Lecture 1

Introduction

What is this course about?

- General area.
  *Formal methods:* Mathematical techniques for the specification, development, and verification of software and hardware systems.

- Specific area.
  *Formal semantics:* Mathematical theories for ascribing meanings to computer languages.

Why do we care?

- Rigour.
  - specification of programming languages
  - justification of program transformations

- Insight.
  - generalisations of notions computability
  - higher-order functions
  - data structures

- Feedback into language design.
  - continuations
  - monads

- Reasoning principles.
  - Scott induction
  - Logical relations
  - Co-induction
Styles of formal semantics

Operational.
Meanings for program phrases defined in terms of the steps of computation they can take during program execution.

Axiomatic.
Meanings for program phrases defined indirectly via the axioms and rules of some logic of program properties.

Denotational.
Concerned with giving mathematical models of programming languages. Meanings for program phrases defined abstractly as elements of some suitable mathematical structure.

Characteristic features of a denotational semantics

- Each phrase (= part of a program), $P$, is given a denotation, $\llbracket P \rrbracket$ — a mathematical object representing the contribution of $P$ to the meaning of any complete program in which it occurs.

- The denotation of a phrase is determined just by the denotations of its subphrases (one says that the semantics is compositional).

Basic idea of denotational semantics

<table>
<thead>
<tr>
<th>Syntax</th>
<th>$\rightarrow$</th>
<th>Semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recursive program</td>
<td>$\mapsto$</td>
<td>Partial recursive function</td>
</tr>
<tr>
<td>Boolean circuit</td>
<td>$\mapsto$</td>
<td>Boolean function</td>
</tr>
</tbody>
</table>

$P \mapsto \llbracket P \rrbracket$

Concerns:
- Abstract models (i.e. implementation/machine independent).
  \(\mapsto\) Lectures 2, 3 and 4.
- Compositionality.
  \(\mapsto\) Lectures 5 and 6.
- Relationship to computation (e.g. operational semantics).
  \(\mapsto\) Lectures 7 and 8.

Basic example of denotational semantics (I)

IMP syntax

**Arithmetic expressions**

$$A ::= n \mid L \mid A + A \mid \ldots$$

where $n$ ranges over integers and $L$ over a specified set of locations $\mathbb{L}$

**Boolean expressions**

$$B ::= \text{true} \mid \text{false} \mid A = A \mid \ldots \mid \neg B \mid \ldots$$

**Commands**

$$C ::= \text{skip} \mid L := A \mid C; C \mid \text{if } B \text{ then } C \text{ else } C \mid \text{while } B \text{ do } C$$
Basic example of denotational semantics (II)

Semantic functions

\[ A : \text{Aexp} \rightarrow (\text{State} \rightarrow \mathbb{Z}) \]
\[ B : \text{Bexp} \rightarrow (\text{State} \rightarrow \mathbb{B}) \]
\[ C : \text{Comm} \rightarrow (\text{State} \rightarrow \text{State}) \]

where

\[ \mathbb{Z} = \ldots, -1, 0, 1, \ldots \]
\[ \mathbb{B} = \{ \text{true}, \text{false} \} \]
\[ \text{State} = (\mathbb{L} \rightarrow \mathbb{Z}) \]

Basic example of denotational semantics (III)

Semantic function \( A \)

\[ A[n] = \lambda s \in \text{State}. n \]
\[ A[L] = \lambda s \in \text{State}. s(L) \]
\[ A[A_1 + A_2] = \lambda s \in \text{State}. A[A_1](s) + A[A_2](s) \]

Basic example of denotational semantics (IV)

Semantic function \( B \)

\[ B[\text{true}] = \lambda s \in \text{State}. \text{true} \]
\[ B[\text{false}] = \lambda s \in \text{State}. \text{false} \]
\[ B[A_1 = A_2] = \lambda s \in \text{State}. \text{eq}(A[A_1](s), A[A_2](s)) \]

where \( \text{eq}(a, a') = \begin{cases} 
  \text{true} & \text{if } a = a' \\
  \text{false} & \text{if } a \neq a' 
\end{cases} \)

Basic example of denotational semantics (V)

Semantic function \( C \)

\[ [\text{skip}] = \lambda s \in \text{State}. s \]

NB: From now on the names of semantic functions are omitted!
A simple example of compositionality

Given partial functions \([C], [C'] : \text{State} \rightarrow \text{State}\) and a function \([B] : \text{State} \rightarrow \{\text{true}, \text{false}\}\), we can define

\[
\text{[if } B \text{ then } C \text{ else } C'] = \lambda s \in \text{State. if } ([B](s), [C](s), [C'](s))
\]

where

\[
\text{if } (b, x, x') = \begin{cases} x \text{ if } b = \text{true} \\ x' \text{ if } b = \text{false} \end{cases}
\]

Basic example of denotational semantics (VI)

Semantic function \(C\)

\[
[L := A] = \lambda s \in \text{State. } \lambda \ell \in \mathbb{L}. \text{ if } (\ell = L, [A](s), s(\ell))
\]

Denotational semantics of sequential composition

Denotation of sequential composition \(C; C'\) of two commands

\[
[C; C'] = [C'] \circ [C] = \lambda s \in \text{State. } [C']([C](s))
\]

given by composition of the partial functions from states to states \([C], [C'] : \text{State} \rightarrow \text{State}\) which are the denotations of the commands.

Cf. operational semantics of sequential composition:

\[
\frac{C, s \Downarrow s'}{C; C', s' \Downarrow s''}. 
\]

Fixed point property of \([\text{while } B \text{ do } C]\)

\[
[\text{while } B \text{ do } C] = f_{[B], [C]}([\text{while } B \text{ do } C])
\]

where, for each \(b : \text{State} \rightarrow \{\text{true, false}\}\) and \(c, w : \text{State} \rightarrow \text{State}\), we define

\[
f_{b, c} : (\text{State} \rightarrow \text{State}) \rightarrow (\text{State} \rightarrow \text{State})
\]

as

\[
f_{b, c} = \lambda w \in (\text{State} \rightarrow \text{State}). \lambda s \in \text{State. if } (b(s), w(c(s)), s).
\]

- Why does \(w = f_{[B], [C]}(w)\) have a solution?
- What if it has several solutions—which one do we take to be \([\text{while } B \text{ do } C]\)?
Approximating $[\text{while } B \text{ do } C]$  

\[
\begin{align*}
    f_{[B],[C]}^{\downarrow}(\bot) &= \lambda s \in \text{State}. \\
    &= \begin{cases} \\
        [C]^k(s) & \text{if } \exists 0 \leq k < n. \ [B](\ [C]^k(s)) = \text{false} \\
        \text{and } \forall 0 \leq i < k. \ [B](\ [C]^i(s)) = \text{true} \\
        \uparrow & \text{if } \forall 0 \leq i < n. \ [B](\ [C]^i(s)) = \text{true}
    \end{cases}
\end{align*}
\]

\[
D \overset{\text{def}}{=} \text{State} \rightarrow \text{State}
\]

- Partial order $\sqsubseteq$ on $D$: 
  \[
  w \sqsubseteq w' \quad \text{iff} \quad \text{for all } s \in \text{State}, \text{if } w \text{ is defined at } s \text{ then so is } w' \text{ and moreover } w(s) = w'(s).
  \]
  \[
  \text{iff} \quad \text{the graph of } w \text{ is included in the graph of } w'.
  \]

- Least element $\bot \in D$ w.r.t. $\sqsubseteq$: 
  \[
  \bot = \text{totally undefined partial function} \\
  = \text{partial function with empty graph}
  \]
  (satisfies $\bot \sqsubseteq w$, for all $w \in D$).