1-9-06: Proving termination via logical relations

Theorem If $\vdash e : \tau$ then $e \downarrow v$.

Case: $e = e_1(e_2)$. By inversion $\vdash e_1 : \tau_2 \to \tau$ and $\vdash e_2 : \tau_2$. By induction $e_1 \downarrow v_1$ and $e_2 \downarrow v_2$. By preservation $\vdash v_1 : \tau_2 \to \tau$. Canonical forms implies $v_1 = \lambda x : \tau_2 . e''$. By β-reduction, $v_1(v_2) \mapsto e''[v_2/x]$. But now we're stuck.

Attempt 2 If $\vdash e : \tau$ then $e \in C$, where

$$C = \left\{ e \mid \ \vdash e : \tau,\ e \downarrow v,\ (v = \lambda x . e'' \wedge \tau = \tau' \to \tau'') \implies \forall v' : \tau' . e''[v'/x] \downarrow v'' \right\}$$

Proof: by induction on e.

Case: $e = e_1(e_2)$. As before (in 1-4 notes) we have $e_1 \downarrow v_1$, $e_2 \downarrow v_2$, $\vdash v_1 : \tau' \to \tau''$, and $v_1 = \lambda x : \tau' . e''$. By induction, for all $v' : \tau'$, we have $e''[v'/x] \downarrow v''$.

[My handwritten notes skip some material. The gist was that we needed to introduce Γ to deal with the λ case, but that got us into trouble with variables. So, we introduced substitutions, as follows]

Substitutions

$$\gamma \quad ::= \quad \emptyset \mid x \mapsto v, \gamma$$

$$\frac{x : \tau \in \Gamma \implies (\gamma(x) = v \wedge \ \vdash v : \tau)}{\vdash \gamma : \Gamma}$$

Theorem If $\Gamma \vdash e : \tau$ and $\gamma : \Gamma$ then $\gamma(e) \in C$, where

$$C = \left\{ e \mid \ \vdash e : \tau,\ e \downarrow v,\ \tau = \tau' \to \tau'' \implies \forall v' : \tau' . v(v') \in C \right\}$$

Lemma [closure under β-expansion] If $e \mapsto e'$ and $e' \in C$ then $e \in C$.

(We need this to handle the λ case of the theorem.)

To handle variables, we add a new judgment:

$$\frac{\vdash \gamma : \Gamma \qquad \forall x : \tau \in \Gamma . \gamma(x) \in C}{\gamma \text{ in } \Gamma}$$

Fixpoints

F is monotone if $A \subseteq B$ implies $F(A) \subseteq F(B)$.

$C = \mu(F) = \bigcup_{n=0}^{\infty} F^n(\emptyset)$

Logical relations

To get a workable version of C, we stratify over types.

$$\begin{array}{rcl} \mathcal{C}[\![\tau]\!] & = & \{e \mid \exists v.e \leadsto^* v \wedge v \in \mathcal{V}[\![\tau]\!]\} \\ \mathcal{V}[\![\mathbf{T}]\!] & = & \{c\} \\ \mathcal{V}[\![\tau_1 \to \tau_2]\!] & = & \{v \mid \forall v' \in \mathcal{V}[\![\tau_1]\!].v(v') \in \mathcal{C}[\![\tau_2]\!]\} \end{array}$$

We adjust the γ in Γ judgment accordingly:

$$\frac{\vdash \gamma : \Gamma \qquad \forall x : \tau \in \Gamma.\gamma(x) \in C[\tau]}{\gamma \text{ in } \Gamma}$$

Lemma (Main lemma) If $e \in \mathcal{C}[\![\tau]\!]$ then $e \downarrow v$.

Immediate.

Lemma (Closure under β-expansion) If $e \leadsto e'$ and $e' \in \mathcal{C}[\![\tau]\!]$ then $e \in \mathcal{C}[\![\tau]\!]$.

Proof: Since $e' \in \mathcal{C}[\![\tau]\!]$, we have $e' \leadsto^* v$ for some value $v \in \mathcal{V}[\![\tau]\!]$. But since $e \leadsto e'$, this means that $e \leadsto^* v \in \mathcal{V}[\![\tau]\!]$, so that $e \in \mathcal{C}[\![\tau]\!]$.

Theorem (Fundamental theorem) If $\Gamma \vdash e : \tau$ and γ in Γ then $\gamma(e) \in \mathcal{C}[\![\tau]\!]$.

Proof: By induction on e.

Case: $e = x$. By inversion $x : \tau \in \Gamma$. Hence $\gamma(x) \in \mathcal{C}[\![\tau]\!]$.

Case: $e = \lambda x : \tau'.e''$. First, note that e is already a value. By inversion, $\Gamma, x : \tau' \vdash e'' : \tau''$. Let $v' \in \mathcal{V}[\![\tau']\!]$ and let $\gamma' = \gamma, x \mapsto v'$. Then by induction $\gamma'(e'') \in \mathcal{C}[\![\tau'']\!]$. Equivalently, $\gamma(e'')[v'/x] \in \mathcal{C}[\![\tau'']\!]$. But $\gamma(e)(v') = (\lambda x : \tau'.\gamma(e''))(v') \leadsto \gamma(e'')[v'/x]$. By the closure under β-expansion lemma, we have $\gamma(e)(v') \in \mathcal{C}[\![\tau'']\!]$. Hence $\gamma(e) \in \mathcal{C}[\![\tau' \to \tau'']\!]$.

Case: $e = e_1(e_2)$. By inversion $\Gamma \vdash e_1 : \tau_2 \to \tau$ and $\Gamma \vdash e_2 : \tau_2$. By induction, $\gamma(e_1) \in \mathcal{C}[\![\tau_2 \to \tau]\!]$ and $\gamma(e_2) \in \mathcal{C}[\![\tau_2]\!]$. Hence $\gamma(e_1) \leadsto^* v_1$ and $\gamma(e_2) \leadsto^* v_2$ with $v_1 \in \mathcal{V}[\![\tau_2 \to \tau]\!]$ and $v_2 \in \mathcal{V}[\![\tau_2]\!]$. This immediately gives us that $v_1(v_2) \in \mathcal{C}[\![\tau]\!]$. But *that* means that $v_1(v_2) \leadsto^* v$ with $v \in \mathcal{V}[\![\tau]\!]$. In all, we have

$$\gamma(e) = \gamma(e_1(e_2)) = \gamma(e_1)(\gamma(e_2)) \leadsto^* v_1(v_2) \leadsto^* v \in \mathcal{V}[\![\tau]\!],$$

so $\gamma(e) \in \mathcal{C}[\![\tau]\!]$.