CS 4110

Programming Languages & Logics

Lecture 4
Inductive Proof and Large-Step Semantics

31 August 2016

~~5 September 2014~~

Announcements

Office Hours

- ~~Nate: Friday at 11–12pm~~
- ~~Fran: Wednesday at 11–12pm~~
- ~~Nitesh: Monday at 10:30am–11:30am and Tuesday at 4:15pm – 5:15pm.~~

`Please see the website for office hours`
`https://www.cs.cornell.edu/Courses/cs4110/2016fa/`

Homework #1

- Due: next Wednesday

Review

So far we've:

- Defined a simple language of arithmetic expressions
- Formalized its semantics as a "small-step" relation:
  $\langle \sigma, e \rangle \rightarrow \langle \sigma', e' \rangle$ and $\langle \sigma, e \rangle \rightarrow^{*} \langle \sigma', e' \rangle$

Review

So far we've:

- Defined a simple language of arithmetic expressions
- Formalized its semantics as a "small-step" relation:
  $\langle \sigma, e \rangle \to \langle \sigma', e' \rangle$ and $\langle \sigma, e \rangle \to^* \langle \sigma', e' \rangle$

Today we'll:

- Proved some basic properties of the small-step relation by induction
- Develop an alternate semantics based on a "large-step" relation
- Prove the equivalence of the two semantics

Induction Principle

Every inductive set A comes with an accompanying induction principle.

To prove $\forall a \in A.\ P(a)$ we must establish several cases.

- Base cases: For each axiom

$$\frac{}{a \in A}$$

  $P(a)$ holds, and

- Inductive cases: For each inference rule

$$\frac{a_1 \in A \quad \dots \quad a_n \in A}{a \in A}$$

  if $P(a_1)$ and $\dots$ and $P(a_n)$ then $P(a)$

Induction Principle

For example, recall the inductive definition of the natural numbers:

$$\frac{}{0 \in \mathbb{N}} \qquad \frac{n \in \mathbb{N}}{succ(n) \in \mathbb{N}}$$

To prove $\forall n.\ P(n)$, we must show:

- Base case: $P(0)$
- Inductive case: $P(m) \Rightarrow P(m+1)$

This is just the usual principle of mathematical induction!

Example: Progress

Recall the progress property.

$$\begin{array}{l}\forall e \in \mathbf{Exp}.\ \forall \sigma \in \mathbf{Store}.\\ \quad \langle \sigma, e \rangle \text{ well-formed} \implies \\ \quad e \in \mathbf{Int} \text{ or } \left(\exists e' \in \mathbf{Exp}.\ \exists \sigma' \in \mathbf{Store}.\ \langle \sigma, e \rangle \to \langle \sigma', e' \rangle\right)\end{array}$$

We'll prove this by induction on the structure of e.

$$\frac{}{x \in \mathbf{Exp}} \qquad \frac{}{n \in \mathbf{Exp}}$$

$$\frac{e_1 \in \mathbf{Exp} \qquad e_2 \in \mathbf{Exp}}{e_1 + e_2 \in \mathbf{Exp}} \qquad \frac{e_1 \in \mathbf{Exp} \qquad e_2 \in \mathbf{Exp}}{e_1 * e_2 \in \mathbf{Exp}}$$

$$\frac{e_1 \in \mathbf{Exp} \qquad e_2 \in \mathbf{Exp}}{x := e_1\ ;\ e_2 \in \mathbf{Exp}}$$

Example: Progress

Recall the progress property.

$$\forall e \in \textbf{Exp}.\ \forall \sigma \in \textbf{Store}.$$
$$\langle \sigma, e\rangle \text{ well-formed } \implies$$
$$e \in \textbf{Int} \text{ or } (\exists e' \in \textbf{Exp}.\ \exists \sigma' \in \textbf{Store}.\ \langle \sigma, e\rangle \to \langle \sigma', e'\rangle)$$

P(e)

We'll prove this by induction on the structure of *e*.

$$\frac{}{x \in \textbf{Exp}} \qquad \frac{}{n \in \textbf{Exp}}$$

$$\frac{e_1 \in \textbf{Exp} \qquad e_2 \in \textbf{Exp}}{e_1 + e_2 \in \textbf{Exp}} \qquad \frac{e_1 \in \textbf{Exp} \qquad e_2 \in \textbf{Exp}}{e_1 * e_2 \in \textbf{Exp}}$$

$$\frac{e_1 \in \textbf{Exp} \qquad e_2 \in \textbf{Exp}}{x := e_1 \,;\, e_2 \in \textbf{Exp}}$$

Large-Step Semantics

Idea: define a large-step a relation that captures the *complete* evaluation of an expression.

Formally: define a relation $\Downarrow$ of type:

$$\Downarrow \subseteq (\textbf{Store} \times \textbf{Exp}) \times (\textbf{Store} \times \textbf{Int})$$

Notation: write $\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle$ to indicate that $((\sigma, e), (\sigma', n)) \in \Downarrow$

Intuition: the expression e with store σ evaluates in one big step to the final store σ' and integer n.

Integers

$$\frac{}{\langle \sigma, n \rangle \Downarrow \langle \sigma, n \rangle}\ \text{Int}$$

Variables

$$\frac{n = \sigma(x)}{\langle \sigma, x \rangle \Downarrow \langle \sigma, n \rangle} \text{ Var}$$

Addition

$$\frac{\langle \sigma, e_1 \rangle \Downarrow \langle \sigma', n_1 \rangle \qquad \langle \sigma', e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle \qquad n = n_1 + n_2}{\langle \sigma, e_1 + e_2 \rangle \Downarrow \langle \sigma'', n \rangle} \text{ Add}$$

Multiplication

$$\frac{\langle \sigma, e_1 \rangle \Downarrow \langle \sigma', n_1 \rangle \qquad \langle \sigma', e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle \qquad n = n_1 \times n_2}{\langle \sigma, e_1 * e_2 \rangle \Downarrow \langle \sigma'', n \rangle}\ \text{Mul}$$

Assignment

$$\frac{\langle \sigma, e_1 \rangle \Downarrow \langle \sigma', n_1 \rangle \qquad \langle \sigma'[x \mapsto n_1], e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle}{\langle \sigma, x := e_1 \,;\, e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle} \text{ Assgn}$$

Large-Step Semantics

$$\frac{}{\langle \sigma, n \rangle \Downarrow \langle \sigma, n \rangle}\ \text{Int} \qquad \frac{n = \sigma(x)}{\langle \sigma, x \rangle \Downarrow \langle \sigma, n \rangle}\ \text{Var}$$

$$\frac{\langle \sigma, e_1 \rangle \Downarrow \langle \sigma', n_1 \rangle \qquad \langle \sigma', e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle \qquad n = n_1 + n_2}{\langle \sigma, e_1 \mathbin{\texttt{+}} e_2 \rangle \Downarrow \langle \sigma'', n \rangle}\ \text{Add}$$

$$\frac{\langle \sigma, e_1 \rangle \Downarrow \langle \sigma', n_1 \rangle \qquad \langle \sigma', e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle \qquad n = n_1 \times n_2}{\langle \sigma, e_1 \mathbin{\texttt{*}} e_2 \rangle \Downarrow \langle \sigma'', n \rangle}\ \text{Mul}$$

$$\frac{\langle \sigma, e_1 \rangle \Downarrow \langle \sigma', n_1 \rangle \qquad \langle \sigma'[x \mapsto n_1], e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle}{\langle \sigma, x \mathrel{\texttt{:=}} e_1 \,\texttt{;}\, e_2 \rangle \Downarrow \langle \sigma'', n_2 \rangle}\ \text{Assgn}$$

Example

Assume that $\sigma(bar) = 7$.

```
sigma' = sigma[foo |-> 3]
```

$$\dfrac{\dfrac{}{\langle \sigma, 3 \rangle \Downarrow \langle \sigma, 3 \rangle}\ \text{Int} \qquad \dfrac{\dfrac{}{\langle \sigma', foo \rangle \Downarrow \langle \sigma', 3 \rangle}\ \text{Var} \qquad \dfrac{}{\langle \sigma', bar \rangle \Downarrow \langle \sigma', 7 \rangle}\ \text{Var}}{\langle \sigma', foo * bar \rangle \Downarrow \langle \sigma', 21 \rangle}\ \text{Mul}}{\langle \sigma, foo \mathtt{:=} 3\,;\ foo * bar \rangle \Downarrow \langle \sigma', 21 \rangle}\ \text{Assgn}$$

Equivalence

Theorem (Equivalence of small-step and large-step)

$$\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle \textit{ if and only if } \langle \sigma, e \rangle \to^* \langle \sigma', n \rangle$$

Equivalence

Theorem (Equivalence of small-step and large-step)

$$\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle \textit{ if and only if } \langle \sigma, e \rangle \rightarrow^* \langle \sigma', n \rangle$$

To streamline the proof, we'll use the following multi-step relation:

$$\frac{}{\langle \sigma, e \rangle \rightarrow^* \langle \sigma, e \rangle}\ \text{Refl}$$

$$\frac{\langle \sigma, e \rangle \rightarrow \langle \sigma', e' \rangle \qquad \langle \sigma', e' \rangle \rightarrow^* \langle \sigma'', e'' \rangle}{\langle \sigma, e \rangle \rightarrow^* \langle \sigma'', e'' \rangle}\ \text{Trans}$$

Equivalence

Theorem (Equivalence of small-step and large-step)

$$\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle \text{ if and only if } \langle \sigma, e \rangle \rightarrow^* \langle \sigma', n \rangle$$

Lemma

1. *If* $\langle \sigma, e \rangle \rightarrow^* \langle \sigma', n \rangle$, *then:*
   - $\langle \sigma, e + e_2 \rangle \rightarrow^* \langle \sigma', n + e_2 \rangle$
   - $\langle \sigma, n_1 + e \rangle \rightarrow^* \langle \sigma', n_1 + n \rangle$
   - $\langle \sigma, e * e_2 \rangle \rightarrow^* \langle \sigma', n * e_2 \rangle$
   - $\langle \sigma, n_1 * e \rangle \rightarrow^* \langle \sigma', n_1 * n \rangle$
   - $\langle \sigma, x := e \, ; \, e_2 \rangle \rightarrow^* \langle \sigma', x := n \, ; \, e_2 \rangle$

Equivalence

Theorem (Equivalence of small-step and large-step)

$$\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle \text{ if and only if } \langle \sigma, e \rangle \rightarrow^* \langle \sigma', n \rangle$$

Lemma

1. *If* $\langle \sigma, e \rangle \rightarrow^* \langle \sigma', n \rangle$, *then:*
   - $\langle \sigma, e + e_2 \rangle \rightarrow^* \langle \sigma', n + e_2 \rangle$
   - $\langle \sigma, n_1 + e \rangle \rightarrow^* \langle \sigma', n_1 + n \rangle$
   - $\langle \sigma, e * e_2 \rangle \rightarrow^* \langle \sigma', n * e_2 \rangle$
   - $\langle \sigma, n_1 * e \rangle \rightarrow^* \langle \sigma', n_1 * n \rangle$
   - $\langle \sigma, x := e\, ;\ e_2 \rangle \rightarrow^* \langle \sigma', x := n\, ;\ e_2 \rangle$
2. *If* $\langle \sigma, e \rangle \rightarrow^* \langle \sigma', e' \rangle$ *and* $\langle \sigma', e' \rangle \rightarrow^* \langle \sigma'', e'' \rangle$, *then* $\langle \sigma, e \rangle \rightarrow^* \langle \sigma'', e'' \rangle$

Equivalence

Theorem (Equivalence of small-step and large-step)

$$\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle \textit{ if and only if } \langle \sigma, e \rangle \rightarrow^{*} \langle \sigma', n \rangle$$

Lemma

1. *If* $\langle \sigma, e \rangle \rightarrow^{*} \langle \sigma', n \rangle$, *then:*
   - $\langle \sigma, e + e_2 \rangle \rightarrow^{*} \langle \sigma', n + e_2 \rangle$
   - $\langle \sigma, n_1 + e \rangle \rightarrow^{*} \langle \sigma', n_1 + n \rangle$
   - $\langle \sigma, e * e_2 \rangle \rightarrow^{*} \langle \sigma', n * e_2 \rangle$
   - $\langle \sigma, n_1 * e \rangle \rightarrow^{*} \langle \sigma', n_1 * n \rangle$
   - $\langle \sigma, x := e\, ;\ e_2 \rangle \rightarrow^{*} \langle \sigma', x := n\, ;\ e_2 \rangle$
2. *If* $\langle \sigma, e \rangle \rightarrow^{*} \langle \sigma', e' \rangle$ *and* $\langle \sigma', e' \rangle \rightarrow^{*} \langle \sigma'', e'' \rangle$, *then* $\langle \sigma, e \rangle \rightarrow^{*} \langle \sigma'', e'' \rangle$
3. *If* $\langle \sigma, e \rangle \rightarrow \langle \sigma'', e'' \rangle$ *and* $\langle \sigma'', e'' \rangle \Downarrow \langle \sigma', n \rangle$, *then* $\langle \sigma, e \rangle \Downarrow \langle \sigma', n \rangle$