Lecturer: Andrew Myers

1 Summary

In this lecture we:

- define induction on a well-founded relation;
- illustrate the definition with some examples, including the inductive definition of free variables $FV(e)$;

2 Introduction

Recall that some of the substitution rules mentioned the function $FV : \{\lambda\text{-terms}\} \to \mathbf{Var}$:

$$\begin{aligned} \mathit{FV}(x) &= \{x\} \\ \mathit{FV}(e_1\ e_2) &= \mathit{FV}(e_1) \cup \mathit{FV}(e_2) \\ \mathit{FV}(\lambda x.\, e) &= \mathit{FV}(e) - \{x\}. \end{aligned}$$

Why does this definition uniquely determine the function *FV*? There are two issues here:

- Existence: whether *FV* is defined on all λ-terms;
- Uniqueness: whether the definition is unique.

Of relevance here is the fact that there are three clauses in the definition of *FV* corresponding to the three clauses in the definition of λ-terms and that a λ-term can be formed in one and only one way by one of these three clauses. Note also that although the symbol *FV* occurs on the right-hand side in two of these three clauses, they are applied to proper (*proper* = strictly smaller) subterms.

The idea underlying this definition is called *structural induction*. This is an instance of a general induction principle called *induction on a well-founded relation*.

3 Well-Founded Relations

A binary relation $\prec$ is said to be *well-founded* if it has no infinite descending chains. An *infinite descending chain* is an infinite sequence of elements $a_0, a_1, a_2, \ldots$ such that $a_{i+1} \prec a_i$ for all $i \geq 0$. Note that a well-founded relation cannot be reflexive.

Here are some examples of well-founded relations:

- the successor relation $\{(m, m+1) \mid m \in \mathbb{N}\}$ on $\mathbb{N}$;
- the less-than relation $<$ on $\mathbb{N}$;
- the element-of relation $\in$ on sets. The axiom of foundation (or axiom of regularity) of Zermelo–Fraenkel (ZF) set theory asserts exactly that $\in$ is well-founded. Among other things, this prevents a set from being a member of itself;
- the proper subset relation $\subset$ on the set of finite subsets of $\mathbb{N}$.

The following are not well-founded relations:

- the predecessor relation $\{(m+1, m) \mid m \in \mathbb{N}\}$ on $\mathbb{N}$ ($0, 1, 2, \ldots$ is an infinite *descending* chain!);
- the greater-than relation $>$ on $\mathbb{N}$;
- the less-than relation $<$ on $\mathbb{Z}$ ($0, -1, -2, \ldots$ is an infinite descending chain);
- the less-than relation $<$ on the real interval $[0, 1]$ ($1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ is an infinite descending chain);
- the proper subset relation $\subset$ on subsets of $\mathbb{N}$ ($\mathbb{N}, \mathbb{N} - \{0\}, \mathbb{N} - \{0, 1\}, \ldots$ is an infinite descending chain).

4 Well-Founded Induction

Let $\prec$ be a well-founded binary relation on a set A. Abstractly, a *property* is just a map $P : A \to \{\mathit{true}, \mathit{false}\}$, or equivalently, a subset $P \subseteq A$ (the set of all elements of A for which the property is true).

The principle of well-founded induction on the relation $\prec$ says that in order to prove that a property P holds for all elements of A, it suffices to prove that P holds of any $a \in A$ whenever P holds for all $b \prec a$. In other words,

$$\forall a \in A.(\forall b \in A.b \prec a \Rightarrow P(b)) \Rightarrow P(a) \quad \Rightarrow \quad \forall a \in A.P(a). \tag{1}$$

Expressed as a proof rule,

$$\frac{\forall a \in A.(\forall b \in A.b \prec a \Rightarrow P(b)) \Rightarrow P(a)}{\forall a \in A.P(a)}. \tag{2}$$

The basis of the induction is the case when a has no $\prec$-predecessors; in that case, the statement $\forall b \in A.b \prec a \Rightarrow P(b)$ is vacuously true.

For the well-founded relation $\{(m, m+1) \mid m \in \mathbb{N}\}$, (1) and (2) reduce to the familiar notion of mathematical induction on $\mathbb{N}$: to prove $\forall n.P(n)$, it suffices to prove that $P(0)$ and that $P(n+1)$ whenever $P(n)$.

For the well-founded relation $<$ on $\mathbb{N}$, (1) and (2) reduce to *strong* induction on $\mathbb{N}$: to prove $\forall n.P(n)$, it suffices to prove that $P(n)$ whenever $P(0), P(1), \ldots, P(n-1)$. When $n = 0$, the induction hypothesis is vacuously true.

4.1 Equivalence of Well-Foundedness and the Validity of Induction

In fact, one can show that the induction principle (1)–(2) is valid for a binary relation $\prec$ on A if and only if $\prec$ is well-founded.

To show that well-foundedness implies the validity of the induction principle, suppose the induction principle is not valid. Then there exists a property P for which the premise of (2) holds but not the conclusion. Thus P is false for some element $a_0 \in A$. The premise of (2) is equivalent to

$$\forall a \in A.\neg P(a) \Rightarrow \exists b \in A\ b \prec a \wedge \neg P(b)$$

This implies that there exists an $a_1 \prec a_0$ such that P is false for a_1. Continuing in this fashion, using the axiom of choice one can construct an infinite descending chain $a_0, a_1, a_2, \ldots$ for which P is false, so $\prec$ is not well-founded.

Conversely, suppose that there is an infinite descending chain $a_0, a_1, a_2, \ldots$. Then the property "$a \notin \{a_0, a_1, a_2, \ldots\}$" violates (2), since the premise of (2) holds but not the conclusion.

5 Structural Induction

Now let's define a well-founded relation on the set of all λ-terms. Define $e < e'$ if e is a *proper* subterm of e'. A λ-term e is a *proper* (or *strict*) subterm of e' if it is a subterm of e' and if $e \neq e'$. If we think of λ-terms as syntax trees, then e' is a tree that has e as a subtree. Since these trees are finite, the relation is well-founded. Induction on this relation is called *structural induction*.

We can now show that $\mathit{FV}(e)$ exists and is uniquely defined for any λ-term e. In the grammar for λ-terms, for any e, exactly one case in the definition of *FV* applies to e, and all references in the definition of *FV* are to subterms, which are strictly smaller. The function *FV* exists and is uniquely defined for the base case of the smallest λ-terms $x \in \mathit{Var}$. So $\mathit{FV}(e)$ exists and is uniquely defined for any λ-term e by induction on the well-founded subexpression relation.

We often have a set of expressions in a language built from a set of *constructors* starting from a set of *generators*. For example, in the case of λ-terms, the generators are the variables $x \in \mathit{Var}$ and the constructors are the application operator $\cdot$ and the abstraction operators λx. The set of expressions defined by the generators and constructors is the smallest set containing the generators and closed under the constructors.

If a function is defined on expressions in such a way that

- there is one clause in the definition for every generator or constructor pattern,
- the right-hand sides refer to the value of the function only on proper subexpressions,

then the function is well-defined and unique.