Logical Relations Part 3

Lecture 3 Monday, September 11, 2017

We continue exploring logical relations for reasoning about contextual equivalence. This lecture is based on lectures by Prof Amal Ahmed at the Oregon Programming Languages Summer School, 2015[1], as reported in the notes by Lau Skorstengaard.[2]

1 Fundamental Theorem

Using our logical relation, the first thing we will do is prove the fundamental property, that a well-typed expression is in the relation.

Theorem 1 (Fundamental Property). *If* $\Delta, \Gamma \vdash e : \tau$ *then* $\Delta, \Gamma \vdash e \approx e : \tau$.

Note that e might have free variables, so even though e is related to itself, a ρ and γ might map type variables and variables to different types and values, giving us very different programs.

We could prove this theorem directly, by induction on the typing derivation of $\Delta, \Gamma \vdash e : \tau$. However, we wcan prove it using a series of *compatibility lemmas*, where each lemma directly proves one of the cases (i.e., each lemma corresponds to a typing rule). Some of the compatibility lemmas are more general than the cases in a direct proof (e.g., for expression application); these slightly more general versions are useful when we want to prove that the logical relation implies contextual equivalence (which we will not do here).

Lemma (Compatibility lemmas). *The following are true:*

1. $\Delta, \Gamma \vdash n \approx n : \textbf{\textit{int}}$
2. $\Delta, \Gamma \vdash x \approx x : \Gamma(x)$
3. *If* $\Delta, \Gamma \vdash e_1 \approx e_2 : \tau' \to \tau$ *and* $\Delta, \Gamma \vdash e_1' \approx e_2' : \tau'$ *then* $\Delta, \Gamma \vdash e_1\ e_1' \approx e_2\ e_2' : \tau$
4. *If* $\Delta, \Gamma, x : \tau \vdash e_1 \approx e_2 : \tau'$ *then* $\Delta, \Gamma \vdash \lambda x : \tau.\, e_1 \approx \lambda x : \tau.\, e_2 : \tau \to \tau'$
5. *If* $\Delta \cup \{X\}, \Gamma \vdash e_1 \approx e_2 : \tau$ *then* $\Delta, \Gamma \vdash \Lambda X.\, e_1 \approx \Lambda X.\, e_2 : \forall X.\, \tau$
6. *If* $\Delta, \Gamma \vdash e_1 \approx e_2 : \forall X.\, \tau$ *and* $\Delta \vdash \tau'$ *ok then* $\Delta, \Gamma \vdash e_1\ [\tau'] \approx e_2\ [\tau'] : \tau\{\tau'/X\}$

2 Proof of Free Theorems

We will see the use of the fundamental theorem to prove some free theorems. Recall Theorem 1 from last lecture: If $\vdash e : \forall X.\, X$ and $\vdash \tau$ ok and $\vdash v : \tau$ then $e\ [\tau]\ v \longrightarrow^* v$.

(Note that System F is strongly normalizing; otherwise the theorem would have to allow for $e\ [\tau]\ v$ failing to terminate.)

Proof of Theorem 1. From the fundamental property and the well-typedness of e we have $\vdash e \approx e : \forall X.\, X \to X$. By definition, this gives us

$$\forall \rho \in \mathcal{D}[\![\Delta]\!].\ \forall \gamma \in \mathcal{G}[\![\Gamma]\!]_\rho.\ (\ \rho_1(\gamma_1(e))\ ,\ \rho_2(\gamma_2(e))\ ) \in \mathcal{E}_{\forall X.\ X \to X}$$

Using an empty ρ and γ, we get $(e, e) \in \mathcal{E}^{\emptyset}_{\forall X.\ X \to X}$. Thus, we know that e evaluates to some function value f, and that $(f, f) \in \mathcal{V}^{\emptyset}_{\forall X.\ X \to X}$. Since f is a value, it must be of the form $\Lambda X.\, e_1$ for some e_1.

---

[1] Videos available at `https://www.cs.uoregon.edu/research/summerschool/summer15/curriculum.html`.
[2] Available at `https://www.cs.uoregon.edu/research/summerschool/summer16/notes/AhmedLR.pdf`.

Using $(f, f) \in \mathcal{V}^{\emptyset}_{\forall X.\ X \to X}$, let's instantiate it with the type τ and the relation $R = \{(v, v)\}$ (i.e., the relation consisting of the single pair (v, v)). Note that $R \in \mathrm{Rel}[\tau, \tau]$. We thus have

$$(e_1\{\tau/X\}, e_1\{\tau/X\}) \in \mathcal{E}^{\emptyset[X \mapsto (\tau,\tau,R)]}_{X \to X}$$

From this, we have that $e_1\{\tau/X\}$ evaluates to some value g and $(g, g) \in \mathcal{V}^{\emptyset[X \mapsto (\tau,\tau,R)]}_{X \to X}$. From the type of g it must be of the form $\lambda x\!:\!\tau.\, e_2$ for some e_2.

Now we instantiate $(g, g) \in \mathcal{V}^{\emptyset[X \mapsto (\tau,\tau,R)]}_{X \to X}$ with $(v, v) \in \mathcal{V}^{\emptyset[X \mapsto (\tau,\tau,R)]}_{X}$ to get

$$(e_2\{v/x\}, e_2\{v/x\}) \in \mathcal{E}^{\emptyset[X \mapsto (\tau,\tau,R)]}_{X}$$

From this we know that $e_2\{v/x\}$ steps to some value v_f such that $(v_f, v_f) \in \mathcal{V}^{\emptyset[X \mapsto (\tau,\tau,R)]}_{X}$. But that means that $(v_f, v_f) \in R$, so $v_f = v$, as required. $\square$

In the proof above, the key part is choosing the relation $R = \{(v, v)\}$. In general with these proofs of free theorems using logical relations, the insight required is how to choose the relation. The rest is mostly just unfolding definitions.

Exercise: prove the following free theorem: If $\vdash e\!:\!\forall X.\ ((\tau \to X) \to X)$ and $\vdash k\!:\!\tau \to \tau_k$ then $\vdash e\ [\tau_k]\ k \approx k\ (e\ [\tau]\ \lambda x\!:\!\tau.\, x)\!:\!\tau_k$.