CS611 Lecture 6 Well Founded Induction 9 September, 2005
Scribe: James Worthington, Soam Vasani Lecturer: Andrew Myers

1 Summary

In this lecture we will

1. Define well-founded induction
2. Show that our definition of free variables gives us a well-defined $FV(e)$
3. Take another look at inference rules

2 Introduction

Recall that some of the substitution rules mentioned the function FV.

$(\lambda y.e_0)\{e_1/x\} = \lambda y.e_0\{e_1/x\}$, where $(y \neq x \wedge y \notin FV(e_1))$.
$(\lambda y.e_0)\{e_1/x\} = \lambda y'.e_0\{y'/y\}\{e_1/x\}$, where $(y' \neq x \wedge y' \notin FV(e_0) \wedge y' \notin FV(e_1))$

Let's examine the definition of the free variable function.

$FV(x) = \{x\}$
$FV(e_1\ e_2) = FV(e_1) \cup FV(e_2)$
$FV(\lambda x.e) = FV(e) - \{x\}$

However, how do we know that this defintion does what we want it to do? FV is a function from abstract syntax trees to sets of variables - but is it well defined? Intuition suggests that when evaluating FV on an expression, e, we will not get stuck in an infinite loop, and that FV uniquely defines a value for each expression. But how do we prove this?

We need to use the idea underlying this definition, which is called induction on well-founded relations.

A *well-founded relation* $\prec$ on a set A is a relation that has no infinite descending chains. A (descending) *chain* of elements of A is a sequence of elements $\{a_i | i \in \mathbb{N}\}$ such that $a_1 \succ a_2 \succ \cdots$
A is known as the *carrier set* of the relation. Note that a well-founded relation can't be reflexive.

Some examples of well-founded relations:

$(\mathbb{N}, \prec)$ where $m \prec n$ if $m + 1 = n$.
$(\mathbb{N}, <)$ where $<$is the less-than relation.
(The class of all sets, $\in$). ZF set theory assumes the Axiom of Foundation (or Regularity) which asserts that $\in$ is a well-founded relation. This prevents (among other things) a set from being a member of itself.

The following are *not* well-founded relations:

$(\mathbb{N}, >)$
$([0, \infty], <)$ is not well-founded because, for example, $1 < \frac{1}{2} < \frac{1}{4} < \frac{1}{8} < ...$

3 Well-Founded Induction

Suppose that A is the carrier set of a well-founded relation. Then if P is some property,

$$(\forall a \in A.P(a)) \iff \forall a \in A.([\forall b \prec a.P(b)] \rightarrow P(a))$$

For $(\mathbb{N}, <)$, this reduces to the familiar notion of (*strong* or *course-of-values*) induction on the natural numbers:

Assuming $P(0), P(1), ..., P(n-1)$, prove $P(n)$. When $n = 0$, the induction hypothesis is vacuously true, which means we need to deal with the base case separately.

Now let's define a well-founded relation on the set of all expressions: $e < e'$ if e is a **strict** sub-expression of e'. If we think of expressions as syntax trees, then e' is a tree which has e as a subtree. Since these trees are finite, the relation is is well-founded. Induction on this relation is called *structural induction.*

We can now show that $FV(e)$ is uniquely defined for any expression e:

Look at the grammar of expressions: one and only one case in the definition of FV applies to any e. All references in the definition of FV are to subexpressions. FV is uniquely defined for the basis case of the smallest expression. So $FV(e)$ is uniquely defined for any expression e.

In general, an inductive definition of a function satisfies the following conditions:

1. one pattern applies to any given argument

2. RHS is defined in terms of arguments that are predecessors.

If a function definition satisfies these two conditions, then the function is well-defined; otherwise, it may or may not be well-defined.

4 Inference rules

Recall how we defined small-step semantics, big-step semantics, etc. using inference rules. We'd like to prove that the rules that we wrote down do in fact work.

First, lets change our view of reduction and look at it as just another relation:

$e \longrightarrow e'$ means that $(e, e') \in$ some *reduces-to* relation, which is a subset of *Expr* × *Expr*.

$\langle c, \sigma \rangle \longrightarrow \langle c', \sigma' \rangle$ means that $(c, \sigma, c', \sigma') \in$ some other *reduces-to* relation, which is a subset of *Command* × *Expr* × *Command* × *Expr*.

Our goal with these inference rules is to define such relations.

Here's an example of the kind of the rules we've been looking at so far:

$$\frac{a_1 \longrightarrow a_1'}{(a_1 + a_2) \longrightarrow (a_1' + a_2)} \; |a_1| > 0$$

a_1, a_2 etc. are *metavariables.* The stuff above the line is the *premise*, the stuff below is the *conclusion.* The stuff on the right side is a *side condition.*

When you do a consistent substitution for all the metavariables, and the side condition is satisfied, you get a *rule instance.* For example, this is an instance of the above rule:

$$\frac{3 * 4 \longrightarrow 12}{(3 * 4 + 1) \longrightarrow (12 + 1)} \; |3 * 4| > 0$$

with the substitutions $a_1 = 3 * 4$, $a_1' = 12$, $a_2 = 1$.

However, this is also a valid instance of the rule:

$$\frac{3 * 4 \longrightarrow 11}{(3 * 4 + 1) \longrightarrow (11 + 1)} \; |3 * 4| > 0$$

with the substitutions $a_1 = 3 * 4$, $a_1' = 11$, $a_2 = 1$. (There's nothing in the premise or side conditions that would make these substitutions invalid.)

With rules like the one above, we are trying to define a relation $A \subseteq S$. Our example rule could be part of the definition of some reduces-to relation, *reduces-to* $\subseteq$ *Expr* $\times$ *Expr*

In general, a rule instance is of the form

$$\frac{X_1 X_2 \ldots X_n}{X}$$

where $X_1, X_2, \ldots, X_n$ are members of the relation, and X is the "new" member of the relation added by this rule.

Here's the difference between a premise and a side condition: the side condition is not part of the relation that the rule is trying to define, while the premises are members of it. The side condition is something else that we are bringing into the definition of the relation. In this sense, the premises are the recursive part of the definition, and the side conditions are the non-recursive part. (Note that in the side condition we didn't write $a_1 > 0$, because a_1 is just a piece of syntax and writing that doesn't make sense; so we wrote $|a_1| > 0$.)

So suppose we have written down a set of rules. How do we know whether the relation that the rules are trying to define is well-defined ?

We can try to define A like this:

$$A = \left\{ X \,\middle|\, \{X_1, X_2, \ldots, X_n\} \subseteq A \wedge \frac{X_1 X_2 \ldots X_n}{X} \text{ is a rule instance} \right\}$$

But this is not a very clear definition. What do we put in A to start with? If there is a rule $\frac{X}{X}$ what do we add to A for this rule? The whole S? Nothing?

Define a *rule operator* R as follows:

$$R(B) = \left\{ X \,\middle|\, \{X_1, X_2, \ldots, X_n\} \subseteq B \wedge \frac{X_1 X_2 \ldots X_n}{X} \text{ is a rule instance} \right\}$$

Then,

- $R(B)$ is the set of members of the relation that can be inferred from the members of set B.
- $R(\emptyset)$ is what we can infer from nothing; that is, the set of axioms.
- $R(R(\emptyset))$ contains the things that we can derive in one step, and the axioms. (The axioms are in this set because they derive from the empty set, which is a subset of $R(\emptyset)$.)

In the next lecture we will use this R operator to precisely define the relation.