Remarks on Typed Equality for the Calculus of Constructions

Andreas Abel

INRIA, Team πr^2
PPS Lab, Paris

GT Types and Semantics
INRIA, Paris, France
12 November 2009

Overview

1. Martin-Löf Type Theory
    1. Evaluation
    2. Type Checking and Subtyping
    3. η-Equality and Normalization by Evaluation
    4. Models of Type Theory
    5. Typed Equality
2. Remarks on Calculus of Constructions

Expressions and Values

- Expressions of core Martin-Löf Type Theory

$$
\begin{array}{lcll}
s & ::= & \Box_i \; (i \geq -1) & \text{sorts } \texttt{Type}_i \\
* & := & \Box_{-1} & \text{base sort } \texttt{Set} \\
M, N, T, U & ::= & s \mid x \mid M\,N & \\
 & \mid & \lambda x M & \text{domain-free } \lambda \\
 & \mid & \Pi\, U\, T & \text{function type} \\
\Pi x\!:\!U.\,T & := & \Pi\, U\, \lambda x T &
\end{array}
$$

- Values as closures

$$
\begin{array}{lcll}
\rho & \in & \text{environment (variables} \to \text{values)} & \\
a, f, A, F & ::= & s \mid \Pi\, A\, F & \text{constructed values} \\
 & \mid & (\lambda x M)\rho & \text{closures} \\
 & \mid & e & \text{neutral values} \\
e & ::= & x \mid e\, a &
\end{array}
$$

A Simple Interpreter

- Evaluation $(\!|M|\!)_\rho$ suspends at λ.

$$\begin{array}{lcl} (\!|s|\!)_\rho & = & s \\ (\!|\Pi\, U\, T|\!)_\rho & = & \Pi\, (\!|U|\!)_\rho\, (\!|T|\!)_\rho \\ (\!|x|\!)_\rho & = & \rho(x) \\ (\!|M\, N|\!)_\rho & = & (\!|M|\!)_\rho \cdot (\!|N|\!)_\rho \\ (\!|\lambda x M|\!)_\rho & = & (\lambda x M)\rho \end{array}$$

- Application $f \cdot a$ continues suspended evaluation.

$$\begin{array}{lcll} (\lambda x M)\rho \cdot a & = & (\!|M|\!)_{\rho[x \mapsto a]} & \\ e \cdot a & = & e\, a & \text{neutral application} \end{array}$$

Bidirectional Type Checking

- Two judgments/logic programs (Δ environment):

$$\begin{array}{ll} \Delta \vdash I \rightrightarrows A & \text{inference: expr. } I \text{ has principal type value } A \\ \Delta \vdash C \leftleftarrows A & \text{checking: expr. } C \text{ can be assigned type value } A \end{array}$$

- Checkable expressions C are β-normal forms.
- Inferable expressions I are Cs except λ.

$$\begin{array}{lll} I & ::= & s \mid x \mid I\,C \mid \Pi\, I\,(\lambda x I') \\ C & ::= & I \mid \lambda x C \end{array}$$

Type Inference Rules

Typing	Inference
$\dfrac{\Gamma \vdash}{\Gamma \vdash \Box_i : \Box_{i+1}}$	$\dfrac{}{\Delta \vdash \Box_i \rightrightarrows \Box_{i+1}}$
$\dfrac{\Gamma \vdash}{\Gamma \vdash x : \Gamma(x)}$	$\dfrac{}{\Delta \vdash x \rightrightarrows \Delta(x)}$
$\dfrac{\Gamma \vdash M : \Pi\, U\, \lambda x T \qquad \Gamma \vdash N : U}{\Gamma \vdash M\, N : (\lambda x T)\, N}$	$\dfrac{\Delta \vdash I \rightrightarrows \Pi\, A\, F \qquad \Delta \vdash C \leftleftarrows A}{\Delta \vdash I\, C \rightrightarrows F \cdot (\!\|C\|\!)}$
$\dfrac{\Gamma \vdash U : s_1 \qquad \Gamma, x \!:\! U \vdash T : s_2}{\Gamma \vdash \Pi\, U\, \lambda x T : \max(s_1, s_2)}$	$\dfrac{\Delta \vdash I \rightrightarrows s_1 \qquad \Delta, x \!:\! (\!\|I\|\!) \vdash I' \rightrightarrows s_2}{\Delta \vdash \Pi\, I\, \lambda x I' \rightrightarrows \max(s_1, s_2)}$

Type Checking Rules

Typing	Checking
$\dfrac{\Gamma, x : U \vdash M : T}{\Gamma \vdash \lambda x M : \Pi\, U\, \lambda x T}$	$\dfrac{\Delta, x : A \vdash C \Leftarrow F \cdot (\!\lvert x \rvert\!)}{\Delta \vdash \lambda x C \Leftarrow \Pi\, A\, F}$
$\dfrac{\Gamma \vdash M : T \qquad \Gamma \vdash T \leq T'}{\Gamma \vdash M : T'}$	$\dfrac{\Delta \vdash I \rightrightarrows A \qquad A \leq A'}{\Delta \vdash I \Leftarrow A'}$

- Soundness: Let $\Gamma \vdash T : s$ and $\Delta = (\!\lvert \Gamma \rvert\!)$.
  - If $\Delta \vdash C \Leftarrow (\!\lvert T \rvert\!)$ then $\Gamma \vdash C : T$.
  - If $\Delta \vdash I \rightrightarrows (\!\lvert T \rvert\!)$ then $\Gamma \vdash I : T$.
- Completeness: Let $\Delta = (\!\lvert \Gamma \rvert\!)$
  - If $\Gamma \vdash C : T$ then $\Delta \vdash C \Leftarrow (\!\lvert T \rvert\!)$.
  - If $\Gamma \vdash I : T$ then $\Delta \vdash I \rightrightarrows A$ and $A \leq (\!\lvert T \rvert\!)$.

Checking Subtyping (modulo β)

- $A \leq A'$ is checked by
  1. computing the β-normal forms $\mathsf{R}_0\, A$ and $\mathsf{R}_0\, A'$,
  2. checking contravariant subtyping on the normal forms.
- Normalization / readback $\mathsf{R}_m\, A$ (Leroy/Gregoire 2002)

$$
\begin{array}{lcl}
\mathsf{R}_m\, s & = & s \\
\mathsf{R}_m(\Pi\, A\, F) & = & \Pi\, (\mathsf{R}_m\, A)\, (\mathsf{R}_m\, F) \\
\mathsf{R}_m((\lambda x M)\rho) & = & \lambda x_m.\ \mathsf{R}_{m+1}((\lambda x M)\rho \cdot x_m) \\
\mathsf{R}_m\, x & = & x \\
\mathsf{R}_m(e\, a) & = & (\mathsf{R}_m\, e)\, (\mathsf{R}_m\, a)
\end{array}
$$

- In just 7 slides: normalizer and type checker!
- Efficient normalization (like compiled reduction): adapt evaluation and application.

Extension to η-Equality

- Values extended by markers $\uparrow^{\Pi A F}, \downarrow^{\Pi A F}$ for η-expansion.

$$
\begin{array}{lcl}
a, f, A, F & ::= & s \mid \Pi A F \mid (\lambda x M)\rho \mid e \mid \uparrow^{\Pi A F} e \\
e & ::= & x \mid e\, d \\
d & ::= & a \mid \downarrow^{\Pi A F} f \qquad \qquad \eta\text{-expanded values}
\end{array}
$$

- $\uparrow^{A} e = e$ and $\downarrow^{A} a = a$ for $A \neq \Pi$.
- Modify application:

$$
\begin{array}{lcl}
(\lambda x M)\rho \cdot a & = & (\!| M |\!)_{\rho[x \mapsto a]} \\
(\uparrow^{\Pi A F} e) \cdot a & = & \uparrow^{F \cdot a}(e \downarrow^{A} a)
\end{array}
$$

η-Normalization

- Adapt readback $\mathsf{R}_m\,A$. Closures replaced by $\downarrow^{\Pi\,A\,F} f$.

$$
\begin{array}{lcl}
\mathsf{R}_m\,s & = & s \\
\mathsf{R}_m(\Pi\,A\,F) & = & \Pi\,(\mathsf{R}_m\,A)\,(\mathsf{R}_m\,F) \\
\mathsf{R}_m(\downarrow^{\Pi\,A\,F} f) & = & \lambda x_m.\ \mathsf{R}_{m+1}(\downarrow^{F\cdot\uparrow^A x_m}(f\cdot\uparrow^A x_m)) \\
\mathsf{R}_m\,x & = & x \\
\mathsf{R}_m(e\,d) & = & (\mathsf{R}_m\,e)\,(\mathsf{R}_m\,d)
\end{array}
$$

- New identity environment $\rho_\Delta(x) = \uparrow^{\Delta(x)} x$ for evaluation in type checker.

$$
\frac{\Delta \vdash I \rightrightarrows \Pi\,A\,F \qquad \Delta \vdash C \Leftarrow A}{\Delta \vdash I\,C \rightrightarrows F\cdot (\!|C|\!)_{\rho_\Delta}}
\qquad
\frac{\Delta, x\!:\!A \vdash C \Leftarrow F\cdot (\!|x|\!)_{\rho_\Delta}}{\Delta \vdash \lambda x C \Leftarrow \Pi\,A\,F}
$$

$$
\frac{\Delta \vdash I \rightrightarrows s_1 \qquad \Delta, x\!:\!(\!|I|\!)_{\rho_\Delta} \vdash I' \rightrightarrows s_2}{\Delta \vdash \Pi\,I\,\lambda x I' \rightrightarrows \max(s_1, s_2)}
$$

Subset Model

- Evaluation and readback are a priori partial.
- Show totality through model of type theory.
- By induction on i:
  - define $[\Box_i] \subseteq \mathsf{D}$ inductively,
  - simultaneously define $[A] \subseteq \mathsf{D}$ by recursion on $A \in \Box_i$.
- Assume extension of D by constants $\mathsf{N}, \mathsf{z}, \mathsf{s}$ for natural numbers.
- Define $\mathbb{N} \subseteq \mathsf{D}$ inductively.

$$\frac{}{\mathsf{z} \in \mathbb{N}} \qquad \frac{a \in \mathbb{N}}{\mathsf{s}\, a \in \mathbb{N}}$$

Inductive-Recursive Definition

- Define base universe $[*] \subseteq \mathsf{D}$.

$$\frac{}{\mathsf{N} \in [*]} \qquad [\mathsf{N}] = \mathbb{N}$$

$$\frac{A \in [*] \qquad \forall a \in [A].\ F \cdot a \in [*]}{\Pi\, A\, F \in [*]} \qquad [\Pi\, A\, F] = \{f \in \mathsf{D} \mid \forall a \in [A].\ f \cdot a \in [F \cdot a]\}$$

- Define next universe $[\square_0] \subseteq \mathsf{D}$.

$$\frac{A \in [*]}{A \in [\square_0]} \qquad \frac{}{* \in \square_0} \qquad [A], [*] \text{ already def.}$$

$$\frac{A \in [\square_0] \qquad \forall a \in [A].\ F \cdot a \in [\square_0]}{\Pi\, A\, F \in [\square_0]} \qquad [\Pi\, A\, F] = \{f \in \mathsf{D} \mid \forall a \in [A].\ f \cdot a \in [F \cdot a]\}$$

Correctness of (Sub)typing

- Let $\rho \in [\Gamma]$ iff $\rho(x) \in [(\!|\Gamma(x)|\!)_\rho]$ for all x.
- Soundness of typing rules. Let $\rho \in [\Gamma]$.
  1. If $\Gamma \vdash M : T$ then $(\!|M|\!)_\rho \in [(\!|T|\!)_\rho]$.
  2. If $\Gamma \vdash T \leq T'$ and then $[(\!|T|\!)_\rho] \subseteq [(\!|T'|\!)_\rho]$.
- Needs $(\!|T|\!)_\rho = (\!|T'|\!)_\rho$ if $T =_{\beta\eta} T'$.
- Our notion of evaluation is not extensional enough.

Applicative Structures and λ-Models

VAR	$(\!\| x \|\!)_\rho = \rho(x)$	
APP	$(\!\| M\,N \|\!)_\rho = (\!\| M \|\!)_\rho \cdot (\!\| N \|\!)_\rho$	
BETA$^-$	$(\!\| \lambda x M \|\!)_\rho \cdot a = (\!\| M \|\!)_{\rho[x \mapsto a]}$	
IRR	$(\!\| M \|\!)_\rho = (\!\| M \|\!)_{\rho'}$	if $\rho = \rho' \restriction \mathrm{FV}(M)$
SUBST	$(\!\| M[N/x] \|\!)_\rho = (\!\| M \|\!)_{\rho[x \mapsto (\!\| N \|\!)_\rho]}$	
BETA$^+$	$(\!\| M \|\!)_\rho = (\!\| M' \|\!)_\rho$	if $M =_\beta M'$
XI	$(\!\| \lambda x M \|\!)_\rho = (\!\| \lambda x M' \|\!)_{\rho'}$	if $\forall a.\, (\!\| M \|\!)_{\rho[x \mapsto a]} = (\!\| M' \|\!)_{\rho'[x \mapsto a]}$
ETA$^-$	$(\!\| \lambda x.\, M\,x \|\!)_\rho \sqsubseteq (\!\| M \|\!)_\rho$	if $x \notin \mathrm{FV}(M)$
EXT	$f = f'$	if $\forall a.\, f \cdot a = f' \cdot a$

PER Model

- Move extensionality from untyped λ-model $(\mathsf{D}, \_ \cdot \_, (\!|\_|\!)\_)$ to model of type theory.
- Equip subsets $[A] \subseteq \mathsf{D}$ with equivalence relation.
- Equivalently, define partial equivalence relations $[A] \subseteq \mathsf{D} \times \mathsf{D}$.

$$\frac{A = A' \in [*] \qquad \forall a = a' \in [A].\ F \cdot d = F' \cdot d' \in [*]}{\Pi\, A\, F = \Pi\, A'\, F' \in [*]}$$

$$[\Pi\, A\, F] = \{(f, f') \mid \forall a = a' \in [A].\ f \cdot a = f' \cdot a' \in [F \cdot a]\}$$

- Move from untyped equality to typed equality.

$$\frac{\Gamma, x\!:\!U \vdash M : T \qquad \Gamma \vdash N : U}{\Gamma \vdash (\lambda x.\, M)\, N = M[N/x] : T[N/x]} \qquad \frac{\Gamma \vdash M : \Pi\, U\, T \qquad x \notin \mathrm{dom}(\Gamma)}{\Gamma \vdash \lambda x.\, M\, x = M : \Pi\, U\, T}$$

Subtyping in the Model

- For $A, A' \in [\Box_i]$ define $A \leq A'$ inductively

$$\frac{}{\Box_i \leq \Box_j}\ i \leq j$$

$$\frac{A' \leq A \qquad \forall a \in [A'].\, F \cdot a \leq F' \cdot a}{\Pi\, A\, F \leq \Pi\, A'\, F'}$$

- Semantic soundness $A \leq A'$ implies $[A] \subseteq [A']$.
- Gives injectivity of Π : If $\Pi\, A\, F \leq \Pi\, A'\, F'$ then $A' \leq A$ and $\forall a \in [A'].\ F \cdot a \leq F' \cdot a$.

Explicit substitutions

- Our applicative structure $(\mathsf{D}, \_ \cdot \_, (\!|\_|\!)\_)$ does not model substitution.

$$\textsf{SUBST} \quad (\!|M[N/x]|\!)_\rho = (\!|M|\!)_{\rho[x \mapsto (\!|N|\!)_\rho]}$$

- Build explicit substitutions into typed equality.
- Leads to categorical presentation (CwF).

Normalization via Model

- Type normalization $\mathsf{Nbe}_\Gamma T = \mathsf{R}_0 (\!| T |\!)_{\rho_{(\!|\Gamma|\!)}}$
- Soundness: If $\Gamma \vdash T : \Box_i$ then $\Gamma \vdash T = \mathsf{Nbe}_\Gamma T : \Box_i$.
- Completeness: If $\Gamma \vdash T = T' : \Box_i$ then $\mathsf{Nbe}_\Gamma T \equiv \mathsf{Nbe}_\Gamma T'$.
- Completeness follows from PER model: If $A = A' \in [\Box_i]$ then $\mathsf{R}_0\, A \equiv \mathsf{R}_0\, A'$.
- Soundness requires Kripke logical relation between expressions and values (similar to PER model).

Remarks on Calculus of Constructions

- Universes cannot be defined inductively. Need *candidates* instead.
- Main problem: injectivity does not fall out of semantic construction.
- Idea: Injectivity from NbE: soundness, completeness, and uniqueness of typing.
- To do:
  1. Construct logical relation for CoC.
  2. Extend PER model to infinite universe hierarchy.
  3. Replace uniqueness of typing by principal typing.