Matthew Fluet

1 Review of Rule Induction

Suppose I_R is an inductively defined set. Then to show that some property P holds for all memebers of the set I_R (formally, $\forall x \in I_R.P(x)$), we can make use of rule induction by considering each rule of the form

$$\frac{x_1 \quad \cdots \quad x_n}{x}$$

and showing that

$$(\forall i \in [1, \dots, n].P(x_i)) \Rightarrow P(x).$$

Complications can arise when proving properties about two or more inductive sets that are defined in terms of one another. Note that this is different than having one set defined in terms of another set. For example, to show that boolean expressions are deterministic, we can first show that arithemetic expressions are deterministic (as a separate proof) and then proceed with rule induction on the definition of boolean expression evaluation. However, suppose that the definition of arithmetic expressions were extended as follows:

$$a ::= \cdots |\mathbf{toint}(b),$$

where b is some boolean expression. Then proving that arithmetic expressions are deterministic requires showing that boolean expressions are deterministic, and proving that boolean expressions are deterministic requires showing that arithmetic expressions are deterministic.

However, we can avoid this complication by considering both arithmetic and boolean expressions as part of some larger inductively defined set. Members of this set will be arithmetic and boolean expressions together with a flag indicating the type, as in the following:

$$(b_1 \ \mathbf{and} \ b_2, boolean) \qquad (a_1 \ + \ a_2, arithmetic).$$

We can then formalize a property about both arithemetic and boolean expressions in the following way:

$$P(x) \equiv (P_A(x) \wedge (x = (a, arithmetic))) \vee (P_B(x) \wedge (x = (b, boolean))),$$

where $P_A(x)$ is a formulation of the property for arithmetic expressions and P_B is a formulation of the property for boolean expressions.

In actual application of this property to a proof by induction, we do not need to think about this entire predicate; we can assume when proving each case that P_A holds for antecedents of the rule that are arithmetic in nature, and P_B holds for the antecedents that are about booleans, and then show that either P_A or P_B holds for the conclusion, depending on what kind of conclusion it is.

2 Equivalence of Large-step and Small-step semantics for IMP

One application of rule induction is the proof of the equivalence of large-step and small-step semantics for **IMP**. Below are the inference rules for **IMP**.

	Large-step Semantics	Small-step Semantics
skip	$\dfrac{}{\langle \mathbf{skip},\, \sigma\rangle \to \sigma}$	
$X := a$	$\dfrac{\langle a,\, \sigma\rangle \to n}{\langle X := a,\, \sigma\rangle \to \sigma[X \mapsto n]}$	$\dfrac{\langle a,\, \sigma\rangle \to n}{\langle X := a,\, \sigma\rangle \to \langle \mathbf{skip},\, \sigma[X \mapsto n]\rangle}$
$c_0\,;c_1$	$\dfrac{\langle c_0,\, \sigma\rangle \to \sigma'' \quad \langle c_1,\, \sigma''\rangle \to \sigma'}{\langle c_0\,; c_1,\, \sigma\rangle \to \sigma'}$	$\dfrac{}{\langle \mathbf{skip}\,; c_1,\, \sigma\rangle \to \langle c_1,\, \sigma\rangle}$ $\dfrac{\langle c_0,\, \sigma\rangle \to \langle c_0',\, \sigma'\rangle}{\langle c_0\,; c_1,\, \sigma\rangle \to \langle c_0'\,; c_1,\, \sigma'\rangle}$
if b **then** c_0 **else** c_1	$\dfrac{\langle b,\, \sigma\rangle \to \mathit{true} \quad \langle c_0,\, \sigma\rangle \to \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1,\, \sigma\rangle \to \sigma'}$ $\dfrac{\langle b,\, \sigma\rangle \to \mathit{false} \quad \langle c_1,\, \sigma\rangle \to \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1,\, \sigma\rangle \to \sigma'}$	$\dfrac{\langle b,\, \sigma\rangle \to \mathit{true}}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1,\, \sigma\rangle \to \langle c_0,\, \sigma\rangle}$ $\dfrac{\langle b,\, \sigma\rangle \to \mathit{false}}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1,\, \sigma\rangle \to \langle c_1,\, \sigma\rangle}$
while b **do** c	$\dfrac{\langle b,\, \sigma\rangle \to \mathit{true} \quad \langle c\,; \mathbf{while}\ b\ \mathbf{do}\ c,\, \sigma\rangle \to \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c,\, \sigma\rangle \to \sigma'}$ $\dfrac{\langle b,\, \sigma\rangle \to \mathit{false}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c,\, \sigma\rangle \to \sigma}$	$\dfrac{\langle b,\, \sigma\rangle \to \mathit{true}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c,\, \sigma\rangle \to \langle c\,; \mathbf{while}\ b\ \mathbf{do}\ c,\, \sigma\rangle}$ $\dfrac{\langle b,\, \sigma\rangle \to \mathit{false}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c,\, \sigma\rangle \to \langle \mathbf{skip},\, \sigma\rangle}$

In order to show that the two types of semantics are equivalent, we wish to show that $\langle c,\, \sigma_0\rangle \to \sigma'$ (a large-step semantics transition) if and only if $\langle c,\, \sigma_0\rangle \to \langle c_1,\, \sigma_1\rangle \to \cdots \to \langle \mathbf{skip},\, \sigma'\rangle$ (a sequence of small-step semantics transitions).

To ease the proof, we introduce the following notation

$$\langle c,\, \sigma\rangle \to^n \langle c',\, \sigma'\rangle$$

to indicate that $\langle c,\, \sigma\rangle$ can be transitioned to $\langle c',\, \sigma'\rangle$ through a sequence of n small-step semantic rule applications. Formally, $\to^n$ is defined by the following inductive definition:

$$\frac{}{\langle c,\, \sigma\rangle \to^0 \langle c,\, \sigma\rangle} \qquad \frac{\langle c,\, \sigma\rangle \to \langle c'',\, \sigma''\rangle \quad \langle c'',\, \sigma''\rangle \to^{n-1} \langle c',\, \sigma'\rangle}{\langle c,\, \sigma\rangle \to^n \langle c',\, \sigma'\rangle}.$$

Finally, we introduce the notation

$$\langle c,\, \sigma\rangle \to^* \langle c',\, \sigma'\rangle$$

to indicate that $\langle c,\, \sigma\rangle$ can be transitioned to $\langle c',\, \sigma'\rangle$ through a sequence of 0 or more small-step semantic rule applications. Formally, $\to^*$ is defined by the following rule:

$$\frac{\langle c,\, \sigma\rangle \to^n \langle c',\, \sigma'\rangle}{\langle c,\, \sigma\rangle \to^* \langle c',\, \sigma'\rangle} \qquad \text{for some } n.$$

Using this notation, to prove the equivalence of large-step and small-step semantics for **IMP**, it suffices to show that

$$\langle c,\, \sigma\rangle \to^* \langle \mathbf{skip},\, \sigma'\rangle. \Leftrightarrow \langle c,\, \sigma\rangle \to \sigma'$$

We will only prove the “if” direction of this statement.

The following is a useful lemma, which shows that a small-step semantic reduction can be "appended" to the begining of a large-step semantic reduction, yielding a valid large-step semantic reduction.

Lemma. $\langle c, \sigma\rangle \to \langle c', \sigma'\rangle \;\&\; \langle c', \sigma'\rangle \to \sigma'' \Rightarrow \langle c, \sigma\rangle \to \sigma''$.

Proof. The proof is by rule induction on the set of legal small-step transitions $\langle c, \sigma\rangle \to \langle c', \sigma'\rangle$. In particular, we show that the following property holds for all small-step transitions:

$$P(\langle c, \sigma\rangle \to \langle c', \sigma'\rangle) \equiv \forall\sigma''.\langle c, \sigma\rangle \to \langle c', \sigma'\rangle \;\&\; \langle c', \sigma'\rangle \to \sigma'' \Rightarrow \langle c, \sigma\rangle \to \sigma''.$$

We proceed by considering the different forms of commands.

$c \equiv \mathbf{skip}$: Since $\langle \mathbf{skip}, \sigma\rangle$ has no reduction rule in the small-step semantics, then the clause $\langle c, \sigma\rangle \to \langle c', \sigma'\rangle$ is vacuously true, as is the clause $\langle c, \sigma\rangle \to \langle c', \sigma'\rangle \;\&\; \langle c', \sigma'\rangle \to \sigma'' \Rightarrow \langle c, \sigma\rangle \to \sigma''$.

$c \equiv X := a$: The only applicable rule in the small-step semantics is

$$\frac{\langle a, \sigma\rangle \to n}{\langle X := a, \sigma\rangle \to \langle \mathbf{skip}, \sigma[X \mapsto n]\rangle}.$$

Hence, $c' = \mathbf{skip}$ and $\sigma' = \sigma[X \mapsto n]$. The only applicable rule in the large-step semantics is

$$\overline{\langle \mathbf{skip}, \sigma[X \mapsto n]\rangle \to \sigma[X \mapsto n]}.$$

Hence, $\sigma'' = \sigma[X \mapsto n]$. This assignment of c, σ, c', σ', and σ'' is consistent with a large-step semantic transition of the form $\langle c, \sigma\rangle \to \sigma''$ since there is the large-step semantic rule:

$$\frac{\langle a, \sigma\rangle \to n}{\langle X := a, \sigma\rangle \to \sigma[X \mapsto n]}.$$

$c \equiv c_0 \,;\, c_1$: There are two applicable rules in the small-step semantics, depending on the form of c_0. Suppose $c_0 = \mathbf{skip}$. Then the only applicable rule in the small step-semantics is

$$\overline{\langle \mathbf{skip} \,;\, c_1, \sigma\rangle \to \langle c_1, \sigma\rangle}.$$

Hence $c' = c_1$ and $\sigma' = \sigma$. To satisfy the clause $\langle c', \sigma'\rangle \to \sigma''$, we assume a transition of the form $\langle c_1, \sigma\rangle \to \sigma''$. This assignment of c, σ, c', σ', and σ'' is consistent with a large-step semantic transition of the form $\langle c, \sigma\rangle \to \sigma'$ since there is the large-step semantic rule:

$$\frac{\langle \mathbf{skip}, \sigma\rangle \to \sigma \quad \langle c_1, \sigma\rangle \to \sigma''}{\langle \mathbf{skip} \,;\, c_1, \sigma\rangle \to \sigma''}$$

Suppose $c_0 \neq \mathbf{skip}$. Then the only applicable rule in the small-step semantics is

$$\frac{\langle c_0, \sigma\rangle \to \langle c_0', \sigma'\rangle}{\langle \mathbf{skip} \,;\, c_1, \sigma\rangle \to \langle c_0' \,;\, c_1, \sigma'\rangle}.$$

Hence $c' = c_0' \,; c_1$ and $\sigma' = \sigma'$. We wish to show $P(\langle c_0 \,; c_1, \sigma\rangle \to \langle c_0' \,; c_1, \sigma'\rangle)$ assuming $P(\langle c_0, \sigma\rangle \to \langle c_0', \sigma'\rangle)$. Hence, we wish to show

$$\forall\sigma''.\langle c_0 \,;\, c_1, \sigma\rangle \to \langle c_0' \,;\, c_1, \sigma'\rangle \;\&\; \langle c_0' \,;\, c_1, \sigma'\rangle \to \sigma'' \Rightarrow \langle c_0 \,;\, c_1, \sigma\rangle \to \sigma''$$

assuming (via the induction hypothesis) that

$$\forall\sigma'''.\langle c_0, \sigma\rangle \to \langle c_0', \sigma'\rangle \;\&\; \langle c_0', \sigma'\rangle \to \sigma''' \Rightarrow \langle c_0, \sigma\rangle \to \sigma'''.$$

Assume the left-hand side of the implication we wish to show:

$$\langle c_0 \,;\, c_1, \sigma\rangle \to \langle c_0' \,;\, c_1, \sigma'\rangle \;\&\; \langle c_0' \,;\, c_1, \sigma'\rangle \to \sigma''.$$

The assumption $\langle c_0 \,\mathbf{;}\, c_1,\, \sigma\rangle \to \langle c_0' \,\mathbf{;}\, c_1,\, \sigma'\rangle$ implies $\langle c_0,\, c_1\rangle \to \langle c_0',\, \sigma'\rangle$ by the small-step semantic rule for sequences.

The assumption $\langle c_0' \,\mathbf{;}\, c_1,\, \sigma'\rangle \to \sigma''$ implies $\langle c_0',\, \sigma'\rangle \to \sigma''''$ and $\langle c_1,\, \sigma''''\rangle \to \sigma''$ (for some σ'''') by the large-step semantic rule for sequences.

By instantiating the inductive hypothesis

$$\forall \sigma'''.\langle c_0,\, \sigma\rangle \to \langle c_0',\, \sigma'\rangle \;\&\; \langle c_0',\, \sigma'\rangle \to \sigma''' \Rightarrow \langle c_0,\, \sigma\rangle \to \sigma'''.$$

with $\sigma''' = \sigma''''$, we conclude $\langle c_0,\, \sigma\rangle \to \sigma''''$.

Therefore, we conclude $\langle c_0 \,\mathbf{;}\, c_1,\, \sigma\rangle \to \sigma''$ by the large-step semantic rule:

$$\frac{\langle c_0,\, \sigma\rangle \to \sigma'''' \quad \langle c_1,\, \sigma''''\rangle \to \sigma''}{\langle c_0 \,\mathbf{;}\, c_1,\, \sigma\rangle \to \sigma''}.$$

$c \equiv \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1$: There are two applicable rules in the small-step semantics, depending on the transition of $\langle b,\, \sigma\rangle$. Suppose $\langle b,\, \sigma\rangle \to \mathit{true}$. Then the only applicable rule in the small-step semantics is

$$\frac{\langle b,\, \sigma\rangle \to \mathit{true}}{\langle \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1,\, \sigma\rangle \to \langle c_0,\, \sigma\rangle}.$$

Hence $c' = c_0$ and $\sigma' = \sigma$. To satisfy the clause $\langle c',\, \sigma'\rangle \to \sigma''$, we assume a transition of the form $\langle c_0,\, \sigma\rangle \to \sigma''$. This assignment of c, σ, c', σ', and σ'' is consistent with a large-step semantic transition of the form $\langle c,\, \sigma\rangle \to \sigma''$ since there is the large-step semantic rule:

$$\frac{\langle b,\, \sigma\rangle \to \mathit{true} \quad \langle c_0,\, \sigma\rangle \to \sigma''}{\langle \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1,\, \sigma\rangle \to \sigma''}.$$

Suppose $\langle b,\, \sigma\rangle \to \mathit{false}$. Then the only applicable rule in the small-step semantics is

$$\frac{\langle b,\, \sigma\rangle \to \mathit{false}}{\langle \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1,\, \sigma\rangle \to \langle c_1,\, \sigma\rangle}.$$

Hence $c' = c_1$ and $\sigma' = \sigma$. To satisfy the clause $\langle c',\, \sigma'\rangle \to \sigma''$, we assume a transition of the form $\langle c_1,\, \sigma\rangle \to \sigma''$. This assignment of c, σ, c', σ', and σ'' is consistent with a large-step semantic transition of the form $\langle c,\, \sigma\rangle \to \sigma''$ since there is the large-step semantic rule:

$$\frac{\langle b,\, \sigma\rangle \to \mathit{false} \quad \langle c_1,\, \sigma\rangle \to \sigma''}{\langle \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1,\, \sigma\rangle \to \sigma''}.$$

$c \equiv \mathbf{while}\, b\, \mathbf{do}\, c$: There are two applicable rules in the small-step semantics, depending on the transition of $\langle b,\, \sigma\rangle$. Suppose $\langle b,\, \sigma\rangle \to \mathit{true}$. Then the only applicable rule in the small-step semantics is

$$\frac{\langle b,\, \sigma\rangle \to \mathit{true}}{\langle \mathbf{while}\, b\, \mathbf{do}\, c,\, \sigma\rangle \to \langle c \,\mathbf{;}\, \mathbf{while}\, b\, \mathbf{do}\, c,\, \sigma\rangle}.$$

Hence $c' = c\mathbf{;}\mathbf{while}\, b\, \mathbf{do}\, c$ and $\sigma' = \sigma$. To satisfly the clause $\langle c',\, \sigma'\rangle \to \sigma''$, we assume a transition of the form $\langle c \,\mathbf{;}\, \mathbf{while}\, b\, \mathbf{do}\, c,\, \sigma\rangle \to \sigma''$. This assignment of c, σ, c', σ', and σ'' is consistent with a large-step semantic transition of the form $\langle c,\, \sigma\rangle \to \sigma''$ since there is the large-step semantic rule

$$\frac{\langle b,\, \sigma\rangle \to \mathit{true} \quad \langle c \,\mathbf{;}\, \mathbf{while}\, b\, \mathbf{do}\, c,\, \sigma\rangle \to \sigma''}{\langle \mathbf{while}\, b\, \mathbf{do}\, c,\, \sigma\rangle \to \sigma''}.$$

Suppose $\langle b,\, \sigma\rangle \to \mathit{false}$. Then the only applicable rule in the small-step semantics is

$$\frac{\langle b,\, \sigma\rangle \to \mathit{false}}{\langle \mathbf{while}\, b\, \mathbf{do}\, c,\, \sigma\rangle \to \langle \mathbf{skip},\, \sigma\rangle}.$$

Hence, $c' = \textbf{skip}$ and $\sigma' = \sigma$. The only applicable rule in the large-step semantics is

$$\frac{}{\langle \textbf{skip},\, \sigma\rangle \to \sigma.}$$

Hence, $\sigma'' = \sigma$. This assignment of c, c', σ, σ', and σ'' is consistent with a large-step semantic transition of the form $\langle c,\, \sigma\rangle \to \sigma''$ since there is the large-step semantic rule

$$\frac{\langle b,\, \sigma\rangle \to \mathit{false}}{\langle \textbf{while}\, b\, \textbf{do}\, c,\, \sigma\rangle \to \sigma.}$$

Hence, by rule induction, we have shown that $\langle c,\, \sigma\rangle \to \langle c',\, \sigma'\rangle \;\&\; \langle c',\, \sigma'\rangle \to \sigma'' \Rightarrow \langle c,\, \sigma\rangle \to \sigma''$. $\square$

This lemma can be applied to a proof of the equivalence of large-step and small-step semantics for **IMP**.

Theorem. The large-step semantics for **IMP** are equivalent to the small-step semantics for **IMP**.

Proof. To prove the equivalence of large-step and small-step semantics, we proceed by rule induction. In particular, we wish to use rule induction to show that

$$\forall c, \sigma, \sigma'. \langle c,\, \sigma\rangle \to^* \langle \textbf{skip},\, \sigma'\rangle \Rightarrow \langle c,\, \sigma\rangle \to \sigma'.$$

Note that this statement asserts that large-step semantics captures all completed small-step evaluations.

We assume the left-hand side $\langle c,\, \sigma\rangle \to^* \langle \textbf{skip},\, \sigma'\rangle$. Recall that $\langle c,\, \sigma\rangle \to^* \langle \textbf{skip},\, \sigma'\rangle$ means $\exists n. \langle c,\, \sigma\rangle \to^n \langle \textbf{skip},\, \sigma'\rangle$. Also recall the inductive definition of $\to^n$:

$$\frac{}{\langle c,\, \sigma\rangle \to^0 \langle c,\, \sigma\rangle} \qquad \frac{\langle c,\, \sigma\rangle \to \langle c'',\, \sigma''\rangle \quad \langle c'',\, \sigma''\rangle \to^{n-1} \langle c',\, \sigma'\rangle}{\langle c,\, \sigma\rangle \to^n \langle c',\, \sigma'\rangle}.$$

We proceed by induction on n.

If $n = 0$, then $\langle \textbf{skip},\, \sigma\rangle \to^0 \langle \textbf{skip},\, \sigma\rangle$ is the only satisfying assignment for $\langle c,\, \sigma\rangle \to^0 \langle \textbf{skip},\, \sigma'\rangle$. Clearly this implies $\langle \textbf{skip},\, \sigma\rangle \to \sigma$, since

$$\frac{}{\langle \textbf{skip},\, \sigma\rangle \to \sigma}$$

is an axiom of the large-step semantics.

If $n > 0$, then the second rule for $\to^n$ applies. Using rule induction, we assume $\langle c,\, \sigma\rangle \to \langle c'',\, \sigma''\rangle$ and $\langle c'',\, \sigma''\rangle \to^{n-1} \langle \textbf{skip},\, \sigma'\rangle$. By the induction hypothesis, we have that

$$\langle c'',\, \sigma''\rangle \to^{n-1} \langle \textbf{skip},\, \sigma'\rangle \Rightarrow \langle c'',\, \sigma''\rangle \to \sigma'.$$

By the previous lemma, we can assert that

$$\langle c,\, \sigma\rangle \to \langle c'',\, \sigma''\rangle \;\&\; \langle c'',\, \sigma''\rangle \to \sigma' \Rightarrow \langle c,\, \sigma\rangle \to \sigma'.$$

Hence, we have shown inductively that $\forall n. \langle c,\, \sigma\rangle \to^n \langle \textbf{skip},\, \sigma'\rangle \Rightarrow \langle c,\, \sigma\rangle \to \sigma'$.

Thus, we have proven that

$$\forall c, \sigma, \sigma'. \langle c,\, \sigma\rangle \to^* \langle \textbf{skip},\, \sigma'\rangle \Rightarrow \langle c,\, \sigma\rangle \to \sigma'.$$

which states that the large-step semantics for **IMP** can model complete evaluations performed by the small-step semantics for **IMP**. The "only-if" direction also holds but is left for the homework. $\square$