Normalization by Evaluation for Martin-Löf Type Theory with One Universe

From PER Model to Subset Model

Andreas Abel[1]

Institut für Informatik, Ludwig-Maximilians-Universität
Oettingenstr. 67, D-80538 München

Abstract

We show how to replace the PER model of the original MFPS 2007 publication by a simpler subset model without losing any results. This observation follows from the general insight that PER semantics is strongly preferable when one models judgemental (aka typed) equality, yet for untyped equality is has no advantage over subset semantics.

The paper under discussion[1] constructs a model of type theory over an untyped λ-model D, by constructing a partial equivalence relation (PER) $\mathcal{T}\mathit{ype} \subseteq \mathsf{D} \times \mathsf{D}$ which identifies the type values in D, plus for each $a \in \mathcal{T}\mathit{ype}$ an associated PER $[a] \subseteq \mathsf{D} \times \mathsf{D}$ which identifies the values of type a in D. Equal types $a = a' \in \mathcal{T}\mathit{ype}$ have equal extensions $[a] = [a']$. The purpose of a PER semantics is to model extensional equality on values, and it defines $f = f' \in [\mathsf{Pi}\, a\, g]$ iff $f \cdot d = f' \cdot d' \in [g(d)]$ for all $d = d' \in [a]$. However, we have already treated η-equality in the term model D; in Lemma 3.4 we show that $t \longrightarrow_{\beta\eta} t'$ implies $[\![t]\!]_\rho \sqsubseteq [\![t']\!]_\rho$ (in particular $[\![\lambda f \lambda x.\, f\, x]\!] \sqsubseteq [\![\lambda f.\, f]\!]$). Also, since we are constructing an open model where *Nat* is inhabited by the neutrals in addition to the numerals, extensionality does not mean more than η-equality.

We can therefore replace the PER model by a simpler subset model. By induction-recursion we define a subset $\mathcal{T}\mathit{ype} \subseteq \mathsf{D}$ and for each $a \in \mathcal{T}\mathit{ype}$ a subset $[a] \subseteq \mathsf{D}$. $\mathcal{T}\mathit{ype}$ and types are upward closed, and improving the definedness of a type does not change its extension. Thus, if $a \in \mathcal{T}\mathit{ype}$ then $a \sqsubseteq a'$ implies $a' \in \mathcal{T}\mathit{ype}$ and $[a] = [a']$, and $d \in [a]$ and $d \sqsubseteq d'$ imply $d' \in [a]$. Improvement does not change the normal form, so $\Downarrow a \equiv \Downarrow a'$ and $\downarrow^a d \equiv \downarrow^{a'} d'$.

[1] Email: abel@tcs.ifi.lmu.de

The resulting subset model fulfills Alexandre Miguel's specification [2, p. 122] of an abstract model of the implicit calculus restricted to two universes and stripped of implicit quantification $\forall$.

To replace the PER model by a subset model, implement the following changes in sections 4 and 5.

PER model.

Replace Per by $\mathcal{P}(\mathsf{D})$ in the whole paper. Define $\Pi \in (\mathcal{A} \in \mathcal{P}(\mathsf{D})) \to (\mathcal{A} \to \mathcal{P}(\mathsf{D})) \to \mathcal{P}(\mathsf{D})$ by

$$\Pi\, \mathcal{A}\, \mathcal{G} = \{e \in \mathsf{D} \mid e \cdot d \in \mathcal{G}(d) \text{ for all } d \in \mathcal{A}\}$$

Let $\mathcal{N}e = \{\mathsf{Ne}\, \hat{s} \mid \hat{s} \in TM\}$.

Semantical natural numbers.

Define $\mathcal{N}at \subseteq \mathsf{D}$ inductively by

$$\frac{}{\mathsf{Zero} \in \mathcal{N}at} \qquad \frac{d \in \mathcal{N}at}{\mathsf{Succ}\, d \in \mathcal{N}at} \qquad \frac{}{\mathsf{Ne}\, \hat{t} \in \mathcal{N}at}.$$

Lemma 4.1 now speaks of subsets instead of PERs, otherwise is remains unchanged. The definition of $\mathcal{S}et$ simplifies to

$$\frac{a \in \mathcal{S}et \qquad g(d) \in \mathcal{S}et \text{ for all } d \in [a]}{\mathsf{Pi}\, a\, g \in \mathcal{S}et} \qquad \frac{}{\mathsf{Nat} \in \mathcal{S}et} \qquad \frac{}{\mathsf{Ne}\, \hat{t} \in \mathcal{S}et}$$

In fact $a \in \mathcal{S}et$ can now be defined just as $(a, \mathcal{A}) \in \mathsf{T}$ for some $\mathcal{A}$. Lemma 4.2 shrinks to the statement that $a \in \mathcal{S}et$ implies that $[a]$ is defined, but this is trivial since $[a] = \mathcal{A}$.

Lemma 4.3 (Semantical sets are upward-closed)

(i) If $c \in \mathcal{S}et$ and $c \sqsubseteq c'$ then $c' \in \mathcal{S}et$ and $[c] = [c']$.

(ii) If $c \in \mathcal{S}et$, $e \in [c]$, and $e \sqsubseteq e'$, then $e' \in [c]$.

The new Lemma 4.3 is proven like the old one, replace instances of the proposition $c = c' \in \mathcal{S}et$ by "$c' \in \mathcal{S}et$ and $[c] = [c']$", and $d = d' \in [a]$ by "$d, d' \in [a]$ and $d \sqsubseteq d'$."

Semantical types.

Analogous changes. We introduce the new notation $d \sqsubseteq d' \in \mathcal{A}$ for $d, d' \in A$ and $d \sqsubseteq d'$. This is for any subset $\mathcal{A}$ of D, including $\mathcal{S}et$ and $\mathcal{T}ype$. The notation $d = d' \in \mathcal{A}$ means now just the literal "$d = d'$ and $d' \in \mathcal{A}$".

Lemma 4.5 (Up and down)

(i) If $c \sqsubseteq c' \in \mathcal{T}ype$ then $\uparrow^c \hat{t} = \uparrow^{c'} \hat{t} \in [c]$.

(ii) If $c \sqsubseteq c' \in \mathcal{S}et$ then $\Downarrow c \equiv \Downarrow c' \in TM$.

(iii) If $c \sqsubseteq c' \in \mathcal{T}ype$ then $\Downarrow c \equiv \Downarrow c' \in TM$.

(iv) If $c \sqsubseteq c' \in \mathcal{T}ype$ and $e \sqsubseteq e' \in [c]$ then $\downarrow^c e \equiv \downarrow^{c'} e' \in TM$.

Lemma 4.6 (Soundness of recursion)
It now suffices to show $\mathsf{rec}\ a\ d_z\ d_s\ e \in [a \cdot e]$ under the appropriate assumptions.

Semantical contexts.
Let

$$\rho \in [\Gamma] \ :\Longleftrightarrow\ \rho(i) \in [[\![\Gamma(i)]\!]_\rho] \text{ for } 0 \le i < |\Gamma|$$

We define valid contexts $\Gamma \models$ inductively by the following rules:

$$\frac{}{\diamond \models} \qquad \frac{\Gamma \models \qquad [\![A]\!]_\rho \in \mathcal{T}\mathit{ype} \text{ for all } \rho \in [\Gamma]}{\Gamma, A \models}$$

Validity.
The definition $\Gamma \models t = t' : A$ never served any purpose, so it could have been dropped already from the original paper, together with Lemma 4.8 (ii). We only have to model *type* equality (in contrast to systems with judgemental equality).

$$\begin{aligned}
\Gamma \models A \ &:\Longleftrightarrow\ \Gamma \models \text{ and } \forall \rho \in [\Gamma].\ [\![A]\!]_\rho \in \mathcal{T}\mathit{ype} \\
\Gamma \models A = A' \ &:\Longleftrightarrow\ \Gamma \models A \text{ and } \Gamma \models A' \text{ and } \forall \rho \in [\Gamma].\ [[\![A]\!]_\rho] = [[\![A']\!]_\rho] \\
\Gamma \models t : A \ &:\Longleftrightarrow\ \Gamma \models A \text{ and } \forall \rho \in [\Gamma].\ [\![t]\!]_\rho \in [[\![A]\!]_\rho]
\end{aligned}$$

Lemma 4.8 (Convertible terms are semantically related)
If $\Gamma \models A, A'$ and $A =_{\beta\eta} A'$ then $\Gamma \models A = A'$.

Proof. Fix some $\rho \in [\Gamma]$. By assumption, $a := [\![A]\!]_\rho \in \mathcal{T}\mathit{ype}$ and $a' := [\![A']\!]_\rho \in \mathcal{T}\mathit{ype}$. Further, $A \longrightarrow^* B\ {}^*\!\longleftarrow A'$, which implies $a \sqsubseteq [\![B]\!]_\rho =: b$ and $a' \sqsubseteq b$. By Lemma 4.4 (modified analogously to Lemma 4.3), $[a] = [b] = [a']$. □

The proof of Theorem 4.9 (Validity) becomes simpler, type conversion goes through unchanged (omitting the intermediate inference $[\![A]\!]_\rho = [\![A']\!]_\rho \in \mathcal{T}\mathit{ype}$).

In Section 5 we need to change

Lemma 5.4 (Equality)
If $c \sqsubseteq c' \in \mathcal{T}\mathit{ype}$ then $\mathsf{R}^c_k = \mathsf{R}^{c'}_k$.

Moral: use subset models for untyped equality and PER models for judgmental equality.

References

[1] Abel, A., K. Aehlig and P. Dybjer, *Normalization by evaluation for Martin-Löf type theory with one universe*, in: M. Fiore, editor, *Proceedings of the 23rd Conference on the Mathematical Foundations of Programming Semantics (MFPS XXIII), New Orleans, LA, USA, 11-14 April 2007*, Electronic Notes in Theoretical Computer Science **173** (2007), pp. 17–39.

[2] Miquel, A., "Le Calcul des Constructions implicite: syntaxe et sÃ©mantique." Ph.D. thesis, Université Paris 7 (2001), thèse de doctorat.