Scribe: Amy Gale, Anirban Das Gupta Lecturer: Andrew Myers

1 Inductive Proofs

There are a number of properties of entities in CS 611 that need inductive proofs, including:

- expression termination
- deterministic evaluation
- equivalence of semantics
- equivalence of expressions

Winskel's discussions of these inductive proofs are built on the notion of a well-founded relation $\prec$, while the lectures mostly utilize induction on the heights of derivation trees.

Well-founded induction generalizes ordinary induction by introducing a *well-founded* predecessor function $\prec$. The predecessor function $\prec$ for the natural numbers is $n \prec n+1$. In well-founded induction, we want to prove that some $P(e)$ holds for all $e \in S$, where S has some well-founded relation $\prec$ on its members, by showing $P(1)$ and $P(e) \wedge n \prec n' \Rightarrow P(n')$.

A function is *well-founded* if there are no infinite downward chains in S ordered by $\prec$. This means that $\prec$ must be irreflexive since if there were some a such that $a \prec a$ then we could construct an infinite downward chain $\ldots \prec a \prec a \prec a$. If there were an infinite downward chain, then there might not be any base case supporting the induction.

The rule for well-founded induction is

$$\frac{\forall e \ . \ (\forall e' \prec e \ . \ P(e')) \Rightarrow P(e)}{\forall e \ . \ P(e)}.$$

It is clear that this corresponds to the induction step in mathematical induction, but less clear that it also accommodates the base case requirement of same, since when e is an element without a predecessor (*eg* 1 in the natural numbers), $(\forall e' \prec e \ . \ P(e')) \Rightarrow P(e)$ is equivalent to $\mathsf{true} \Rightarrow P(e)$, which is to say we must be able to derive $P(e)$ without the benefit of an induction hypothesis, just as in standard induction.

Recall that structural induction involves proving that $P(e)$ holds if $P(e')$ holds for each subexpression e' of e. Then we can define $\prec$ via

$$e' \prec e \stackrel{\text{def}}{=} e' \text{ a subexpression of } e.$$

Given that expressions can only have finite length and any expression is strictly longer than each of its subexpressions the set of expressions ordered by $\prec$ has no infinite downward chain and so we can use well-founded induction.

2 Inductively Defined Sets

In our discussions of induction so far we have been trying to show that some $P(e)$ holds for all e in some inductively defined set. What do we mean by an inductively defined set? Intuitively we mean a set of elements such that for each element we can construct a finite proof of membership using the inference rules given for the set. Part of this intuition is that the only expressions we will see in a proof of e will be shorter than e, so that we are in a sense proving $P(e)$ assuming $P(e')$ for all shorter e'.

We can express a more generalized (and formal) notion of an inductively defined set as follows. Recall that an inductive definition of a set is a set of inference rules (a "proof system") and that given any

substitution of metavariables subject to side conditions. Then we can define a rule operator R by

$$R(A) \stackrel{\text{def}}{=} \{x : \frac{x_1 \ldots x_m}{x} \text{ is a rule instance } \wedge \{x_1, \ldots, x_m\} \subseteq A\}$$

Note that R is defined on all sets A (not just on subsets of the inductively defined set).

Some properties of R:

- $R(\emptyset) = \{x : \overline{\ x\ }\}$ = the set of elements of the set that can be concluded from axioms.
- $R(R(\emptyset))$ = the set of elements that have proof trees of height ≤ 1.
- $R(A_1 \cup A_2) \supseteq R(A_1) \cup R(A_2)$.
- $A_1 \subseteq A_2 \Rightarrow R(A_1) \subseteq R(A_2)$ — R is monotonic with respect to $\subseteq$.

Let S be the set of all elements we can derive by from the rules and axioms of the system. Intuitively, we require that applying the rules of the system to S should not produce any new elements; that is, S should be *closed* under the rule operator R: $S \supseteq R(S)$. We will see that $S = R(S)$, that is S is a *fixed point* of the operator R, in fact S is the least fixed point of R, which we denote as *fix*(R).

- x is a *fixed point* of $f : D \to D$ iff $x = f(x)$.
- *fix*$(R) : (D \to D) \to D$ takes a function and returns the least fixed point of that function.

In order to find this fixed point, we need a solution to $S = R(S)$.

The things we can prove with trees of finite height are the members of the sets $\emptyset = R^0(\emptyset), R(\emptyset), R^2(\emptyset), \ldots$ which are related in a monotonic sequence $R^0(\emptyset) \subseteq R^1(\emptyset) \subseteq R^2(\emptyset) \subseteq \ldots$ We can see that this sequence exists by induction using the fact that R is monotonic: observe that $R^0(\emptyset) \subseteq R^1(\emptyset)$, then $R^1(\emptyset) \subseteq R^2(\emptyset)$, and so on.

Then we can define S by

$$S = \bigcup_{n \in \omega} R^n(\emptyset).$$

Now we can show $S = \mathit{fix}(R)$ as follows:

$S \supseteq R(S)$

Assume $x \in R(S)$. Then for some rule instance $\frac{x_1 \ldots x_m}{x}$, $\{x_1, \ldots, x_m\} \subseteq S$. Because m is finite and each x_i must enter $S = \bigcup_{n \in \omega} R^n(\emptyset)$ at a finite stage $R^a(\emptyset)$, there must be some finite n such that $\{x_1, \ldots, x_m\} \subseteq R^n(\emptyset)$. Then $x \in R(R^n(\emptyset)) = R^{n+1}(\emptyset)$ and so by the definition of S it must be that $x \in S$.

$S \subseteq R(S)$

Assume $x \in S = \bigcup_{n \in \omega} R^n(\emptyset)$. Then for some n, $x \in R^n(\emptyset) = R(R^{n-1}(\emptyset))$, and $R(R^{n-1}(\emptyset) \subseteq R(S)$ by the definition of S and the monotonicity of R, so $x \in R(S)$.

For all fixpoints $B = R(B)$, $S \subseteq B$

Let B be any other fixpoint $B = R(B)$. Then

$$\begin{array}{rcl}
\emptyset & \subseteq & B \\
R(\emptyset) & \subseteq & B \\
R^2(\emptyset) & \subseteq & B \\
\vdots & & \vdots \\
\text{(union all above)} & & \text{(union all above)} \\
\vdots & & \vdots \\
S & \subseteq & B
\end{array}$$

We can use a similar argument to observe that S is not only the least fixed point, but also the least set that is closed under R. If B is a set closed under R, then $B \supseteq R(B)$, so the right-hand side of the set inclusions above will be $B, R(B), R^2(B), \ldots$, which are monotonically *decreasing* sets. Thus we have $S \subseteq B$ for any such B.

3 Final Remarks

We try in induction to show $P(e)$ for all e in $S = \mathit{fix}(R)$.

Assume for the induction hypothesis that there is some e contained in $R^n(\emptyset)$ for some n, then the induction step is to prove $P(e)$ assuming $P(e')$ for all $e' \in R^{n'}$ where $n' < n$.

Conclude that

$$\forall n \ . \ \forall e \in R^n(\emptyset) \ . \ P(e) \Rightarrow \forall e \in \mathit{fix}(R) \ . \ P(e)$$

.