Homework 3: Gödel's T and PCF

15-814: Types and Programming Languages
TA: Carlo Angiuli (cangiuli@cs.cmu.edu)

Out: 10/17/13
Due: 10/31/13 (12 PM)

Please submit your work by the start of lecture on the due date, as a PDF to `cangiuli@cs.cmu.edu`. Include the phrase "15-814 Homework 3" in the subject line of your email.

1 Termination for Gödel's T

Recall the statics and dynamics for Gödel's T:

$$\frac{}{\Gamma, x : \tau \vdash x : \tau} \qquad \frac{\Gamma, x : \tau_1 \vdash M : \tau_2}{\Gamma \vdash \lambda x : \tau_1 .\, M : \tau_1 \to \tau_2} \qquad \frac{\Gamma \vdash M : \tau_1 \to \tau_2 \quad \Gamma \vdash N : \tau_1}{\Gamma \vdash M\, N : \tau_2}$$

$$\frac{}{\Gamma \vdash \mathbf{z} : \mathbf{nat}} \qquad \frac{\Gamma \vdash M : \mathbf{nat}}{\Gamma \vdash \mathbf{s}(M) : \mathbf{nat}} \qquad \frac{\Gamma \vdash M : \mathbf{nat} \quad \Gamma \vdash N_0 : \tau \quad \Gamma, x : \tau \vdash N_1 : \tau}{\Gamma \vdash \mathbf{natind}(M; N_0; x.N_1) : \tau}$$

$$\frac{M \to_\beta M'}{M\, N \to_\beta M'\, N} \qquad \frac{M \ \mathsf{val} \quad N \to_\beta N'}{M\, N \to_\beta M\, N'} \qquad \frac{N \ \mathsf{val}}{(\lambda x : \tau .\, M)\, N \to_\beta [N/x]M}$$

$$\frac{}{\mathbf{natind}(\mathbf{z}; N_0; x.N_1) \to_\beta N_0} \qquad \frac{M \ \mathsf{val}}{\mathbf{natind}(\mathbf{s}(M); N_0; x.N_1) \to_\beta [\mathbf{natind}(M; N_0; x.N_1)/x]N_1}$$

$$\frac{M \to_\beta M'}{\mathbf{s}(M) \to_\beta \mathbf{s}(M')} \qquad \frac{M \to_\beta M'}{\mathbf{natind}(M; N_0; x.N_1) \to_\beta \mathbf{natind}(M'; N_0; x.N_1)}$$

$$\frac{}{\mathbf{z} \ \mathsf{val}} \qquad \frac{M \ \mathsf{val}}{\mathbf{s}(M) \ \mathsf{val}} \qquad \frac{}{\lambda x : \tau_1 .\, M \ \mathsf{val}}$$

In class, we proved the progress and preservation theorems for this system.

Lemma 1.1 (Preservation)**.** *If $\cdot \vdash M : \tau$ and $M \to_\beta M'$ then $\Gamma \vdash M' : \tau$.*

Lemma 1.2 (Progress)**.** *If $\cdot \vdash M : \tau$ then either $M \ \mathsf{val}$ or $M \to_\beta M'$, for some M'.*

Use these theorems to prove type safety for Gödel's T.

Task 1 (Type Safety)**.** *Show that if $\cdot \vdash M : \tau$ and $M \to_\beta^* M'$, then $M' \ \mathsf{val}$ or $M' \to_\beta M''$ for some M''.*

Type safety ensures that well-typed terms reduce until they reach a value, but it's possible that some term might never reach a value. In the next few tasks, we will prove *termination*, the property that every well-typed term reduces to a value.

We saw in class that a simple inductive proof of termination breaks down for application. Our fix will be to strengthen the inductive hypothesis to a property of terms called *hereditary* *termination*. Hereditary termination is defined at each type (inductively on the structure of types) as a predicate on closed terms of that type, as follows:

Definition 1 (Hereditary Termination)**.**

1. $\mathbf{HT}_{\mathbf{nat}}(M)$ *iff* $M \to_\beta^* N$ *and* N val*.*
2. $\mathbf{HT}_{\tau_1 \to \tau_2}(M)$ *iff* $M \to_\beta^* \lambda x : \tau_1 .\, M'$*, and for any* M_1 *such that* $\mathbf{HT}_{\tau_1}(M_1)$*,* $\mathbf{HT}_{\tau_2}([M_1/x]M')$*.*

For any context Γ, a *total substitution* γ is a mapping from $\mathsf{dom}(\Gamma)$ to closed terms which preserves types; that is, for each $x : \tau$ in Γ, $\gamma(x) : \tau$. Given a total substitution γ and a term $\Gamma \vdash M : \tau$, we can form a closed term $\hat{\gamma}(M)$ by performing the substitution. For example, if $\Gamma = (x : \tau \to \tau', y : \tau)$, $M = x\, y$, and γ is a total substitution for Γ, then $\hat{\gamma}(M) = \gamma(x)\, \gamma(y)$.

We say that $\mathbf{HT}_\Gamma(\gamma)$ iff for all $x : \tau$ in Γ, we have $\mathbf{HT}_\tau(\gamma(x))$.

We need one more lemma before proving our main theorem.

Task 2 (Head Expansion)**.** *Show that if* $\mathbf{HT}_\tau(M)$*,* $\cdot \vdash M' : \tau$*, and* $M' \to_\beta M$ *then* $\mathbf{HT}_\tau(M')$*.*

We can now prove all terms are hereditarily terminating. You may use without proof a canonical forms lemma.

Task 3. *Show that if* $\Gamma \vdash M : \tau$ *and* $\mathbf{HT}_\Gamma(\gamma)$ *then* $\mathbf{HT}_\tau(\hat{\gamma}(M))$*.*

(Hint) Use induction on the typing derivation. You will need an additional induction inside the case for the recursor.

Task 4 (Termination)**.** *Show that if* $\cdot \vdash M : \tau$*, then* M *terminates.*

(Hint) Prove that if $\mathbf{HT}_\tau(M)$, then M terminates.

2 Big-step operational semantics

Because reduction in Gödel's T is deterministic and terminating, we know that we can compute any term to its unique fully-evaluated form by reducing until we reach a value. Because we are describing computation by means of an iterated process of reduction, $\to_\beta$ is called a *small-step operational semantics.*

Another approach is to directly define the relation between any term and its fully-evaluated form, all in one go; this is called a *big-step operational semantics*, and is written $M \Downarrow M'$. It is defined by the following rules:

$$\frac{M \Downarrow \lambda x : \tau .\, M' \quad N \Downarrow N' \quad [N'/x]M' \Downarrow M''}{M\, N \Downarrow M''}$$

$$\frac{M \Downarrow \mathbf{z} \quad N_0 \Downarrow N_0'}{\mathbf{natind}(M; N_0; x.N_1) \Downarrow N_0'} \qquad \frac{M \Downarrow \mathbf{s}(M') \quad [\mathbf{natind}(M'; N_0; x.N_1)/x]N_1 \Downarrow N_1'}{\mathbf{natind}(M; N_0; x.N_1) \Downarrow N_1'}$$

$$\frac{}{\mathbf{z} \Downarrow \mathbf{z}} \qquad \frac{M \Downarrow M'}{\mathbf{s}(M) \Downarrow \mathbf{s}(M')} \qquad \frac{}{\lambda x : \tau .\, M \Downarrow \lambda x : \tau .\, M}$$

We want to show that the notions of computation described by $\Downarrow$ and $\to_\beta$ coincide, in the sense that they associate the same fully-evaluated form to each term.

As in the previous homework, you may use the fact that $\to_\beta^*$ is transitive, and various compatibility lemmas (below).

Lemma 2.1. *If* $M \to_\beta^* M'$ *and* $M' \to_\beta^* M''$ *then* $M \to_\beta^* M''$*.*

Lemma 2.2. *If* $M \to_\beta^* M'$*, then* $\mathbf{s}(M) \to_\beta^* \mathbf{s}(M')$*.*

Lemma 2.3. *If $M \to_\beta^* M'$, then for any x, N_0, N_1, we have* $\mathbf{natind}(M; N_0; x.N_1) \to_\beta^* \mathbf{natind}(M'; N_0; x.N_1)$.

Lemma 2.4. *If $M \to_\beta^* M'$ then for any M'' we have $M\,M'' \to_\beta^* M'\,M''$.*

Lemma 2.5. *If $M \to_\beta^* M'$ then for any M'' we have $M''\,M \to_\beta^* M''\,M'$.*

Lemma 2.6. *If $M \to_\beta^* M'$ then for any x we have $\lambda x.M \to_\beta^* \lambda x.M'$.*

One direction of the correspondence between $\Downarrow$ and $\to_\beta^*$ is the following:

Task 5. *Show that if $M \Downarrow M'$, then $M \to_\beta^* M'$ and M' val.*

To prove the other direction, we need two lemmas:

Task 6. *Show that if M val, then $M \Downarrow M$.*

Task 7. *Show that if $M \to_\beta M'$ and $M' \Downarrow M''$, then $M \Downarrow M''$.*

(Hint) Use induction on the derivation of $M \to_\beta M'$. In each case, consider which rules of $\Downarrow$ could apply to M'.

And now we can complete the proof of the other direction:

Task 8. *Show that if $M \to_\beta^* M'$ and M' val, then $M \Downarrow M'$.*

3 Halting Problem in PCF

In this exercise we will show that there is no PCF term T which, given a PCF term $M : \mathbf{nat}$, decides whether or not M reduces to a value. Such a term $T : \mathbf{nat} \to \mathbf{nat}$ must obey the following specification:

$$\begin{array}{lll} T\,M \to_\beta 0 & \text{or} & T\,M \to_\beta 1 \\ T\,M \to_\beta 1 & & \text{iff } M \text{ reduces to a value (converges)} \\ T\,M \to_\beta 0 & & \text{iff } M \text{ does not reduce to a value (diverges)} \end{array}$$

To prove that no such T is definable in the λ-calculus, we will replicate the diagonal argument used to prove the undecidability of the Halting Problem, but in a *higher-order* setting.

Task 9. *Use the* **fix** *operator to write a divergent closed term of type* **nat**.

Task 10. *Show that T is not definable in PCF.*

(Hint) Assume that T is definable, and define another term $D : \mathbf{nat}$ that applies T to D itself, such that if the outcome is 1 then D diverges, and otherwise it is equal to 0. (Use **natrec** to check the value of $T\,D$.) Since D is a PCF term, we can try and observe the behavior of applying T to D itself, from which a contradiction should arise.