All System F programs terminate

This proof is based on notes by Bob Harper and Greg Morrisett.

Extend System F with a new constant $\mathbf{0}$ of type $\forall\alpha.\alpha$. For every type τ, $\mathbf{0}[\tau]$ is a value. At higher types, we have the following evaluation rules for $\mathbf{0}$.

$$\mathbf{0}[\tau_1 \to \tau_2]v \to \mathbf{0}[\tau_2]$$

$$\mathbf{0}[\forall\alpha.\tau][\tau'] \to \mathbf{0}[\tau\{\tau'/\alpha\}]$$

Definition 1 *A* candidate *for a closed type τ is a non-empty set of closed values of type τ such that $\mathbf{0}[\tau] \in T$ for every $T \in Cand_\tau$. (Where $Cand_\tau$ is the set of all candidates for type τ.)*

Definition 2 *Define the interpretation of types as sets of* compuations *and* values *by induction on the structure of types. Below, δ is a closed type substitution for the free type variables of τ and η assigns a candidate for $\delta(\alpha)$ to each variable α.*

$$\begin{array}{lcl}
\mathcal{C}[\![\tau]\!]^\delta_\eta & = & \{e \mid e \to^* v \in \mathcal{V}[\![\tau]\!]^\delta_\eta\} \\
\\
\mathcal{V}[\![int]\!]^\delta_\eta & = & \{i, 0[int]\} \\
\mathcal{V}[\![\tau_1 \to \tau_2]\!]^\delta_\eta & = & \{v \mid\ \vdash v : \delta(\tau_1 \to \tau_2),\ \textit{for all } v' \in \mathcal{V}[\![\tau_1]\!]^\delta_\eta, vv' \in \mathcal{C}[\![\tau_2]\!]^\delta_\eta\} \\
\mathcal{V}[\![\alpha]\!]^\delta_\eta & = & \eta(\alpha) \\
\mathcal{V}[\![\forall\alpha.\tau]\!]^\delta_\eta & = & \{v \mid\ \vdash v : \delta(\forall\alpha.\tau),\ \textit{for all closed } \tau', \\
 & & \qquad v[\tau'] \in \bigcap_{T \in Cand_{\tau'}} \mathcal{C}[\![\tau]\!]^{\delta+\{\alpha\mapsto\tau'\}}_{\eta+\{\alpha\mapsto T\}}\}
\end{array}$$

Observation 3 *All values are computations. If $e \in \mathcal{V}[\![\tau]\!]^\delta_\eta$ then $e \in \mathcal{C}[\![\tau]\!]^\delta_\eta$.*

Observation 4 *Anything that steps to a computation is a computation. If $e \in \mathcal{C}[\![\tau]\!]^\delta_\eta$ and $e' \to e$, then $e' \in \mathcal{C}[\![\tau]\!]^\delta_\eta$.*

Lemma 5 *If $\Delta \vdash \tau$ then $\mathcal{V}[\![\tau]\!]^\delta_\eta \in Cand_{\delta(\tau)}$ for every closed type substitution δ for Δ and every candidate assignment η for δ.*

By inspection of the definition, we can see that $\mathcal{V}[\![\tau]\!]^\delta_\eta$ contains only closed values of the correct type. What remains to be shown is that it contains $\mathbf{0}[\tau]$.

Proof

Proof is by induction on $\Delta \vdash \tau$.

- If $\Delta \vdash \alpha$, by definition $\eta(\alpha) \in Cand_{\delta(\alpha)}$.
- If $\Delta \vdash int$, by definition $\mathbf{0}[int] \in \mathcal{V}[\![int]\!]^\delta_\eta$.
- If $\Delta \vdash \tau_1 \to \tau_2$. To show that $\mathbf{0}[\delta(\tau_1 \to \tau_2)]$ is a member of $\mathcal{V}[\![\delta(\tau_1 \to \tau_2)]\!]^\delta_\eta$, suppose that $v_1 \in \mathcal{V}[\![\tau_1]\!]^\delta_\eta$. By the evaluation rule, $\mathbf{0}[\delta(\tau_1 \to \tau_2)]v_1 \to \mathbf{0}[\delta\tau_2]$. By induction, $\mathbf{0}[\delta(\tau_2)] \in \mathcal{V}[\![\tau_2]\!]^\delta_\eta$, so $\mathbf{0}[\delta(\tau_1 \to \tau_2)] \in \mathcal{C}[\![\tau_1 \to \tau_2]\!]^\delta_\eta$.
- If $\Delta \vdash \forall\alpha.\tau$. Do this branch yourself.

$\square$

Lemma 6 (Substitution) *The interpretation of types is compositional.*

$$\mathcal{V}[\![\tau\{\tau'/\alpha\}]\!]^{\delta}_{\eta} = \mathcal{V}[\![\tau]\!]^{\delta+\{\alpha\mapsto\delta(\tau')\}}_{\eta+\{\alpha\mapsto\mathcal{V}[\![\tau']\!]^{\delta}_{\eta}\}}$$

The proof of this lemma is by a straightforward induction on the structure of τ. Because the value sets are the same, we can extend this result to the computation sets.

Corollary 7

$$\mathcal{C}[\![\tau\{\tau'/\alpha\}]\!]^{\delta}_{\eta} = \mathcal{C}[\![\tau]\!]^{\delta+\{\alpha\mapsto\delta(\tau')\}}_{\eta+\{\alpha\mapsto\mathcal{V}[\![\tau']\!]^{\delta}_{\eta}\}}$$

Lemma 8 *If $\Delta\Gamma \vdash e : \tau$ then $\gamma(\delta(e)) \in \mathcal{C}[\![\tau]\!]^{\delta}_{\eta}$ for every closed type substitution δ for Δ, every candidate assignment η for δ, and every closed value substitution γ such that $\gamma(x) \in \mathcal{V}[\![\Gamma(x)]\!]^{\delta}_{\eta}$ for every $x \in dom(\Gamma)$.*

Proof

Proof is by induction on $\Delta\Gamma \vdash e : \tau$.

- If $\Delta\Gamma \vdash x : \Gamma(x)$.
- If the last rule of the derivation was

  $$\frac{\Delta\Gamma \vdash e_1 : \tau_1 \to \tau \quad \Delta\Gamma \vdash e_1 : \tau_1}{\Delta\Gamma \vdash e_1 e_2 : \tau_1}$$

  Let γ, δ and η be arbitrary. We want to show that $\gamma(\delta(e_1 e_2)) \in \mathcal{C}[\![\tau_2]\!]^{\delta}_{\eta}$.

  By induction $\gamma(\delta(e_1)) \in \mathcal{C}[\![\tau_1 \to \tau_2]\!]^{\delta}_{\eta}$ and $\gamma(\delta(e_2)) \in \mathcal{C}[\![\tau_1]\!]^{\delta}_{\eta}$, so $\gamma(\delta(e_1)) \to^* v_1 \in \mathcal{V}[\![\tau_1 \to \tau_2]\!]^{\delta}_{\eta}$ and $\gamma(\delta(e_2)) \to^* v_2 \in \mathcal{V}[\![\tau_1]\!]^{\delta}_{\eta}$.

  Therefore $\gamma(\delta(e_1 e_2))$ evaluates to $v_1 v_2$, and by the definition of $\mathcal{V}[\![\tau_1 \to \tau_2]\!]^{\delta}_{\eta}$, this expression is in $\mathcal{C}[\![\tau_2]\!]^{\delta}_{\eta}$.
- If the last rule of the derivation was

  $$\frac{\Delta\Gamma \vdash e : \forall\alpha.\tau \qquad \Delta \vdash \tau'}{\Delta\Gamma \vdash e[\tau'] : \tau\{\tau'/\alpha\}}$$

  Let γ, δ and η be arbitrary. We want to show that $\gamma(\delta(e[\tau'])) \in \mathcal{C}[\![\tau\{\tau'/\alpha\}]\!]^{\delta}_{\eta}$.

  By induction $\gamma(\delta(e)) \in \mathcal{C}[\![\forall\alpha.\tau]\!]^{\delta}_{\eta}$ so $\gamma(\delta(e)) \to^* v \in \mathcal{V}[\![\forall\alpha.\tau]\!]^{\delta}_{\eta}$

  Therefore $\gamma(\delta(e[\tau']))$ evaluates to $v[\delta(\tau')]$, and by the definition of $\mathcal{V}[\![\forall\alpha.\tau]\!]^{\delta}_{\eta}$, $v[\delta(\tau')] \in \bigcap_{T\in Cand_{\delta\tau'}} \mathcal{C}[\![\tau]\!]^{\delta+\{\alpha\mapsto\delta(\tau')\}}_{\eta+\{\alpha\mapsto T\}}$.

  Because $\mathcal{V}[\![\tau']\!]^{\delta}_{\eta}$ is in $Cand_{\delta\tau'}$, $v[\delta(\tau')] \in \mathcal{C}[\![\tau]\!]^{\delta+\{\alpha\mapsto\delta(\tau')\}}_{\eta+\{\alpha\mapsto\mathcal{V}[\![\tau']\!]^{\delta}_{\eta}\}}$. By the substitution lemma, this set is equivalent to $\mathcal{C}[\![\tau\{\tau'/\alpha\}]\!]^{\delta}_{\eta}$.

- If the last rule of the derivation was

$$\frac{\Delta\Gamma, x : \tau_1 \vdash e : \tau_2 \qquad \Delta \vdash \tau_1}{\Delta\Gamma \vdash \lambda x : \tau_1.e : \tau_1 \to \tau_2}$$

  (Do yourself.)

- If the last rule of the derivation was

$$\frac{\Delta, \alpha\ \Gamma \vdash e : \tau}{\Delta\Gamma \vdash \Lambda\alpha.e : \forall\alpha.\tau}$$

  (Do yourself.)

$\square$

Theorem 9 *If* $\vdash e : \tau$ *then there exists* v *such that* $e \to^* v$.

Proof

By the above lemma, $e \in \mathcal{C}[\![\tau]\!]^\delta_\eta$ where δ and η are empty. $\square$