2-20-06: Relational parametricity

Relational parametricity

From last time:

Suppose $\gamma \vdash f : \forall\alpha.\alpha \to \alpha \to \alpha$. Then $\forall\sigma.\forall v_1, v_2 : \sigma.f[\sigma](v_1)(v_2) \downarrow v \in \{v_1, v_2\}$.

We'd like to show:

Let **true** and **false** be the standard Church encodings of booleans.

$\exists b \in \{\mathbf{true}, \mathbf{false}\}.\forall\sigma.\forall v_1, v_2 : \sigma.f[\sigma](v_1)(v_2) \equiv b[\sigma](v_1)(v_2)$

(This shows that f behaves exactly like either **true** or **false**)

Definition (Kleene equivalence) $e_1 \equiv e_2$ if $\exists v.e_1 \downarrow v \wedge e_2 \downarrow v$.

For simple base types, Kleene equivalence works well. At higher types (functions), Kleene equivalence is too fine a notion of equivalence. For example $\lambda x.1 + 1$ is not Kleene equivalent to $\lambda x.2$.

$\mathrm{VRel}(\sigma_1, \sigma_2) = \{R \mid \forall(v_1, v_2) \in R. \vdash v_1 : \sigma_1 \wedge \vdash v_2 : \sigma_2\}$

$\delta ::= \emptyset \mid \delta, \alpha \mapsto (\sigma_1, \sigma_2, R)$ where $R \in \mathrm{VRel}(\sigma_1, \sigma_2)$.

Given δ where $\delta(\alpha) = (\sigma_1, \sigma_2, R)$, let:

- $\delta_1(\alpha) = \sigma_1$
- $\delta_2(\alpha) = \sigma_2$
- $\delta_R(\alpha) = R$

Term equivalence: $\boxed{\delta \vdash e_1 \approx e_2 : \tau}$

$\vdash e_1 \approx e_2 : \tau \Leftrightarrow (e_1, e_2) \in C[\tau]$.

$$\frac{e_1 \downarrow v_1 \qquad e_2 \downarrow v_2 \qquad \delta \vdash v_1 \approx v_2 : \tau}{\delta \vdash e_1 \approx e_2 : \tau}$$

Value equivalence: $\boxed{\delta \vdash v_1 \approx v_2 : \tau}$

$$\frac{v_1 = v_2}{\delta \vdash v_1 \approx v_2 : \mathbf{nat}} \qquad \frac{\forall v_1', v_2'.\delta \vdash v_1' \approx v_2' : \tau' \implies \delta \vdash v_1(v_1') \approx v_2(v_2') : \tau''}{\delta \vdash v_1 \approx v_2 : \tau' \to \tau''}$$

$$\frac{\begin{array}{c}\delta' = \delta, \alpha \mapsto (\sigma_1, \sigma_2, R) \vdash v_1[\sigma_1] \approx v_2[\sigma_2] : \tau \\ \forall \text{ closed } \sigma, \sigma_2.\forall R \in \mathrm{VRel}(\sigma_1, \sigma_2).\delta'\end{array}}{\delta \vdash v_1 \approx v_2 : \forall\alpha : \tau}$$

$$\frac{(v_1, v_2) \in \delta_R(\alpha)}{\delta \vdash v_1 \approx v_2 : \alpha}$$

$\mathcal{D}[\![\Delta]\!] = \{\delta \mid \forall \alpha \in \Delta. \vdash \delta_1(\alpha) \text{ type}, \vdash \delta_2(\alpha) \text{ type}, \vdash \delta_R(\alpha) \in \text{VRel}(\delta_1(\alpha), \delta_2(\alpha))\}$

$$\frac{\forall x : \tau \in \Gamma. \delta \vdash \gamma_1(x) \approx \gamma_2(x) : \tau}{\delta \vdash \gamma_1 \approx \gamma_2 : \Gamma}$$

Theorem (Parametricity/Abstraction) If $\vdash e : \tau$ then $e \approx e : \tau$.

Will be a corollary to the following lemma:

Lemma If $\Delta; \Gamma \vdash e : \tau$ and $\delta \in \mathcal{D}[\![\Delta]\!]$ and $\delta \vdash \gamma_1 \approx \gamma_2 : \Gamma$ then $\delta \vdash \gamma_1(e) \approx \gamma_2(e) : \tau$.

Case:

$$\frac{\Delta; \Gamma \vdash e_1 : \tau_2 \to \tau \qquad \Delta; \Gamma \vdash e_2 : \tau_2}{\Delta; \Gamma \vdash e_1(e_2) : \tau}$$

By induction, $\delta \vdash \gamma_1 e_1 \approx \gamma_2 e_1 : \tau_2 \to \tau$ and $\delta \vdash \gamma_1 e_2 \approx \gamma_2 e_2 : \tau_2$. So $\gamma_1 e_1 \downarrow v_1$, $\gamma_2 e_1 \downarrow v_2$, $\gamma_1 e_2 \downarrow v_1'$, and $\gamma_2 e_2 \downarrow v_2'$ with $\delta \vdash v_1 \approx v_2 : \tau_2 \to \tau$ and $\delta \vdash v_1' \approx v_2' : \tau_2$. By the LR, $\delta \vdash v_1 v_1' \approx v_2 v_2' : \tau$. By expansion, $\delta \vdash \gamma_1(e_1 e_2) \approx \gamma_2(e_1 e_2) : \tau$.

Lemma (Useful) If $\delta \vdash e_1 \approx e_2 : \tau' \to \tau''$ and $\delta \vdash e_1' \approx e_2' : \tau'$ then $\delta \vdash e_1 e_1' \approx e_2 e_2' : \tau''$.

Now, the result we want

Recall:

$\mathbf{true} = \Lambda\alpha.\lambda x.\lambda y.x$ $\mathbf{false} = \Lambda\alpha.\lambda x.\lambda y.y$

By parametricity, $\vdash f \approx f : \forall\alpha.\alpha \to \alpha \to \alpha$. Let σ and $v_1, v_2 : \sigma$. Let $\sigma_1 = \mathbf{bool}$, $\sigma_2 = \sigma$. Let $R = \{(\mathbf{true}, v_1), (\mathbf{false}, v_2)\}$. Let $\delta = \alpha \mapsto (\mathbf{bool}, \sigma, R)$. By LR, $\delta \vdash f[\mathbf{bool}] \approx f[\sigma] : \alpha \to \alpha \to \alpha$. Again by the LR, $\delta \vdash f[\mathbf{bool}](\mathbf{true})(\mathbf{false}) \approx f[\sigma](v_1)(v_2) : \alpha$. So, there are w_1, w_2 with $f[\mathbf{bool}](\mathbf{true})(\mathbf{false}) \downarrow w_1$ and $f[\sigma](v_1)(v_2) \downarrow w_2$ and $(w_1, w_2) \in R$.

Let $b = w_1$. We know that $f[\mathbf{bool}](\mathbf{true})(\mathbf{false}) \downarrow b$ "always." (By determinism of evaluation). So, for any σ and $v_1, v_2 : \sigma$, $(b, w_2) \in R$ where $f[\sigma](v_1)(v_2) \downarrow w_2$. If b is **true** then $w_2 = v_1$. Otherwise, $w_2 = v_2$. In both cases, $f[\sigma](v_1)(v_2) \equiv b[\sigma](v_1)(v_2)$.