1 Inference rules and rule instances

We defined small-step and big-step semantics using inference rules. These rules are another kind of inductive definition. To prove properties of them, we would like to use well-founded induction.

To do this, we can change our view and look at reduction as a binary relation. To say that $\langle c, \sigma\rangle \longrightarrow \langle c', \sigma'\rangle$ according to the small-step SOS rules just means that $(\langle c, \sigma\rangle,\ \langle c', \sigma'\rangle)$ is a member of some reduction relation, which is a subset of $(Com \times \Sigma) \times (Com \times \Sigma)$. In fact, not only is it a relation, it is a partial function.

Here is an example of the kind of the rule we have been looking at so far.

$$\frac{a_1 \longrightarrow a_1'}{a_1 + a_2 \longrightarrow a_1' + a_2}\ (|a_1| > 0) \tag{1}$$

Here a_1, a_2, and a_1' are *metavariables*. Everything above the line is part of the *premise*, and everything below the line is the *conclusion*. The expression on the right side is a *side condition*.

A *rule instance* is a substitution for all the metavariables such that the side condition is satisfied. For example, here is an instance of the above rule:

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

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

Another valid instance of the rule is

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

where the substitutions are $a_1 = 3 * 4$, $a_1' = 11$, $a_2 = 1$.

Note that since an inductively defined set is defined by the rule instances, we are free to introduce metanotation in rules as long as it is clear what rule instances are generated.

With rules like (1), we are usually trying to define some set or relation. For example, this rule might be part of the definition of some reduction relation $\longrightarrow$ that is a subset of $AExp \times AExp$. Such rules are typically of the form

$$\frac{X_1\ X_2\ \ldots\ X_n}{X}\ (\phi) \tag{2}$$

where $X_1, X_2, \ldots, X_n$ represent elements that are already members of the set or relation being defined, X represents a new member of the relation added by this rule, and ϕ is a collection of side conditions that must hold in order for the rule to be applied.

The difference between a premise and a side condition is that the side condition is not part of the relation that the rule is trying to define, while the premises are. The side condition is some restriction that determines when an instance of the rule may be applied.

Now suppose we have written down a set of rules in an attempt to define a set A. How do we know whether A is well-defined? Certainly we would like to have $X \in A$ whenever $X_1, X_2, \ldots, X_n \in A$ and

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

is a rule instance, but this is hardly a definition of A. What do we put in A to start with?

2 Rule operator

One approach is to find a well-founded relation such that the rules constitute an inductively defined function, as described above. Define a *rule operator* R on sets as follows. Given a set B, let

$$R(B) \triangleq \{X \mid \{X_1, X_2, \ldots, X_n\} \subseteq B \text{ and } \frac{X_1\ X_2\ \ldots\ X_n}{X} \text{ is a rule instance}\}$$

Then

- $R(B)$ is the set of members of A that can be inferred from the members of set B;
- $R(\varnothing)$ is the set of members that can be inferred from nothing;
- $R(R(\varnothing))$ is the set of members that can be inferred from $R(\varnothing)$; the elements of $R(\varnothing)$ are in this set because they are inferred from the empty set, which is a subset of $R(\varnothing)$.

Formally, given a set of rules and a subset $B \subseteq S$, define a rule operator R that captures the inferences that can be made from the rule instances:

$$R(B) \triangleq \{X \mid \{X_1, X_2, \ldots, X_n\} \subseteq B \text{ and } \frac{X_1\ X_2\ \ldots\ X_n}{X} \text{ is a rule instance}\}. \tag{3}$$

Then R is a function mapping subsets of S to subsets of S; that is, $R : 2^S \to 2^S$, where 2^S denotes the *powerset* (set of all subsets) of S. An important property of R is that it is clearly *monotone*: if $B \subseteq C$, then $R(B) \subseteq R(C)$. This is because if $x \in R(B)$, then there must exist in B the premises $\{x_i\}$ for some rule that has x in the conclusion. Therefore, we have $\{x_i\} \subseteq B \subseteq C$. By the definition of R, the same rule can be used on C, so $x \in R(C)$ as well.

What set $A \subseteq S$ is defined by the rules? At the very least, we would like A to satisfy the following two properties:

- A is *R-consistent*: $A \subseteq R(A)$. We would like this to hold because we would like every element of A to be included in A only as a result of applying a rule.
- A is *R-closed*: $R(A) \subseteq A$. We would like this to hold because we would like every element that the rules say should be in A to actually be in A.

These two properties together say that $A = R(A)$, or in other words, A should be a fixed point of R. There are two natural questions to ask:

- Does R actually have a fixed point?
- Is the fixed point unique? If not, which one should we take?

3 Least fixed points

In fact, any monotone set operator R always has at least one fixed point. It may have many. But among all its fixed points, it has a unique minimal one with respect to set inclusion $\subseteq$; that is, a fixed point that is a subset of all other fixed points of R. We call this the *least fixed point* of R, and we take A to be this set.

The least fixed point of R can be defined in two different ways, "from below" and "from above":

$$A_* \triangleq \bigcup \{R^n(\varnothing) \mid n \geq 0\} = R(\varnothing) \cup R(R(\varnothing)) \cup R(R(R(\varnothing))) \cup \cdots \tag{4}$$

$$A^* \triangleq \bigcap \{B \subseteq S \mid R(B) \subseteq B\}. \tag{5}$$

The set A_* is the union of all sets of the form $R^n(\varnothing)$, the sets obtained by applying R some finite number of times to the empty set. It consists of all elements of S that are in $R^n(\varnothing)$ for some $n \geq 0$.

The set A^* is the intersection of all the R-closed subsets of S. It consists of all elements of S that are in every R-closed set.

We will show that $A_* = A^*$ and that this set is the least fixed point of R, so we will take $A \triangleq A_* = A^*$.

4 Proof

Obviously, $\varnothing \subseteq R(\varnothing)$. Since R is monotone, we can apply it to both sides, obtaining $R(\varnothing) \subseteq R^2(\varnothing)$. Clearly $R^n(\varnothing) \subseteq R^{n+1}(\varnothing)$ for all n. So we can see that the successive sets $R^n(\varnothing)$ in the union defining A_* are in a chain with respect to $\subseteq$:

$$\varnothing \subseteq R(\varnothing) \subseteq R^2(\varnothing) \subseteq R^3(\varnothing) \subseteq R^4(\varnothing) \subseteq \ldots$$

4.1 Closure

First, we show that A_* is R-closed: i.e., $R(A_*) \subseteq A_*$. Consider an arbitrary $x \in R(A_*)$. It must be there is a rule $\frac{x_1,\ldots x_n}{x}$ where all of the x_i are in A_*. Each of x_i must be found first in one of the sets $R^m(\varnothing)$. Since there are a finite number of premises (n), there must be a set $R^m(\varnothing)$ in the chain that includes all of the x_i. But then $R^{m+1}(\varnothing)$ must include x, so therefore so does A_*. Since this is true for arbitrary $x \in R(A_*)$, we have $R(A_*) \subseteq A_*$.

4.2 Consistency

We need to show that $A_* \subseteq R(A_*)$. Consider an arbitrary $x \in A_*$. We must have $x \in R^m(\varnothing)$ for some m. In this case, we know that all its premises x_i are found in $R^{m-1}(\varnothing)$. Since $R^{m-1}(\varnothing) \subseteq A_*$, we can apply R to both sides to obtain $R^m(\varnothing) \subseteq R(A_*)$. Therefore x must be in $R(A_*)$, and so A_* is R-consistent.

4.3 Least fixed point

Suppose we have another fixed point of R. Call it B. Given $B = R(B)$, we want to show that $A_* \subseteq B$. Clearly we have $\varnothing \subseteq B$. Applying R to both sides, we obtain $R(\varnothing) \subseteq R(B) = B$ We can repeat as necessary to obtain $R^n(\varnothing) \subseteq B$ (that is, this holds by induction on n). Therefore the union of all $R^n(\varnothing)$ cannot contain any elements not in B, so $A_* \subseteq B$. In fact, by the same argument, not only is A_* the least fixed point, it is the least R-closed set.

5 Other fixed points

In general the rule operator will have other fixed points. These correspond to allowing some proof trees with infinite derivations. For example, consider these three rules over $\mathbb{Z}$:

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

The least fixed point will consist of $\{n \mid n \geq 1\}$. The *greatest* fixed point will be $\mathbb{N}$, including 0, because $\{0, 1, \ldots\}$ is a fixed point of R, even though there is no finite proof tree deriving 0. The greatest fixed point is the union of all R-consistent sets.

However, we use the least fixed point because it ensures that all the proof trees are finite. Hence, the subderivation relation on proof trees is well-founded. This would not be the case with other fixed points.

6 Finiteness of premises

One importance feature of inference rules is that the number of premises is finite. We saw that was needed in the argument that A_* is R-closed. If inference rules have an infinite number of premises, A_* need not be closed! Consider these rules over $\mathbb{Z}$:

$$\frac{}{1} \quad \frac{n}{n+1} \quad \frac{m \quad {\scriptstyle (\forall m > n)}}{n}$$

In this case, the A_* construction gives us the set $\{1, 2, \ldots\}$, but $0 \in R(A_*)$.

7 The Knaster–Tarski Theorem

This material is optional.

The fact that $A_* = A^*$ is a special case of a more general theorem called the *Knaster–Tarski theorem*. It states that any monotone set operator R has a unique least fixed point, and that this fixed point can be obtained either "from below" by iteratively applying R to the empty set, or "from above" by taking the intersection of all R-closed sets.

For general monotone operators R, the "from below" construction may require iteration through transfinite ordinals. However, the operators R defined from rule systems as described above are *chain-continuous* (definition below). This is a stronger property than monotonicity. It guarantees that the "from below" construction converges to a fixed point after only ω steps, where ω is the first transfinite ordinal.

7.1 Monotone, continuous, and finitary operators

A set operator $R : 2^S \to 2^S$ is said to be

- *monotone* if $B \subseteq C$ implies $R(B) \subseteq R(C)$;
- *chain-continuous* if for any chain of sets $\mathcal{C}$,

  $$R(\bigcup \mathcal{C}) \quad = \quad \bigcup \{R(B) \mid B \in \mathcal{C}\}$$

  (a *chain* is a set $\mathcal{C}$ of subsets of S that is linearly ordered by the set inclusion relation $\subseteq$; that is, for all $B, C \in \mathcal{C}$, either $B \subseteq C$ or $C \subseteq B$);
- *finitary* if for any set C, the value of $R(C)$ is determined by the values of $R(B)$ for finite subsets $B \subseteq C$ in the following sense:

  $$R(C) \quad = \quad \bigcup \{R(B) \mid B \subseteq C,\ B \text{ finite}\}.$$

One can show

1. Every rule-based operator of the form (3) is finitary;
2. Every finitary operator is chain-continuous (in fact, the converse holds as well);
3. Every chain-continuous operator is monotone.

The proofs of 1, 2, and 3 are fairly straightforward and we will leave them as exercises. The converse of 2 requires transfinite induction and is more difficult.

7.2 Proof of the Knaster–Tarski Theorem for chain-continuous operators

Let us prove the Knaster–Tarski theorem in the special case of chain-continuous operators, which will allow us to avoid introducing transfinite ordinals (not that they are not worth introducing!), and that is all we need to handle rule-based inductive definitions.

Theorem (Knaster–Tarski)
Let $R : 2^S \to 2^S$ be a chain-continuous set operator, and let A_* and A^* be defined as in (4) and (5), respectively. Then $A_* = A^*$, and this set is the $\subseteq$-least fixed point of R.

Proof. The theorem follows from two observations:

(i) For every n and every R-closed set B, $R^n(\varnothing) \subseteq B$. This can be proved by induction on n. It follows that $A_* \subseteq A^*$.

(ii) A_* is a fixed point of R, thus is R-closed. Since A^* is contained in all R-closed sets, $A^* \subseteq A_*$.

For (i), let B be an R-closed set. We proceed by induction on n. The basis for $n = 0$ is $\varnothing \subseteq B$, which is trivially true. Now suppose $R^n(\varnothing) \subseteq B$. We have

$$\begin{aligned} R^{n+1}(\varnothing) &= R(R^n(\varnothing)) \\ &\subseteq R(B) \quad \text{by the induction hypothesis and monotonicity} \\ &\subseteq B \quad \text{since } B \text{ is } R\text{-closed.} \end{aligned}$$

We conclude that for all n and all R-closed sets B, $R^n(\varnothing) \subseteq B$, therefore

$$A_* = \bigcup \{R^n(\varnothing) \mid n \geq 0\} \subseteq \bigcap \{B \subseteq S \mid R(B) \subseteq B\} = A^*.$$

For (ii), we want to show that $R(A_*) = A_*$. It can be proved by induction on n that the sets $R^n(\varnothing)$ form a chain:

$$\varnothing \subseteq R(\varnothing) \subseteq R^2(\varnothing) \subseteq R^3(\varnothing) \subseteq \cdots$$

We have $\varnothing \subseteq R(\varnothing)$ trivially, and by monotonicity, if $R^n(\varnothing) \subseteq R^{n+1}(\varnothing)$, then

$$R^{n+1}(\varnothing) = R(R^n(\varnothing)) \subseteq R(R^{n+1}(\varnothing)) = R^{n+2}(\varnothing).$$

Now by chain-continuity,

$$R(A_*) = R(\bigcup_{n\geq 0} R^n(\varnothing)) = \bigcup_{n\geq 0} R(R^n(\varnothing)) = \bigcup_{n\geq 0} R^{n+1}(\varnothing) = A_*.$$

□