Scribe: Stephen Chong and Prakash Linga Lecturer: Andrew Myers

Motivation

We have been using inference rules to define evaluation. For example,

$$\frac{\langle a_0,\, \sigma\rangle \Downarrow n_0 \quad \langle a_1,\, \sigma\rangle \Downarrow n_1}{\langle a_0 + a_1,\, \sigma\rangle \Downarrow n}\ (n_0 + n_1 = n)$$

However, when we do proof trees we use rule instances:

$$\frac{\langle 2,\, \sigma\rangle \Downarrow 2 \quad \langle x,\, \sigma\rangle \Downarrow 2}{\langle 2 + x,\, \sigma\rangle \Downarrow 4}$$

Note that we don't bother writing the side condition for rule instances: $2 + 2 = 4$. The side condition is only used to decide that this is a valid rule instance.

We have been interested in finding the set A of *all* valid evaluations. An evaluation maps a command and a state onto a new state, so $A \subseteq \mathbf{Com} \times \Sigma \times \Sigma$. More generally, consider defining an arbitary set A using inference rules.

The Rule Operator

Suppose we have a rule instance of the form

$$\frac{x_1 \quad x_2 \quad \dots \quad x_n}{x}$$

This rule instance means that if the elements $x_1, x_2, \dots, x_n$ are all in A then x is also in A.

Needless to say, if we have an axiom of the form

$$\frac{}{x}$$

then $x \in A$, as there are no premises to satisfy.

For a given set of axioms and inference rules, we define the rule operator $R : \mathcal{P}(\mathbf{Com} \times \Sigma \times \Sigma) \rightarrow \mathcal{P}(\mathbf{Com} \times \Sigma \times \Sigma)$ as follows:

$$R(S) = \left\{ x \,\middle|\, \frac{x_1\ x_2\ \dots\ x_n}{x} \text{ is a rule instance and } x_1, \dots, x_n \in S \right\}$$

The operator R "encapsulates" everything we know about the axioms and inference rules.

Properties of the Rule Operator

The rule operator R satisfies the following properties -

- $R(A \bigcup B) \supseteq R(A) \bigcup R(B)$
- $R(A \bigcap B) \subseteq R(A) \bigcap R(B)$
- $A \subseteq B \Rightarrow R(A) \subseteq R(B)$ (Operator R is monotonic)

$R(\emptyset)$ gives all instances of the axioms. $R^2(\emptyset)$ gives all evaluations that can be deduced in one step, i.e. that have a proof tree of depth 1.

What properties do we need for A?

- Consistent — every element in A should be derivable from a rule, i.e. $A \subseteq R(A)$
- Closed — there are no new elements to derive, i.e. $A \supseteq R(A)$

These properties imply $A = R(A)$. A is therefore a fixed point of R.

Definition: For some function $f : D \to D$ and some $x \in D$, if $f(x) = x$ then x is said to be a *fixed point of* f.

One function could have multiple fixed points, and indeed our rule operator R does in general have multiple fixed points.

Defining A

For inductively defined sets, we want A to contain all and only the evaluations with finite proof trees, i.e. we would like

$$\begin{aligned} A &= R(\emptyset) \cup R^2(\emptyset) \cup \dots \\ &= \bigcup_{n\in\omega} R_n(\emptyset) \end{aligned}$$

Claim: $A = \bigcup_{n\in\omega} R_n(\emptyset)$ is a fixed point of R.

Proof:

(1) $A \supseteq R(A)$

Let $x \in R(A)$. We need to show that $x \in A$.

For this we will first show that $\forall n\ R^n(\emptyset) \subseteq R^{n+1}(\emptyset)$

For $n = 0$ this trivially holds for $\emptyset \subseteq R(\emptyset)$.

Now assume the inductive hypothesis,

$$R^n(\emptyset) \subseteq R^{n+1}(\emptyset)$$

Using the monotonicity property of R we have

$$R^{n+1}(\emptyset) \subseteq R^{n+2}(\emptyset)$$

Hence, by induction, $\forall n\ R^n(\emptyset) \subseteq R^{n+1}(\emptyset)$.

Now, $x \in R(A)$, so there is some rule instance

$$\frac{x_1 \quad x_2 \quad \dots \quad x_n}{x}$$

with $x_1, x_2, \dots, x_n \in A$.

Since all the premises $x_1, x_2, \dots, x_n \in A$ have finite proof trees, there must be some finite m such that $x_1, x_2, \dots, x_n \in R^m(\emptyset)$, which implies $x \in R^{m+1}(\emptyset) \subseteq A$. (Note: if there were an infinite number of premises in the rule instance, then we would not be able to find a finite m. However, as all our inference rules have a finite number of premises, we are safe!)

So, $x \in R(A) \Rightarrow x \in A$ and thus $A \supseteq R(A)$.

(2) $A \subseteq R(A)$

Let $x \in A$. x has a finite proof tree, so there exists some finite m such that $x \in R^m(\emptyset)$. So $x_1, x_2, \dots, x_n \in R^{m-1}(\emptyset)$. Therefore $x \in R(R^{m-1}(\emptyset))$.

Since $R^{m-1}(\emptyset) \subseteq A$, from monotonicity, $R(R^{m-1}(\emptyset)) \subseteq R(A)$. Therefore $x \in R(A)$.

So $A \subseteq R(A)$.

From (1) and (2) it follows that $A = R(A)$ and so A is a fixed point.

Claim: A is the least closed set of R.

Proof: Suppose B is closed under R, that is $B \supseteq R(B)$. We need to show that $A \subseteq B$.

$$\begin{array}{lrcl} & \emptyset & \subseteq & B \\ \text{So} & R(\emptyset) & \subseteq & R(B) \\ & R^2(\emptyset) & \subseteq & R^2(B) \\ & \vdots & & \vdots \\ & R^n(\emptyset) & \subseteq & R^n(B) \\ \Rightarrow & A = \bigcup_{n\in\omega} R^n(\emptyset) & \subseteq & \bigcup_{n\in\omega} R^n(B) = B \end{array}$$

So A is the least closed set of R.

Since all fixed points of R must be closed, A is also the least fixed point of R:

$$\forall B \subseteq \mathbf{Com} \times \Sigma \times \Sigma, \ \ R(B) = B \Rightarrow A \subseteq B$$

Definition: $\mathit{fix} : (D \to D) \to D$ is the least fixed point operator. It takes some relationship defined on $D \to D$, and returns the least fixed point that the relationship implies. This is relative to some ordering on D: in this case, $\subseteq$.

We have just shown that $\mathit{fix}(R) = A$.

Functions

A function $f : A \to B$ can be regarded as a set

$$\{\langle a_0, b_0\rangle, \langle a_0, b_0\rangle, \ldots\} \equiv \{a_0 \mapsto b_0, a_1 \mapsto b_1, \ldots\} \ a_i \in A, b_i \in B$$

This set is known as the *extension of* f. When f is regarded in this way $f \subseteq A \times B$.

Alternatively, we could write $f \in A \to B \subseteq \mathcal{P}(A \times B)$ where $\mathcal{P}(X)$ is the power set of X — the set of all possible subsets of X. Note that we can also write B^A for $A \to B$.

By convention $A \to B$ means *total* functions from A to B, and $A \rightharpoonup B$ means *partial* functions from A to B. In general we will only be dealing with total functions.

Total functions must have certain properties:

1. No a shows up more than once in the extension of f. That is, if $f(a) = b_1$ and $f(a) = b_2$ then $b_1 = b_2$.

2. Every a shows up at least once in the extension of f.

We can write functions like inference rules provided the following conditions are met:

1. Every a is covered by exactly 1 rule.

2. There is a well-founded relation on A that the rules respect.

For example, consider the successor function $s : \mathbf{N} \to \mathbf{N}$:

$$s(a) = \begin{cases} 2 & \text{if } a = 1 \\ s(n) + 1 & \text{if } a = n + 1 \end{cases}$$

Each natural number is covered by exactly one rule for s: 1 is covered by the first rule, and all numbers greater than 1 are covered by the second. Since $s(a)$ is defined in terms of $s(n)$, we need some well–founded ordering $\prec$ on the natural numbers such that $n \prec a$ to ensure no infinite descending chains occur. The natural ordering on natural numbers satisifes this.

The axiom and inference rule for s are:

$$\frac{}{s(a) = 2} \ (\text{where } a = 1)$$

$$\frac{s(n) = y}{s(a) = x} \text{ (where a = n+1, x=y+1)}$$

An instance of the inference rule is

$$\frac{s(37) = 38}{s(38) = 39}$$