Denotational Semantics

10 lectures for Part II CST 2019/20

Marcelo Fiore

Course web page:

http://www.cl.cam.ac.uk/teaching/1920/DenotSem/

Topic 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.

Basic idea of denotational semantics

$$\text{Syntax} \quad \xrightarrow{[\![-]\!]} \quad \text{Semantics}$$

$$P \quad \mapsto \quad [\![P]\!]$$

Examples

Prop. Formula $\longmapsto$ Truth value

Partial rec. function $\longmapsto$ $\mathbb{N} \to \mathbb{N}$

Basic idea of denotational semantics

$$\begin{array}{rcl} \text{Syntax} & \xrightarrow{[\![-]\!]} & \text{Semantics} \\ \text{Recursive program} & \mapsto & \text{Partial recursive function} \\ \text{Boolean circuit} & \mapsto & \text{Boolean function} \\ P & \mapsto & [\![P]\!] \end{array}$$

Concerns:

- Abstract models (*i.e.* implementation/machine independent).

  $\rightsquigarrow$ Lectures 2, 3 and 4.

- Compositionality.

  $\rightsquigarrow$ Lectures 5 and 6.

- Relationship to computation (*e.g.* operational semantics).

  $\rightsquigarrow$ Lectures 7 and 8.

Characteristic features of a denotational semantics

- Each phrase (= part of a program), P, is given a denotation, $[\![P]\!]$ — 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 example of denotational semantics (I)

IMP$^-$ syntax

Arithmetic expressions

$$A \in \mathbf{Aexp} \quad ::= \quad \underline{n} \mid L \mid A + A \mid \ldots$$

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

Boolean expressions

$$\begin{aligned} B \in \mathbf{Bexp} \quad ::= \quad & \mathbf{true} \mid \mathbf{false} \mid A = A \mid \ldots \\ \mid \quad & \neg B \mid \ldots \end{aligned}$$

Commands

$$\begin{aligned} C \in \mathbf{Comm} \quad ::= \quad & \mathbf{skip} \mid L := A \mid C ; C \\ \mid \quad & \mathbf{if}\ B\ \mathbf{then}\ C\ \mathbf{else}\ C \end{aligned}$$

Basic example of denotational semantics (II)

$A \in \underline{Aexp}$

Semantic functions

$\mathcal{A}[\![A]\!] : State \to \mathbb{Z}$

$$\mathcal{A} : \quad \mathbf{Aexp} \to \underbrace{(State \to \mathbb{Z})}_{\text{the set of functions from the set of states to the set of integers.}} \quad \text{(total)}$$

where

$$\mathbb{Z} \quad = \quad \{\ldots, -1, 0, 1, \ldots\}$$

$\mathbb{L}$: The set of locations.

$$State \quad = \quad (\mathbb{L} \to \mathbb{Z})$$

Idea
$s \in State$
Then for a location $L \in \mathbb{L}$, $s(L) \in \mathbb{Z}$ is the value of L in state s.

Basic example of denotational semantics (II)

Semantic functions

$$
\begin{aligned}
\mathcal{A} :& \quad \mathbf{Aexp} \to (State \to \mathbb{Z}) \\
\mathcal{B} :& \quad \mathbf{Bexp} \to (State \to \mathbb{B}) \\
\mathcal{C} :& \quad \mathbf{Comm} \to \underbrace{(State \rightharpoonup State)}_{\text{partial functions from State to State.}}
\end{aligned}
$$

where

$$
\begin{aligned}
\mathbb{Z} &= \{\ldots, -1, 0, 1, \ldots\} \\
\mathbb{B} &= \{\, true, false \,\} \\
State &= (\mathbb{L} \to \mathbb{Z})
\end{aligned}
$$

= State transformers.

Basic example of denotational semantics (III)

Semantic function $\mathcal{A}$

Syntax Semantics

number

$$\mathcal{A}[\![\underline{n}]\!] = \lambda s \in State.\, n$$

token

$$\mathcal{A}[\![L]\!] = \lambda s \in State.\, s(L)$$

$$\underbrace{\mathcal{A}[\![A_1 + A_2]\!]}_{\text{syntax}} = \lambda s \in State.\, \underbrace{\mathcal{A}[\![A_1]\!](s) + \mathcal{A}[\![A_2]\!](s)}_{\text{semantics (addition)}}$$

Basic example of denotational semantics (IV)

Semantic function $\mathcal{B}$

$$\begin{aligned}
\mathcal{B}[\![\mathbf{true}]\!] &= \lambda s \in \mathit{State}.\, \mathit{true} \\
\mathcal{B}[\![\mathbf{false}]\!] &= \lambda s \in \mathit{State}.\, \mathit{false} \\
\mathcal{B}[\![A_1 = A_2]\!] &= \lambda s \in \mathit{State}.\, \mathit{eq}\big(\mathcal{A}[\![A_1]\!](s), \mathcal{A}[\![A_2]\!](s)\big)
\end{aligned}$$

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

Basic example of denotational semantics (V)

Semantic function $\mathcal{C}$

identity function

$$[\![\mathbf{skip}]\!] \quad = \quad \lambda s \in State.\, s$$

NB: From now on the names of semantic functions are omitted!

A simple example of compositionality

Given partial functions $[\![C]\!], [\![C']\!] : \mathit{State} \rightharpoonup \mathit{State}$ and a function $[\![B]\!] : \mathit{State} \to \{\mathit{true}, \mathit{false}\}$, we can define

$$[\![\mathbf{if}\ B\ \mathbf{then}\ C\ \mathbf{else}\ C']\!] = \lambda s \in \mathit{State}.\ \mathit{if}\big([\![B]\!](s), [\![C]\!](s), [\![C']\!](s)\big)$$

where

$$\mathit{if}\,(b, x, x') = \begin{cases} x & \text{if } b = \mathit{true} \\ x' & \text{if } b = \mathit{false} \end{cases}$$

Basic example of denotational semantics (VI)

Semantic function $\mathcal{C}$

$$[\![L := A]\!] \quad = \quad \lambda s \in State.\, \lambda \ell \in \mathbb{L}.\, if\left(\ell = L, [\![A]\!](s), s(\ell)\right)$$

Denotational semantics of sequential composition

Denotation of sequential composition $C; C'$ of two commands

$$[\![C; C']\!] = [\![C']\!] \circ [\![C]\!] = \lambda s \in State.\, [\![C']\!]\big([\![C]\!](s)\big)$$

given by composition of the partial functions from states to states $[\![C]\!], [\![C']\!] : State \rightharpoonup State$ which are the denotations of the commands.

<u>Syntax</u> <u>Semantics</u>

Sequencing $\longmapsto$ Composition.

$\mathrm{skip}; C \equiv C \equiv C; \mathrm{skip}$ $\qquad$ $id \circ f = f = f \circ id$

$(C_1; C_2); C_3 \equiv C_1; (C_2; C_3)$ $\qquad$ $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$

Denotational semantics of sequential composition

Denotation of sequential composition $C; C'$ of two commands

$$[\![C; C']\!] = [\![C']\!] \circ [\![C]\!] = \lambda s \in State.\, [\![C']\!]\big([\![C]\!](s)\big)$$

given by composition of the partial functions from states to states $[\![C]\!], [\![C']\!] : State \rightharpoonup State$ which are the denotations of the commands.

Cf. operational semantics of sequential composition:

$$\frac{C, s \Downarrow s' \quad C', s' \Downarrow s''}{C; C', s \Downarrow s''} \;.$$

$[\![\textbf{while } B \textbf{ do } C]\!]$

$[\![\text{while } B \text{ do } C]\!] : State \to State$

$s \in State$

$[\![\text{while } B \text{ do } C]\!](s) \overset{?}{=} \ldots [\![B]\!](s) \ldots [\![C]\!](s) \ldots$

$\text{while } B \text{ do } C \equiv \text{if } B \text{ then } (C; \text{while } B \text{ do } C) \text{ else skip}$

$[\![\text{while } B \text{ do } C]\!]s = [\![\text{if } B \text{ then } (C; \text{while } B \text{ do } C) \text{ else skip}]\!]s$

$= \text{if}([\![B]\!](s), [\![C; \text{while } B \text{ do } C]\!](s), s)$

$[\![\text{while } B \text{ do } C]\!]s \overset{\text{DEF?}}{=} \text{if}([\![B]\!](s), [\![\text{while } B \text{ do } C]\!]([\![C]\!]s), s)$