Homotopy type theory

Simon Huber

University of Gothenburg

Summer School on Types, Sets and Constructions,
Hausdorff Research Institute for Mathematics,
Bonn, 3–9 May, 2018

Lecture II: Overview

1. H-Levels
2. Univalence Axiom
3. Higher Inductive Types

Recap

1. Voevodsky: model of type theory in simplicial sets!
   "Types as spaces"
2. $$\begin{array}{lcl} \mathsf{isContr}(A) & \equiv & \Sigma(a : A)\Pi(x : A).\, a =_A x \\ \mathsf{isProp}(A) & \equiv & \Pi(x\ y : A).\, x =_A y \\ \mathsf{isSet}(A) & \equiv & \Pi(x\ y : A).\, \mathsf{isProp}(x =_A y) \end{array}$$
3. propositions and types with decidable equality are sets
4. $\mathsf{isContr}(\mathsf{singl}\, a)$ where $\mathsf{singl}\, a \equiv \Sigma(x : A)a = x$
5. with function extensionality: being contractible/a proposition/a set is a propositions again
   good closure properties

Homotopy levels

One of Voevodsky's main contributions to type theory!

$\text{h-level}\, n\, A$ expresses that *homotopy-level* of a type A is n:

$$\text{h-level}\, 0\, A \equiv \text{isContr}(A)$$
$$\text{h-level}\, (n+1)\, A \equiv \Pi(x\ y : A).\, \text{h-level}\, n\, (x =_A y)$$

h-level		
0	contractible	N_1
1	proposition	N_0, N_1
2	set	N, N_2
3	groupoids	**?**
4	2-groupoids	
...		

Homotopy equivalences (Voevodsky)

1. Let $f\colon A \to B$.
2. For $y : B$ define $\mathsf{fib}_f(y) :\equiv \Sigma(x : A).f\,x = y$
3. f is an *equivalence* if it has contractible fibers:

$$\mathsf{isEquiv}(f) :\equiv \Pi(y : B).\,\mathsf{isContr}(\mathsf{fib}_f(y))$$

4. $A \simeq B$ iff $\Sigma(f\colon A \to B).\,\mathsf{isEquiv}(f)$
5. $\mathsf{isEquiv}(\mathrm{id}_A)$ like $\mathsf{isContr}(\mathsf{singl}(a))$

Homotopy equivalences (Voevodsky)

1. Type of *quasi-inverses* of f denoted qinv(f):

   $$\Sigma(g\colon B \to A).(\Pi(x : A).\, g(f\, x) = x) \times (\Pi(y : B).\, f(g\, y) = y)$$

   (Compare this with 'homotopy equivalences' of spaces.)
2. qinv$(f) \leftrightarrow$ isEquiv(f)
3. Assuming function extensionality: isProp(isEquiv(f))
   But not necessarily isProp(qinv(f)).

The univalence axiom

The univalence axiom specifies what the equality for universes should be.

Define

$$\mathsf{idToEquiv}_{\mathsf{U}} : \Pi(A\ B : \mathsf{U}).A =_{\mathsf{U}} B \to A \simeq B$$

by path induction, mapping $\mathsf{refl}\,A$ to id_A proving $A \simeq A$.

Univalence axiom (Voevodsky)

$$\Pi(A\ B : \mathsf{U}).\,\mathsf{isEquiv}(\mathsf{idToEquiv}_{\mathsf{U}}\,A\,B)$$

1. The univalence axiom is a statement about a universe U

$$\mathsf{UA_U} \qquad \Pi(A\ B : \mathsf{U}).\, \mathsf{isEquiv}(\mathsf{idToEquiv_U}\, A\, B)$$

2. $(A =_{\mathsf{U}} B) \simeq (A \simeq B)$
3. UA implies function extensionality! (Voevodsky)
4. UA implies

$$\begin{aligned} \mathsf{ua} \quad &: \quad \Pi(A\, B : \mathsf{U}).\, A \simeq B \to A =_{\mathsf{U}} B && \text{“naive univalence”} \\ \mathsf{ua}_\beta \quad &: \quad \Pi(A\, B : \mathsf{U})(f : A \simeq B)(x : A). && \text{“computation” rule} \\ &\qquad \mathsf{transport}^{\lambda(X:\mathsf{U}).X}(\mathsf{ua}\, f)\, x = f\, x \end{aligned}$$

5. ua and ua_β also imply UA (Licata)
6. Open problem: does “naive univalence” already imply UA?

UA and UIP?

Univalence is incompatible with uniqueness of identity proofs.

1. Define $\mathsf{swap} \colon \mathsf{N}_2 \to \mathsf{N}_2$ by:

$$\mathsf{swap}(\mathsf{true}) = \mathsf{false} \qquad \mathsf{swap}(\mathsf{false}) = \mathsf{true}$$

2. swap is its own quasi-inverse, thus an equivalence;
3. by UA we get: $\mathsf{ua\ swap} : \mathsf{N}_2 =_{\mathsf{U}} \mathsf{N}_2$;
4. we know: $\mathsf{transport}\,(\mathsf{ua\ swap})\,\mathsf{true} = \mathsf{swap\ true} \equiv \mathsf{false}$,
5. but: $\mathsf{transport}\,1_{\mathsf{N}_2}\,\mathsf{true} \equiv \mathsf{true}$,
6. so: $\mathsf{ua\ swap} \neq_{\mathsf{N}_2 =_{\mathsf{U}} \mathsf{N}_2} 1_{\mathsf{N}_2}$ and hence $\neg\,\mathsf{isSet}(\mathsf{U})$.

Sharpening of $\neg\,\mathsf{isSet}(\mathsf{U})$

Theorem (Kraus/Sattler)

Given a hierarchy of univalent universes $\mathsf{U}_0, \mathsf{U}_1, \mathsf{U}_2, \ldots$

$$\mathsf{U}_0 : \mathsf{U}_1 \qquad \mathsf{U}_1 : \mathsf{U}_2 \qquad \mathsf{U}_2 : \mathsf{U}_3 \qquad \ldots$$

we have

$$\neg(\mathsf{h\text{-}level}\,(n+2)\,\mathsf{U}_n).$$

Special cases of univalence

1. If A, B : U are propositions (so have isProp(A) and isProp(B)), then:

$$(A \leftrightarrow B) \to A \simeq B$$

   So UA implies propositional extensionality:

$$(A \leftrightarrow B) \to A = B$$

2. If A and B are sets, equivalence specializes to bijection/isomorphism between sets.
3. If A and B are groupoids, equivalence specializes to categorical equivalence.

Equality of structures

Recall example of type CBin of types with a commutative operation:

$\Sigma(A : \mathsf{U})(\alpha : \mathsf{isSet}(A))(m : A \times A \to A)\Pi(x\ y : A).\, m(x, y) = m(y, x)$

Given $A' = (A, \alpha_A, m_A, p_A)$ and $B' = (B, \alpha_B, m_B, p_B)$ there is an obvious candidate of homomorphism:

$$f : A \to B \text{ such that } f(m_A(x, y)) = m_B(f\,x, f\,y)$$

Univalence lifts to isomorphisms of this algebraic structure:

$$(A' \cong B') \simeq (A' = B')$$

This works for many other algebraic structures (Aczel, Coquand/Danielsson)

Voevodsky gave a model of UA using Kan simplicial sets formulated in a *classical* meta-theory (ZFC plus two inaccessible cardinals).

(Various *constructive* models based on cubical sets; more later. . .)

So MLTT can't distinguish equivalent types:
Given $P \colon \mathsf{U} \to \mathsf{U}$ and $A, B : \mathsf{U}$ with $A \simeq B$, we can't have $P\,A$ but $\neg(P\,B)$.

In contrast to set theory: $\{0\} \cong \{1\}$ and $0 \in \{0\}$, but $0 \notin \{1\}$.

Propositional truncation

- When is $f : A \to B$ surjective?

$$\Pi(y : B)\Sigma(x : A).\, f\, x = y$$

Propositional truncation

- When is $f\colon A \to B$ surjective?

$$\Pi(y : B)\Sigma(x : A).\, f\, x = y$$

This is the space of sections!?

Propositional truncation

- When is $f\colon A \to B$ surjective?

$$\Pi(y : B)\Sigma(x : A).\, f\,x = y$$

This is the space of sections!?

- Given a type A its *propositional truncation* is a proposition $\|A\|$ with $\mathsf{inc}\colon A \to \|A\|$, such that for any other type B with $\mathsf{isProp}(B)$ there is a map

$$\mathsf{rec}\colon (A \to B) \to \|A\| \to B$$

with: $\mathsf{rec}\, f\,(\mathsf{inc}\, a) \equiv f\,a : B$

Propositional truncation

- When is $f\colon A \to B$ surjective?

$$\Pi(y : B)\Sigma(x : A).\, f\,x = y$$

  This is the space of sections!?

- Given a type A its *propositional truncation* is a proposition $\|A\|$ with $\mathsf{inc}\colon A \to \|A\|$, such that for any other type B with $\mathsf{isProp}(B)$ there is a map

$$\mathsf{rec}\colon (A \to B) \to \|A\| \to B$$

  with: $\mathsf{rec}\, f\, (\mathsf{inc}\, a) \equiv f\, a : B$

- If $A : \mathsf{U}$ is a proposition, then $A \leftrightarrow \|A\|$, so $A \simeq \|A\|$, so $A = \|A\|$.
- $\|A\|$ expresses that A is inhabited, but we can't extract its witness in general

The logic of h-propositions

We can define surjective as:

$$\Pi(y : B)\,\|\Sigma(x : A).\, f\,x = y\|$$

This suggest a interpretation of the logical connectives as (h-)propositions

$$\begin{array}{rcl}
\top & \equiv & \mathsf{N}_1 \\
\bot & \equiv & \mathsf{N}_0 \\
A \Rightarrow B & \equiv & A \to B \\
A \wedge B & \equiv & A \times B \\
A \vee B & \equiv & \|A + B\| \\
\forall(x : A)\, B & \equiv & \Pi(x : A)\, B \\
\exists(x : A)\, B & \equiv & \|\Sigma(x : A)\, B\|
\end{array}$$

This interpretation satisfies all the expected properties from logic.

Classical logic

Voevodsky's simplicial set model validates the following form of excluded middle:

LEM $\Pi(A : \mathsf{U}).\, \mathsf{isProp}(A) \to (A + \neg A)$

(**NB:** $A + \neg A$ is $A \vee \neg A$ here since $\neg(A \times \neg A)$.)

Omitting "isProp(A)" is inconsistent with UA.

Propositional truncation

What kind of type former is $\|-\|$?

$$\frac{a : A}{\mathsf{inc}\, a : \|A\|} \qquad \frac{u : \|A\| \qquad v : \|A\|}{\mathsf{squash}\, u\, v : \mathsf{Id}_{\|A\|}(u, v)}$$

Has constructors for points and paths! (From the recursor one can derive a suitable induction principle.)

Compare: inductive types specified by point constructors

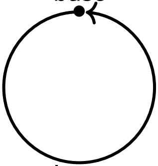
$$\frac{}{0 : \mathsf{N}} \qquad \frac{n : \mathsf{N}}{\mathsf{S}\, n : \mathsf{N}}$$

Propositional truncation is a **higher inductive type** (HIT).

The circle $\mathbb{S}^1$

We can represent the circle $\mathbb{S}^1$ as HIT

$$\frac{}{\mathbb{S}^1 : \mathsf{U}} \qquad \frac{}{\mathsf{base} : \mathbb{S}^1} \qquad \frac{}{\mathsf{loop} : \mathsf{base} = \mathsf{base}}$$



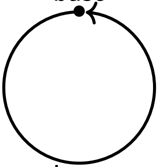
What should be the eliminator for $\mathbb{S}^1$?

$$\frac{x : \mathbb{S}^1 \vdash C(x) \quad b : C(\mathsf{base}) \qquad l : b = b \ \textbf{????}}{\mathbb{S}^1\text{-}\mathsf{elim}_C\, b\, l : \Pi(x : \mathbb{S}^1)\, C(x)}$$

The circle $\mathbb{S}^1$

We can represent the circle $\mathbb{S}^1$ as HIT

$$\frac{}{\mathbb{S}^1 : \mathsf{U}} \qquad \frac{}{\mathsf{base} : \mathbb{S}^1} \qquad \frac{}{\mathsf{loop} : \mathsf{base} = \mathsf{base}}$$



What should be the eliminator for $\mathbb{S}^1$?

$$\frac{x : \mathbb{S}^1 \vdash C(x) \qquad b : C(\mathsf{base}) \qquad l : \mathsf{transport}^C\ \mathsf{loop}\ b = b}{\mathbb{S}^1\text{-}\mathsf{elim}_C\, b\, l : \Pi(x : \mathbb{S}^1)\, C(x)}$$

$$\mathbb{S}^1\text{-}\mathsf{elim}_C\, b\, l\, \mathsf{base} \equiv b : C(\mathsf{base})$$
$$\mathsf{apd}\, (\mathbb{S}^1\text{-}\mathsf{elim}_C\, b\, l\,)\, \mathsf{loop} =_{C(\mathsf{base})} l$$

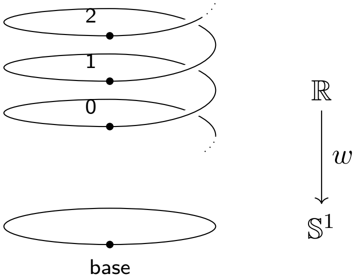
$\Omega(\mathbb{S}^1, \mathsf{base}) = \mathbb{Z}$ in HoTT (Licata/Shulman)

Recall: $\Omega(\mathbb{S}^1, \mathsf{base})$ is $\mathsf{base} =_{\mathbb{S}^1} \mathsf{base}$

The classical proof uses a winding map w projecting a helix onto the circle. Represent the fibers of this map (which is a fibration) as dependent type:

$$\mathsf{Cover} : \mathbb{S}^1 \to \mathsf{U}$$
$$\mathsf{Cover}\,\mathsf{base} = \mathbb{Z}$$
$$\mathsf{ap}\ \mathsf{Cover}\ \mathsf{loop} = \mathsf{ua}\ \mathsf{sucEquiv}$$

where sucEquiv is the equivalence $\mathbb{Z} \simeq \mathbb{Z}$ induced by successor.



We *want* to prove $(\text{base} =_{\mathbb{S}^1} \text{base}) \simeq \mathbb{Z}$ and then use univalence.
So we need maps:

1. $\text{base} = \text{base} \to \mathbb{Z}$
2. $\mathbb{Z} \to \text{base} = \text{base}$

which are inverses of each other.

We *want* to prove $(\mathsf{base} =_{\mathbb{S}^1} \mathsf{base}) \simeq \mathbb{Z}$ and then use univalence.
So we need maps:

1. $\mathsf{base} = \mathsf{base} \to \mathbb{Z}$
2. $\mathbb{Z} \to \mathsf{base} = \mathsf{base}$ Take: $n \mapsto \mathsf{loop}^n$ ✓

which are inverses of each other.

We *want* to prove $(\mathsf{base} =_{\mathbb{S}^1} \mathsf{base}) \simeq \mathbb{Z}$ and then use univalence.
So we need maps:

1. $\mathsf{base} = \mathsf{base} \to \mathbb{Z}$ Take: $p \mapsto \mathsf{transport}^{\mathsf{Cover}}\, p\, 0$ ✓
2. $\mathbb{Z} \to \mathsf{base} = \mathsf{base}$ Take: $n \mapsto \mathsf{loop}^n$ ✓

which are inverses of each other.
But how to prove that the composite

$$\mathsf{base} = \mathsf{base} \to \mathbb{Z} \to \mathsf{base} = \mathsf{base}$$

is the identity?? X

We need to generalize using the *"encode-decode"* method!

Contribution of type theory to homotopy theory!

The encode-decode method

Basic idea: generalize to maps

1. $\text{encode} : \Pi(x : \mathbb{S}^1).\,\text{base} = x \to \text{Cover}\,x$
2. $\text{decode} : \Pi(x : \mathbb{S}^1).\ \text{Cover}\,x \to \text{base} = x$

and show

3. $\Pi(x : \mathbb{S}^1)\Pi(p : \text{base} = x).\,\text{decode}_x(\text{encode}_x\,p) = p$
4. $\Pi(x : \mathbb{S}^1)\Pi(c : \text{Cover}\,x).\,\text{encode}_x(\text{decode}_x\,c) = c$

For (3) we can now use induction on p!

Instantiating to $x :\equiv \text{base}$ gives and equivalence $\Omega(\mathbb{S}^1, \text{base}) \simeq \mathbb{Z}$.
(Recall: Cover base $= \mathbb{Z}$)

Generalizing the maps from before:

$$\begin{aligned}&\mathsf{encode}\colon \Pi(x:\mathbb{S}^1).\,\mathsf{base}=x\to\mathsf{Cover}\,x\\&\mathsf{encode}_x\,p:\equiv\mathsf{transport}^{\mathsf{Cover}}\ p\ 0\end{aligned}$$

$$\begin{aligned}&\mathsf{decode}\colon \Pi(x:\mathbb{S}^1).\ \mathsf{Cover}\,x\to\mathsf{base}=x\\&\mathsf{decode}\,\mathsf{base}\,n=\mathsf{loop}^n\\&\mathsf{apd}\,\mathsf{decode}\,\mathsf{loop}=\dots\end{aligned}$$

Now

$$\Pi(x:\mathbb{S}^1)\Pi(p:\mathsf{base}=x).\,\mathsf{decode}_x(\mathsf{encode}_x\,p)=p,$$

by induction follows from

$$\mathsf{decode}_{\mathsf{base}}(\mathsf{encode}_{\mathsf{base}}\,1_{\mathsf{base}})=\mathsf{decode}_{\mathsf{base}}\,0=\mathsf{loop}^0=1_{\mathsf{base}}$$

Higher inductive types

- Many other results from classical homotopy theory have been proved synthetically.
- Synthetic development in HoTT suggested generalizations of the Blakers-Massey theorem in homotopy theorem.
- There are many other interesting HITs: quotients, pushouts, suspensions, set truncations, the torus, ...
- The main examples of HITs work in the cubical set model (Coquand/SH/Mörtberg LICS'18).
- So far: no general schema for HITs

HoTT as a programming language?

Intensional MLTT **without axioms** explains each of its constants computationally (e.g., induction for N).

Canonicity of MLTT

For $\vdash t : \mathsf{N}$ (in the empty context!) there exists $n \in \mathbb{N}$ with $\vdash t \equiv \mathsf{S}^n\, 0 : \mathsf{N}$.

This breaks with axioms (e.g., $\mathsf{transport}^{\lambda(X:\mathsf{U}).\mathsf{N}}\,(\mathsf{ua}\ldots)\,0$)!

Can we somehow explain the computational content of the univalence axiom?

- Voevodsky's model uses the theory of Kan simplicial sets (and fibrations), formulated in ZFC (plus inaccessible cardinals).
- Bezem/Coquand/Parman: various parts of the theory of Kan simplicial sets are *provably* not constructive! Example: B^A Kan whenever B is.
- Bezem/Coquand/SH (2013): constructive model using cubical sets
- Cohen/Coquand/SH/Mörtberg (2015): refined cubical set model giving rise to cubical type theory and proof assistant `cubicaltt`[1]
- SH (2016): canonicity for cubical type theory

[1] `https://github.com/mortberg/cubicaltt`

Voevodsky's Conjecture

Voevodsky conjectured (2011):

> *There is a terminating algorithm that for any* $t : \mathsf{N}$ *which is closed except that it may use the univalence axiom returns a* $n \in \mathbb{N}$ *and a proof that* $\mathsf{Id}_{\mathsf{N}}(t, \mathsf{S}^n\, 0)$ *(which may use the univalence axiom).*

Shulman (2015) has proved a truncated version of this.

Coquand's modification (2018)

> *Is it possible to extend* ordinary type theory *with suitable computation rules which "explain" the univalence axiom in an effective way?*

A concrete problem

Homotopy groups: $\pi_n(A, a) :\equiv \|\Omega^n(A, a)\|_{\mathsf{set}}$

Brunerie's number

$\pi_4(\mathbb{S}^3) \simeq \mathbb{Z}/n\mathbb{Z}$ for a term $n : \mathsf{N}$ involving UA and HITs

This is a result from Bruneries thesis (2016); it takes more than half his of thesis to prove $n = 2$.

We formalized Brunerie's $n : \mathsf{N}$ in `cubicaltt`. However, the computation of the normal form of n has been unfeasible (so far).