CS 4110

Programming Languages & Logics

Lecture 8
Denotational Semantics

10 September 2012

Announcements

- Homework #2 due tonight at 11:59pm
- Foster office hours today 4-5pm in Upson 4137
- Rajkumar office hours today 5-6pm in 4135
- Homework #3 goes out today

Recap

So far, we've:

- Formalized the operational semantics of an imperative language
- Developed the theory of inductive sets
- Used this theory to prove formal properties:
  - Determinism
  - Soundness (via Progress and Preservation)
  - Termination
  - Equivalence of small-step and large-step semantics
- Developed an implementation in OCaml
- Extended to IMP, a more complete imperative language

Today we'll develop a denotational semantics for IMP

Denotational Semantics

An operational semantics models *how* a program executes on an idealized machine:

$$\langle \sigma, e \rangle \rightarrow \langle \sigma', e' \rangle \qquad\qquad \langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle$$

Denotational Semantics

An operational semantics models *how* a program executes on an idealized machine:

$$\langle \sigma, e \rangle \to \langle \sigma', e' \rangle \qquad\qquad \langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle$$

A denotational semantics models *what* a program computes.

Denotational Semantics

An operational semantics models *how* a program executes on an idealized machine:

$$\langle \sigma, e \rangle \to \langle \sigma', e' \rangle \qquad\qquad \langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle$$

A denotational semantics models *what* a program computes.

More specifically, a denotational semantics defines the meaning of a program directly, as a mathematical function:

$$\mathcal{C}[\![c]\!] \in \textbf{Store} \rightharpoonup \textbf{Store}$$

IMP

Syntax

$$
\begin{array}{lrl}
a \in \textbf{Aexp} & a ::= & x \mid n \mid a_1 + a_2 \mid a_1 \times a_2 \\
b \in \textbf{Bexp} & b ::= & \textbf{true} \mid \textbf{false} \mid a_1 < a_2 \\
c \in \textbf{Com} & c ::= & \textbf{skip} \mid x := a \mid c_1 ; c_2 \\
 & \mid & \textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2 \mid \textbf{while } b \textbf{ do } c
\end{array}
$$

IMP

Syntax

$$
\begin{array}{llcl}
a \in \textbf{Aexp} & a & ::= & x \mid n \mid a_1 + a_2 \mid a_1 \times a_2 \\
b \in \textbf{Bexp} & b & ::= & \textbf{true} \mid \textbf{false} \mid a_1 < a_2 \\
c \in \textbf{Com} & c & ::= & \textbf{skip} \mid x := a \mid c_1 ; c_2 \\
 & & \mid & \textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2 \mid \textbf{while } b \textbf{ do } c
\end{array}
$$

Semantic Domains

$$
\begin{array}{rcl}
\mathcal{C}[\![c]\!] & \in & \textbf{Store} \rightharpoonup \textbf{Store} \\
\mathcal{A}[\![a]\!] & \in & \textbf{Store} \rightharpoonup \textbf{Int} \\
\mathcal{B}[\![b]\!] & \in & \textbf{Store} \rightharpoonup \textbf{Bool}
\end{array}
$$

IMP

Syntax

$$
\begin{array}{llrl}
a \in \textbf{Aexp} & & a ::= & x \mid n \mid a_1 + a_2 \mid a_1 \times a_2 \\
b \in \textbf{Bexp} & & b ::= & \textbf{true} \mid \textbf{false} \mid a_1 < a_2 \\
c \in \textbf{Com} & & c ::= & \textbf{skip} \mid x := a \mid c_1 ; c_2 \\
& & \mid & \textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2 \mid \textbf{while } b \textbf{ do } c
\end{array}
$$

Semantic Domains

$$
\begin{array}{rcl}
\mathcal{C}[\![c]\!] & \in & \textbf{Store} \rightharpoonup \textbf{Store} \\
\mathcal{A}[\![a]\!] & \in & \textbf{Store} \rightharpoonup \textbf{Int} \\
\mathcal{B}[\![b]\!] & \in & \textbf{Store} \rightharpoonup \textbf{Bool}
\end{array}
$$

Why partial functions?

Conventions

Represent functions $f : A \rightharpoonup B$ as sets of pairs:

$$S = \{(a, b) \mid a \in A \text{ and } b = f(a) \in B\}$$

such that, for each $a \in A$, there is at most one pair $(a, \_)$ in S.

That is, $(a, b) \in S$ if and only if $f(a) = b$.

Convention #2: Define functions point-wise.

Equation $\mathcal{C}[\![c]\!] = S$ defines the denotation function $\mathcal{C}[\![\cdot]\!]$ on c.

Denotational Semantics of IMP

$$
\begin{aligned}
\mathcal{A}[\![n]\!] &= \{(\sigma, n)\} \\
\mathcal{A}[\![x]\!] &= \{(\sigma, \sigma(x))\} \\
\mathcal{A}[\![a_1 + a_2]\!] &= \{(\sigma, n) \mid (\sigma, n_1) \in \mathcal{A}[\![a_1]\!] \wedge (\sigma, n_2) \in \mathcal{A}[\![a_2]\!] \wedge n = n_1 + n_2\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{B}[\![\mathbf{true}]\!] &= \{(\sigma, \mathbf{true})\} \\
\mathcal{B}[\![\mathbf{false}]\!] &= \{(\sigma, \mathbf{false})\} \\
\mathcal{B}[\![a_1 < a_2]\!] &= \{(\sigma, \mathbf{true}) \mid (\sigma, n_1) \in \mathcal{A}[\![a_1]\!] \wedge (\sigma, n_2) \in \mathcal{A}[\![a_2]\!] \wedge n_1 < n_2\} \cup \\
&\quad\; \{(\sigma, \mathbf{false}) \mid (\sigma, n_1) \in \mathcal{A}[\![a_1]\!] \wedge (\sigma, n_2) \in \mathcal{A}[\![a_2]\!] \wedge n_1 \geq n_2\}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{C}[\![\mathbf{skip}]\!] &= \{(\sigma, \sigma)\} \\
\mathcal{C}[\![x := a]\!] &= \{(\sigma, \sigma[x \mapsto n]) \mid (\sigma, n) \in \mathcal{A}[\![a]\!]\} \\
\mathcal{C}[\![c_1; c_2]\!] &= \{(\sigma, \sigma') \mid \exists \sigma''.\, ((\sigma, \sigma'') \in \mathcal{C}[\![c_1]\!] \wedge (\sigma'', \sigma') \in \mathcal{C}[\![c_2]\!])\} \\
\mathcal{C}[\![\mathbf{if}\ b\ \mathbf{then}\ c_1\ \mathbf{else}\ c_2]\!] &= \{(\sigma, \sigma') \mid (\sigma, \mathbf{true}) \in \mathcal{B}[\![b]\!] \wedge (\sigma, \sigma') \in \mathcal{C}[\![c_1]\!]\} \cup \\
&\quad\; \{(\sigma, \sigma') \mid (\sigma, \mathbf{false}) \in \mathcal{B}[\![b]\!] \wedge (\sigma, \sigma') \in \mathcal{C}[\![c_2]\!]\} \\
\mathcal{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!] &= \{(\sigma, \sigma) \mid (\sigma, \mathbf{false}) \in \mathcal{B}[\![b]\!]\} \cup \\
&\quad\; \{(\sigma, \sigma') \mid (\sigma, \mathbf{true}) \in \mathcal{B}[\![b]\!] \wedge \exists \sigma''.\, ((\sigma, \sigma'') \in \mathcal{C}[\![c]\!] \wedge \\
&\qquad\qquad (\sigma'', \sigma') \in \mathcal{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!])\}
\end{aligned}
$$

Recursive Definitions

Problem: the last "definition" in our semantics is not really a definition!

$$\begin{aligned}\mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!] = {} & \{(\sigma,\sigma) \mid (\sigma,\textbf{false}) \in \mathcal{B}[\![b]\!]\} \ \cup \\ & \{(\sigma,\sigma') \mid (\sigma,\textbf{true}) \in \mathcal{B}[\![b]\!] \wedge \exists\sigma''.\ ((\sigma,\sigma'') \in \mathcal{C}[\![c]\!] \ \wedge \\ & \qquad (\sigma'',\sigma') \in \mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!])\}\end{aligned}$$

Why?

Recursive Definitions

Problem: the last "definition" in our semantics is not really a definition!

$$\begin{aligned}\mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!] = \{(\sigma,\sigma) \mid (\sigma, \textbf{false}) \in \mathcal{B}[\![b]\!]\} \;\cup \\ \{(\sigma,\sigma') \mid (\sigma, \textbf{true}) \in \mathcal{B}[\![b]\!] \wedge \exists \sigma''.\, ((\sigma,\sigma'') \in \mathcal{C}[\![c]\!] \;\wedge \\ (\sigma'',\sigma') \in \mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!])\}\end{aligned}$$

Why?

It expresses $\mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!]$ in terms of itself.

So this is not a definition but a recursive equation.

What we want is the solution to this equation.

Recursive Equations

Example:

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ f(x-1) + 2x - 1 & \text{otherwise} \end{cases}$$

Recursive Equations

Example:

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ f(x-1) + 2x - 1 & \text{otherwise} \end{cases}$$

Question: What functions satisfy this equation?

Recursive Equations

Example:

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ f(x-1) + 2x - 1 & \text{otherwise} \end{cases}$$

Question: What functions satisfy this equation?

Answer: $f(x) = x^2$

Recursive Equations

Example:

$$g(x) = g(x) + 1$$

Recursive Equations

Example:

$$g(x) = g(x) + 1$$

Question: Which functions satisfy this equation?

Recursive Equations

Example:

$$g(x) = g(x) + 1$$

Question: Which functions satisfy this equation?

Answer: None!

Recursive Equations

Example:

$$h(x) = 4 \times h\left(\frac{x}{2}\right)$$

Recursive Equations

Example:

$$h(x) = 4 \times h\left(\frac{x}{2}\right)$$

Question: Which functions satisfy this equation?

Recursive Equations

Example:

$$h(x) = 4 \times h\left(\frac{x}{2}\right)$$

Question: Which functions satisfy this equation?

Answer: There are multiple solutions.

Solving Recursive Equations

Returning the first example...

$$f(x) = \begin{cases} 0 & \text{if } x = 0 \\ f(x-1) + 2x - 1 & \text{otherwise} \end{cases}$$

Solving Recursive Equations

Can build a solution by taking successive approximations:

$$f_0 = \emptyset$$

Solving Recursive Equations

Can build a solution by taking successive approximations:

$$
\begin{aligned}
f_0 &= \emptyset \\
f_1 &= \begin{cases} 0 & \text{if } x = 0 \\ f_0(x-1) + 2x - 1 & \text{otherwise} \end{cases} \\
&= \{(0,0)\}
\end{aligned}
$$

Solving Recursive Equations

Can build a solution by taking successive approximations:

$$
\begin{aligned}
f_0 &= \emptyset \\
f_1 &= \begin{cases} 0 & \text{if } x = 0 \\ f_0(x-1) + 2x - 1 & \text{otherwise} \end{cases} \\
&= \{(0,0)\} \\
f_2 &= \begin{cases} 0 & \text{if } x = 0 \\ f_1(x-1) + 2x - 1 & \text{otherwise} \end{cases} \\
&= \{(0,0), (1,1)\}
\end{aligned}
$$

Solving Recursive Equations

Can build a solution by taking successive approximations:

$$
\begin{aligned}
f_0 &= \emptyset \\
f_1 &= \begin{cases} 0 & \text{if } x = 0 \\ f_0(x-1) + 2x - 1 & \text{otherwise} \end{cases} \\
&= \{(0,0)\} \\
f_2 &= \begin{cases} 0 & \text{if } x = 0 \\ f_1(x-1) + 2x - 1 & \text{otherwise} \end{cases} \\
&= \{(0,0),(1,1)\} \\
f_3 &= \begin{cases} 0 & \text{if } x = 0 \\ f_2(x-1) + 2x - 1 & \text{otherwise} \end{cases} \\
&= \{(0,0),(1,1),(2,4)\} \\
&\;\;\vdots
\end{aligned}
$$

Solving Recursive Equations

We can model this process using a higher-order function F that takes one approximation f_k and returns the next approximation f_{k+1}:

$$F : (\mathbb{N} \rightharpoonup \mathbb{N}) \to (\mathbb{N} \rightharpoonup \mathbb{N})$$

where

$$(F(f))(x) = \begin{cases} 0 & \text{if } x = 0 \\ f(x-1) + 2x - 1 & \text{otherwise} \end{cases}$$

Fixed Points

A solution to the recursive equation is an f such that $f = F(f)$.

Definition: Given a function $F : A \to A$, we have that $a \in A$ is a fixed point of F if and only if $F(a) = a$.

Notation: Write $a = \text{fix}(F)$ to indicate that a is a fixed point of F.

Idea: Compute fixed points iteratively, starting from the completely undefined function. The fixed point is the limit of this process:

$$\begin{aligned} f &= \text{fix}(F) \\ &= f_0 \cup f_1 \cup f_2 \cup f_3 \cup \ldots \\ &= \emptyset \cup F(\emptyset) \cup F(F(\emptyset)) \cup F(F(F(\emptyset))) \cup \ldots \\ &= \bigcup_{i \geq 0}^{\infty} F^i(\emptyset) \end{aligned}$$

Denotational Semantics for **while**

Now we can complete our denotational semantics:

$$\mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!] = \mathrm{fix}(F)$$

Denotational Semantics for **while**

Now we can complete our denotational semantics:

$$\mathcal{C}[\![\textbf{while } b \textbf{ do } c]\!] = \text{fix}(F)$$

where

$$\begin{aligned} F(f) = \{(\sigma, \sigma) \mid (\sigma, \textbf{false}) \in \mathcal{B}[\![b]\!]\} \ \cup \\ \{(\sigma, \sigma') \mid (\sigma, \textbf{true}) \in \mathcal{B}[\![b]\!] \wedge \\ \exists \sigma''.\ ((\sigma, \sigma'') \in \mathcal{C}[\![c]\!] \ \wedge (\sigma'', \sigma') \in f)\} \end{aligned}$$