CS611 Lecture 16 — Equivalence of semantics for REC+ — 09/29/00

Scribe: Mark Sandler and Martin Pal — Lecturer: Andrew Myers

In this lecture we shall show the equivalence of operational and denotational semantics for REC+ (i.e. REC plus let). Namely, we will use strict evaluation and full function scope (A3 from prev. lecture). Winskel proves the equivalence of large step operational and denotational semantics, we shall prove the equivalence of small step and denotational semantics. The proof techniques are similar.

We want to prove

$$\mathcal{C}[\![e]\!]\mathcal{D}[\![d]\!]\emptyset = \lfloor n \rfloor \quad \Leftrightarrow \quad (d, e) \rightarrow^* (d, n)$$

We will use $\delta = \mathcal{D}[\![d]\!]$ as a shorthand. Recall that $\mathcal{D}[\![d]\!] = \mathsf{fix}\ \lambda\phi.\ \langle \mathcal{F}_1(\phi), \ldots, \mathcal{F}_n(\phi)\rangle$, where $\mathcal{F}_n(\phi)(n_1, \ldots, n_{a_i}) = \mathcal{C}[\![e_i]\!]\phi\emptyset[x_1 \mapsto n_1, \ldots, x_1 \mapsto n_{a_i}]$ and $d = (e_1, \ldots e_n)$. The $\rightarrow$ implication is usually called *adequacy*, the $\leftarrow$ implication is *soundness* of the operational semantics. We will show adequacy by induction on the structure of the expression, then we will show soundness in two steps. In the first step we show that if $(d, e) \rightarrow (d, e')$, then e and e' have the same meaning, i.e. $\mathcal{C}[\![e]\!]\delta\emptyset = \mathcal{C}[\![e']\!]\delta\emptyset$. The second step is a straightforward induction to show that if $(d, e) \rightarrow^* (d, n)$, then $\mathcal{C}[\![e]\!]\delta\emptyset = \lfloor n \rfloor$.

Adequacy

We need to prove a slightly stronger statement. Namely,

$$\mathcal{C}[\![e]\!]\delta\{x_1 \mapsto n_1, \ldots, x_1 \mapsto n_K\} = \lfloor n \rfloor \quad \Rightarrow \quad (d, e\{n_1/x_1, \ldots, n_K/x_K\}) \rightarrow^* (d, n)$$

We shall use $\{x_k \mapsto n_k\}$ as a shorthand for $\emptyset[x_1 \mapsto n_1, \ldots, x_1 \mapsto n_K]$ and $e\{n_k/x_k\}$ for $e\{n_1/x_1, \ldots, n_K/x_K\}$.

To be precise, we prove this not for δ, but for a different function environment ϕ defined as

$$\begin{array}{rcll} \pi_i\phi(n_1, \ldots, n_{a_i}) & = & \lfloor n \rfloor & \text{if } (d, e_i\{n_k/x_k\}) \rightarrow^* (d, n) \text{ for some } n \\ & & \bot & \text{otherwise} \end{array}$$

and then we prove that $\delta \sqsubseteq \phi$, which gives us that $\mathcal{C}[\![e]\!]\phi\rho = \lfloor n \rfloor$ whenever $\mathcal{C}[\![e]\!]\delta\rho = \lfloor n \rfloor$.

- $\mathcal{C}[\![n']\!]\phi\{x_k \mapsto n_k\} = \lfloor n \rfloor$. The only possibility is $n = n'$ and $(d, n'\{n_k/x_k\}) \rightarrow^* (d, n\{n_k/x_k\})$ in zero steps.
- $\mathcal{C}[\![x]\!]\phi\{x_k \mapsto n_k\} = \lfloor n \rfloor$. It must be the case that $x = x_k$ for some k. Thus, $n = n_k$, $x\{n_k/x_k\} = n_k$ and $(d, n_k) \rightarrow^* (d, n_k)$ in zero steps.
- $\mathcal{C}[\![e_1 \oplus e_2]\!]\phi\{x_k \mapsto n_k\} = \lfloor n \rfloor$. Thus, it must be the case that

  $$\begin{array}{ll} \mathcal{C}[\![e_1]\!]\phi\{x_k \mapsto n_k\} = \lfloor n_1 \rfloor & \quad \text{and} \\ \mathcal{C}[\![e_2]\!]\phi\{x_k \mapsto n_k\} = \lfloor n_2 \rfloor & \end{array}$$

  for some n_1, n_2, such that $n_1 \oplus n_2 = n$ (the only case when $\oplus_\bot$ does not return $\bot$ is when none of its arguments is $\bot$). From the induction hypothesis we know that

  $$\begin{array}{ll} (d, e_1\{n_k/x_k\}) \rightarrow^* (d, n_1) & \quad \text{and} \\ (d, e_2\{n_k/x_k\}) \rightarrow^* (d, n_2) & \end{array}$$

  Thus there are sequences $e_1^1, \ldots, e_1^s$ and $e_2^1, \ldots, e_2^t$ such that

  $$\begin{array}{ll} (d, e_1\{n_k/x_k\}) = (d, e_1^1) \rightarrow (d, e_1^2) \rightarrow \ldots \rightarrow (d, n_1) & \quad \text{and} \\ (d, e_2\{n_k/x_k\}) = (d, e_2^1) \rightarrow (d, e_2^2) \rightarrow \ldots \rightarrow (d, n_2) & \end{array}$$

  It is not hard to see that

  $$(d, (e_1 \oplus e_2)\{n_k/x_k\}) = (d, e_1^1 \oplus e_2^1) \rightarrow (d, e_1^2 \oplus e_2^1) \rightarrow \ldots \rightarrow (d, n_1 \oplus e_2^1) \rightarrow \ldots \rightarrow (d, n_1 \oplus n_2) \rightarrow (d, n)$$

- $\mathcal{C}[\![f_i(e_1,\dots e_{a_i})]\!]\phi\{x_k \mapsto n_k\} = \lfloor n \rfloor$. The most difficult case. Since we have strict evaluation, it must be the case that
$$\mathcal{C}[\![e_j]\!]\phi\{x_k \mapsto n_k\} = \lfloor n_j \rfloor$$
for each $j = 1,\dots,a_i$ and some $n_1,\dots,n_{a_i}$ and
$$(\pi_i\phi)\langle\lfloor n_1\rfloor,\dots,\lfloor n_{a_i}\rfloor\rangle = \lfloor n \rfloor$$
$\rangle$From definition of ϕ, this implies $(d, e_i\{n_1/x_1,\dots,n_{a_i}/x_{a_i}\}) \rightarrow^* (d,n)$. From the induction hypothesis we know that $(d,e_j) \rightarrow^* (d,n_j)$ for $j = 1,\dots,a_i$. $\rangle$From these (a_i+1) derivations we easily construct a derivation for $(d, f_i(e_1,\dots,e_{a_i})) \rightarrow^* (d,n)$.

We omitted some cases (like **ifz then else**) in our proof but their proof would follow one of the above patterns.

We have shown $\mathcal{C}[\![e]\!]\phi\{x_k \mapsto n_k\} = \lfloor n \rfloor \;\Rightarrow\; (d, e\{n_k/x_k\}) \rightarrow^* (d,n)$. Now we need to show $\delta \sqsubseteq \phi$ to complete the proof.

We know that δ is the least fixed point of the function $\lambda\phi.\ \langle\mathcal{F}_1(\phi),\dots,\mathcal{F}_n(\phi)\rangle$, and thus also the least prefixed point of this function. We show that ϕ is a prefixed point of $\lambda\phi.\ \langle\mathcal{F}_1(\phi),\dots,\mathcal{F}_n(\phi)\rangle$ (which implies $\delta \sqsubseteq \phi$). We need to show that $\mathcal{F}_i(\phi) \sqsubseteq \pi_i\phi$ for any i. To prove this we will use the following lemma:

Substitution Lemma

$$\mathcal{C}[\![e_i]\!]\phi\rho[x_1 \mapsto n_1,\dots,x_{a_i} \mapsto n_{a_i}] = \mathcal{C}[\![e_i\{n_1/x_1,\dots n_{a_i}/x_{a_i}\}]\!]\phi\rho$$

The proof of this lemma is an easy induction on the structure of the formula e.

Now, by definition of $\mathcal{F}_i$ we have $\mathcal{F}_i(\phi)(n_1,\dots n_{a_i}) = \mathcal{C}[\![e_i]\!]\phi\emptyset\{x_k \mapsto n_k\}$, by applying the substitution lemma we get $\mathcal{F}_i(\phi)(n_1,\dots n_{a_i}) = \mathcal{C}[\![e_i\{n_1/x_1,\dots n_{a_i}/x_{a_i}\}]\!]\phi\emptyset$. We have already proven that if $\mathcal{C}[\![e_i\{n_1/x_1\dots n_{a_i}/x_{a_i}]\!]\phi\emptyset = \lfloor n \rfloor$ for some n, then $(d, e_i\{n_1/x_1\dots n_{a_i}/x_{a_i}) \rightarrow^* (d,n)$ and therefore (by definition of ϕ) we also have $\pi_i\phi = \lfloor n \rfloor$. Thus $\mathcal{F}_i(\phi)(n_1,\dots n_{a_i}) \sqsubseteq \phi(n_1,\dots n_{a_i})$ for all $n_1,\dots n_{a_i}$, thus $\mathcal{F}_i(\phi) \sqsubseteq \pi_i\phi$ and hence ϕ is a prefixed point.

Soundness

We need to show that if $(d,e) \rightarrow^* (d,n)$ then $\mathcal{C}[\![e]\!]\delta\emptyset = \lfloor n \rfloor$. Definitely it is enough to show that if $(d,e) \rightarrow (d,e')$, then $\mathcal{C}[\![e]\!]\delta\emptyset = \mathcal{C}[\![e']\!]\delta\emptyset$. The proof of this goes by induction on the height of the derivation of $(d,e) \rightarrow (d,e')$.
Base of induction. We show only two cases:

- $(d, n_1 \oplus n_2) \rightarrow (d,n)$. $\mathcal{C}[\![n_1 \oplus n_2]\!]\delta\emptyset = \lfloor n_1 \rfloor \oplus_\perp \lfloor n_2 \rfloor = \lfloor n \rfloor$.

- $(d, f_i(n_1,\dots,n_{a_i})) \rightarrow (d, e_i\{n_1/x_1,\dots,n_{a_i}/x_{a_i}\})$. Then by definition of δ we have
$$\mathcal{C}[\![f_i(n_1,\dots,n_{a_i})]\!]\delta\emptyset = (\pi_i\delta)(n_1,\dots,n_{a_i}) = \mathcal{C}[\![e_i]\!]\delta\emptyset\{x_1 \mapsto n_1,\dots,x_{a_i} \mapsto n_{a_i}\}$$
by applying the substitution lemma we have
$$\mathcal{C}[\![e_i]\!]\delta\emptyset\{x_1 \mapsto n_1,\dots,x_{a_i} \mapsto n_{a_i}\} = \mathcal{C}[\![e_i\{n_1/x_1,\dots n_{a_i}/x_{a_i}\}]\!]$$
And finally we get $\mathcal{C}[\![f_i(n_1,\dots,n_{a_i})]\!]\delta\emptyset = \mathcal{C}[\![e_i\{n_1/x_1,\dots n_{a_i}/x_{a_i}\}]\!]$.

Now we need to prove the induction step. We consider only the case when the expression is of the form $e_1 \oplus e_2$, other cases are similar. Let $(d, e_1 \oplus e_2) \rightarrow (d, e_1' \oplus e_2)$. Then we know that $(d,e_1) \rightarrow (d,e_1')$. Thus by the induction hypothesis $\mathcal{C}[\![e_1']\!]\delta\emptyset = \mathcal{C}[\![e_1]\!]\delta\emptyset$. And therefore $\mathcal{C}[\![e_1 \oplus e_2]\!]\delta\emptyset = \mathcal{C}[\![e_1]\!]\delta\emptyset \oplus \mathcal{C}[\![e_2]\!]\delta\emptyset = \mathcal{C}[\![e_1']\!]\delta\emptyset \oplus \mathcal{C}[\![e_2]\!]\delta\emptyset = \mathcal{C}[\![e_1' \oplus e_2]\!]\delta\emptyset$.

Comparison of Denotational and Operational Semantics

Operational	**Denotational (fixed-pt)**
allowed transition between syntactic forms	translates syntax into a model
results are just syntax: easy to define	results are domain elements: harder to define
easily express simple concurrency and non-determinism (sm-step)	non-determinism: powerdomains, concurrency: scheduling
termination behavior not obvious	termination behavior implicit in domain
does not explain compilation	gives insight: e.g. fixed points signal extra pass or back-patch