Scribe: Piti Irawan, Milind Kulkarni Lecturer: Radu Rugina

1 Well Founded Induction

- **Definition** Let A be a set. A binary relation $\prec$ is a well founded on A if and only if there are no infinite downward chains: $... \prec a_i \prec a_{i-1} \prec ... \prec a_1 \prec a_0$ where $a_0, a_1, ...a_i, ... \in A$
- By the definition above, $\forall a \in A \;.\; a \not\prec a$ (otherwise we would have an infinite chain consisting only of a). More generally, there can be no cycles of the form $a_{i_1} \prec \ldots \prec a_{i_n} \prec a_{i_1}$.
- **Theorem** $\prec$ is a well founded relation on A if for each non-empty subset Q of A, there is a minimal element of Q (i.e. there is an element of Q which has no predecessor in Q). Formally:

$$\forall Q \subseteq A, Q \neq \emptyset, \exists m \in Q : \forall b \prec m, b \notin Q$$

- **Well-founded Induction Principle**. If A is a set and $\prec$ is a well founded relation on A then

$$\forall a \in A \;.\; P(a) \quad \text{iff} \quad \forall a \;.\; [(\forall b \prec a \;.\; P(b)) \Rightarrow P(a)]$$

We can see that the various forms of induction that we have already examined are particular instances of this general principle. The table below defines the set A and the relation $\prec$ for each of these forms of induction:

Tpye of Induction	A	$\prec$
Standard Induction	$A = \mathbb{N}$	$n \prec n' \Leftrightarrow n + 1 = n'$
Course of Values	$A = \mathbb{N}$	$n \prec n' \Leftrightarrow n < n'$
Structural Induction	$A = \mathbf{Aexp}$	$a \prec a' \Leftrightarrow a$ is a direct subexpression of a'
Induction on Derivations	$A = \{d \mid d \Vdash \langle c, \sigma\rangle \to \sigma'\}$	$d \prec d' \Leftrightarrow d$ is included in d'
Induction on Derivations (alternative)	$A = \to_c$	$\langle c_0, \sigma_0, \sigma_0'\rangle \prec \langle c_1, \sigma_1, \sigma_1'\rangle$ iff there is a rule $\dfrac{\ldots \quad \langle c_0, \sigma_0\rangle \to \sigma_0' \quad \ldots}{\langle c_1, \sigma_1\rangle \to \sigma_1'}$

2 Inductive Definitions

So far, we have seen several inductively defined sets ($\mathbb{N}$, **Aexp**, **Bexp**, **Com**, $\to_a$, $\to_b$, $\to_c$) and applied different forms of induction for each of them. Let's compare the definitions of these sets:

Inductively defined set	How it is defined
$\mathbb{N}$	?
Aexp	BNF grammar
$\to_c$	Semantics (rules + axioms)

We would like to have a common framework for inductively defining such sets. For this, we will use the form from operational semantics, that is we will express set definition using axioms and rules.

An **inductive definition** of a set A consists of a set of Axioms and Rules:

- Axioms of the form $\overline{x}$, meaning that $x \in A$;
- Rules of the form $\dfrac{x_1, x_2, \ldots, x_n}{x}$, meaning that $x_1, x_2, ..., x_n \in A \Rightarrow x \in A$.

Examples

- $\mathbb{N}$ can be inductively defined as follows:

$$\overline{0} \quad \frac{n}{n+1}$$

- **Aexp** can be inductively defined as follows:

$$\overline{n} \quad \overline{X} \quad \frac{a_0 \quad a_1}{a_0 + a_1} \quad \frac{a_0 \quad a_1}{a_0 - a_1} \quad \frac{a_0 \quad a_1}{a_0 * a_1}$$

3 Rule Application

We will define the operator $\hat{R}$ as follows:

$$\begin{aligned} \hat{R} &: \mathcal{P}(A) \to \mathcal{P}(A) \\ \hat{R}(X) &= \{x \mid \exists\, X' \subseteq X, \frac{X'}{x}\} \end{aligned}$$

Intuitively, $\hat{R}(X)$ represents the set of facts (elements of A) that can be inferred from X by applying the rules exactly once. The application of the operator multiple times is:

$$\hat{R}^n(X) = \underbrace{\hat{R}(\hat{R}(...\hat{R}}_{n \text{ times}}(X)...))$$

Thus, $\hat{R}(\emptyset)$ represents the facts that can be inferred from the axioms. That is, everything that can be proved from no prior knowledge. Furthermore, $\hat{R}(\hat{R}(\emptyset))$ is the set of facts with proof trees of height 0 or 1. In general, $\hat{R}^n(\emptyset)$ is the set of facts having proof trees of height strictly less than n.

Thus, we can express the inductively defined set A as a union of all these sets: $\hat{R}^n(\emptyset)$, $n \geq 0$; in other words, A is the set of elements that have finite proof trees.

$$\begin{aligned} A &= \hat{R}(\emptyset) \cup \hat{R}(\hat{R}(\emptyset)) \cup ... \\ &= \bigcup_{n \in \mathbb{N}} \hat{R}^n(\emptyset) \end{aligned}$$

4 Properties of A

There are several properties of A that we would like to prove:

- A is closed: $\hat{R}(A) \subseteq A$ (the application of rules one more time doesn't yield new elements in A);
- A is consistent: $A \subseteq \hat{R}(A)$ (each element in A can be inferred from a rule);
- Hence, A is a fixed point[1] of $\hat{R}$: $A = \hat{R}(A)$
- A is the least fixed point with respect to set inclusion: $B = \hat{R}(B) \Rightarrow A \subseteq B$

[1] **Def:** If $f : D \to D, x$ is a fixed point of f if $f(x) = x$

5 Properties of $\hat{R}$

- $A \subseteq B \Rightarrow \hat{R}(A) \subseteq \hat{R}(B)$ (in other words, $\hat{R}$ is monotonic)
- $\hat{R}(A) \cup \hat{R}(B) \subseteq \hat{R}(A \cup B)$
- $\hat{R}(A) \cap \hat{R}(B) \supseteq \hat{R}(A \cap B)$

6 Proofs

Lemma: For any $n \geq 0$: $\hat{R}^n(\emptyset) \subseteq \hat{R}^{n+1}(\emptyset)$. In other words, the sets $\hat{R}^n(\emptyset)$ form an ascending chain:

$$\emptyset \subseteq \hat{R}(\emptyset) \subseteq \hat{R}^2(\emptyset) \subseteq ...$$

Proof (by standard induction)

Basis: $\emptyset \subseteq \hat{R}(\emptyset)$ This is trivial

Inductive step: We need to show that $\hat{R}^n(\emptyset) \subseteq \hat{R}^{n+1}(\emptyset) \Rightarrow \hat{R}^{n+1}(\emptyset) \subseteq \hat{R}^{n+2}(\emptyset)$. For this, we apply the rule operator to each side of the inclusion in the induction hypothesis and, by monotonicity of $\hat{R}$, we get: $\hat{R}^n(\hat{R}^n(\emptyset)) \subseteq \hat{R}^n(\hat{R}^{n+1}(\emptyset))$, which is what we needed to prove.

Proof that A is closed. ($\hat{R}(A) \subseteq A$)

$$\begin{array}{rcl} x \in \hat{R}(A) & \Rightarrow & \exists\, x_1, x_2, ..., x_n \in A : \dfrac{x_1, x_2, ..., x_n}{x} \\ x_1 \in A & \Rightarrow & \exists m_1 : x_1 \in \hat{R}^{m_1}(\emptyset) \\ & \vdots & \\ x_n \in A & \Rightarrow & \exists m_n : x_n \in \hat{R}^{m_n}(\emptyset) \end{array}$$

Then take $m = \max(m_1, ..., m_n)$. Using the lemma it follows that:

$$\begin{array}{rcl} x_1 \in \hat{R}^{m_1}(\emptyset),\ m_1 \leq m & \Rightarrow & x_1 \in \hat{R}^m(\emptyset) \\ & & \vdots \\ x_n \in \hat{R}^{m_n}(\emptyset),\ m_n \leq m & \Rightarrow & x_n \in \hat{R}^m(\emptyset) \end{array}$$

Finally:

$$x_1 \in \hat{R}^m(\emptyset), \ldots, x_n \in \hat{R}^{m_n}(\emptyset) \text{ and } \frac{x_1, x_2, ..., x_n}{x} \quad \Rightarrow \quad x \in \hat{R}^{m_n+1}(\emptyset) \quad \Rightarrow \quad x \in A$$

Proof that A is consistent and is the least fixed point of $\hat{R}$ can be found in Winskel, Section 4.4.

7 Rule Induction Principle

For an set A inductivley defined using rules and axioms, we have:

$\forall a \in A \,.\, P(a)$ iff

$$\begin{array}{l} [\ \forall \text{ axiom } \overline{x} \,.\, P(x)\ ] \wedge \\ [\ \forall \text{ rule } \dfrac{x_1, x_2, ..., x_n}{x} \,.\, (x_1 \in A \wedge ... \wedge x_n \in A \wedge P(x_1) \wedge ... \wedge P(x_n) \Rightarrow P(x))\ ] \end{array}$$

We can express rule induction as well founded induction, using the following well founded relation:

$$x' \prec x \quad \text{iff} \quad \text{there exists a rule } \frac{\ldots\ x'\ \ldots}{x}$$

(if the elements in A cannot have both finite and infinite proof trees)