

Homework 5: System F: Termination and Parametricity

15-814: Types and Programming Languages
TA: Bernardo Toninho (btoninho@cs.cmu.edu)

Out: 8/11/11
Due: 22/11/11

1 Termination of System F

In this exercise you will show that all well-typed terms in System F are terminating.
Recall the statics of System F:

$$\frac{}{\Delta, X \text{ type} \vdash X \text{ type}} \quad \frac{\Delta \vdash \tau_1 \text{ type} \quad \Delta \vdash \tau_2 \text{ type}}{\Delta \vdash \tau_1 \rightarrow \tau_2 \text{ type}} \quad \frac{\Delta, X \text{ type} \vdash \tau \text{ type}}{\Delta \vdash \forall X. \tau \text{ type}}$$

$$\frac{}{\Delta; \Gamma, x : \tau \vdash x : \tau} \quad \frac{\Delta; \Gamma, x : \tau_1 \vdash M : \tau_2}{\Delta; \Gamma \vdash \lambda x : \tau_1. M : \tau_1 \rightarrow \tau_2} \quad \frac{\Delta; \Gamma \vdash M : \tau_1 \rightarrow \tau_2 \quad \Delta; \Gamma \vdash N : \tau_2}{\Delta; \Gamma \vdash M N : \tau_2}$$

$$\frac{\Delta, X \text{ type}; \Gamma \vdash M : \tau}{\Delta; \Gamma \vdash \Lambda X. M : \forall X. \tau} \quad \frac{\Delta \vdash \tau \text{ type} \quad \Delta; \Gamma \vdash M : \forall X. \tau_1}{\Delta; \Gamma \vdash M[\tau] : [\tau/X]\tau_1}$$

We define a predicate R to be a reducibility candidate (at a type σ) when all of the following hold:

1. If $R(M)$ then $M : \sigma$
2. If $R(M')$ and $M \mapsto^* M'$ then $R(M)$
3. If $R(M)$ then $M \mapsto^* M'$ with $M' \text{ val}$

We define hereditary termination $\mathbf{HT}_\tau^{\delta, \eta}$ as a predicate on terms of type $\hat{\delta}(\tau)$, as follows (this definition is slightly different from the one given in class, avoiding the need for the type **2**):

1. $\mathbf{HT}_X^{\delta, \eta}(M)$ iff $\eta(X)(M)$.
2. $\mathbf{HT}_{\tau_1 \rightarrow \tau_2}^{\delta, \eta}(M)$ iff $M \mapsto^* \lambda x : \hat{\delta}(\tau_1). M'$ and for all M_1 such that $\mathbf{HT}_{\tau_1}^{\delta, \eta}(M_1)$ we have $\mathbf{HT}_{\tau_2}^{\delta, \eta}([M_1/x]M')$.
3. $\mathbf{HT}_{\forall X. \tau}^{\delta, \eta}(M)$ iff $M \mapsto^* \Lambda X. M'$ and for all closed types σ and all reducibility candidates R at σ , we have:

$$\mathbf{HT}_\tau^{\delta[X \mapsto \sigma], \eta[X \mapsto R]}([\sigma/t]M')$$

If Δ is a type context (a set of type variables), we write $\delta : \Delta$ to denote that δ is an assignment of closed types to the variables in Δ . We write $\eta : \delta$ to denote that η is an assignment of reducibility candidates to the type variables in Δ , at the types given in δ .

Task 1 (Hereditary Termination is a reducibility candidate) Assume that δ is as assignment of closed type variables and that $\eta : \delta$ is an assignment of reducibility candidates for those types. Show that $\mathbf{HT}_\tau^{\delta, \eta}$ is a reducibility candidate at type $\hat{\delta}(\tau)$.

Task 2 (Compositionality) Show that, for all closed types σ , the following holds:

$$\mathbf{HT}_{\tau}^{\delta[X \mapsto \sigma], \eta[X \mapsto \mathbf{HT}_{\sigma}^{\delta, \eta}]}(M) \text{ iff } \mathbf{HT}_{[\sigma/X]\tau}^{\delta, \eta}(M)$$

In the following task, you may use a slightly stronger version of compositionality (where σ can be an open type):

$$\mathbf{HT}_{\tau}^{\delta[X \mapsto \hat{\delta}(\sigma)], \eta[X \mapsto \mathbf{HT}_{\sigma}^{\delta, \eta}]}(M) \text{ iff } \mathbf{HT}_{[\sigma/X]\tau}^{\delta, \eta}(M)$$

We write $\mathbf{HT}_{\Gamma}^{\delta, \eta}(\gamma)$ to denote that for each assignment $x : \tau \in \Gamma$, we have that $\mathbf{HT}_{\tau}^{\delta, \eta}(\gamma(x))$.

Task 3 (Fundamental Lemma) Assume that $\Delta; \Gamma \vdash M : \tau$. Show that for all $\delta : \Delta$, $\eta : \delta$ and all γ such that $\mathbf{HT}_{\Gamma}^{\delta, \eta}(\gamma)$ we have $\mathbf{HT}_{\tau}^{\delta, \eta}(\hat{\gamma}(\hat{\delta}(M)))$.

The fact that well-typed terms terminate follows straightforwardly from the fundamental lemma: all well-typed terms terminate, and \mathbf{HT} is a reducibility candidate (which requires termination by definition).

2 Parametricity

In this exercise we will extend the key idea of candidates of the previous section to the general case of binary relations over terms. We will consider the extension of System F with natural numbers and polymorphic lists $\mathbf{list}[\tau]$. All these are definable in System F:

$$\frac{}{\Delta; \Gamma \vdash \mathbf{z} : \omega} \quad \frac{\Delta; \Gamma \vdash M : \omega}{\Delta; \Gamma \vdash \mathbf{s}(M) : \omega} \quad \frac{\Delta; \Gamma \vdash M : \omega \quad \Delta; \Gamma \vdash M_0 : \tau \quad \Delta; \Gamma, x : \tau \vdash M_1 : \tau}{\Delta; \Gamma \vdash \mathbf{rec}(M; M_0; x.M_1) : \tau}$$

$$\frac{\Delta \vdash \tau \text{ type}}{\Delta; \Gamma \vdash \mathbf{nil} : \mathbf{list}[\tau]} \quad \frac{\Delta; \Gamma \vdash M_1 : \tau \quad \Delta; \Gamma \vdash M_2 : \mathbf{list}[\tau]}{\Delta; \Gamma \vdash M_1 :: M_2 : \mathbf{list}[\tau]}$$

$$\frac{\Delta; \Gamma \vdash M : \mathbf{list}[\tau] \quad \Delta; \Gamma \vdash M_0 : \tau_1 \quad \Delta; \Gamma, x : \tau, y : \tau_1 \vdash M_1 : \tau_1}{\Delta; \Gamma \vdash \mathbf{irec}(M; M_0; x.y.M_1) : \tau_1}$$

An equivalence relation is a congruence iff it is preserved by all contexts. A binary relation R is called consistent if there is something it doesn't relate. We define observational equivalence $M \cong M' : \tau$ to be the coarsest consistent congruence (coarsest means that it relates as much as possible). We say that R is an equivalence candidate at types ρ and ρ' , written $R : \rho \leftrightarrow \rho'$ iff the following implication holds: if $R(M, M')$ and $N \cong M : \rho$ and $N' \cong M' : \rho'$, then $R(N, N')$.

We define parametric logical equivalence as a binary relation $M \sim M' : \tau[\eta : \delta \leftrightarrow \delta']$ such that:

- $M \sim M' : X[\eta : \delta \leftrightarrow \delta']$ iff $\eta(X)(M, M')$.
- $\cdot \sim \cdot : \omega[\eta : \delta \leftrightarrow \delta']$ is the strongest relation $\mathcal{R}(\cdot, \cdot)$ closed by the following rules:
 - If $M \mapsto^* \mathbf{z}$ and $N \mapsto^* \mathbf{z}$ then $\mathcal{R}(M, N)$.
 - If $M \mapsto \mathbf{s}(M')$ and $N \mapsto^* \mathbf{s}(N')$ and $\mathcal{R}(M', N')$ then $\mathcal{R}(M, N)$.
- $\cdot \sim \cdot : (\mathbf{list}[\tau])[\eta : \delta \leftrightarrow \delta']$ is the strongest relation $\mathcal{R}(\cdot, \cdot)$ closed under the following rules:
 - If $M \mapsto^* \mathbf{nil}$ and $N \mapsto^* \mathbf{nil}$ then $\mathcal{R}(M, N)$.
 - If $M \mapsto M' :: M''$ and $N \mapsto^* N' :: N''$ and $M' \sim N' : \tau[\eta : \delta \leftrightarrow \delta']$ and $\mathcal{R}(M'', N'')$ then $\mathcal{R}(M, N)$.
- $M \sim M' : \tau_1 \rightarrow \tau_2[\eta : \delta \leftrightarrow \delta']$ iff $N \sim N' : \tau_1[\eta : \delta \leftrightarrow \delta']$ implies $M N \sim M' N' : \tau_2[\eta : \delta \leftrightarrow \delta']$.

- $M \sim M' : \forall X. \tau[\eta : \delta \leftrightarrow \delta']$ iff for every ρ and ρ' and every $R : \rho \leftrightarrow \rho'$ we have $M[\rho] \sim M'[\rho'] : \tau[\eta[X \mapsto R] : \delta[X \mapsto \rho] \leftrightarrow \delta'[X \mapsto \rho']]$

In the following exercises, you may use the following lemma without proof: $\cdot \sim \cdot : \tau[\eta : \delta \leftrightarrow \delta']$ is an equivalence candidate at types $\hat{\delta}(\tau)$ and $\hat{\delta}'(\tau)$, assuming δ and δ' are mappings of type variables to closed types and η is a mapping from type variables to equivalence candidates at the appropriate types.

Theorem 1 (Parametricity) *If $\Delta; \Gamma \vdash M : \tau$ then, for all assignments δ and δ' of closed types to type variables in Δ and every relation assignment η such that $\eta : \delta \leftrightarrow \delta'$ and every closed term assignments γ, γ' such that $\gamma \sim \gamma' : \Gamma[\eta : \delta \leftrightarrow \delta']$ (i.e. γ and γ' map variables in Γ to parametric logically equivalent terms according to η, δ and δ' at the appropriate type) we have: $\hat{\gamma}(\hat{\delta}(M)) \sim \hat{\gamma}'(\hat{\delta}'(M)) : \tau[\eta : \gamma \leftrightarrow \gamma']$.*

The theorem above allows us to prove that parametric logical equivalence as defined above is a consistent congruence and thus contained in observational equivalence (i.e. if $M \sim M' : \tau$ then $M \cong M' : \tau$). The converse also holds. You may use these two facts in the remaining tasks, which are particular instances of the general theorem of parametricity.

Task 4 (Map Function) *Assume $f : \tau \rightarrow \sigma$ and let R be the graph of f (i.e. $R(x, y)$ iff $f(x) \cong y : \sigma$). Show that if:*

$$M \sim N : \mathbf{list}[X][\eta[X \mapsto R] : \delta[X \mapsto \tau] \leftrightarrow \delta'[X \mapsto \sigma]]$$

Then:

$$(\mathbf{map}[\tau][\sigma] f)M \sim N : \mathbf{list}[\sigma][\eta : \delta \leftrightarrow \delta']$$

where $\mathbf{map} : \forall X. \forall Y. (X \rightarrow Y) \rightarrow \mathbf{list}[X] \rightarrow \mathbf{list}[Y]$ is the standard map function on lists, defined as:

$$\Lambda X. \Lambda Y. \lambda f : X \rightarrow Y. \lambda l : \mathbf{list}[X]. \mathbf{lrec}(l; \mathbf{nil}; x. y. f(x) :: y)$$

The theorem above states the expected behavior of the `map` function at the relational level. We will now show that that `map` commutes with functions that “rearrange” lists, in the sense that rearranging the list before mapping it produces a list that is equivalent to the one obtained by mapping it before the rearrangement.

Task 5 (Rearrangements and Maps) *Consider terms $r : \forall X. \mathbf{list}[X] \rightarrow \mathbf{list}[X]$ and $f : \tau \rightarrow \tau'$. Prove that:*

$$\mathbf{map}[\tau][\tau'](f) \circ r[\tau] \cong r[\tau'] \circ \mathbf{map}[\tau][\tau'](f) : \mathbf{list}[\tau] \rightarrow \mathbf{list}[\tau']$$

Finally, we show that the behavior of a function with the type of `map` is equivalent to that of the actual map function, in the following sense:

Task 6 (Map maps) *Consider terms $m : \forall X. \forall Y. (X \rightarrow Y) \rightarrow \mathbf{list}[X] \rightarrow \mathbf{list}[Y]$ and $f : \tau \rightarrow \tau'$. Show that (where I is the polymorphic identity function):*

$$m[\tau][\tau'] \cong \mathbf{map}[\tau_1][\tau_2](f) \circ m[\tau][\tau](I[\tau]) : \mathbf{list}[\tau] \rightarrow \mathbf{list}[\tau']$$