Towards a Computational Justification of the Axiom of Univalence

Simon Huber
(j.w.w. Thierry Coquand)

University of Gothenburg

TYPES 2011, Bergen, September 9–11

Univalent Foundations for Mathematics

- Vladimir Voevodsky (2009) formulated the *Univalence Axiom* (UA) in Martin-Löf Type Theory as a strong form of the Axiom of Extensionality
- Inspired by the interpretation of type theory in homotopy theory, where types are interpreted as homotopy types

Univalent Foundations for Mathematics

- Implies that "isomorphic" types satisfy the same statements:

  $$A \cong B \Rightarrow P(A) \Rightarrow P(B)$$

  This does not hold for set theory: $\{0\} \cong \{1\}$ and $0 \in \{0\}$, but $0 \notin \{1\}$.
  The constructions of set theory are *not* invariant under isomorphism! ("problem of equivalence")
- UA also implies *functional extensionality*:

  $$\forall x : A \, \mathsf{Id}_{B(x)}(f(x), g(x)) \Rightarrow \mathsf{Id}_{\Pi x:A.B(x)}(f, g).$$

Univalence Axiom

- The Univalence Axiom resolves many problems of formulating mathematics in Martin-Löf Type Theory!
- But adding axioms destroys the computational structure of type theory! They don't follow the introduction/elimination structure.
- It destroys canonicity! E.g., there are closed terms of type $\mathbf{N}$ which don't reduce to a numeral!

Univalence Axiom

- We don't have a computational justification of the axiom via computation rules
- Conjecture (Voevodsky): Given a term $t : \mathbf{N}$ using UA, we can effectively find a term $t' : \mathbf{N}$ not using UA, and a proof of $\mathsf{Id}_{\mathbf{N}}(t, t')$ which may use UA.

Gandy's Elimination of Extensionality

Robin Gandy (JSL 1956) interprets *extensional* simple type theory into *intensional* simple type theory.
This is done by redefining equality essentially using the technique of logical relations, so equality is defined by induction on types.
Extensionality is then expressed as reflexivity of this relation which holds for any given closed term.

General Idea

- For now only non-dependent types: $\mathbf{N}, A \to B, A \times B : \mathbf{U}$ if $A, B : \mathbf{U}$.
- On top of that we add propositions:

$$\bot, \top, \mathrm{Id}_A(a_0, a_1), C \Rightarrow D, C \wedge D, \exists A(\lambda x B), \forall A(\lambda x B) : \Omega$$

whenever $C, D : \Omega$, $A : U$, and $B : \Omega \ \ [x : A]$.

General Idea, cont.

- $\mathsf{Id}_A(a_0, a_1)$ is defined by induction on the type $A : \mathbf{U}$. For the functions $\mathsf{Id}_{A\to B}(f, g)$ is defined as

$$\forall x, y : A\big(\mathsf{Id}_A(x, y) \Rightarrow \mathsf{Id}_B(fx, gy)\big).$$

- We force the equality to be reflexive:

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t' : \mathsf{Id}_A(t, t)}$$

General Idea, cont.

- Additionally:

$$\frac{\Gamma \vdash \rho : \mathsf{Id}_\Delta \qquad \Delta \vdash t : A : \mathbf{U}}{\Gamma \vdash t\rho : \mathsf{Id}_A(t\rho_0, t\rho_1)}$$

$$\begin{aligned} \text{where } \rho &:= [x_1 = (a_1, b_1, c_1), \ldots, x_n = (a_n, b_n, c_n)], \\ \rho_0 &:= (x_1 = a_1, \ldots, x_n = a_n), \\ \rho_1 &:= (x_1 = b_1, \ldots, x_n = b_n) \end{aligned}$$

are explicit substitutions such that $\Gamma \vdash c_i : \mathsf{Id}(a_i, b_i)$.

General Idea, cont.

- Add computation rules for t' and $t\rho$, e.g.,

$$(r\,s)' \longrightarrow r'\,s\,s\,s'$$
$$(\lambda x.t)\rho\,a\,b\,c \longrightarrow t[\rho, x = (a, b, c)]$$

Main Result

This system is confluent, normalizing, and satisfies canonicity. In particular: $\vdash t : \exists \mathbf{N}(\lambda x B)$ implies $t[] \longrightarrow^* (n, r)$ with a numeral n and $\vdash r : B(x = n)$.

Example

Let

$$\begin{aligned} F &: (\mathbf{N} \to \mathbf{N}) \to \mathbf{N} & F &:= \lambda h.h\,1 + h\,2 \\ f &: \mathbf{N} \to \mathbf{N} & f &:= \lambda x.x \\ g &: \mathbf{N} \to \mathbf{N} & g &:= \lambda x.0 + x. \end{aligned}$$

We have a closed proof $p : \mathrm{Id}_{\mathbf{N}\to\mathbf{N}}(f, g)$. Then:

$$F' : \forall f, g : \mathbf{N}\big(\mathrm{Id}_{\mathbf{N}\to\mathbf{N}}(f, g) \Rightarrow \mathrm{Id}_{\mathbf{N}}(Ff, Fg)\big)$$

so

$$F'\,f\,g\,p : \mathrm{Id}_{\mathbf{N}}(1 + 2, (0 + 1) + (0 + 2))$$

We want $F'\,f\,g\,p$ to compute to a proof without $\cdot'$!

More Details: Syntax

$$
\begin{aligned}
\Box &::= \mathbf{U} \mid \Omega \\
x &::= x_{\mathbf{U}} \mid x_{\Omega} && \text{(sorted variables)} \\
r, s, t, A, B &::= x \mid rs \mid \lambda x t \mid t\sigma \mid t\rho \mid t' \mid \mathrm{C}\,\vec{t} \mid \tilde{\mathrm{C}}\,\vec{t} \\
\sigma &::= () \mid (\sigma, x = t) \\
\rho &::= [] \mid [\rho, x = (r, s, t)]
\end{aligned}
$$

Constants

$$
\begin{aligned}
\mathsf{C} ::= {} & \mathbf{N} \mid \times \mid \to \\
& \mid \bot \mid \top \mid \wedge \mid \Rightarrow \mid \exists \mid \forall \mid \mathbf{Id} \\
& \mid * \\
& \mid O \mid S \mid \mathsf{natrec} \mid \mathsf{natind} \\
& \mid (\cdot, \cdot) \mid \mathsf{exelim} \mid \langle \cdot, \cdot \rangle \mid \pi_i \\
& \mid \mathsf{efq} \mid \langle\rangle \mid \mathsf{unitelim} \\
\tilde{\mathsf{C}} ::= {} & \tilde{0} \mid \tilde{S} \mid \widetilde{\mathsf{natrec}} \mid \tilde{\pi}_i \mid \widetilde{\langle \cdot, \cdot \rangle}
\end{aligned}
$$

Typing: σ-substitutions

The σ-substitutions are context morphisms:

$$\frac{\Gamma \vdash}{\Gamma \vdash () : \diamond} \qquad \frac{\Gamma \vdash \sigma : \Delta \quad \Gamma \vdash t : A\sigma \quad \Delta \vdash A : \Omega}{\Gamma \vdash (\sigma, x = t) : (\Delta, x : A)}$$

$$\frac{\Gamma \vdash \sigma : \Delta \quad \Gamma \vdash t : A \quad \Delta \vdash A : \mathbf{U}}{\Gamma \vdash (\sigma, x = t) : (\Delta, x : A)}$$

$$\frac{\Gamma \vdash \sigma : \Delta \quad \Delta \vdash t : A : \mathbf{U}}{\Gamma \vdash t\sigma : A} \qquad \frac{\Gamma \vdash \sigma : \Delta \quad \Delta \vdash t : A : \Omega}{\Gamma \vdash t\sigma : A\sigma}$$

Typing: ρ-substitutions

The ρ-substitutions carry equality proofs:

$$\frac{\Gamma \vdash}{\Gamma \vdash [] : \mathsf{Id}_{\diamond}} \qquad \frac{\Gamma \vdash \rho : \mathsf{Id}_{\Delta} \quad \Gamma \vdash c : \mathsf{Id}_A(a_0, a_1) \quad \Delta \vdash A : \mathbf{U}}{\Gamma \vdash [\rho, x = (a_0, a_1, c)] : \mathsf{Id}_{\Delta, x:A}}$$

$$\frac{\Gamma \vdash \mathsf{Id}_{\Delta} \quad \Gamma \vdash a_i : A\rho_i \quad \Delta \vdash A : \Omega}{\Gamma \vdash [\rho, x = (a_0, a_1, *)] : \mathsf{Id}_{\Delta, x:A}}$$

$$\frac{\Gamma \vdash \rho : \mathsf{Id}_{\Delta} \quad \Delta \vdash t : A : \mathbf{U}}{\Gamma \vdash t\rho : \mathsf{Id}_A(t\rho_0, t\rho_1)}$$

with $[]_i := ()$ and $[\rho, x = (a_0, a_1, c)]_i := (\rho_i, x = a_i)$.

Typing, cont.

- Reflexivity:

$$\frac{\Gamma \vdash t : A : \mathbf{U}}{\Gamma \vdash t' : \mathsf{Id}_A(t, t)}$$

Reduction

$$
\begin{aligned}
x(\sigma, x = s) &\longrightarrow s \\
x(\sigma, y = s) &\longrightarrow x\sigma \\
(r\, s)\sigma &\longrightarrow r\sigma\, s\sigma \\
(\mathsf{C}\, \vec{t})\sigma &\longrightarrow \mathsf{C}\, \vec{t}\sigma \\
(t\sigma_0)\sigma_1 &\longrightarrow t(\sigma_0\sigma_1)
\end{aligned}
$$

where $(x_1 = t_1, \ldots, x_n = t_n)\sigma := (x_1 = t_1\sigma, \ldots, x_n = t_n\sigma)$

$$(\lambda x t)\sigma s \longrightarrow t(\sigma, x = s)$$

Reduction, cont.

Define $\text{sort}(t) \in \{\mathbf{U}, \Omega\}$ such that $\Gamma \vdash t : A : \Box$ implies $\text{sort}(t) = \Box$.
For $\text{sort}(t) = \Omega$:

$$
\begin{aligned}
t\rho &\longrightarrow * \\
t' &\longrightarrow * \\
*s &\longrightarrow * \\
*\rho &\longrightarrow * \\
*' &\longrightarrow *
\end{aligned}
$$

Reduction, cont.

$$
\begin{aligned}
x[\rho, x = (a_0, a_1, c)] &\longrightarrow c \\
x[\rho, y = (a_0, a_1, c)] &\longrightarrow x\rho \\
(r\,s)\rho &\longrightarrow r\rho\, s\rho_0\, s\rho_1\, s\rho \\
(r\,s)' &\longrightarrow r'\, s\, s\, s' \\
t'\sigma &\longrightarrow t\sigma'
\end{aligned}
$$

where $()' := []$ and $(\sigma, x = t)' := [\sigma', x = (t, t, t')]$

$$
(\lambda x t)\rho\, a_0\, a_1\, c \longrightarrow t[\rho, x = (a_0, a_1, c)]
$$

Reduction, cont.

$$
\begin{aligned}
(C\vec{t})\rho &\longrightarrow \tilde{\mathsf{C}}\,\vec{t}\rho \quad \text{where } (\vec{t}, t)\rho := \vec{t}\rho, t\rho_0, t\rho_1, t\rho \\
(C\vec{t})' &\longrightarrow \tilde{\mathsf{C}}\,\vec{t}' \quad \text{where } (\vec{t}, t)' := \vec{t}', t, t, t' \\
(t\rho)\sigma &\longrightarrow t(\rho\sigma) \\
(t\sigma)\rho &\longrightarrow t(\sigma\rho)
\end{aligned}
$$

where

$$
\begin{aligned}
[\dots, x = (a_0, a_1, c), \dots]\sigma &:= [\dots, x = (a_0\sigma, a_1\sigma, c\sigma), \dots], \\
(\dots, x = t, \dots)\rho &:= [\dots, x = (t\rho_0, t\rho_1, t\rho), \dots].
\end{aligned}
$$

Reduction, cont.

Allow reduction anywhere in a term, *except* under a λ (no ξ-rule).

Confluence

- The parallel reduction technique is not directly applicable
- Use a technique by Curien, Hardin, and Lévy (1991): divide $\longrightarrow$ into a substitution part $\longrightarrow_{\mathsf{s}}$ (strongly normalizing and confluent) and $\longrightarrow_{\beta}$. Define $\longrightarrow_{\beta_{\mathsf{w}}} \subseteq \longrightarrow^{*}$ on $\longrightarrow_{s}$-normal forms such that:

$$t \longrightarrow_{\beta} r \quad \Rightarrow \quad \mathsf{nf}_{\mathsf{s}}(t) \longrightarrow^{*}_{\beta_{\mathsf{w}}} \mathsf{nf}_{\mathsf{s}}(r).$$

  Then the confluence of $\longrightarrow$ follows from the confluence of $\longrightarrow_{\beta_{\mathsf{w}}}$.

Normalization

- Define computability predicates:

$$
\begin{array}{rl}
A\downarrow & (A \text{ is a computable type}) \\
a \Vdash A & \text{given a proof of } A\downarrow
\end{array}
$$

- Relativize in $A \to B$, $\forall AB$, and $\exists AB$ to $a \Vdash A$ with $a' \Vdash \mathrm{Id}_A(a, a)$, e.g.,

$$
\frac{f \text{ introduced} \quad \forall a \Vdash A\,(a' \Vdash \mathrm{Id}_A(a, a) \Rightarrow fa \Vdash Ba)}{f \Vdash \forall AB}
$$

Normalization, cont.

Theorem

1. $\Gamma \vdash A : \Omega \ \ \& \ \ \sigma' \Vdash \mathsf{Id}_\Gamma \Rightarrow A\sigma \downarrow$,
2. $\Gamma \vdash t : A : \mathbf{U} \ \ \& \ \ \rho \Vdash \mathsf{Id}_\Gamma \Rightarrow t\rho_i \Vdash A \ \ \& \ \ t\rho \Vdash \mathsf{Id}_A(t\rho_0, t\rho_1)$,
3. $\Gamma \vdash t : A : \Omega \ \ \& \ \ \sigma' \Vdash \mathsf{Id}_\Gamma \Rightarrow A\sigma \downarrow \& \ \ t\sigma \Vdash A\sigma$,
4. $\Gamma \vdash \sigma : \Delta \ \ \& \ \ \rho \Vdash \mathsf{Id}_\Gamma \Rightarrow \sigma\rho \Vdash \mathsf{Id}_\Delta$,
5. $\Gamma \vdash \rho : \mathsf{Id}_\Delta \ \ \& \ \ \sigma' \Vdash \mathsf{Id}_\Gamma \Rightarrow \rho\sigma \Vdash \mathsf{Id}_\Delta$.

Related and Future Work

- Setoid model (Hofmann; Altenkirch LICS 99)
- Observational Type Theory (Altenkirch, McBride, Swiestra)
- Internalized Parametricity (Bernardy, Moulin)
- Add $\mathrm{Id}_{\Omega}(p, q)$ as $p \Leftrightarrow q$, and allow arrow types like $A \to \Omega$ to get proper substitutivity.
- Dependent types!
- Allow repeated applications of ρ and $\cdot'$.
- Do we get a system where the Univalence Axiom is provable?

Thank you!