Canonicity for Cubical Type Theory

Simon Huber

University of Gothenburg

Ljubljana, January 31, 2017

Review of Cubical Type Theory

(j.w.w. Cohen, Coquand, Mörtberg in TYPES 2015)

- allow variables to range over (formal) **interval** $\mathbb{I}$

$i : \mathbb{I} \vdash t(i) : A$	line from $t(0)$ to $t(1)$ in A
$i : \mathbb{I}, j : \mathbb{I} \vdash r(i,j) : A$	square in A

- **path types** Path $A\,a\,b$ for A type, $a : A$, and $b : A$

$$\frac{\Gamma \vdash A \qquad \Gamma, i : \mathbb{I} \vdash t(i) : A}{\Gamma \vdash \langle i \rangle t : \mathsf{Path}\, A\, t(0)\, t(1)}$$

- **composition operations** to justify rules for identity types
- univalence provable from **glueing**

Partial Elements

New operations on contexts: context restrictions Γ, φ

$$\mathbb{F} \ \ni \ \varphi, \psi ::= 0_{\mathbb{F}} \mid 1_{\mathbb{F}} \mid (i = 0) \mid (i = 1) \mid \varphi \vee \psi \mid \varphi \wedge \psi$$

(with relation $(i = 0) \wedge (i = 1) = 0_{\mathbb{F}}$)

$\Gamma, \varphi \vdash A$ is a **partial type**. Examples:

$$i : \mathbb{I}, (i = 0) \vee (i = 1) \vdash A \qquad A(i/0) \bullet \qquad \bullet \, A(i/1)$$

$$i : \mathbb{I}, j : \mathbb{I}, (i = 0) \vee (j = 1) \vdash A \qquad \begin{array}{ccc} A(i/0, j/1) & \xrightarrow{A(j/1)} & A(i/1, j/1) \\ {\scriptstyle A(i/0)} \big\uparrow & & \\ A(i/0, j/0) & & \end{array}$$

Systems

Can introduce partial types (and terms) using systems:

$$\frac{\Gamma \vdash \varphi_1 \vee \cdots \vee \varphi_n = 1 : \mathbb{F} \qquad \Gamma, \varphi_i \vdash A_i \qquad \Gamma, \varphi_i \wedge \varphi_j \vdash A_i = A_j}{\Gamma \vdash [\varphi_1 \ A_1, \ldots, \varphi_n \ A_n]}$$

If $\Gamma \vdash \varphi_k = 1 : \mathbb{F}$, then $\Gamma \vdash [\varphi_1 \ A_1, \ldots, \varphi_n \ A_n] = A_k$.

Similar: $\Gamma \vdash [\varphi_1 \ t_1, \ldots, \varphi_n \ t_n] : A$.

Composition Operations

Operation giving the "lid" to an open box

$$\frac{\Gamma, i : \mathbb{I} \vdash A \qquad \Gamma \vdash \varphi : \mathbb{F} \qquad \Gamma, \varphi, i : \mathbb{I} \vdash u : A \qquad \Gamma \vdash u_0 : A(i/0) \qquad \Gamma, \varphi \vdash u(i/0) = u_0 : A(i/0)}{\Gamma \vdash \mathsf{comp}^i\, A\, [\varphi \mapsto u]\, u_0 : A(i/1)}$$

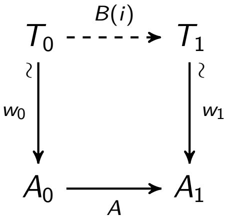
$$\Gamma, \varphi \vdash \mathsf{comp}^i\, A\, [\varphi \mapsto u]\, u_0 = u(i/1) : A(i/1)$$

Explained by induction on the type

Glueing

Allows to "glue" types to parts of another type along an equivalence. Justifies compositions for universes and univalence.

Example: $\varphi = (i = 0) \vee (i = 1)$, $i : \mathbb{I} \vdash A$, $i : \mathbb{I}, \varphi \vdash T$, $i : \mathbb{I}, \varphi \vdash w : \text{Equiv}\ T\ A$



$$B(i) = \text{Glue}\,[(i = 0) \mapsto (T_0, w_0),\ (i = 1) \mapsto (T_1, w_1)]\, A$$

Have: equivalence $(\text{unglue}, \ldots) : \text{Equiv}\, B\, A$ extending w.

Aim

Theorem (Canonicity)

Given a derivation $i_1 : \mathbb{I}, \ldots, i_n : \mathbb{I} \vdash t : \mathsf{N}$ *(*$n \geqslant 0$*) there exists a unique* $m \in \mathbb{N}$ *such that* $i_1 : \mathbb{I}, \ldots, i_n : \mathbb{I} \vdash t = \mathsf{S}^m\, 0 : \mathsf{N}$*.*

We are interested in a proof that provides an algorithm.

Overview of the Proof

1. Typed and deterministic operational semantics
2. Computability predicates and relations
3. Soundness

Notation

$I, J, K, \ldots$ for contexts build only from **names**, i.e., of the form $i_1 : \mathbb{I}, \ldots, i_n : \mathbb{I}$ ($n \geqslant 0$)

$f : J \to I$ for substitutions between such contexts

(Compare this to the cube category!)

Operational Semantics

Naive reduction on untyped terms not confluent!

Instead: One-step reduction on types and terms

$$I \vdash A \succ B$$
$$I \vdash t \succ u : A$$

well-typed and deterministic:

- $\begin{cases} I \vdash A \succ B & \Rightarrow \; I \vdash A = B \\ I \vdash t \succ u : A & \Rightarrow \; I \vdash t = u : A \end{cases}$
- $\begin{cases} I \vdash A \succ B \;\&\; I \vdash A \succ C & \Rightarrow \; B \equiv C \\ I \vdash t \succ u : A \;\&\; I \vdash t \succ v : B & \Rightarrow \; u \equiv v \end{cases}$

Operational Semantics

Weak-head reduction

$$\frac{I, x : A \vdash t : B \qquad I \vdash u : A}{I \vdash (\lambda x : A.t)\, u \succ t(x/u) : B(x/u)}$$

$$\frac{I \vdash t \succ t' : (x : A) \to B \qquad I \vdash u : A}{I \vdash t\, u \succ t' u : B(x/u)}$$

$$\frac{I \vdash A \qquad I, i : \mathbb{I} \vdash t : A \qquad I \vdash r : \mathbb{I}}{I \vdash (\langle i \rangle t)\, r \succ t(i/r) : A}$$

$$\frac{I \vdash t \succ t' : \mathrm{Path}\, A\, u\, v \qquad I \vdash r : \mathbb{I}}{I \vdash t\, r \succ t' r : A}$$

Reductions for Compositions

- First, reduction in the type: if $I, i : \mathbb{I} \vdash A \succ B$, then

$$I \vdash \mathsf{comp}^i\, A\, [\varphi \mapsto u]\, u_0 \succ \mathsf{comp}^i\, B\, [\varphi \mapsto u]\, u_0 : B(i1)$$

- Reductions for each type former are then explained as a directed form of the corresponding judgmental equality. Example:

$$\begin{aligned} I \vdash \mathsf{comp}^i\, ((x : A) \times B)\, [\varphi \mapsto u]\, u_0 \succ \\ (v(i1), \mathsf{comp}^i\, B(x/v)\, [\varphi \mapsto u.2]\, (u_0.2)) \\ : (x : A(i1)) \times B(i1) \end{aligned}$$

where $v = \mathsf{fill}^i\, A\, [\varphi \mapsto u.1]\, (u_0.1)$.

Reductions for Compositions

We never have to reduce in restricted contexts I, φ (for now).

$$\frac{I \vdash \varphi : \mathbb{F} \qquad I, \varphi, i : \mathbb{I} \vdash u : \mathsf{N} \qquad I, \varphi, i : \mathbb{I} \vdash u = 0 : \mathsf{N}}{I \vdash \mathsf{comp}^i\, \mathsf{N}\, [\varphi \mapsto u]\, 0 \succ 0 : \mathsf{N}}$$

Reductions for Systems

Let $I \vdash \varphi_1 \vee \cdots \vee \varphi_n = 1 : \mathbb{F}$.

$$\frac{I, \varphi_i \wedge \varphi_j \vdash A_i = A_j \qquad \begin{array}{c} I, \varphi_i \vdash A_i \\ k \textbf{ minimal} \text{ with } I \vdash \varphi_k = 1 : \mathbb{F} \end{array}}{I \vdash [\varphi_1\ A_1, \ldots, \varphi_n\ A_n] \succ A_k}$$

$$\frac{\begin{array}{c} I \vdash A \qquad I, \varphi_i \vdash t_i : A \\ I, \varphi_i \wedge \varphi_j \vdash t_i = t_j : A \qquad k \textbf{ minimal} \text{ with } I \vdash \varphi_k = 1 : \mathbb{F} \end{array}}{I \vdash [\varphi_1\ t_1, \ldots, \varphi_n\ t_n] \succ t_k : A}$$

Reductions for Glue

For $I \vdash \varphi = 1 : \mathbb{F}$:

- $I \vdash \mathrm{Glue}\,[\varphi \mapsto T]\,A \succ T$
- $I \vdash \mathrm{glue}\,[\varphi \mapsto t]\,a \succ t : T$
- $I \vdash \mathrm{unglue}\,[\varphi \mapsto w]\,u \succ w.1\,u : A$

For $I \vdash \varphi \neq 1 : \mathbb{F}$:

- $I \vdash \mathrm{unglue}\,[\varphi \mapsto w]\,(\mathrm{glue}\,[\varphi \mapsto t]\,a) \succ a : A$
- $I \vdash \mathrm{unglue}\,[\varphi \mapsto w]\,u \succ \mathrm{unglue}\,[\varphi \mapsto w]\,u' : A$ whenever $I \vdash u \succ u' : \mathrm{Glue}\,[\varphi \mapsto T]\,A$

Reductions are in general **not** closed under name substitutions:

$$I \vdash u \succ v : A \;\;\&\;\; f : J \to I \not\Rightarrow J \vdash uf \succ vf : Af$$

Examples:

- If $u = [(i = 0)\ v, 1_{\mathbb{F}}\ w]$, then $u \succ w$ but $u(i/0) \succ v$. We only have $\vdash v = w(i/0)$.
- If $u = \text{unglue}\,[\varphi \mapsto w]\,(\text{glue}\,[\varphi \mapsto t]\,a)$ with $\varphi \neq 1$ and $\varphi f = 1$, then $u \succ a$ but $uf \succ wf.1\,(\text{glue}\,[\varphi f \mapsto tf]\,af)$

Computability Predicates

- want to adapt Tait's (1967) computability method
- Reduction adds names $i : \mathbb{I}$ (in comp^{i})!
- So: need to consider expressions with name variables $i_1 : \mathbb{I}, \ldots, i_n : \mathbb{I}$
- Being computable should be stable under substituting in name variables!
- We only consider well-typed expressions.

Computability Predicates and Relations

Define by (simultaneous) induction-recursion:

$I \Vdash A$	
$I \Vdash A = B$	
$I \Vdash u : A$	by recursion on $I \Vdash A$
$I \Vdash u = v : A$	by recursion on $I \Vdash A$

(Actually, with a universe we need $\Vdash_0$ and $\Vdash_1$ ...)

Some Properties

- Closed under substitutions: e.g., $I \Vdash A$ and $f : J \to I$ imply $J \Vdash Af$.
- $I \Vdash \cdot = \cdot : A$ and $I \Vdash \cdot = \cdot$ are PERs with domain given by $I \Vdash \cdot : A$ and $I \Vdash \cdot$, respectively.
- $I \Vdash u = v : A$ and $I \Vdash A = B$ imply $I \Vdash u = v : B$.

Π-types

$I \Vdash (x : A) \to B$ whenever:

- $J \Vdash Af$ for all $f : J \to I$,
- $J \Vdash B(f, x/u)$ for all $f : J \to I$ and $J \Vdash u : Af$, and
- $J \Vdash B(f, x/u) = B(f, x/v)$ for all $f : J \to I$ and $J \Vdash u = v : Af$.

In this case, $I \Vdash w : (x : A) \to B$ whenever:

- $J \Vdash wf\ u : B(f, x/u)$ for all $f : J \to I$ and $J \Vdash u : Af$, and
- $J \Vdash wf\ u = wf\ v : B(f, x/u)$ for all $f : J \to I$ and $J \Vdash u = v : Af$.

Path types

$I \Vdash \mathrm{Path}\, A\, a\, b$ whenever

- $J \Vdash Af$ for all $f : J \to I$,
- $I \Vdash a : A$ and $I \Vdash b : A$.

In this case, $I \Vdash u : \mathrm{Path}\, A\, a\, b$ whenever

- $I \Vdash u\, 0 = a : A$ and $I \Vdash u\, 1 = b : A$, and
- $J \Vdash uf\, r : Af$ for all $f : J \to I$ and $r \in \mathbb{I}(J)$.

Naturals

$I \Vdash \mathsf{N}$ by definition.
When should a natural $I \vdash u : \mathsf{N}$ be computable?

Usually something like $u \succ^{*} \mathsf{S}^{m}\,0$ ... but reduction is not closed under substitution!

Reducts have to be coherent...

Naturals

- $I \Vdash 0 : \mathsf{N}$ and $I \Vdash 0 = 0 : \mathsf{N}$
- if $I \Vdash u : \mathsf{N}$, then $I \Vdash \mathsf{S}\, u : \mathsf{N}$
  if $I \Vdash u = v : \mathsf{N}$, then $I \Vdash \mathsf{S}\, u = \mathsf{S}\, v : \mathsf{N}$
- $I \Vdash u : \mathsf{N}$ for u is not an introduction whenever
  - for all $f : J \to I$, $J \vdash uf \succ uf{\downarrow} : Af$ and $J \Vdash uf{\downarrow}$, and
  - for all $f : J \to I$ and $g : K \to J$,

$$K \Vdash uf{\downarrow}g = u{\downarrow}fg : \mathsf{N}$$

- $I \Vdash u = v : \mathsf{N}$ for u or v not an introduction whenever
  $I \Vdash u : \mathsf{N}$, $I \Vdash v : \mathsf{N}$, and $J \Vdash uf{\downarrow} = vf{\downarrow} : \mathsf{N}$

Similar conditions appear in the work of Angiuli/Harper/Wilson.

Expansion Lemma

If $I \vdash u : A$ is not an introduction, $I \Vdash A$, $J \vdash uf \succ v_f : Af$ for all $f : J \to I$, satisfying $J \Vdash v_f = v_{\mathbf{1}} f : Af$, then

$$I \Vdash u : A \text{ and } I \Vdash u = v_{\mathbf{1}} : A.$$

Key ingredient of the canonicity proof!

Soundness

We extend computability to open judgments:

$$
\begin{aligned}
\Gamma \models A \quad &:\Leftrightarrow \quad \Gamma \vdash A \ \& \ \Vdash \Gamma \ \& \\
&\qquad \forall I, \sigma, \tau (I \Vdash \sigma = \tau : \Gamma \Rightarrow I \Vdash A\sigma = A\tau) \\
\Gamma \models a : A \quad &:\Leftrightarrow \quad \Gamma \vdash a : A \ \& \ \Gamma \models A \ \& \\
&\qquad \forall I, \sigma, \tau (I \Vdash \sigma = \tau : \Gamma \Rightarrow I \Vdash a\sigma = a\tau : A\sigma)
\end{aligned}
$$

Theorem (Soundness)

$\Gamma \vdash \mathcal{J} \Rightarrow \Gamma \models \mathcal{J}$

Theorem (Canonicity)

If $I \vdash u : \mathsf{N}$, *then* $I \vdash u = \mathsf{S}^n\,0 : \mathsf{N}$ *for a unique* $n \in \mathbb{N}$.

Proof.

By soundness, $I \models u : \mathsf{N}$, so $I \Vdash u : \mathsf{N}$ using $\mathbf{1} : I \to I$, and hence $I \Vdash u = \mathsf{S}^n\,0 : \mathsf{N}$ for some n, thus also $I \vdash u = \mathsf{S}^n\,0 : \mathsf{N}$. Uniqueness: $I \vdash \mathsf{S}^n\,0 = \mathsf{S}^m\,0 : \mathsf{N}$ implies $I \Vdash \mathsf{S}^n\,0 = \mathsf{S}^m\,0 : \mathsf{N}$, and hence $n = m$. □

Theorem (Consistency)

$\mathsf{Path}\,\mathsf{N}\,0\,1$ *is not inhabited.*

Proof.

If $\vdash u : \mathsf{Path}\,\mathsf{N}\,0\,1$, then $i : \mathbb{I} \vdash u\,i = S^n 0 : \mathsf{N}$ for some n by canonicity. But then $\vdash 0 = u\,0 = S^n 0 = u\,1 = 1 : \mathsf{N}$, contradicting uniqueness. □

Conclusion

- canonicity for cubical type theory; can be extended with circle S^1
- first step towards normalization and decidability of type checking
- proof not proof-theoretically optimal (least fixpoint vs. a fixpoint)
- Formalization would be desirable!
- Related work: Abel/Scherer, Coquand/Mannaa, Angiuli/Harper/Wilson