

Lecture #5: Proof Techniques for Large-step Operational Semantics

CS 6371: Advanced Programming Languages

September 5, 2007

A proof by *structural induction* consists of two major steps: First, one proves that the theorem holds for minimal derivations (that is, derivations that consist of only one rule application). This is the base case of the induction. Second, one proves that for any derivation \mathcal{D} , if all derivations smaller than \mathcal{D} satisfy the theorem, then derivation \mathcal{D} satisfies the theorem.

Here is an example proof by structural induction:

Theorem. *If $\sigma(x) = n$ and $\langle c, \sigma \rangle \Downarrow \sigma'$ and x is not in c , then $\sigma'(x) = n$.*

Proof. There exists some derivation \mathcal{D} of judgment $\langle c, \sigma \rangle \Downarrow \sigma'$. We will prove the theorem by structural induction on \mathcal{D} .

Base Case: Suppose \mathcal{D} consists of only one rule. Then $\mathcal{D} = \langle \text{skip}, \sigma \rangle \Downarrow \sigma$, so $\sigma' = \sigma$. Thus, $\sigma'(x) = \sigma(x) = n$.

Inductive Hypothesis: Assume that the theorem holds for all derivations that are strictly smaller than \mathcal{D} . That is, assume that if $\sigma_0(x) = n$, and $\langle c_0, \sigma_0 \rangle \Downarrow \sigma'_0$ has a derivation strictly smaller than \mathcal{D} , and x is not in c_0 , then $\sigma'_0(x) = n$.

Inductive Case: Suppose that \mathcal{D} consists of more than one rule. In that case, \mathcal{D} must end with one of the five large-step rules for commands other than the rule for **skip**. We therefore must consider five cases:

Case 1: Suppose \mathcal{D} ends with the sequence rule:

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle c_1, \sigma \rangle \Downarrow \sigma_2} \quad \frac{\mathcal{D}_2}{\langle c_2, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1; c_2, \sigma \rangle \Downarrow \sigma'}$$

Since x is not in c , we know that x is not in c_1 . Since $\sigma(x) = n$ (by assumption) and derivation \mathcal{D}_1 is strictly smaller than derivation \mathcal{D} , we conclude by inductive hypothesis that $\sigma_2(x) = n$. Likewise, since $\sigma_2(x) = n$, and derivation \mathcal{D}_2 is strictly smaller than derivation \mathcal{D} , and x is not in c_2 , we conclude by inductive hypothesis that $\sigma'(x) = n$.

Case 2: Suppose \mathcal{D} ends with the assignment rule:

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle a, \sigma \rangle \Downarrow i}}{\langle v := a, \sigma \rangle \Downarrow \sigma[v \mapsto i]}$$

Since x does not appear in c , we know that $v \neq x$. Therefore, $\sigma[v \mapsto i](x) = \sigma(x) = n$.

Case 3: Suppose \mathcal{D} ends with the positive rule for `if` :

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow T} \quad \frac{\mathcal{D}_2}{\langle c_1, \sigma \rangle \Downarrow \sigma'}}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \Downarrow \sigma'}$$

Since x does not appear in c , we know that x does not appear in c_1 . Since $\sigma(x) = n$ and derivation \mathcal{D}_2 is strictly smaller than derivation \mathcal{D} , we conclude by inductive hypothesis that $\sigma'(x) = n$.

Case 4: Suppose \mathcal{D} ends with the negative rule for `if` :

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow F} \quad \frac{\mathcal{D}_2}{\langle c_2, \sigma \rangle \Downarrow \sigma'}}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \Downarrow \sigma'}$$

Since x does not appear in c , we know that x does not appear in c_2 . Since $\sigma(x) = n$ and derivation \mathcal{D}_2 is strictly smaller than derivation \mathcal{D} , we conclude by inductive hypothesis that $\sigma'(x) = n$.

Case 5: Suppose \mathcal{D} ends with the rule for `while` :

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle \text{if } b \text{ then } (c; \text{while } b \text{ do } c) \text{ else skip}, \sigma \rangle \Downarrow \sigma'}}{\langle \text{while } b \text{ do } c, \sigma \rangle \Downarrow \sigma'}$$

Since x does not appear in c , we know that x does not appear in b . Thus, x does not appear in `if b then $(c; \text{while } b \text{ do } c)$ else skip`. Since $\sigma(x) = n$ and derivation \mathcal{D}_1 is strictly smaller than derivation \mathcal{D} , we conclude by inductive hypothesis that $\sigma'(x) = n$.

□

Another useful proof technique involves rearranging derivations to produce a new derivation. Here is an example:

Theorem. *The judgment $\langle \text{if } !b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \Downarrow \sigma'$ holds if and only if the judgment $\langle \text{if } b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \Downarrow \sigma'$ holds.*

Proof. We first prove the forward implication. Suppose judgment $\langle \text{if } !b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \Downarrow \sigma'$ holds. Then there exists some derivation \mathcal{D} of this judgment. Derivation \mathcal{D} must have one of two possible forms:

Case 1: Suppose \mathcal{D} ends in the positive rule for `if` :

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow F} \quad \frac{\mathcal{D}_2}{\langle c_1, \sigma \rangle \Downarrow \sigma'}}{\langle !b, \sigma \rangle \Downarrow T} \quad \frac{\mathcal{D}_2}{\langle c_1, \sigma \rangle \Downarrow \sigma'}}{\langle \text{if } !b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \Downarrow \sigma'}$$

Using derivations \mathcal{D}_1 and \mathcal{D}_2 , we can therefore derive the following:

$$\mathcal{D}' = \frac{\frac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow F} \quad \frac{\mathcal{D}_2}{\langle c_1, \sigma \rangle \Downarrow \sigma'}}{\langle \text{if } b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \Downarrow \sigma'}$$

Derivation \mathcal{D}' is a proof of judgment $\langle \text{if } b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \Downarrow \sigma'$.

Case 2: Suppose \mathcal{D} ends in the negative rule for `if` :

$$\mathcal{D} = \frac{\frac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow T} \quad \frac{\mathcal{D}_2}{\langle c_2, \sigma \rangle \Downarrow \sigma'}}{\langle !b, \sigma \rangle \Downarrow F} \quad \frac{\mathcal{D}_2}{\langle c_2, \sigma \rangle \Downarrow \sigma'}}{\langle \text{if } !b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \Downarrow \sigma'}$$

Using derivations \mathcal{D}_1 and \mathcal{D}_2 , we can therefore derive the following:

$$\mathcal{D}' = \frac{\frac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow T} \quad \frac{\mathcal{D}_2}{\langle c_2, \sigma \rangle \Downarrow \sigma'}}{\langle \text{if } b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \Downarrow \sigma'}$$

Derivation \mathcal{D}' is a proof of judgment $\langle \text{if } b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \Downarrow \sigma'$.

The proof of the reverse implication is symmetric, and is left as an exercise to the reader. \square