubseteq) \to (D', \sqsubseteq') \) monotone iff
  \[ x \sqsubseteq y \quad \text{implies} \quad \mathcal{F}(x) \sqsubseteq' \mathcal{F}(y) \]

- Monotone functions preserve chains:
  \[ \{d_n \mid n \in \mathbb{N}\} \text{ chain implies } \{\mathcal{F}(d_n) \mid n \in \mathbb{N}\} \text{ chain} \]

  - However, they do not always preserve l.u.b. of chains

- \( \mathcal{F} : (D, \sqsubseteq) \to (D', \sqsubseteq') \) continuous iff monotone and preserves l.u.b. of chains:
  \[ \sqcup \mathcal{F}(d_n) = \mathcal{F}(\sqcup d_n) \]

- \( Cont((D, \sqsubseteq, \bot), (D', \sqsubseteq', \bot')) \), the domain of continuous functions between two BCPOs, is itself a BCPO
**Fixed-Point Theorem**

- Let \((D, \sqsubseteq, \bot)\) be a BCPO and \(\mathcal{F} : (D, \sqsubseteq, \bot) \to (D, \sqsubseteq, \bot)\) be a continuous function. Then the l.u.b. of the chain \(\{\mathcal{F}^n(\bot) \mid n \in \mathbb{N}\}\) is the least fixed-point of \(\mathcal{F}\).

- Typically written \(\text{fix}(\mathcal{F})\)

- Proof sketch:

\[
\mathcal{F}(\text{fix}(\mathcal{F})) = \mathcal{F}(\bigsqcup_{n \in \mathbb{N}} \mathcal{F}^n(\bot)) \\
= \bigsqcup_{n \in \mathbb{N}} \mathcal{F}^{n+1}(\bot) \\
= \bigsqcup_{n \in \mathbb{N}} \mathcal{F}^n(\bot) \\
= \text{fix}(\mathcal{F}).
\]
Applications of Fixed-Point Theorem

- Consider the following “definition” of the factorial:

\[ f(n) = \begin{cases} 
1, & \text{if } n = 0 \\
 n \times f(n - 1), & \text{if } n > 0 
\end{cases} \]

- This is a recursive definition

  - Is it well-defined? Why?
  - Yes. Because it is the least fixed-point of the following continuous (prove it!) function from \(\mathbb{N} \to \mathbb{N}\) to itself

\[ \mathcal{F}(g)(n) = \begin{cases} 
1, & \text{if } n = 0 \\
 n \times g(n - 1), & \text{if } n > 0 \text{ and } g(n - 1) \text{ defined} \\
\text{undefined}, & \text{if } n > 0 \text{ and } g(n - 1) \text{ undefined}
\end{cases} \]
Denotational Semantics of IMP
Arithmetic Expressions

\[
\begin{align*}
\llbracket - \rrbracket &: AExp \to (State \to Int) \\
\llbracket i \rrbracket_\sigma &= i \\
\llbracket x \rrbracket_\sigma &= \sigma(x) \\
\llbracket a_1 + a_2 \rrbracket_\sigma &= \llbracket a_1 \rrbracket_\sigma + \text{Int} \llbracket a_2 \rrbracket_\sigma \\
\llbracket a_1 / a_2 \rrbracket_\sigma &= \begin{cases} \\
\llbracket a_1 \rrbracket_\sigma / \text{Int} \llbracket a_2 \rrbracket_\sigma & \text{if } \llbracket a_2 \rrbracket_\sigma \neq 0 \\
\bot & \text{if } \llbracket a_2 \rrbracket_\sigma = 0 \\
\end{cases}
\end{align*}
\]
Denotational Semantics of IMP

Boolean Expressions

\[
\sem{\_} : BExp \rightarrow (\text{State} \rightarrow \text{Bool})
\]

\[
\sem{t}\sigma = t
\]

\[
\sem{a_1 \leq a_2}\sigma = \sem{a_1}\sigma \leq_{\text{Int}} \sem{a_2}\sigma
\]

\[
\sem{\neg b}\sigma = \neg_{\text{Bool}}(\sem{b}\sigma)
\]

\[
\sem{b_1 \& \& b_2}\sigma = \begin{cases} 
\sem{b_2}\sigma & \text{if } \sem{b_1}\sigma = \text{true} \\
\text{false} & \text{if } \sem{b_1}\sigma = \text{false} \\
\bot & \text{if } \sem{b_1}\sigma = \bot
\end{cases}
\]
Denotational Semantics of IMP
Statements (without loops)

\[ \text{\texttt{[-]} : Stmt \rightarrow (State \rightarrow State)} \]

\[ \text{\texttt{[{}]}\sigma = \sigma} \]

\[ \text{\texttt{[\{} s \text{\texttt{)}}\sigma = [s]\sigma} \]

\[ \text{\texttt{[x = a ;]}\sigma = \begin{cases} \sigma[[a]\sigma/x] & \text{if } \sigma(x) \neq \bot \\ \bot & \text{if } \sigma(x) = \bot \end{cases}} \]

\[ \text{\texttt{[s_1 s_2]}\sigma = [s_2][s_1]\sigma} \]

\[ \text{\texttt{[if (b) s_1 else s_2]}\sigma = \begin{cases} [s_1]\sigma & \text{if } [b]\sigma = \text{true} \\ [s_2]\sigma & \text{if } [b]\sigma = \text{false} \\ \bot & \text{if } [b]\sigma = \bot \end{cases}} \]
Denotational Semantics of IMP

While

- We first define a continuous function as follows

\[ \mathcal{F} : (\text{State} \to \text{State}) \to (\text{State} \to \text{State}) \]

\[ \mathcal{F}(\alpha)(\sigma) = \begin{cases} \alpha(\alpha s) & \text{if } [b]_\sigma = \text{true} \\ \sigma & \text{if } [b]_\sigma = \text{false} \\ \bot & \text{if } [b]_\sigma = \bot \end{cases} \]

- Then we define the denotational semantics of while

\[ [\text{while } (b) \ s] = \text{fix}(\mathcal{F}) \]
Formalizing Denotational Semantics

- A denotational semantics is like a “compiler” of the defined programming language into mathematics.

- Formalizing denotational semantics in RL reduces to formalizing the needed mathematical domains:
  - Integers, Booleans, etc.
  - Functions (with cases) and function applications
  - Fixed-points

- Such mathematics is already available in functional programming languages, which makes them excellent candidates for denotational semantics!
Rewriting/equational logics do not have builtin functions and fixed-points, so they need be defined.

They are, however, easy to define using rewriting.

In fact, we do not need rewrite rules, all we need is equations to define these simple domains.

See next slide.
Functional CPO Domain

sorts:

\( \text{Var}_{\text{CPO}}, \ CPO \)

subsorts:

\( \text{Var}_{\text{CPO}}, \ \text{Bool} < \ CPO \)

operations:

\( \text{fun}_{\text{CPO}} \rightarrow \_ \) : \( \text{Var}_{\text{CPO}} \times \ CPO \rightarrow \ CPO \)

\( \text{app}_{\text{CPO}}(\_ , \_ ) \) : \( \ CPO \times \ CPO \rightarrow \ CPO \)

\( \text{fix}_{\text{CPO}} \_ \) : \( \ CPO \rightarrow \ CPO \)

\( \text{if}_{\text{CPO}}(\_ , \_ , \_ ) \) : \( \ CPO \times \ CPO \times \ CPO \rightarrow \ CPO \)

equations:

\( \text{app}_{\text{CPO}}(\text{fun}_{\text{CPO}} \ V \rightarrow \ C, C') = C[C'/V] \)

\( \text{fix}_{\text{CPO}} \ \text{fun}_{\text{CPO}} \ V \rightarrow \ C = C[((\text{fix}_{\text{CPO}} \ \text{fun}_{\text{CPO}} \ V \rightarrow \ C)/V] \)

\( \text{if}_{\text{CPO}}(\text{true}, C, C') = C \)

\( \text{if}_{\text{CPO}}(\text{false}, C, C') = C' \)
Denotational Semantics of IMP in RL

Signature

sort:

Syntax

// generic sort for syntax

subsorts:

AExp, BExp, Stmt, Pgm < Syntax  // syntactic categories fall under Syntax
Int, Bool, State < CPO          // basic domains are regarded as CPOs

operation:

⟦·⟧ : Syntax → CPO

// denotation of syntax
Denotational Semantics of IMP in RL

Arithmetic Expressions

\[
\begin{align*}
\llbracket I \rrbracket &= \text{fun}_{\text{CPO}} \sigma \to I \\
\llbracket X \rrbracket &= \text{fun}_{\text{CPO}} \sigma \to \sigma(X) \\
\llbracket A_1 + A_2 \rrbracket &= \text{fun}_{\text{CPO}} \sigma \to \text{app}_{\text{CPO}}([A_1], \sigma) +_{\text{Int}} \text{app}_{\text{CPO}}([A_2], \sigma) \\
\llbracket A_1 / A_2 \rrbracket &= \text{fun}_{\text{CPO}} \sigma \to \text{if}_{\text{CPO}}(\text{app}_{\text{CPO}}([A_2], \sigma) \neq_{\text{Int}} 0, \text{app}_{\text{CPO}}([A_1], \sigma) /_{\text{Int}} \text{app}_{\text{CPO}}([A_2], \sigma), \bot)
\end{align*}
\]
Denotational Semantics of IMP in RL

Boolean Expressions

\[ [T] = \text{fun}_{\text{CPO}} \sigma \rightarrow T \]

\[ [A_1 \leq A_2] = \text{fun}_{\text{CPO}} \sigma \rightarrow \text{app}_{\text{CPO}}([A_1], \sigma) \leq_{\text{Int}} \text{app}_{\text{CPO}}([A_2], \sigma) \]

\[ [\neg B] = \text{fun}_{\text{CPO}} \sigma \rightarrow \neg_{\text{Bool}} \text{app}_{\text{CPO}}([B], \sigma) \]

\[ [B_1 \&\& B_2] = \text{fun}_{\text{CPO}} \sigma \rightarrow \text{if}_{\text{CPO}}(\text{app}_{\text{CPO}}([B_1], \sigma), \text{app}_{\text{CPO}}([B_2], \sigma), \text{false}) \]
Denotational Semantics of IMP in RL

Statements and Programs

\[
\begin{align*}
\llbracket \{} \rrbracket &= \text{fun}_{\text{CPO}} \sigma \rightarrow \sigma \\
\llbracket \{ S \} \rrbracket &= \text{fun}_{\text{CPO}} \sigma \rightarrow \text{app}_{\text{CPO}}(\llbracket S \rrbracket, \sigma) \\
\llbracket X = A; \rrbracket &= \text{fun}_{\text{CPO}} \sigma \rightarrow \text{app}_{\text{CPO}}(\text{fun}_{\text{CPO}} \text{arg} \rightarrow \text{if}_{\text{CPO}}(\sigma(X) \neq \bot, \sigma[\text{arg}/X], \bot), \text{app}_{\text{CPO}}(\llbracket A \rrbracket, \sigma)) \\
\llbracket S_1 S_2 \rrbracket &= \text{fun}_{\text{CPO}} \sigma \rightarrow \text{app}_{\text{CPO}}(\llbracket S_2 \rrbracket, \text{app}_{\text{CPO}}(\llbracket S_1 \rrbracket, \sigma)) \\
\llbracket \text{if} (B) S_1 \text{else} S_2 \rrbracket &= \text{fun}_{\text{CPO}} \sigma \rightarrow \text{if}_{\text{CPO}}(\text{app}_{\text{CPO}}(\llbracket B \rrbracket, \sigma), \text{app}_{\text{CPO}}(\llbracket S_1 \rrbracket, \sigma), \text{app}_{\text{CPO}}(\llbracket S_2 \rrbracket, \sigma)) \\
\llbracket \text{while} (B) S \rrbracket &= \text{fix}_{\text{CPO}} \text{fun}_{\text{CPO}} \alpha \rightarrow \text{fun}_{\text{CPO}} \sigma \rightarrow \text{if}_{\text{CPO}}(\text{app}_{\text{CPO}}(\llbracket B \rrbracket, \sigma), \text{app}_{\text{CPO}}(\alpha, \text{app}_{\text{CPO}}(\llbracket S \rrbracket, \sigma)), \sigma) \\
\llbracket \text{int} X!; S \rrbracket &= \text{app}_{\text{CPO}}(\llbracket S \rrbracket, (X! \mapsto 0))
\end{align*}
\]
MSOS

Modular structural operational semantics
Modular Structural Operational Semantics (Modular SOS, or MSOS)

- Peter Mosses (1999)
- Addresses the non-modularity aspects of SOS
  - A definitional framework is non-modular when, in order to add a new feature to an existing language, one needs to revisit and change some of the already defined, unrelated language features
  - The non-modularity of SOS becomes clear when we define IMP++
- Why modularity is important
  - Modifying existing rules when new rules are added is error prone
  - When experimenting with language design, one needs to make changes quickly; having to do unrelated changes slows us down
  - Rapid language development, e.g., domain-specific languages
Philosophy of MSOS

- Separate the syntax from configurations and treat it differently
- Transitions go from syntax to syntax, hiding the other configuration components into transition labels
- Labels encode all the non-syntactic configuration changes
- Specialized notation in transition labels, to
  - Say that certain configuration components stay unchanged
  - Say that certain configuration changes are propagated from the premise to the conclusion of a rule
An MSOS transition has the form

\[ P \xrightarrow{\Delta} P' \]

- \( P \) and \( P' \) are programs or fragments of program
- \( \Delta \) is a label describing the changes in the configuration components, defined as a record; primed fields stay for “after” the transition

Example:

\[ x := i \xrightarrow{\{\text{state}=\sigma, \text{state'}=\sigma[i/x], \ldots\}} \text{skip} \quad \text{if } \sigma(x) \neq \bot \]

This rule can be automatically “desugared” into the SOS rule

\[ \langle x := i, \sigma \rangle \rightarrow \langle \text{skip}, \sigma[i/x] \rangle \quad \text{if } \sigma(x) \neq \bot \]

But also into (if the configuration contains more components, like in IMP++)

\[ \langle x := i, \sigma, \omega \rangle \rightarrow \langle \text{skip}, \sigma[i/x], \omega \rangle \quad \text{if } \sigma(x) \neq \bot \]
Labels are field assignments, or records, and can use “…” for “and so on”, called *record comprehension*.

Fields can be primed or not.
- Unprimed = configuration component *before* the transition is applied
- Primed = configuration component *after* the transition is applied

Some fields appear both unprimed and primed (called read-write), while others appear only primed (called write-only) or only unprimed (called read-only).
Field types

- Read/write = fields which appear both unprimed and unprimed

\[
x := i \quad \{\text{state}=\sigma, \text{state}'=\sigma[i/x], \ldots\} \quad \text{skip} \quad \text{if } \sigma(x) \neq \bot
\]

- Write-only = fields which appear only primed

\[
\text{print } i \quad \{\text{output}'=i, \ldots\} \quad \text{skip}
\]

- Read-only = fields which appear only unprimed

\[
\begin{align*}
\text{let } x = v_1 \text{ in } e_2 \quad \{\text{env}=\rho, \ldots\} \quad \text{let } x = v_1 \text{ in } e'_2
\end{align*}
\]
MSOS Rules

- Like in SOS, but using MSOS transitions as sequents
- Same labels or parts of them can be used multiple times in a rule
- Example:

\[
\frac{s_1 \xrightarrow{\Delta} s'_1}{s_1 \rightarrow s'_1}
\]

\[
\frac{s_1 \xrightarrow{\Delta} s'_1}{s_1 \land s_2 \rightarrow s'_1 \land s_2}
\]

- Same $\Delta$ means that changes propagate from premise to conclusion
- The author of MSOS now promotes a simplifying notation
  - If the premise and the conclusion repeat the same label or part of it, simply drop that label or part of it. For example:

\[
\frac{s_1 \rightarrow s'_1}{s_1 \land s_2 \rightarrow s'_1 \land s_2}
\]
**MSOS of IMP - Arithmetic**

\[
\begin{align*}
\{\text{state}=\sigma, \ldots\} \xrightarrow{x} \sigma(x) \quad \text{if } \sigma(x) \neq \bot \\
\frac{a_1 \rightarrow a'_1}{a_1 + a_2 \rightarrow a'_1 + a_2} \quad \text{(MSOS-Add-Arg1)} \\
\frac{a_2 \rightarrow a'_2}{a_1 + a_2 \rightarrow a_1 + a'_2} \quad \text{(MSOS-Add-Arg2)} \\
i_1 + i_2 \rightarrow i_1 +_{\text{int}} i_2 \quad \text{(MSOS-Add)}
\end{align*}
\]
MSOS of IMP - Arithmetic

\[
\frac{a_1 \rightarrow a'_1}{a_1 / a_2 \rightarrow a'_1 / a_2}
\]

\[
\frac{a_2 \rightarrow a'_2}{a_1 / a_2 \rightarrow a_1 / a'_2}
\]

\[
i_1 / i_2 \rightarrow i_1 /_{\text{Int}} i_2 \quad \text{if } i_2 \neq 0
\]

\[(\text{MSOS-Div-Arg1})\]

\[(\text{MSOS-Div-Arg2})\]

\[(\text{MSOS-Div})\]
**MSOS of IMP - Boolean**

\[
\begin{align*}
\frac{a_1 \rightarrow a'_1}{a_1 \leq a_2 \rightarrow a'_1 \leq a_2} & \quad (\text{MSOS-Leq-Arg1}) \\
\frac{a_2 \rightarrow a'_2}{i_1 \leq a_2 \rightarrow i_1 \leq a'_2} & \quad (\text{MSOS-Leq-Arg2}) \\
i_1 \leq i_2 \rightarrow i_1 \leq_{\text{Int}} i_2 & \quad (\text{MSOS-Leq})
\end{align*}
\]
MSOS of IMP - Boolean

\[ b \rightarrow b' \]
\[
\frac{\text{not } b}{\text{not } b'}
\]

not true → false

not false → true

\[ b_1 \rightarrow b'_1 \]
\[
\frac{b_1 \text{ and } b_2}{b'_1 \text{ and } b_2}
\]

false and \( b_2 \) → false

true and \( b_2 \) → \( b_2 \)

(MSOS-Not-Arg)

(MSOS-Not-True)

(MSOS-Not-False)

(MSOS-And-Arg1)

(MSOS-And-False)

(MSOS-And-True)
MSOS of IMP - Statements

\[
\frac{a \rightarrow a'}{x := a \rightarrow x := a'}
\]  
\[
\frac{\{\text{state}=\sigma, \text{state}'=\sigma[i/x], \ldots\}}{x := i \quad \text{skip} \quad \text{if } \sigma(x) \neq 1}
\]  
\[
\frac{s_1 \rightarrow s_1'}{s_1; s_2 \rightarrow s_1'; s_2}
\]  
\[
\frac{\text{skip} \quad \text{if } \sigma(x) \neq 1}{s_2 \rightarrow s_2}
\]
**MSOS of IMP - Statements**

\[
\begin{align*}
    & b \rightarrow b' \\
    \text{if } b \text{ then } s_1 \text{ else } s_2 \rightarrow \text{ if } b' \text{ then } s_1 \text{ else } s_2 \\
    \text{if true then } s_1 \text{ else } s_2 \rightarrow s_1 \\
    \text{if false then } s_1 \text{ else } s_2 \rightarrow s_2 \\
    \text{while } b \text{ do } s \rightarrow \text{ if } b \text{ then } (s; \text{ while } b \text{ do } s) \text{ else } \text{ skip} \\
    \text{var } x_l; s \rightarrow \text{ s} \\
\end{align*}
\]

\text{(MSOS-IF-ARG1)} \quad \text{(MSOS-IF-TRUE)} \quad \text{(MSOS-IF-FALSE)} \quad \text{(MSOS-WHILE)} \quad \text{(MSOS-VAR)}
Any MSOS can be associated a rewrite logic theory (or, equivalently, a Maude module)

Idea:
- Desugar MSOS into SOS
- Apply the SOS-to-rewriting-logic representation, but
- Hold the non-syntactic configuration components in an ACI-data-structure, so that we can use ACI matching to retrieve only the fields of interest (which need to be read or written to)
MSOS of IMP in Maude

- See file
  - `imp-semantics-msos.maude`
RSEC

Reduction semantics with evaluation contexts
Reduction Semantics with Evaluation Contexts (RSEC)

- Matthias Felleisen and collaborators (1992)
- Previous operational approaches encoded the program execution context as a proof context, by means of rule conditions or premises
  - This has a series of advantages, but makes it hard to define control intensive features, such as abrupt termination, exceptions, call/cc, etc.
- We would like to have the execution context explicit, so that we can easily save it, change it, or even delete it
- Reduction semantics with evaluation contexts does precisely that
  - It allows to formally define *evaluation contexts*
  - Rules become mostly *unconditional*
  - Reductions can only happen “in context”
Splitting and Plugging

- RSEC relies on reversible implicit mechanisms to
  - Split syntax into an evaluation context and a redex
  - Plug a redex into an evaluation contexts and obtain syntax again

\[
p = c[e]
\]
Evaluation Contexts

- Evaluation contexts are typically defined by the same means that we use to define the language syntax, that is, grammars.
- The hole □ represents the place where redex is to be plugged.
- Example:

\[
\text{Context} ::= \square \\
\quad \text{Context} <= AExp \\
\quad \text{Int} <= \text{Context} \\
\quad \text{Id} ::= \text{Context} \\
\quad \text{Context} ; \text{Stmt} \\
\quad \text{if Context then Stmt else Stmt} \\
\ldots
\]
Correct Evaluation Contexts

\[ 3 \leq □ \]

\[ □ \leq 3 \]

\[ □ ; x := 5 \]

\[ \text{if } □ \text{ then } s_1 \text{ else } s_2 \]
Wrong Evaluation Contexts

\[
\square \leq \square \\
x \leq 3 \\
x \leq \square \\
x := 5 ; \square \\
\square := 5 \\
\text{if } x \leq 7 \text{ then } \square \text{ else } x := 5
\]
Splitting/Plugging of Syntax

\[ 7 = (\square)[7] \]

\[ 3 \leq x = (3 \leq \square)[x] = (\square \leq x)[3] \]
\[ = (\square)[3 \leq x] \]

\[ 3 \leq (2 + x) + 7 = (3 \leq \square + 7)[2 + x] \]
\[ = (\square \leq (2 + x) + 7)[3] \]
\[ = \ldots \]
The characteristic rule of RSEC allows us to only define semantic rules stating how redexes are reduced.

- This significantly reduces the number of rules.
- The semantic rules are mostly unconditional (no premises).
- The overall result is a semantics which is compact and easy to read and understand.
# RSEC of IMP – Evaluation Contexts

<table>
<thead>
<tr>
<th>IMP evaluation contexts syntax</th>
<th>IMP language syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong> ::= □</td>
<td><strong>AExp</strong> ::= <strong>Int</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AExp + AExp</strong></td>
</tr>
<tr>
<td><strong>Context + AExp</strong></td>
<td><strong>AExp / AExp</strong></td>
</tr>
<tr>
<td><strong>Context / AExp</strong></td>
<td><strong>not BExp</strong></td>
</tr>
<tr>
<td><strong>Context &lt;= AExp</strong></td>
<td><strong>BExp and BExp</strong></td>
</tr>
<tr>
<td><strong>Int &lt;= Context</strong></td>
<td>** Stmt ; Stmt**</td>
</tr>
<tr>
<td><strong>not Context</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Context and BExp</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Id := Context</strong></td>
<td><strong>Stmt</strong> ::= <strong>Id := AExp</strong></td>
</tr>
<tr>
<td><strong>Context ; Stmt</strong></td>
<td><strong>if BExp then Stmt else Stmt</strong></td>
</tr>
<tr>
<td><strong>if Context then Stmt else Stmt</strong></td>
<td><strong>while BExp do Stmt</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Pgm</strong> ::= <strong>var List</strong>{<strong>Id</strong>} ; <strong>Stmt</strong></td>
</tr>
</tbody>
</table>
RSEC of IMP — Rules

\[
\text{Context ::= } \ldots \mid \langle \text{Context}, \text{State} \rangle
\]

\[
e \rightarrow e' \\
\overline{c[e] \rightarrow c[e']}
\]

\[
\langle c, \sigma \rangle[x] \rightarrow \langle c, \sigma \rangle[\sigma(x)] \quad \text{if } \sigma(x) \neq \bot
\]

\[
i_1 + i_2 \rightarrow i_1 +_{\text{Int}} i_2
\]

\[
i_1 / i_2 \rightarrow i_1 /_{\text{Int}} i_2 \quad \text{if } i_2 \neq 0
\]

\[
i_1 \leq_{\text{Int}} i_2
\]

\[
\text{not true } \rightarrow \text{false}
\]

\[
\text{not false } \rightarrow \text{true}
\]

\[
\text{true and } b_2 \rightarrow b_2
\]

\[
\text{false and } b_2 \rightarrow \text{false}
\]

\[
\langle c, \sigma \rangle[x := i] \rightarrow \langle c, \sigma[i/x] \rangle[\text{skip}] \quad \text{if } \sigma(x) \neq \bot
\]

\[
\text{skip } ; s_2 \rightarrow s_2
\]

\[
\text{if true then } s_1 \text{ else } s_2 \rightarrow s_1
\]

\[
\text{if false then } s_1 \text{ else } s_2 \rightarrow s_2
\]

\[
\text{while } b \text{ do } s \rightarrow \text{if } b \text{ then } (s ; \text{while } b \text{ do } s) \text{ else } \text{skip}
\]

\[
\langle \text{var } x_l ; s \rangle \rightarrow \langle s, (x_l \mapsto 0) \rangle
\]
RSEC Derivation

\[
\langle\boxed{x := 1}; y := 2; \text{ if } x \leq y \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 0, y \mapsto 0)\rangle
\]

\rightarrow \langle\boxed{\text{skip}}; y := 2; \text{ if } x \leq y \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 0)\rangle

\rightarrow \langle y := 2; \text{ if } x \leq y \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 0)\rangle

\rightarrow \langle\text{skip}; \text{ if } x \leq y \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 2)\rangle

\rightarrow \langle\text{if } x \leq y \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 2)\rangle

\rightarrow \langle\text{if } 1 \leq y \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 2)\rangle

\rightarrow \langle\text{if } 1 \leq 2 \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 2)\rangle

\rightarrow \langle\text{if } \text{true} \text{ then } x := 0 \text{ else } y := 0, (x \mapsto 1, y \mapsto 2)\rangle

\rightarrow \langle x := 0, (x \mapsto 1, y \mapsto 2)\rangle

\rightarrow \langle\text{skip}, (x \mapsto 0, y \mapsto 2)\rangle
Like with the other styles, RSEC can also be faithfully represented in rewriting logic and, implicitly, in Maude.

However, RSEC is context sensitive, while rewriting logic is not (rewriting logic allows rewriting strategies, but one can still not match and modify the context, as we can do in RSEC).

We therefore need

- A mechanism to achieve context sensitivity (the splitting/plugging) in rewriting logic
- Use that mechanism to represent the characteristic rule of RSEC
Evaluation Contexts in Rewriting Logic

- An evaluation context CFG production in RSEC has the form

\[ \text{Context} ::= \pi(N_1, \ldots, N_n, \text{Context}) \]

- Associate to each such production one rule and one equation:

\[
\begin{align*}
\text{split}(\pi(T_1, \ldots, T_n, T)) & \rightarrow \pi(T_1, \ldots, T_n, C)[\text{Syn}] \text{ if } \text{split}(T) \rightarrow C[\text{Syn}] \\
\text{plug}(\pi(T_1, \ldots, T_n, C)[\text{Syn}]) & = \pi(T_1, \ldots, T_n, \text{plug}(C[\text{Syn}]))
\end{align*}
\]

- Plus, we add one generic rule and one generic equation:

\[
\begin{align*}
\text{split}(\text{Syn}) & \rightarrow \Box[\text{Syn}] \\
\text{plug}(\Box[\text{Syn}]) & = \text{Syn}
\end{align*}
\]
IMP Examples:

- For productions

\[
\begin{align*}
\text{Context} & ::= \quad \text{Context} <= AExp \\
& \quad | \quad \text{Int} <= \text{Context} \\
& \quad | \quad \text{Id} ::= \text{Context}
\end{align*}
\]

we add the following rewrite logic rules and equations:

\[
\begin{align*}
\text{split}(A_1 <= A_2) & \rightarrow (C <= A_2)[\text{Syn}] \quad \text{if} \quad \text{split}(A_1) \rightarrow C[\text{Syn}] \\
\text{plug}((C <= A_2)[\text{Syn}]) &= \text{plug}(C[\text{Syn}]) <= A_2 \\
\text{split}(I_1 <= A_2) & \rightarrow (I_1 <= C)[\text{Syn}] \quad \text{if} \quad \text{split}(A_2) \rightarrow C[\text{Syn}] \\
\text{plug}((I_1 <= C)[\text{Syn}]) &= I_1 <= \text{plug}(C[\text{Syn}]) \\
\text{split}(X ::= A) & \rightarrow (X ::= C)[\text{Syn}] \quad \text{if} \quad \text{split}(A) \rightarrow C[\text{Syn}] \\
\text{plug}((X ::= C)[\text{Syn}]) &= X ::= \text{plug}(C[\text{Syn}])
\end{align*}
\]
RSEC Reduction Rules in Rewriting Logic

// for each term $l$ that appears as the left-hand side of a reduction rule
// "\(l(c_1[l_1], \ldots, c_n[l_n]) \rightarrow \ldots\)”, add the following conditional
// rewrite rule (there could be one $l$ for many reduction rules):

$$\circ \bar{l}(T_1, \ldots, T_n) \rightarrow T \ \text{if} \ \text{plug}(\circ \bar{l}(\text{split}(T_1), \ldots, \text{split}(T_n))) \rightarrow T$$

// for each non-identity term $r$ appearing as right-hand side in a reduction rule
// "\(\ldots \rightarrow r(c_1[r_1], \ldots, c_n[r_n])\)”, add the following equation
// (there could be one $r$ for many reduction rules):

$$\text{plug}(\bar{r}(\text{Syn}_1, \ldots, \text{Syn}_n)) = \bar{r}(\text{plug}(\text{Syn}_1), \ldots, \text{plug}(\text{Syn}_n))$$

// for each reduction semantics rule “\(l(c_1[l_1], \ldots, c_n[l_n]) \rightarrow r(c'_1[r_1], \ldots, c'_n[r_n'])\)”
// add the following “semantic” rewrite rule:

$$\circ \bar{l}(c_1[l_1], \ldots, c_n[l_n]) \rightarrow \bar{r}(c'_1[r_1], \ldots, c'_n[r_n'])$$
IMP Examples

- One rule of first kind
  \[ \text{plug} \circ \text{split}(\text{Cfg}) \rightarrow \text{Cfg}' \]

- No need for equations of second kind

- Characteristic rule of RSEC:
  \[ C[\text{Syn}] \rightarrow C[\text{Syn}'] \quad \text{if} \quad C \neq \square \land \text{plug} \circ \text{Syn} \rightarrow \text{Syn}' \]

- The remaining rules are as natural as can be:
  \[ \circ I_1 \leq I_2 \rightarrow I_1 \leq_{\text{Int}} I_2 \]
  \[ \circ \text{skip} ; S_2 \rightarrow S_2 \]
  \[ \circ \text{if true then } S_1 \text{ else } S_2 \rightarrow S_1 \]
RSEC of IMP in Maude

- See file
  - imp-split-plug.maude

- See files
  - imp-semantics-evaluation-contexts-1.maude
  - imp-semantics-evaluation-contexts-2.maude
  - imp-semantics-evaluation-contexts-3.maude
CHAM

The chemical abstract machine
The Chemical Abstract Machine (CHAM)

- Berry and Boudol (1992)
- Both a model of concurrency and a specific semantic style
- Chemical metaphor
  - States regarded as chemical solutions containing floating molecules
  - Molecules can interact with each other by means of reactions
  - Reactions take place concurrently, unrestricted by context
  - Solutions are encapsulated within new molecules, using membranes
    - The following is a solution containing $k$ molecules:
      $$\{m_1, m_2, \ldots, m_k\}$$
**CHAM Syntax and Rules**

\[
\begin{align*}
    \text{Molecule} &::= \text{Solution} \\
    & \mid \text{Molecule} \bowtie \text{Solution} \\
    \text{Solution} &::= \text{Bag}\{\text{Molecule}\}
\end{align*}
\]
CHAM Rules

- Ordinary rewrite rules between solution terms:
  \[ m_1 \ m_2 \ldots \ m_k \rightarrow m'_1 \ m'_2 \ldots m'_l \]

- Rewriting takes place only within solutions

- Three (metaphoric) kinds of rules
  - *Heating* rules using \( \rightarrow \) : structurally rearrange solution
  - *Cooling* rules using \( \rightarrow \) : clean up solution after reactions
  - *Reaction* rules using \( \rightarrow \) : change solution irreversibly
CHAM Airlock

- Allows to extract molecules from encapsulated solutions
- Governed by two rules coming in a heating/cooling pair:

\[ \{m_1, m_2, \ldots, m_k\} \Leftrightarrow \{m_1 \triangleleft \{m_2, \ldots, m_k\}\} \]
CHAM Molecule Configuration for IMP

- A top-level solution containing two subsolution molecules
  - One for holding the syntax
  - Another for holding the state

\[
\{ \{ \text{Syntax} \} \quad \{ \text{State} \} \}
\]

- Example:

\[
\{ \{ x := (3 / (x + 2)) \} \quad \{ x \mapsto 1 \quad y \mapsto 0 \} \}
\]
Airlock can be Problematic

- Airlock cannot be used to encode evaluation strategies; heating/cooling rules of the form

\[
x := a \iff a \triangleleft \{ x := \Box \}
\]
\[
a_1 + a_2 \iff a_1 \triangleleft \{ \Box + a_2 \}
\]
\[
a_1 + a_2 \iff a_2 \triangleleft \{ a_1 + \Box \}
\]

are problematic, because they yield ambiguity, e.g.,

\[
\{ x := (3 / (x + 2)) \} \iff x := ((3 / x) + 2)
\]
Correct Representation of Syntax

- Other attempts fail, too (see the lecture notes)
- We need some mechanism which is not based on airlocks
- We borrow the representation approach of K
  - Term \( x := (3 / (x + 2)) \) represented as
    \[
    x \sim (\Box + 2) \sim (3 / \Box) \sim (x := \Box) \sim \Box
    \]
- Can be achieved using heating/cooling rules of the form
  - \( (x := a) \sim c \quad \Rightarrow \quad a \sim (x := \Box) \sim c \)
  - \( (a_1 / a_2) \sim c \quad \Rightarrow \quad a_2 \sim (a_1 / \Box) \sim c \)
  - \( (a_1 + a_2) \sim c \quad \Rightarrow \quad a_1 \sim (\Box + a_2) \sim c \)
  - \( s \quad \Rightarrow \quad s \sim \Box \)
CHAM Heating-Cooling Rules for IMP

\[
\begin{align*}
  a_1 + a_2 \sim c & \iff a_1 \sim \square + a_2 \sim c \\
  a_1 + a_2 \sim c & \iff a_2 \sim a_1 + \square \sim c \\
  a_1 / a_2 \sim c & \iff a_1 \sim \square / a_2 \sim c \\
  a_1 / a_2 \sim c & \iff a_2 \sim a_1 / \square \sim c \\
  a_1 <= a_2 \sim c & \iff a_1 \sim \square <= a_2 \sim c \\
  i_1 <= a_2 \sim c & \iff a_2 \sim i_1 <= \square \sim c \\
  \text{not } b \sim c & \iff b \sim \text{not } \square \sim c \\
  b_1 \text{ and } b_2 \sim c & \iff b_1 \sim \square \text{ and } b_2 \sim c \\
  x := a \sim c & \iff a \sim x := \square \sim c \\
  s_1 ; s_2 \sim c & \iff s_1 \sim \square ; s_2 \sim c \\
  s & \iff s \sim \square \\
  \text{if } b \text{ then } s_1 \text{ else } s_2 \sim c & \iff b \sim \text{if } \square \text{ then } s_1 \text{ else } s_2 \sim c
\end{align*}
\]
Examples of Syntax Heating/Cooling

- The following is correct heating/cooling of syntax:

\[
\{x := 1 ; x := (3 / (x + 2))\} \iff^* \\
\{x := 1 \sim (\Box ; x := (3 / (x + 2))) \sim \Box\} 
\]

- The following is incorrect heating/cooling of syntax:

\[
\{x := 1 ; x := (3 / (x + 2))\} \iff^* \\
\{x := 1 ; (x \sim (\Box + 2) \sim (3 / \Box) \sim (x := \Box) \sim \Box)\} 
\]
CHAM Reaction Rules for IMP

\[
\begin{align*}
\{x \sim c\} \{x \mapsto i \triangleright \sigma\} & \rightarrow \{i \sim c\} \{x \mapsto i \triangleright \sigma\} \\
i_1 + i_2 \sim c & \rightarrow i_1 +_{\text{Int}} i_2 \sim c \\
i_1 / i_2 \sim c & \rightarrow i_1 /_{\text{Int}} i_2 \sim c \quad \text{when } i_2 \neq 0 \\
i_1 \leq i_2 \sim c & \rightarrow i_1 \leq_{\text{Int}} i_2 \sim c \\
\text{not true} \sim c & \rightarrow \text{false} \sim c \\
\text{not false} \sim c & \rightarrow \text{true} \sim c \\
\text{true and }b_2 \sim c & \rightarrow b_2 \sim c \\
\text{false and }b_2 \sim c & \rightarrow \text{false} \sim c \\
\{x := i \sim c\} \{x \mapsto j \triangleright \sigma\} & \rightarrow \{\text{skip} \sim c\} \{x \mapsto i \triangleright \sigma\} \\
\text{skip ; } s_2 \sim c & \rightarrow s_2 \sim c \\
\text{if true then } s_1 \text{ else } s_2 \sim c & \rightarrow s_1 \sim c \\
\text{if false then } s_1 \text{ else } s_2 \sim c & \rightarrow s_2 \sim c \\
\text{while } b \text{ do } s \sim c & \rightarrow \text{if } b \text{ then } (s ; \text{ while } b \text{ do } s) \text{ else skip } \sim c \\
\text{var }xl ; s & \rightarrow \{s\} \{xl \mapsto 0\} \\
(x, xl) \mapsto i & \rightarrow x \mapsto i \triangleright \{xl \mapsto i\}
\end{align*}
\]
Sample CHAM Rewriting

\[
\begin{align*}
\{ \{ \text{var } x, y ; x := 1 ; x := (3 / (x + 2)) \} \} & \rightarrow \\
\{ \{ x := 1 ; x := (3 / (x + 2)) \} \} & \{ x, y \mapsto 0 \} \\
\{ \{ x := 1 ; x := (3 / (x + 2)) \} \} & \{ x, y \mapsto 0 \} \\
\{ \{ x := 1 \sim \Box ; x := (3 / (x + 2)) \} \} & \{ x \mapsto 0 \mapsto \emptyset \} \\
\{ \{ x := 1 \sim \Box ; x := (3 / (x + 2)) \} \} & \{ x \mapsto 0 \mapsto \emptyset \} \\
\{ \{ \text{skip} \sim \Box ; x := (3 / (x + 2)) \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ \text{skip} ; x := (3 / (x + 2)) \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ x := (3 / (x + 2)) \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ x \sim \Box + 2 \sim 3 / \Box \sim x := \Box \sim \Box \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ 1 \sim \Box + 2 \sim 3 / \Box \sim x := \Box \sim \Box \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ 1 + 2 \sim 3 / \Box \sim x := \Box \sim \Box \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ 3 \sim 3 / \Box \sim x := \Box \sim \Box \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ x := 1 \sim \Box \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ \text{skip} \sim \Box \} \} & \{ x \mapsto 1 \mapsto \emptyset \} \\
\{ \{ \text{skip} \} \} & \{ x \mapsto 1 \mapsto \emptyset \}
\end{align*}
\]
CHAM in Rewriting Logic

- CHAM rules cannot be used unchanged as rewrite rules
  - They need to only apply in solutions, not anywhere they match

- We represent each CHAM rule

\[
m_1 \ m_2 \ \ldots \ m_k \rightarrow m_1' \ m_2' \ \ldots \ m_l'
\]

into a rewrite logic rule

\[
\{\overline{m_1} \ \overline{m_2} \ \ldots \ \overline{m_k} \ \text{Ms}\} \rightarrow \{\overline{m_1'} \ \overline{m_2'} \ \ldots \ \overline{m_l'} \ \text{Ms}\}
\]

where Ms is a fresh bag-of-molecule variable and the overlined molecules are the algebraic variants of the original ones, replacing in particular their meta-variables by variables
CHAM of IMP in Maude

- See file
  - imp-heating-cooling.maude

- See file
  - imp-semantics-cham.maude
How good are the various semantic approaches?
We next discuss the conventional executable semantics approaches in depth, aiming at understanding their pros and cons.

Our approach is to extend each semantics of IMP with various common features (we call the resulting language IMP++):

- **Variable increment** – this will add side effects to expressions
- **Input/Output** – this will require changes in the configuration
- **Abrupt termination** – this requires explicit handling of control
- **Dynamic threads** – this requires handling concurrency and sharing
- **Local variables** – this requires handling environments

We will first treat each extension of IMP independently, i.e., we do not pro-actively take semantic decisions when defining a feature that will help the definition of other features later on. Then, we will put all features together into our IMP++ final language.
IMP++ Variable Increment

- Syntax:

\[ AEexp ::= \ldots \mid ++ Id \]

- Variable increment is very common (C, C++, Java, etc.)
  - We only consider pre-increment (first increment, then return value)
- The problem with increment in some semantic approaches is that it adds side effects to expressions. Therefore, if one did not pro-actively account for that then one needs to change many existing and unrelated semantics rules, if not all.
Previous big-step SOS rules had the form:

\[
\frac{\langle a_1, \sigma \rangle \Downarrow \langle i_1 \rangle \quad \langle a_2, \sigma \rangle \Downarrow \langle i_2 \rangle}{\langle a_1 / a_2, \sigma \rangle \Downarrow \langle i_1 / \text{Int} i_2 \rangle}, \text{ where } i_2 \neq 0
\]

Big-step SOS is the most affected by side effects

- Needs to change its sequents from \( \langle a, \sigma \rangle \Downarrow \langle i \rangle \) to \( \langle a, \sigma \rangle \Downarrow \langle i, \sigma' \rangle \)
- And all the existing rules accordingly, e.g.:

\[
\frac{\langle a_1, \sigma \rangle \Downarrow \langle i_1, \sigma_1 \rangle, \quad \langle a_2, \sigma_1 \rangle \Downarrow \langle i_2, \sigma_2 \rangle}{\langle a_1 / a_2, \sigma \rangle \Downarrow \langle i_1 / \text{Int} i_2, \sigma_2 \rangle}, \text{ where } i_2 \neq 0
\]
Recall IMP operators like `/` were non-deterministically strict. Here is an attempt to achieve that with big-step SOS:

\[
\langle a_1, \sigma \rangle \downarrow \langle i_1, \sigma_1 \rangle, \langle a_2, \sigma_1 \rangle \downarrow \langle i_2, \sigma_2 \rangle \\
\langle a_1 \middle/ a_2, \sigma \rangle \downarrow \langle i_1/\text{Int}i_2, \sigma_2 \rangle
\]

, where \( i_2 \neq 0 \)

\[
\langle a_1, \sigma_2 \rangle \downarrow \langle i_1, \sigma_1 \rangle, \langle a_2, \sigma \rangle \downarrow \langle i_2, \sigma_2 \rangle \\
\langle a_1 \middle/ a_2, \sigma \rangle \downarrow \langle i_1/\text{Int}i_2, \sigma_1 \rangle
\]

, where \( i_2 \neq 0 \)

All we got is “non-deterministic choice” strictness: choose an order, then evaluate the arguments in that order.

Some behaviors are thus lost, but this is relatively acceptable in practice since programmers should not rely on those behaviors in their programs anyway (the loss of behaviors when we add threads is going to be much worse).
We are now ready to add the big-step SOS for variable increment (this is easy now, the hard part was to get here):

\[
\langle \mathcal{I} x, \sigma \rangle \downarrow \langle \sigma(x) +_{\text{Int}} 1, \sigma[(\sigma(x) +_{\text{Int}} 1)/x] \rangle
\]

Example:

- How many values can the following expression possibly evaluate to under the big-step SOS of IMP++ above (assume \(x\) is initially 1)?

\[
++ x / (++ x / x)
\]

- Can it evaluate to 0 or even be undefined under a fully non-deterministic evaluation strategy?
IMP++ Variable Increment
Small-Step SOS

- Previous small-step SOS rules had the form:

\[
\begin{align*}
\langle a_1, \sigma \rangle & \rightarrow \langle a'_1, \sigma \rangle \\
\langle a_1 / a_2, \sigma \rangle & \rightarrow \langle a'_1 / a_2, \sigma \rangle
\end{align*}
\]

- Small-step SOS less affected than big-step SOS, but still requires many rule changes to account for the side effects:

\[
\begin{align*}
\langle a_1, \sigma \rangle & \rightarrow \langle a'_1, \sigma_1 \rangle \\
\langle a_1 / a_2, \sigma \rangle & \rightarrow \langle a'_1 / a_2, \sigma_1 \rangle
\end{align*}
\]
IMP++ Variable Increment
Small-Step SOS

- Since small-step SOS “gets back to the top” at each step, it actually does not lose any non-deterministic behaviors
  - We get fully non-deterministic evaluation strategies for all the IMP constructs instead of “non-deterministic choice” ones
- The semantics of variable increment almost the same as in big-step SOS (indeed, variable increment is an atomic operation):

\[
\langle \text{++ } x, \sigma \rangle \rightarrow \langle \sigma(x) +_{\text{Int}} 1, \sigma[(\sigma(x) +_{\text{Int}} 1)/x] \rangle
\]
Previous MSOS rules had the form:

\[
\begin{align*}
    a_1 \rightarrow a'_1 \\
    a_1 / a_2 \rightarrow a'_1 / a_2
\end{align*}
\]

All semantic changes are hidden within labels, which are implicitly propagated through the general MSOS mechanism.

Consequently, the MSOS of IMP only needs the following rule to accommodate variable updates; nothing else changes!
IMP++ Variable Increment
Reduction Semantics with Eval. Contexts

- Previous RSEC evaluation contexts and rules had the form:

\[
\text{Context} \ ::= \ \square \ | \ \text{Context} / \ AExp \ | \ AExp / \ \text{Context}
\]

\[
i_1 / i_2 \rightarrow i_1 /_{\text{Int}} i_2, \ \text{when } i_2 \neq 0
\]

\[
\langle c, \sigma \rangle[x] \rightarrow \langle c, \sigma \rangle[\sigma(x)]
\]

- Evaluation contexts, together with the characteristic rule of RSEC, allows for compact unconditional rules, mentioning only what is needed from the entire configuration.

- Consequently, the RSED of IMP only needs the following rule to accommodate variable updates; nothing else changes!

\[
\langle c, \sigma \rangle[++ x] \rightarrow \langle c, \sigma[ \{(\sigma(x) +_{\text{Int}} 1)/x\}] [\sigma(x) +_{\text{Int}} 1] \rangle
\]
Previous CHAM heating/cooling/reaction rules had the form:

\[
\begin{align*}
    a_1 / a_2 \sim c & \quad \Rightarrow \quad a_1 \sim \Box / a_2 \sim c \\
    a_1 / a_2 \sim c & \quad \Rightarrow \quad a_2 \sim a_1 / \Box \sim c \\
    i_1 / i_2 \sim c & \quad \Rightarrow \quad i_1 /_{Int} i_2 \sim c \quad \text{when } i_2 \neq 0 \\
    \{x \sim c\} \quad \{x \mapsto i \triangleright \sigma\} & \quad \Rightarrow \quad \{i \sim c\} \quad \{x \mapsto i \triangleright \sigma\}
\end{align*}
\]

Since the heating/cooling rules achieve the role of the evaluation contexts and since one can only mention the necessary molecules in each rule, one does not need to change anything either!

All one needs to do is to add the following rule:

\[
\begin{align*}
    \{++x \sim c\} \quad \{x \mapsto i \triangleright \sigma\} & \quad \Rightarrow \quad \{i +_{Int} 1 \sim c\} \quad \{x \mapsto i +_{Int} 1 \triangleright \sigma\}
\end{align*}
\]
Where is the rest?

- We discussed the remaining features in class, using the whiteboard and colors.
- The lecture notes contain the complete information, even more than we discussed in class.