Denotational semantics
Semantics and Application to Program Verification

Antoine Miné
École normale supérieure, Paris
year 2014–2015

Course 4
4 March 2015
Operational semantics (state and trace) (last two weeks)
Defined as small execution steps (transition relation) over low-level internal configurations (states)
Transitions are chained to define (maximal) traces

Denotational semantics (today)
Direct functions from programs to mathematical objects (denotations) by induction on the program syntax (compositional) ignoring intermediate steps and execution details (no state)

⇒ Higher-level, more abstract, more modular.
Tries to decouple a program meaning from its execution.
Focus on the mathematical structures that represent programs.
(founded by Strachey and Scott in the 70s: [Scott-Strachey71])

“Assembly” of semantics vs. “Functional programming” of semantics
Two very different programs

<table>
<thead>
<tr>
<th>Bubble sort in C</th>
<th>Quick sort in OCaml</th>
</tr>
</thead>
<tbody>
<tr>
<td>int swapped;</td>
<td>let rec sort = function</td>
</tr>
<tr>
<td>do {</td>
<td></td>
</tr>
<tr>
<td>swapped = 0;</td>
<td></td>
</tr>
<tr>
<td>for (int i=1; i&lt;n; i++) {</td>
<td></td>
</tr>
<tr>
<td>if (a[i-1] &gt; a[i]) {</td>
<td></td>
</tr>
<tr>
<td>swap(&amp;a[i-1], &amp;a[i]);</td>
<td></td>
</tr>
<tr>
<td>swapped = 1;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>} while (swapped);</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

- **different languages** (C / OCaml)
- **different algorithms** (bubble sort / quick sort)
- **different programming principles** (loop / recursion)
- **different data-types** (array / list)

Can we give them the same semantics?
Denotation worlds

- **imperative programs**

  effect of a program: mutate a memory state
  natural denotation: input/output function
  \[ D \simeq \text{memory} \to \text{memory} \]

  challenge: build a whole program denotation
  from denotations of atomic language constructs (**modularity**)

- **functional programs**

  effect of a program: return a value
  model a program of type \( a \to b \) as a function \( D_a \to D_b \),
  of type \( (a \to b) \to c \) as a function \( (D_a \to D_b) \to D_c \), etc.

  challenge: polymorphic or untyped languages

- **other paradigms**: parallel, probabilistic, etc.

   \[ \implies \text{very rich theory of mathematical structures} \]
   (Scott domains, cartesian closed categories, coherent spaces, event structures, game semantics, etc. We will not present them in this overview!)
Course overview

- **Imperative programs**
  - deterministic programs
  - handling errors
  - handling non-determinism
  - modularity
  - linking denotational and operational semantics

- **Higher-order programs**
  - monomorphic typed programs: PCF
  - linking denotational and operational semantics: full abstraction
  - untyped λ—calculus: recursive domain equations

- **Practical session** (room INFO 3)
  - program the denotational semantics of a simple imperative (non-)deterministic language
Deterministic imperative programs
A simple imperative language: **IMP**

**IMP expressions**

\[
\text{expr} ::= \begin{aligned}
& X \quad \text{(variable)} \\
| & c \quad \text{(constant)} \\
| & \diamond \text{expr} \quad \text{(unary operation)} \\
| & \text{expr} \diamond \text{expr} \quad \text{(binary operation)} 
\end{aligned}
\]

- variables in a fixed set \( X \in \mathcal{V} \)
- constants \( I \overset{\text{def}}{=} \mathbb{B} \cup \mathbb{Z} \):
  - booleans \( \mathbb{B} \overset{\text{def}}{=} \{ \text{true, false} \} \)
  - integers \( \mathbb{Z} \)
- operations \( \diamond \):
  - integer operations: +, −, ×, /, <, ≤
  - boolean operations: ¬, ∧, ∨
  - polymorphic operations: =, ≠
A simple imperative language: **IMP**

### Statements

\[
\text{stat} ::= \text{skip} \quad \text{(do nothing)} \\
X \leftarrow \text{expr} \quad \text{(assignment)} \\
\text{stat}; \text{stat} \quad \text{(sequence)} \\
\text{if expr then stat else stat} \quad \text{(conditional)} \\
\text{while expr do stat} \quad \text{(loop)}
\]

(inspired from the presentation in [Benton96])
Expression semantics

\[ E[\text{expr}] : \mathcal{E} \rightarrow \mathcal{I} \]

- Environments \(\mathcal{E} \overset{\text{def}}{=} \mathcal{V} \rightarrow \mathcal{I}\) map variables in \(\mathcal{V}\) to values in \(\mathcal{I}\).
- \(E[\text{expr}]\) returns a value in \(\mathcal{I}\).
- \(\ast\) denotes partial functions (as opposed to \(\rightarrow\))
  necessary because some operations are undefined:
  - \(1 + \text{true}, 1 \land 2\) (type mismatch)
  - \(3/0\) (invalid value)
- Defined by structural induction on abstract syntax trees
  (*next slide*)

(when we use the notation \(X[\![ y ]\!]\), \(y\) is a syntactic object; \(X\) serves to distinguish between different semantic functions with different signatures, often varying with the kind of syntactic object \(y\) (expression, statement, etc.);
\(X[\![ y ]\!]\) \(z\) is the application of the function \(X[\![ y ]\!]\) to the object \(z\))
### Expression semantics

\[ \text{E[ expr ] : } \mathcal{E} \ast \]  

<table>
<thead>
<tr>
<th>Expression</th>
<th>Definition</th>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{E[ c ] } \rho )</td>
<td>( \text{def} )</td>
<td></td>
<td>( c \in \mathbb{I} )</td>
</tr>
<tr>
<td>( \text{E[ V ] } \rho )</td>
<td>( \text{def} )</td>
<td></td>
<td>( \rho(V) \in \mathbb{I} )</td>
</tr>
<tr>
<td>( \text{E[ } -e \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( \nu \in \mathbb{Z} ) if ( \nu = \text{E[ e ] } \rho \in \mathbb{Z} )</td>
<td>( -\nu )</td>
</tr>
<tr>
<td>( \text{E[ } -e \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( \nu \in \mathbb{B} ) if ( \nu = \text{E[ e ] } \rho \in \mathbb{B} )</td>
<td>( -\nu )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 + e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 + v_2 \in \mathbb{Z} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{Z} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{Z} )</td>
<td>( v_1 + v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 - e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 - v_2 \in \mathbb{Z} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{Z} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{Z} )</td>
<td>( v_1 - v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 \times e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 \times v_2 \in \mathbb{Z} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{Z} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{Z} )</td>
<td>( v_1 \times v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 / e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 / v_2 \in \mathbb{Z} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{Z} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{Z} \setminus {0} )</td>
<td>( v_1 / v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 \land e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 \land v_2 \in \mathbb{B} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{B} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{B} )</td>
<td>( v_1 \land v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 \lor e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 \lor v_2 \in \mathbb{B} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{B} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{B} )</td>
<td>( v_1 \lor v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 &lt; e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 &lt; v_2 \in \mathbb{B} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{B} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{B} )</td>
<td>( v_1 &lt; v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 \leq e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 \leq v_2 \in \mathbb{B} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{B} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{B} )</td>
<td>( v_1 \leq v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 = e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 = v_2 \in \mathbb{B} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{B} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{B} )</td>
<td>( v_1 = v_2 )</td>
</tr>
<tr>
<td>( \text{E[ } e_1 \neq e_2 \text{ ] } \rho )</td>
<td>( \text{def} )</td>
<td>( v_1 \neq v_2 \in \mathbb{B} ) if ( v_1 = \text{E[ } e_1 \text{ ] } \rho \in \mathbb{B} ), ( v_2 = \text{E[ } e_2 \text{ ] } \rho \in \mathbb{B} )</td>
<td>( v_1 \neq v_2 )</td>
</tr>
</tbody>
</table>

undefined otherwise
Statement semantics

\[ S[\text{stat}] : E \times E \]

- maps an environment before the statement to an environment after the statement
- partial function due to
  - errors in expressions
  - non-termination
- also defined by structural induction
Statement semantics

\[ S[\text{stat}] : \mathcal{E} \times \mathcal{E} \]

- **skip**: do nothing
  \[ S[\text{skip}] \rho \overset{\text{def}}{=} \rho \]

- **assignment**: evaluate expression and mutate environment
  \[ S[X \leftarrow e] \rho \overset{\text{def}}{=} \rho[X \mapsto v] \quad \text{if} \ E[e] \rho = v \]

- **sequence**: function composition
  \[ S[s_1; s_2] \overset{\text{def}}{=} \overset{\circ}{S[s_2]} \circ \overset{\circ}{S[s_1]} \]

- **conditional**
  \[ S[\text{if } e \text{ then } s_1 \text{ else } s_2] \rho \overset{\text{def}}{=} \begin{cases} 
  S[s_1] \rho \quad & \text{if } E[e] \rho = \text{true} \\
  S[s_2] \rho \quad & \text{if } E[e] \rho = \text{false} \\
  \text{undefined} \quad & \text{otherwise}
\end{cases} \]

\((f[x \mapsto y])\) denotes the function that maps \(x\) to \(y\), and any \(z \neq x\) to \(f(z)\).
How do we handle loops?

the semantics of loops must satisfy:

$$S[\texttt{while } e \texttt{ do } s ] \rho = \begin{cases} 
\rho & \text{if } E[ e ] \rho = \text{false} \\
S[\texttt{while } e \texttt{ do } s ] (S[ s ] \rho) & \text{if } E[ e ] \rho = \text{true} \\
\text{undefined} & \text{otherwise}
\end{cases}$$

this is a recursive definition, we must prove that:

- the equation has solution(s)
- in case there are several, choose the right one

$\implies$ we use fixpoints on partially ordered sets
Flat orders and partial functions

- Flat ordering \((\bot, \sqsubseteq)\) on \(\mathbb{Z}\)
  - \(\bot \triangleq \mathbb{Z} \cup \{\bot\}\) (pointed set)
  - \(a \sqsubseteq b \iff a = \bot \lor a = b\) (partial order)
  - Every chain is finite, and so has a lub \(\sqcup\)
  - \(\Rightarrow\) it is a pointed complete partial order (cpo)

\(\bot\) denotes the value “undefined” (\(\sqsubseteq\) is an information order)

Similarly for \(E \bot \triangleq E \cup \{\bot\}\)

Note that \((E \ast E) \simeq (E \rightarrow E \bot)\)
Poset of continuous partial functions

Partial order structure on partial functions \((\mathcal{E}_\perp \rightarrow \mathcal{E}_\perp, \sqsubseteq)\)

- \(\mathcal{E}_\perp \rightarrow \mathcal{E}_\perp\) extends \(\mathcal{E} \rightarrow \mathcal{E}_\perp\)
  - domain = co-domain \(\implies\) allows composition \(\circ\)
  - \(f \in \mathcal{E} \rightarrow \mathcal{E}_\perp\) extended with \(f(\perp) \overset{\text{def}}{=} \perp\) (strictness)
    \(\implies\) if \(S[\mathcal{S}]x\) is undefined, so is \((S[\mathcal{S}'] \circ S[\mathcal{S}] )x\)
    such functions are monotonic and continuous
    \((a \sqsubseteq b \implies f(a) \sqsubseteq f(b) \text{ and } f(\sqcup X) = \sqcup \{ f(x) \mid x \in X \})\)
  \(\implies\) we restrict \(\mathcal{E}_\perp \rightarrow \mathcal{E}_\perp\) to continuous functions: \(\mathcal{E}_\perp \rightarrow \mathcal{E}_\perp\)

- point-wise order \(\sqsubseteq\) on functions
  \(f \sqsubseteq g \overset{\text{def}}{\iff} \forall x: f(x) \sqsubseteq g(x)\)

- \(\mathcal{E}_\perp \rightarrow \mathcal{E}_\perp\) has a least element: \(\bot \overset{\text{def}}{=} \lambda x. \perp\)

- by point-wise lub \(\sqcup\) of chains, it is also complete \(\implies\) a cpo
  \(\sqcup F = \lambda x. \sqcup \{ f(x) \mid f \in F \}\)
Fixpoint semantics of loops

to solve the semantic equation, we use a fixpoint of a functional

we use the least fixpoint (most precise for the information order)

\[ S[\textbf{while } e \textbf{ do } s ] \overset{\text{def}}{=} \text{Ifp } F \]

where:

\[ F : (\mathcal{E}_\bot \rightarrow \mathcal{E}_\bot) \rightarrow (\mathcal{E}_\bot \rightarrow \mathcal{E}_\bot) \]

\[ F(f)(\rho) = \begin{cases} 
\rho & \text{if } \mathcal{E}[e] \rho = \text{false} \\
 f(S[ s ] \rho) & \text{if } \mathcal{E}[e] \rho = \text{true} \\
 \bot & \text{otherwise} 
\end{cases} \]

\textbf{Theorem}

\text{Ifp } F \text{ is well-defined}

(remember our equation on \( S[\textbf{while } e \textbf{ do } s ] \) ?
it can be rewritten exactly as: \( S[\textbf{while } e \textbf{ do } s ] = F(S[\textbf{while } e \textbf{ do } s ]) \))
To use the theorem we prove that $S[\text{stat}]$ is continuous (and is well-defined) by induction on the syntax of stat:

- **base cases:** $S[\text{skip}]$ and $S[X \leftarrow e]$ are continuous
- $S[\text{if } e \text{ then } s_1 \text{ else } s_2]$: by induction hypothesis, as $S[s_1]$ and $S[s_2]$ are
- $S[s_1; s_2]$: by induction hypotheses and because $\circ$ respects continuity
- $F$ is continuous in $(\mathcal{E}_\bot \xrightarrow{\circ} \mathcal{E}_\bot) \xrightarrow{\circ} (\mathcal{E}_\bot \xrightarrow{\circ} \mathcal{E}_\bot)$ by induction hypotheses
  $\implies \text{lfp } F$ exists by Kleene's theorem
  moreover, $\text{lfp } F$ is continuous (simple consequence of Kleene's proof)
  $\implies S[\text{while } e \text{ do } s]$ is continuous
Recall another fact about Kleene’s fixpoints: \( \text{lf} F = \bigcup_{n \in \mathbb{N}} F^n(\bot) \)

- \( F^0(\bot) = \bot \) is completely undefined (no information)
- \( F^1(\bot)(\rho) = \begin{cases} \rho & \text{if } E[e]\rho = \text{false} \\ \bot & \text{otherwise} \end{cases} \)
  environment if the loop is never entered (partial information)
- \( F^2(\bot)(\rho) = \begin{cases} \rho & \text{if } E[e]\rho = \text{false} \\ S[s]\rho & \text{else if } E[e](S[s]\rho) = \text{false} \\ \bot & \text{otherwise} \end{cases} \)
  environment if the loop is iterated at most once
- \( F^n(\bot)(\rho) \)
  environment if the loop is iterated at most \( n - 1 \) times
- \( \bigcup_{n \in \mathbb{N}} F^n(\bot) \)
  environment when exiting the loop whatever the number of iterations (total information)
Rewriting the semantics using total functions on cpos with $\bot$:

- $E[\text{expr}] : E_\bot \xrightarrow{c} I_\bot$

  returns $\bot$ for an error or if its argument is $\bot$

- $S[\text{stat}] : E_\bot \xrightarrow{c} E_\bot$

  - $S[\text{skip}] \rho \overset{\text{def}}{=} \rho$
  - $S[e_1; e_2] \overset{\text{def}}{=} S[e_2] \circ S[e_1]$
  - $S[X \leftarrow e] \rho \overset{\text{def}}{=} \begin{cases} \bot & \text{if } E[e] \rho = \bot \\ \rho[X \mapsto E[e] \rho] & \text{otherwise} \end{cases}$
  - $S[\text{if } e \text{ then } s_1 \text{ else } s_2] \rho \overset{\text{def}}{=} \begin{cases} S[s_1] \rho & \text{if } E[e] \rho = \text{true} \\ S[s_2] \rho & \text{if } E[e] \rho = \text{false} \\ \bot & \text{otherwise} \end{cases}$
  - $S[\text{while } e \text{ do } s] \overset{\text{def}}{=} \text{lfp } F$

  where $F(f)(\rho) = \begin{cases} \rho & \text{if } E[e] \rho = \text{false} \\ f(S[s] \rho) & \text{if } E[e] \rho = \text{true} \\ \bot & \text{otherwise} \end{cases}$
Errors
Error vs. non-termination

In our semantics $S[\text{stat}] \rho = \bot$ can mean:
- either stat starting on input $\rho$ loops for ever
- or it stops prematurely with an error

$\implies$ we would like to distinguish these two cases

Solution:
- add an error value $\Omega$, distinct from $\bot$
- propagate it in the semantics, bypassing computations
  (no further computation after an error)
Expression semantics with errors

We set $\mathcal{E}_{\perp,\Omega} \overset{\text{def}}{=} \mathcal{E} \cup \{\perp, \Omega\}$, $\mathcal{I}_{\perp,\Omega} \overset{\text{def}}{=} \mathcal{I} \cup \{\perp, \Omega\}$

$E[\text{expr}] : \mathcal{E}_{\perp,\Omega} \overset{c}{\rightarrow} \mathcal{I}_{\perp,\Omega}$

$E[e] \perp \overset{\text{def}}{=} \perp$

$E[e] \Omega \overset{\text{def}}{=} \Omega$

if $\rho \notin \{\Omega, \perp\}$ then

$E[V] \rho \overset{\text{def}}{=} \rho(V) \in \mathcal{I}$

$E[c] \rho \overset{\text{def}}{=} c \in \mathcal{I}$

$E[-e] \rho \overset{\text{def}}{=} \begin{cases} -v \in \mathbb{Z} & \text{if } v = E[e] \rho \in \mathbb{Z} \\ \Omega & \text{if } E[e] \rho = \Omega \end{cases}$

$E[e_1 + e_2] \rho \overset{\text{def}}{=} \begin{cases} v_1 + v_2 \in \mathbb{Z} & \text{if } v_1 = E[e_1] \rho \in \mathbb{Z} \text{ and } v_2 = E[e_2] \rho \in \mathbb{Z} \\ \Omega & \text{if } E[e_1] \rho \notin \mathbb{Z} \text{ or } E[e_2] \rho \notin \mathbb{Z} \end{cases}$

$E[e_1/e_2] \rho \overset{\text{def}}{=} \begin{cases} v_1/v_2 \in \mathbb{Z} & \text{if } v_1 = E[e_1] \rho \in \mathbb{Z} \text{ and } v_2 = E[e_2] \rho \in \mathbb{Z} \setminus \{0\} \\ \Omega & \text{if } E[e_1] \rho \notin \mathbb{Z} \text{ or } E[e_2] \rho \notin \mathbb{Z} \setminus \{0\} \end{cases}$

\[\ldots\]

(note that $x = \perp \iff E[e] x = \perp$, $x = \Omega \implies E[e] x = \Omega$)
Statement semantics with errors

\[ S[ \text{stat} ] : E_{⊥,Ω} \rightarrow C \rightarrow E_{⊥,Ω} \]

- \( S[ s ] \bot \overset{\text{def}}{=} \bot \)
- \( S[ s ] \Omega \overset{\text{def}}{=} \Omega \)
- \( S[ \text{skip} ] \rho \overset{\text{def}}{=} \rho \)
- \( S[ s_1; s_2 ] \overset{\text{def}}{=} S[ s_2 ] \circ S[ s_1 ] \)
- \( S[ X \leftarrow e ] \rho \overset{\text{def}}{=} \left\{ \begin{array}{ll}
\rho[X \mapsto v] & \text{if } v = E[ e ] \rho \in I \\
\Omega & \text{if } E[ e ] \rho \in \Omega
\end{array} \right. \)
- \( S[ \text{if } e \text{ then } s_1 \text{ else } s_2 ] \rho \overset{\text{def}}{=} \left\{ \begin{array}{ll}
S[ s_1 ] \rho & \text{if } E[ e ] \rho = \text{true} \\
S[ s_2 ] \rho & \text{if } E[ e ] \rho = \text{false} \\
\Omega & \text{otherwise}
\end{array} \right. \)
Errors

Statement semantics with errors

\[ S[\textbf{while } e \textbf{ do } s] \overset{\text{def}}{=} \text{lf}p \ F \text{ where} \]

\[
F(f)(\rho) = \begin{cases} 
    \bot & \text{if } \rho = \bot \\
    \rho & \text{if } E[\ e \ ] \rho = \text{false} \\
    f(S[\ s \ ] \rho) & \text{if } E[\ e \ ] \rho = \text{true} \\
    \Omega & \text{otherwise}
\end{cases}
\]

using the **flat ordering** \( a \sqsubseteq b \iff a = \bot \lor a = b \)

i.e., \( \Omega \) is not comparable with elements of \( \mathcal{E} \)

\( \implies \) the loop exits immediately at the first error

**Several outcome when computing for** \( S[\ stat \ ] \rho \)

- \( \rho' \in \mathcal{E} \): the program terminates successfully
- \( \Omega \): the program terminates with an error
- \( \bot \): the program loops forever
We can also:

- distinguish different kinds of errors
- tag errors with their location
- track more errors

  e.g., use of uninitialized variables:
  
  \[
  \mathcal{E} \overset{\text{def}}{=} \forall \rightarrow (\emptyset \cup \{\text{uninit}\})
  \]
Non-determinism
Why non-determinism?

It is useful to consider non-deterministic programs, to:

- model partially unknown environments (user input)
- abstract away unknown program parts (libraries)
- abstract away too complex parts (rounding errors in floats)
- handle a set of programs as a single one (parametric programs)

Kinds of non-determinism

- control non-determinism: \( \text{stat ::= either } s_1 \text{ or } s_2 \)
- data non-determinism: \( \text{expr ::= random()} \)

(we can write “either \( s_1 \) or \( s_2 \)” as “if \( \text{random()} = 0 \) then \( s_1 \) else \( s_2 \)”)

Consequence on semantics and verification

we want to verify all the possible executions
\[ \Rightarrow \text{ the semantics should express all the possible executions} \]
We extend **IMP** to **NIMP**, an imperative language with non-determinism

\[
\begin{align*}
\text{expr} &::= X \quad \text{(variable)} \\
&\quad | c \quad \text{(constant)} \\
&\quad | [c_1, c_2] \quad \text{(constant interval)} \\
&\quad | \Diamond \text{expr} \quad \text{(unary operation)} \\
&\quad | \text{expr} \Diamond \text{expr} \quad \text{(binary operation)}
\end{align*}
\]

\[c_1 \in \mathbb{Z} \cup \{-\infty\}, \ c_2 \in \mathbb{Z} \cup \{+\infty\}\]

\([c_1, c_2]\) means: a fresh random value between \(c_1\) and \(c_2\) each time the expression is evaluated

**Question:** is \([0, 1] = [0, 1]\) true or false?

**NIMP** has the same statements as **IMP**
Expression semantics

\[ E[ expr ] : \mathcal{E} \rightarrow \mathcal{P}(\emptyset) \]

- \( E[ V ] \rho \defeq \{ \rho(V) \} \)
- \( E[ c ] \rho \defeq \{ c \} \)
- \( E[ [c_1, c_2] ] \rho \defeq \{ c \in \mathbb{Z} \mid c_1 \leq c \leq c_2 \} \)
- \( E[ -e ] \rho \defeq \{ -v \mid v \in E[ e ] \rho \cap \mathbb{Z} \} \)
- \( E[ \neg e ] \rho \defeq \{ \neg v \mid v \in E[ e ] \rho \cap \mathbb{B} \} \)
- \( E[ e_1 + e_2 ] \rho \defeq \{ v_1 + v_2 \mid v_1 \in E[ e_1 ] \rho \cap \mathbb{Z}, v_2 \in E[ e_2 ] \rho \cap \mathbb{Z} \} \)
- \( E[ e_1 / e_2 ] \rho \defeq \{ v_1/v_2 \mid v_1 \in E[ e_1 ] \rho \cap \mathbb{Z}, v_2 \in E[ e_2 ] \rho \cap \mathbb{Z} \setminus \{0\} \} \)
- \( E[ e_1 < e_2 ] \rho \defeq \{ \text{true} \mid \exists v_1 \in E[ e_1 ] \rho, v_2 \in E[ e_2 ] \rho : v_1 \in \mathbb{Z}, v_2 \in \mathbb{Z}, v_1 < v_2 \} \cup \{ \text{false} \mid \exists v_1 \in E[ e_1 ] \rho, v_2 \in E[ e_2 ] \rho : v_1 \in \mathbb{Z}, v_2 \in \mathbb{Z}, v_1 \geq v_2 \} \)

...  

- we output a set of values, to account for non-determinism
- we can have \( E[ e ] \rho = \emptyset \) due to errors
  (no need for a special \( \Omega \) nor \( \perp \) element)
Semantic domain:

- a statement can output a set of environments
  \[ \Rightarrow \text{use } \mathcal{E} \to \mathcal{P}(\mathcal{E}) \]
- to allow composition, extend it to \[ \mathcal{P}(\mathcal{E}) \to \mathcal{P}(\mathcal{E}) \]
- non-termination and errors can be modeled by \[ \emptyset \]
  (no need for a special \( \Omega \) nor \( \bot \) element)

Note:
we could use \[ \mathcal{P}(\mathbb{I} \cup \{\Omega\}) \] and \[ \mathcal{P}(\mathcal{E} \cup \{\Omega\}) \] to distinguish again non-termination from errors
we won’t, to lighten the presentation, but this is not difficult
Statement semantics

\[ S[\text{stat}] : \mathcal{P}(\mathcal{E}) \rightarrow \mathcal{P}(\mathcal{E}) \]

- \( S[\text{skip}] R \overset{\text{def}}{=} R \)
- \( S[ s_1; s_2 ] \overset{\text{def}}{=} S[ s_2 ] \circ S[ s_1 ] \)
- \( S[ X \leftarrow e ] R \overset{\text{def}}{=} \{ \rho[X \mapsto v] \mid \rho \in R, \ v \in E[ e ] \rho \} \)
  - pick an environment \( \rho \)
  - pick an expression value \( v \) in \( E[ e ] \rho \)
  - generate an updated environment \( \rho[X \mapsto v] \)

- \( S[ \text{if} \ e \ \text{then} \ s_1 \ \text{else} \ s_2 ] R \overset{\text{def}}{=} \)
  \[ S[ s_1 ] \{ \rho \in R \mid \text{true} \in E[ e ] \rho \} \cup \]
  \[ S[ s_2 ] \{ \rho \in R \mid \text{false} \in E[ e ] \rho \} \]
  - filter environments according to the value of \( e \)
  - execute both branch independently
  - join them with \( \cup \)
Statement semantics

- \( S[ \text{while } e \text{ do } s ] R \overset{\text{def}}{=} \{ \rho \in \text{lfp } F \mid \text{false } \in E[e] \rho \} \)

where \( F(X) \overset{\text{def}}{=} R \cup S[s] \{ \rho \in X \mid \text{true } \in E[e] \rho \} \)

Justification: \( \text{lfp } F \) exists

- \((\mathcal{P}(\mathcal{E}), \subseteq, \cup, \cap, \emptyset, \mathcal{E})\) forms a complete lattice
- all semantic functions and \( F \) are monotonic and continuous
  in fact, they are strict complete join morphisms
  \( S[s](\cup_{i \in \Delta} X_i) = \cup_{i \in \Delta} S[s]X_i \) and \( S[s]\emptyset = \emptyset \)
  which we write as \( S[s] \in \mathcal{P}(\mathcal{E}) \overset{\cup}{\rightarrow} \mathcal{P}(\mathcal{E}) \)
  it is really the image function of a function in \( \mathcal{E} \rightarrow \mathcal{P}(\mathcal{E}) \)
  \( S[s]X = \cup \{ S[s] \{x\} \mid x \in X \} \)
- we can apply both Kleene’s and Tarski’s fixpoint theorems
Join semantics of loops

$$S[\text{while } e \text{ do } s] \ R \overset{\text{def}}{=} \{ \rho \in \text{lfp } F \mid \text{false } \in \mathcal{E}[\ e \ ] \ \rho \}$$

where $F(X) \overset{\text{def}}{=} \mathcal{R} \cup S[\ s] \ \{ \rho \in X \mid \text{true } \in \mathcal{E}[\ e \ ] \ \rho \}$

($F$ applies a loop iteration to $X$ and adds back the environments $R$ before the loop)

Recall that $\text{lfp } F = \bigcup_{n \in \mathbb{N}} F^n(\emptyset)$

- $F^0(\emptyset) = \emptyset$
- $F^1(\emptyset) = \mathcal{R}$
  - environments before entering the loop
- $F^2(\emptyset) = \mathcal{R} \cup S[\ s] \ \{ \rho \in \mathcal{R} \mid \text{true } \in \mathcal{E}[\ e \ ] \ \rho \}$
  - environments after zero or one loop iteration
- $F^n(\emptyset)$: environments after at most $n - 1$ loop iterations
  - (just before testing the condition to determine if we should iterate a $n$–th time)
- $\bigcup_{n \in \mathbb{N}} F^n(\emptyset)$: loop invariant
“Angelicious” non-determinism and termination

If *stat* is deterministic (no \([c_1, c_2]\) in expressions)
the semantics is equivalent to our semantics on \(E_\bot \rightarrow E_\bot\)

*Justification:* \(\{E \subseteq E \mid \|E\| \leq 1\}, \subseteq, \cup, \emptyset\) is isomorphic to \((E_\bot, \sqsubseteq, \sqcup, \bot)\)

In general, we can have several outputs for \(S[\text{stat}]\) \(\{\rho\} \subseteq E \cup \{\Omega\}\):

- \(\emptyset\): the program never terminates at all
- \(\{\Omega\}\): the program never terminates correctly
- \(R \subseteq E \setminus \{\Omega\}\): when the program terminates, it terminates correctly, in an environment in \(R\)

\(\implies\) we cannot express that a program always terminates!

This is called the “Angelicious” semantics, useful for partial correctness
Note on non-determinism and termination

Other (more complex) ways to mix non-termination and non-determinism exist

Based on distinguishing $\emptyset$ and $\perp$, and on different order relations $\sqsubseteq$

(this is a complex subject, we will say no more)
Modularity
Contexts: statements with holes

\[
\begin{align*}
\text{ctx} & ::= \text{skip} \quad & \text{(do nothing)} \\
& \quad | \quad X \leftarrow \text{expr} \quad & \text{(assignment)} \\
& \quad | \quad \text{ctx}; \text{ctx} \quad & \text{(sequence)} \\
& \quad | \quad \text{if expr then ctx else ctx} \quad & \text{(conditional)} \\
& \quad | \quad \text{while expr do ctx} \quad & \text{(loop)} \\
& \quad | \quad \square \quad & \text{(hole)}
\end{align*}
\]

Substitution: \( \text{ctx}[\square \mapsto \text{stat}] \in \text{stat} \), defined by induction

- \( \square[\square \mapsto s] \overset{\text{def}}{=} s \) (fill hole)
- \( c[\square \mapsto s] \overset{\text{def}}{=} c \) for assignments and skip contexts (no hole to fill)
- \( (c_1; c_2)[\square \mapsto s] \overset{\text{def}}{=} c_1[\square \mapsto s]; c_2[\square \mapsto s] \)
- \( (\text{if } e \text{ then } c_1 \text{ else } c_2)[\square \mapsto s] \overset{\text{def}}{=} \text{if } e \text{ then } c_1[\square \mapsto s] \text{ else } c_2[\square \mapsto s] \)
- \( (\text{while } e \text{ do } c)[\square \mapsto s] \overset{\text{def}}{=} \text{while } e \text{ do } c[\square \mapsto s] \) (recursively fill holes in substatements)
Modularity

Semantics of statements with holes

**Context semantics:**

\[ C[\text{ctx}] : (\mathcal{P}(E) \xrightarrow{\cup} \mathcal{P}(E)) \xrightarrow{\cup} \mathcal{P}(E) \xrightarrow{\cup} \mathcal{P}(E) \]

\( \simeq \) semantics of statements in \( S[\text{stat}] : \mathcal{P}(E) \xrightarrow{\cup} \mathcal{P}(E) \)

but parameterized by the semantics of the hole

\[
\begin{align*}
C[\text{skip}](H)(R) & \overset{\text{def}}{=} R \\
C[s_1; s_2](H) & \overset{\text{def}}{=} C[s_2](H) \circ C[s_1](H) \\
&(H \text{ is not used}) \\
C[X \leftarrow e](H)(R) & \overset{\text{def}}{=} \{ \rho[X \mapsto v] | \rho \in R, \ v \in E[e] \rho \} \\
C[\text{if } e \text{ then } s_1 \text{ else } s_2](H)(R) & \overset{\text{def}}{=} \\
& C[s_1](H)(\{ \rho \in R | \text{true} \in E[e] \rho \}) \cup \\
& C[s_2](H)(\{ \rho \in R | \text{false} \in E[e] \rho \}) \\
C[\text{while } e \text{ do } s](H)(R) & \overset{\text{def}}{=} \{ \rho | \text{false} \in E[e] \rho \} \\
& \text{where } F(X) \overset{\text{def}}{=} R \cup C[s](H)(\{ \rho \in X | \text{true} \in E[e] \rho \}) \\
&(H \text{ is passed nown recursively to substatements}) \\
C[\square](H)(R) & \overset{\text{def}}{=} H(R) \\
&(H \text{ is used in place of } \square)
\]
Modularity

Substitution vs. context semantics

Theorem

\[ C\[ c \] (S\[ s \]) = S\[ c[\square \leftrightarrow s] \] \]

\[ \implies \] we can exploit this to perform modular reasoning

- extract a program part \( s \), s.t. \( \text{prog} = c[\square \leftrightarrow s] \)
- compute its semantics in isolation: \( S[\ s \ ] \)
- use it as \( C[\ c \ ] (S[\ s \ ]) \) to get \( S[\ \text{prog} \ ] \)

useful if \( s \) is repeated often in \( \text{prog} \) as \( |c| + |s| \lesssim |\text{prog}| \)

Proof: easy by structural induction on \( c \)
Modularity

Application: first order procedures

Statements

\[ stat ::= \text{skip} \]
\[ | \text{stat};\text{stat} \]
\[ | \ldots \]
\[ | f() \quad (\text{procedure call } f \in F) \]

\( F \): set of procedure names

\( body : F \to \text{stat} \): procedure definition

Assume: no local variable, no recursivity

- substitution semantics:
  \[
  S[ f() ] \overset{\text{def}}{=} S[ body(f) ], \simeq \text{procedure inlining}
  \]

- modular semantics:
  \[
  f \mapsto S[ f() ] \quad \text{tabulated “bottom-up” on the call graph}
  \]
  \[
  \text{(leaf procedures first)}
  \]
Link between operational and denotational semantics
Motivation

Are the operational and denotational semantics consistent with each other?

Note that:

- systems are actually described operationally (previous courses)
- the denotational semantics is a more abstract representation (more suitable for some reasoning on the system)

⇒ the denotational semantics must be proven faithful (in some sense) to the operational model to be of any use
Labelled syntax

\[\ell \text{stat} ::= \ell \text{skip} \]
\[\quad | \ell X \leftarrow \text{expr} \]
\[\quad | \ell \text{if expr then stat else stat} \]
\[\quad | \ell \text{while expr do stat} \]
\[\quad | \ell \text{stat; stat} \]

`\in \mathcal{L}`: control labels

- statements are decorated with unique control labels `\in \mathcal{L}`
- program configurations in \(\Sigma \overset{\text{def}}{=} \mathcal{L} \times \mathcal{E}\) (lower-level than \(\mathcal{E}\): we must track program locations)
- transition relation \(\tau \subseteq \Sigma \times \Sigma\) models atomic execution steps
Transition systems for our language

\( \tau \) is defined by induction on the syntax of statements

\((\sigma, \sigma') \in \tau \) is denoted as \( \sigma \rightarrow \sigma' \)

\[
\begin{align*}
\tau[\ell_1 \text{skip} \ell_2] & \overset{\text{def}}{=} \{ (\ell_1, \rho) \rightarrow (\ell_2, \rho) \mid \rho \in \mathcal{E} \} \\
\tau[\ell_1 X \leftarrow e \ell_2] & \overset{\text{def}}{=} \{ (\ell_1, \rho) \rightarrow (\ell_2, \rho[X \mapsto \nu]) \mid \rho \in \mathcal{E}, \nu \in \mathbb{E} \} \\
\tau[\ell_1 \text{if } e \text{ then } \ell_2 s_1 \text{ else } \ell_3 s_2 \ell_4] & \overset{\text{def}}{=} \\
& \quad \{ (\ell_1, \rho) \rightarrow (\ell_2, \rho) \mid \rho \in \mathcal{E}, \text{true} \in \mathbb{E} \} \cup \\
& \quad \{ (\ell_1, \rho) \rightarrow (\ell_3, \rho) \mid \rho \in \mathcal{E}, \text{false} \in \mathbb{E} \} \cup \\
& \quad \tau[\ell_2 s_1 \ell_4] \cup \tau[\ell_3 s_2 \ell_4] \\
\tau[\ell_1 \text{while } e \text{ do } \ell_3 s_4] & \overset{\text{def}}{=} \\
& \quad \{ (\ell_1, \rho) \rightarrow (\ell_2, \rho) \mid \rho \in \mathcal{E} \} \cup \\
& \quad \{ (\ell_2, \rho) \rightarrow (\ell_3, \rho) \mid \rho \in \mathcal{E}, \text{true} \in \mathbb{E} \} \cup \\
& \quad \{ (\ell_2, \rho) \rightarrow (\ell_4, \rho) \mid \rho \in \mathcal{E}, \text{false} \in \mathbb{E} \} \cup \tau[\ell_3 s_2] \\
\tau[\ell_1 s_1; \ell_2 s_2] & \overset{\text{def}}{=} \tau[\ell_1 s_1 \ell_2] \cup \tau[\ell_2 s_2 s_3] 
\end{align*}
\]

Defines the small-step semantics of a statement

(the semantics of expressions is still in denotational form)
Special states

Given a labelled statement $\ell e s^{\ell x}$ and its transition system, we define:

- **initial states**: $I \overset{\text{def}}{=} \{ (\ell e, \rho) | \rho \in \mathcal{E} \}$
  
  note that $\sigma \rightarrow \sigma' \implies \sigma' \notin I$

- **blocking states**: $B \overset{\text{def}}{=} \{ \sigma \in \Sigma | \forall \sigma': \in \Sigma, \sigma \not\rightarrow \sigma' \}$

- **correct termination**: $OK \overset{\text{def}}{=} \{ (\ell x, \rho) | \rho \in \mathcal{E} \}$
  
  note that $OK \subseteq B$

- **error**: $ERR \overset{\text{def}}{=} B \cap \{ (\ell, \rho) | \ell \neq \ell x, \rho \in \mathcal{E} \}$

$$B = ERR \cup OK$$

$$ERR \cap OK = \emptyset$$
Link between operational and denotational semantics

Reminder: maximal trace semantics

**Trace:** in $\Sigma^\infty$ (finite or infinite sequence of states)
- starting in an initial state $I$
- following transitions $\rightarrow$
- can only end in a blocking state $B$ (traces are maximal)

i.e.: $t[s] = t[s]^* \cup t[s]^{\omega}$ where

- **finite traces:**
  $t[s]^* \overset{\text{def}}{=} \{(\sigma_0, \ldots, \sigma_n) \mid n \geq 0, \sigma_0 \in I, \sigma_n \in B, \forall i < n: \sigma_i \rightarrow \sigma_{i+1}\}$

- **infinite traces:**
  $t[s]^{\omega} \overset{\text{def}}{=} \{(\sigma_0, \ldots) \mid \sigma_0 \in I, \forall i \in \mathbb{N}: \sigma_i \rightarrow \sigma_{i+1}\}$
From traces to big-step semantics

**Big-step semantics:** abstraction of traces
only remembers the input-output relations

many variants exist:

- **“angelic”** semantics, in $\mathcal{P}(\Sigma \times \Sigma)$:
  \[
  \mathcal{A}[s] \overset{\text{def}}{=} \{(\sigma, \sigma') \mid \exists (\sigma_0, \ldots, \sigma_n) \in t[s]^* : \sigma = \sigma_0, \sigma' = \sigma_n\}
  \]
  (only give information on the terminating behaviors; can only prove partial correctness)

- **natural** semantics, in $\mathcal{P}(\Sigma \times \Sigma_\perp)$:
  \[
  \mathcal{N}[s] \overset{\text{def}}{=} \mathcal{A}[s] \cup \{(\sigma, \perp) \mid \exists (\sigma_0, \ldots) \in t[s]^{\omega} : \sigma = \sigma_0\}
  \]
  (models the terminating and non-terminating behaviors; can prove total correctness)

- **“demoniac”** semantics, in $\mathcal{P}(\Sigma \times \Sigma)$:
  \[
  \mathcal{D}[s] \overset{\text{def}}{=} \mathcal{A}[s] \cup \{(\sigma, \sigma') \mid \exists (\sigma_0, \ldots) \in t[s]^{\omega} : \sigma = \sigma_0, \sigma' \in \Sigma\}
  \]
  (models non-termination as chaos; cannot prove any property of possibly non-terminating executions)

Exercise: compute the semantics of “\textbf{while }X > 0 \textbf{ do } X \leftarrow X - [0, 1]”
Link between operational and denotational semantics

From big-step to denotational semantics

The angelic denotational and big-step semantics are isomorphic
(isomorphism between relations and strict complete join morphisms)

\[ S[s] = \alpha(A[s]) \]

where

\[ \alpha(X) \overset{\text{def}}{=} \lambda R. \{ \rho' \mid \rho \in R, ((\ell_e, \rho), (\ell_x, \rho')) \in X \} \]

\[ \alpha^{-1}(Y) = \{ ((\ell_e, \rho), (\ell_x, \rho')) \mid \rho \in E, \rho' \in Y(\{\rho\}) \} \]

Proof idea: by induction on the syntax of \( s \)

\[ \longrightarrow \text{our operational and denotational semantics match} \]

Also, the denotational semantics is an abstraction of the natural semantics
(it forgets about infinite computations)

Thesis
All semantics can be compared for equivalence or abstraction

this can be made formal in the abstract interpretation theory
(see [Cousot02])
Link between operational and denotational semantics

Semantic diagram

denotational world

\[ S[s] \]

operation

\[ A[s] \]

statement

natural

\[ N[s] \]

traces

\[ t[s] \]

transition system

(small step)

\[ \tau[s] \]
Recall that traces can be expressed as fixpoints:

- $t^*_{s} = (\text{lfp } F) \cap (I \Sigma^\infty)$
  where $F(X) \equiv B \cup \{ (\sigma, \sigma_0, \ldots, \sigma_n) | \sigma \rightarrow \sigma_0 \land (\sigma_0, \ldots, \sigma_n) \in X \}$

- $t^\omega_{s} = (\text{gfp } F) \cap (I \Sigma^\infty)$
  where $F(X) \equiv \{ (\sigma, \sigma_0, \ldots) | \sigma \rightarrow \sigma_0 \land (\sigma_0, \ldots) \in X \}$

This also holds for the angelic denotational semantics:

- $S^s = \alpha(\text{lfp } F)$
  where $F(X) \equiv (B \times B) \cup \{ (\sigma, \sigma'') | \exists \sigma': \sigma \rightarrow \sigma' \land (\sigma', \sigma'') \in X \}$

and many others: natural, denotational, big-step, denotational, . . .

**Thesis**

All semantics can be expressed through fixpoints

(again [Cousot02])
Higher-order programs
Higher-order programs

Monomorphic typed higher order language

PCF language (introduced by Scott in 1969)

\[
\begin{align*}
type & ::= \text{int} & \text{(integers)} \\
& | \text{bool} & \text{(booleans)} \\
& | type \to type & \text{(functions)} \\
term & ::= X & \text{(variable } X \in V) \\
& | c & \text{(constant)} \\
& | \lambda X^{type}.term & \text{(abstraction)} \\
& | term \ term & \text{(application)} \\
& | \Omega^{type} & \text{(failure)} \\
\end{align*}
\]

PCF (programming computable functions) is a \(\lambda\)-calculus with:

- a monomorphic type system (unlike ML)
- explicit type annotations \(X^{type}, Y^{type}, \Omega^{type}\) (unlike ML)
- an explicit recursion combiner \(Y\) (unlike untyped \(\lambda\)-calculus)
- constants, including \(\mathbb{Z}, \mathbb{B}\) and a few built-in functions (arithmetic and comparisons in \(\mathbb{Z}\), if-then-else, etc.)
What should be the domain of $T[\text{term}]$?

**Difficulty:** term contains heterogeneous objects: constants, functions, second order functions, etc.

**Solution:** use the type information

Each term $m$ can be given a type $\text{typ}(m)$

Use one semantic domain $D_t$ per type $t$

Then $T[\text{m}] : \mathcal{E} \rightarrow D_{\text{typ}(m)}$ where $\mathcal{E} \overset{\text{def}}{=} \forall \rightarrow (\bigcup_{t\in\text{type}} D_t)$

Domain definition by induction on the syntax of types

- $D_{\text{int}} \overset{\text{def}}{=} \mathbb{Z}_\bot$
- $D_{\text{bool}} \overset{\text{def}}{=} \mathbb{B}_\bot$
- $D_{t_1 \rightarrow t_2} \overset{\text{def}}{=} (D_{t_1} \overset{c}{\rightarrow} D_{t_2})_\bot$
Higher-order programs

Order on semantic domains

**Order:** all domains are cpos

- $\mathcal{D}_{\text{int}} \overset{\text{def}}{=} \mathbb{Z}_\bot$, $\mathcal{D}_{\text{bool}} \overset{\text{def}}{=} \mathbb{B}_\bot$ use a flat ordering

- $\mathcal{D}_{t_1 \rightarrow t_2} \overset{\text{def}}{=} (\mathcal{D}_{t_1} \xrightarrow{c} \mathcal{D}_{t_2})_\bot$

with order $f \sqsubseteq g \iff f = \bot \lor (f, g \neq \bot \land \forall x : f(x) \sqsubseteq g(x))$

- $\mathcal{D}_{t_1} \xrightarrow{c} \mathcal{D}_{t_2}$ is ordered point-wise

- each domain has its fresh minimal $\bot$ element
  
  (to distinguish $\Omega_{\text{int} \rightarrow \text{int}}$ from $\lambda X^{\text{int}}. \Omega^{\text{int}}$)

- we restrict $\rightarrow$ to continuous functions
  
  (to be able to take fixpoints)

(see [Scott93])
Higher-order programs

Denotational semantics

**Environments:** \( \mathcal{E} \overset{\text{def}}{=} \forall \rightarrow (\bigcup_{t \in \text{type}} D_t) \)

**Semantics:** \( T[m] : \mathcal{E} \rightarrow D_{\text{typ}(m)} \)

\[
\begin{align*}
T[X] \rho & \overset{\text{def}}{=} \rho(X) \\
T[c] \rho & \overset{\text{def}}{=} c \\
T[\lambda X^t.m] \rho & \overset{\text{def}}{=} \lambda x. T[m] (\rho[X \mapsto x]) \\
T[m_1 m_2] \rho & \overset{\text{def}}{=} (T[m_1] \rho)(T[m_2] \rho) \\
T[Y^t m] \rho & \overset{\text{def}}{=} \text{lfp} (T[m] \rho) \\
T[\Omega^t] \rho & \overset{\text{def}}{=} \bot^t
\end{align*}
\]

- program functions \( \lambda \) are mapped to mathematical functions \( \lambda \)
- program recursion \( Y \) is mapped to fixpoints \( \text{lfp} \)
- errors and non-termination are mapped to (typed) \( \bot \)
- we should prove that \( T[m] \) is indeed continuous (by induction) so that \( \text{lfp} \)
  exists, and also that \( T[m_1] \) is indeed a function (by soundness of typing)
Operational semantics: based on the $\lambda$—calculus

- states are terms: $\Sigma \overset{\text{def}}{=} \text{term}$

- transition is reduction:
  
  \[
  (\lambda X^t.m_1)\ m_2 \rightarrow m_1[X \mapsto m_2] \quad \text{(\(\lambda\)-reduction)}
  \]
  \[
  \Omega^t \rightarrow \Omega^t \quad \text{(failure)}
  \]
  \[
  Y^t \ m \rightarrow m \ (Y^t \ m) \quad \text{(iteration)}
  \]
  
  plus $c_1 \ c_2 \rightarrow (c_1 + c_2)$
  
  if true $m_1 \ m_2 \rightarrow m_1$
  
  if false $m_1 \ m_2 \rightarrow m_2$

- big-step semantics $m \downarrow$: maximal reductions
  
  $m \downarrow = m' \iff m \rightarrow^* m' \land \forall m'' : m' \rightarrow m''$

  \text{(PCF is deterministic)}
How do we check that operational and denotational semantics match?

check that they have the same view of “semantically equal programs”

- denotational way: we can use $T[m_1] = T[m_2]$
- we need an operational way to compare functions
  comparing the syntax is too fine grained,
  Example: $(\lambda X^{\text{int}}.0) \neq (\lambda X^{\text{int}}.\text{minus} \ 1 \ 1)$, but they have the same denotation

Observational equivalence: observe terms in all contexts

- contexts $c$: terms with holes $\Box$
- $c[m]$ term obtained by substituting $m$ in hole
- ground is the set of terms of type int or bool
- term equivalence $\approx$:
  $m_1 \approx m_2 \iff (\forall c: c[m_1] \downarrow = c[m_2] \downarrow \text{ when } c[m_1] \in \text{ground})$
  (don’t look at a function’s syntax, force its full evaluation and look at the value result)
Higher-order programs

Full abstraction

**Full abstraction:** $\forall m_1, m_2: m_1 \approx m_2 \iff T[ m_1 ] = T[ m_2 ]$

Unexpected result: for PCF, $\Leftarrow$ holds (adequacy), but not $\Rightarrow$!

(full abstraction concept introduced by Milner in 1975, proof by Plotkin 1977)

Compare with: **IMP, NIMP** are fully abstract

$\forall s_1, s_2 \in \text{stat}: S[ s_1 ] = S[ s_2 ] \iff \forall c: A[ c[ s_1 ] ] = A[ c[ s_2 ] ]$

Intuitive explanation:

Domains such as $\mathcal{D}_{t_1 \rightarrow t_2}$ contain many functions, most of them do not correspond to any program (this is expected: many functions are not computable).

The problem is that, if $m_1, m_2$ have the form $\lambda X^{t_1 \rightarrow t_2}.m$, $T[ m_1 ] = T[ m_2 ]$ imposes $T[ m_1 ] f = T[ m_2 ] f$ for all $f \in \mathcal{D}_{t_1 \rightarrow t_2}$, including many $f$ that are not computable.

It is actually possible to construct $m_1, m_2$ where $T[ m_1 ] f \neq T[ m_2 ] f$ only for some non-program functions $f$, so that $m_1 \approx m_2$ actually holds

Two solutions come to mind:

- enrich the language to express more functions in $\mathcal{D}_{t_1 \rightarrow t_2}$ (next slide)
- restrict $\mathcal{D}_{t_1 \rightarrow t_2}$ to contain less non-program objects

Fruitful but complex research topic...
Example: the parallel or function $por$

$$por(a)(b) \overset{\text{def}}{=} \begin{cases} 
\text{true} & \text{if } a = \text{true} \lor b = \text{true} \\
\text{false} & \text{if } a = \text{false} \land b = \text{false} \\
\bot & \text{otherwise}
\end{cases}$$

$por$ can observe $a$ and $b$ concurrently, and return as soon as one returns true compare with sequential or, where $\forall b: or(\bot)(b) = \bot$

We have the following non-obvious result:

- $por$ cannot be defined in PCF
  ($por$ is a parallel construct, PCF is a sequential language)
- PCF$+por$ is fully abstract

(see [Ong95], [Winskel97] for references on the subject)
Recursive domain equations
Recursive domain equations

Untyped higher order language

\[\text{term} ::= X \quad (\text{variable } X \in \mathcal{V})
\]

\[\quad | \quad c \quad (\text{constants})
\]

\[\quad | \quad \lambda X. \text{term} \quad (\text{abstraction})
\]

\[\quad | \quad \text{term} \text{ term} \quad (\text{application})
\]

\[\quad | \quad \Omega \quad (\text{failure})
\]

we can write truly polymorphic functions: e.g., \(\lambda X. X\)
(in \text{PCF} we would have to choose a type: \text{int} \rightarrow \text{int} or \text{bool} \rightarrow \text{bool} or \text{(int} \rightarrow \text{int}) \rightarrow \text{(int} \rightarrow \text{int}) or \ldots)

no need for a recursion combinator \(Y\)
(we can define \(Y \overset{\text{def}}{=} \lambda F.(\lambda X.F (X X))(\lambda X.F (X X)), \text{not typable in } \text{PCF})

operational semantics based on reduction, similarly to \text{PCF}

denotational semantics also similar to \text{PCF}, \text{but} \ldots
Recursive domain equations

Domain equations

How to choose the domain of denotations $T[\ m\ ]$?

- we need a unique domain $D$ for all terms
  *(no type information to help us)*

- $\lambda X.X$ is a function
  $\implies$ it should have denotation in $(\mathcal{X} \to \mathcal{Y})_\perp$ for some $\mathcal{X}, \mathcal{Y} \subseteq D$

- $\lambda X.X$ is polymorphic; it accepts any term as argument
  $\implies D \subseteq \mathcal{X}, \mathcal{Y}$

We have a domain equation to solve:

$$D \simeq (\mathbb{Z} \cup \mathbb{B} \cup (D \to D))_\perp$$

**Problem:** no solution in set theory

$(D \to D$ has a strictly larger cardinal than $D)$
Recursive domain equations

Inverse limits

Given a fixpoint domain equation $D = F(D)$ we construct an infinite sequence of domains:

- $D_0 \overset{\text{def}}{=} \{ \bot \}$
- $D_{i+1} \overset{\text{def}}{=} F(D_i)$

We require the existence of continuous rejections:

- $\gamma_i : D_i \overset{c}{\to} D_{i+1}$ (embedding)
- $\alpha_i : D_{i+1} \overset{c}{\to} D_i$ (projection)
- $\alpha_i \circ \gamma_i = \lambda x.x$ ($D_i \simeq$ a subset of $D_{i+1}$)
- $\gamma_i \circ \alpha_i \sqsubseteq \lambda x.x$ ($D_{i+1}$ can be approximated by $D_i$)

This is denoted: $D_0 \xleftarrow{\alpha_0} \gamma_0 \xrightarrow{\alpha_1} \gamma_1 \xrightarrow{\alpha_1} \cdots$

**Inverse limit:** $D_\infty \overset{\text{def}}{=} \{ (a_0, a_1, \ldots) \mid \forall i: a_i \in D_i \land a_i = \alpha(a_{i+1}) \}$

(infinite sequences of elements; able to represent an element of any $D_i$)
Inverse limits: \( \mathcal{D}_\infty \overset{\text{def}}{=} \{(a_0, a_1, \ldots) \mid \forall i: a_i \in \mathcal{D}_i \land a_i = \alpha(a_{i+1})\} \)

**Theorem**

\( \mathcal{D}_\infty \) is a cpo and \( F(\mathcal{D}_\infty) \) is isomorphic to \( \mathcal{D}_\infty \)

**Application** to \( \lambda \)-calculus

If we restrict ourself to continuous functions, retractions can be computed for \( F(\mathcal{D}) \overset{\text{def}}{=} (\mathbb{Z} \cup \mathbb{B} \cup (\mathcal{D} \to \mathcal{D}))_\perp \)

\( \gamma_i(f) \overset{\text{def}}{=} \lambda x. f \)

\( \alpha_i(x) \overset{\text{def}}{=} x \) if \( x \in \mathbb{Z} \cup \mathbb{B} \cup \{\perp\} \) and \( \alpha_i(f) \overset{\text{def}}{=} f(\perp) \) if \( f \in \mathcal{D}_i \to \mathcal{D}_i \)

\( \implies \) we found our semantic domain!

(pioneered by [Scott-Strachey71], see [Abramsky-Jung94] for a reference)
Recursive domain equations

Restrictions of function spaces

The restriction to continuous functions seems merely technical but there are some valid justifications:

- all the denotations in **IMP**, **NIMP**, **PCF** were continuous
  (this appeared naturally, not as an a priori restriction)

- intuitively, computable functions should at least be **monotonic**
  recall that $\sqsubseteq$ is an information order
  a function cannot give a more precise result with less information
  e.g.: if $f(a) = \perp$ for some $a \neq \perp$, then $f(\perp) = \perp$

- **continuity** is also reasonable
  given a problem on an infinite data set $S$
  computers can only process finite parts $S_i$ of $S$
  continuity ensures that the solution of $S$ is contained in that of all $S_i$
  e.g.: if $0 \sqsubseteq 1 \sqsubseteq \cdots \sqsubseteq \omega$ and $\forall i < \omega: f(i) = 0$, then $f(\omega)$ should also be 0
Recursive domain equations

Data-types

Solution domains of recursive equations can also give the semantics of a variety of inductive or polymorphic data-types

Examples:

- **integer lists:**
  \[ D = (\{\text{empty}\} \cup (\mathbb{Z} \times D)) \bot \]

- **pairs:**
  \[ D = (\mathbb{Z} \cup (D \times D)) \bot \]
  (allows arbitrary nested pairs, and also contains trees and lists)

- **records:**
  \[ D = (\mathbb{Z} \cup (\mathbb{N} \rightarrow D)) \bot \]
  (fields are named by integer position)

- **sum types:**
  \[ D = (\mathbb{Z} \cup (\{1\} \times D) \cup (\{2\} \times D)) \bot \]
  (we “tag” each case of the sum with an integer)
Courses and references on denotational semantics:


Research articles and surveys:


