Logic in univalent type theory

Martín Hötzel Escardó

University of Birmingham, UK

Big Proof, Newton Institute, Cambridge, July 2017

What a univalent type theory is for

1. General mathematics performed in a certain way (univalent mathematics).

2. Synthetic homotopy theory (homotopy type theory, or HoTT).

This talk is about *general mathematics* in univalent type theory:

(1) rather than just (2).

What a univalent type theory is

As a first approximation, it is a mathematical language for expressing definitions, theorems and proofs that is invariant under isomorphism:

> If you can say something about the object X, and Y is an object isomorphic to X, then you can say the same thing about Y:
>
> $P(X)$ *and* $X \simeq Y$ *together imply* $P(Y)$.

A precursor

1. It may also happen for a language for mathematics that it makes impossible to distinguish isomorphic objects, even if it wasn't designed with that purpose in mind.

2. Such a language is intensional Martin-Löf type theory (MLTT).

3. For example, in MLTT we can't exhibit any property P of $\mathbb{N}$ that $\mathbb{N} \times \mathbb{N}$ hasn't. (Metatheorem.)

4. In *set theory*, they can be distinguished by the property $P(X) \equiv (0 \in X)$.

   (There isn't a global membership relation in MLTT.)

   NB. One should be careful: the answer in set theory depends on how we decide to encode 0 and pairs as sets. A perverse choice may actually allow $0 \in \mathbb{N} \times \mathbb{N}$.

Some univalent type theories

1. A spartan MLTT + univalence axiom + resizing rules.

   (UniMath)

2. A more generous MLTT + univalence axiom + higher-inductive types.

   (Homotopy type theory book)

3. Cubical Type Theory.

   - Has univalence as a theorem.
   - Has some higher-inductive types.
   - Extends a spartan MLTT.
   - Has intrinsic computational content.

- I will deliberately not commit myself to any particular univalent type theory here.
- I will formulate the univalence axiom after we have developed enough material.

A spartan (intensional) Martin-Löf type theory

1. Base types $\mathbb{0}$, $\mathbb{1}$, $\mathbb{2}$, $\mathbb{N}$.
2. Cartesian products $A \times B$ and $\Pi(x : X), A(x)$.
3. Function types $X \to A$ also written A^X.
4. Sums $A + B$ and $\Sigma(x : X), A(x)$.
5. A large type $\mathcal{U}$ of small types (universe).

   Sometimes an extra large type $\mathcal{V}$ of large types.
6. An identity type $\mathsf{Id}_X(x, y)$ for any $X : \mathcal{U}$ and $x, y : X$.

Identity type discussion

1. The type $\mathsf{Id}_X(x, y)$ collects the ways in which the points $x, y : X$ are identified.
2. For some types the identity type can be defined from the other types.
3. E.g. for the type of natural numbers, it can be constructed by double induction:

$$\begin{array}{rcl} \mathsf{Id}_{\mathbb{N}}(0,0) & \equiv & \mathbb{1}, \\ \mathsf{Id}_{\mathbb{N}}(0,n+1) & \equiv & \mathbb{0}, \\ \mathsf{Id}_{\mathbb{N}}(m+1,0) & \equiv & \mathbb{0}, \\ \mathsf{Id}_{\mathbb{N}}(m+1,n+1) & \equiv & \mathsf{Id}_{\mathbb{N}}(m,n). \end{array}$$

4. In this example, $\mathsf{Id}_X(x, y)$ is always a subsingleton.
5. In general, there may be more identifications of x and y in the identity type.
6. We often write $x =_X y$ or simply $x = y$ to denote $\mathsf{Id}_X(x, y)$.
7. We write $\equiv$ for definitions.

Universe discussion

- We assume a large type $\mathcal{U}$ whose elements are small types.
- This has many uses, e.g.:

1. Define type families as functions $X \to \mathcal{U}$, for example by induction if X is the type of natural numbers.

   (Like in the previous slide.)

2. Define the type of groups:

   $$Group \equiv \Sigma(G : \mathcal{U}), \mathrm{isSet}(G) \times \Sigma(\cdot : G \times G \to G), \Sigma(e : G), (\Pi(x : G), x \cdot e = x) \times \cdots$$

   Define the type of categories. Or of topological spaces. Etc.

Two kinds of type-theoretic logic

- Curry–Howard logic.
  1. Propositions are types.
  2. Proofs are elements of types.

- Univalent logic.
  1. Propositions are subsingleton types. (As in topos logic.)
  2. Proofs are again elements of types.

- Both are constructive by default.

- But we can consistently postulate excluded middle and choice if we wish.
  (At the expense of losing implicit computational content.)

Curry–Howard propositional logic

Given two propositions (that is, types) A and B, we define

1. Conjunction. $A \wedge B \equiv A \times B$.

   "A proof of $A \wedge B$ is a pair (a, b) consisting of a proof a of A and a proof b of B."

2. Disjunction. $A \vee B \equiv A + B$.

   "A proof of $A \vee B$ is either a proof of A or a proof of B."

3. Implication. $A \to B$ is the function space, which has the same notation.

   "A proof of $A \to B$ transforms any proof of A into a proof of B."

4. Negation $\neg A \equiv A \to \mathbb{0}$.

Curry–Howard quantifiers

Given a family A of propositions (that is, types) indexed by a type X, we have:

1. Universal quantification: $\forall(x : X), A(x) \equiv \Pi(x : X), A(x)$.

   "A proof of $\forall(x : X), A(x)$ is a function that gives a proof of $A(x)$ for any given $x : X$."

2. Existential quantification: $\exists(x : X), A(x) \equiv \Sigma(x : X), A(x)$.

   "A proof of $\exists(x : X), A(x)$ is a pair (x, a) consisting of a witness $x : X$ and a proof a of $A(x)$."

Curry–Howard logic

false	$\bot$	$\mathbb{0}$	empty type
true	$\top$		any type for which a point can be exhibited
and	$\wedge$	$\times$	cartesian product of two types
or	$\vee$	$+$	disjoint sum of two types
implies	$\to$	$\to$	function space
for all	$\forall$	Π	product of a type family
for some	$\exists$	Σ	disjoint sum of a type family
equals	$=$	Id	identity type

Martin-Löf introduced the identity type precisely to extend Curry-Howard logic with equality.

Example: there are infinitely many prime numbers

$$f : \Pi(n : \mathbb{N}), \Sigma(p : \mathbb{N}), (p > n) \times \mathrm{isPrime}(p).$$

1. A point of this type is a function f that for any $n : \mathbb{N}$ gives a prime $p > n$.
2. The type $n > p$ can be defined by induction on n and p like we defined the identity type $m = n$.

   Or in many other equivalent ways, e.g. $(n > p) \equiv \Sigma(k : \mathbb{N}), p + k + 1 = n$, after we have defined addition by induction.
3. After we define multiplication by induction, we define $\mathrm{isPrime}(p)$ in the usual way.

A lot of mathematics can be formulated and proved in this way.

Preparation: Univalence gives function extensionality (funext)

Pointwise equal functions are equal:

$$\Pi(X:\mathcal{U}),\Pi(A:X\to\mathcal{U}),\Pi(f,g:\Pi(x:X),A(x)),(\Pi(x:X),f(x)=g(x))\to f=g.$$

- Something we don't have in intensional Martin-Löf type theories.
- We don't have univalence yet, so we assume funext when needed, for the moment.

Univalent propositions

Or *propositions*, for short, also known as *h-propositions* or *mere propositions*.

(But "mere" is too derrogatory for my taste, and "h-" is strange.)

1. A type X is a proposition if any two of its elements are equal:

   $$\mathrm{isProp}(X) \equiv \Pi(x, y : X), x = y.$$

   $\mathrm{Prop} \equiv \Sigma(P : \mathcal{U}), \mathrm{isProp}(P)$.

   We also say that X is a subsingleton.

2. We have $\mathrm{funext} \to \mathrm{isProp}(\mathrm{isProp}(X))$.

   Being a proposition is itself a proposition.

3. Assuming *funext*, also any two maps into the same proposition are equal.

Example of a non-trivial type that is a univalent proposition

$$\Sigma(n : \mathbb{N}), \mathrm{isPrime}(n) \times (\text{n is the difference of two squares of primes}).$$

1. Although propositions are subsingletons, they are not necessarily "proof-irrelevant".
   - They have information content.
   - The number 5 can be extracted from any proof of this proposition.
2. But for the above type to really be a proposition, we additionally need:
   - propositional extensionality (any two logically equivalent propositions are equal).
   - Which is not provable in MLTT, but follows from univalence, like funext.

A subtler example (the mystery of MLTT's identity type)

Although the type $x = y$ need not be a subsingleton for $x, y : X$, the type

$$\Sigma(x : X), x = y$$

is always a subsingleton for any $y : Y$, and in fact even a singleton (or contractible):

$$\text{isSingleton}(A) \equiv \Sigma(a_0 : A), \Pi(a : A), a = a_0.$$

This doesn't require propositional or function extensionality, or anything beyond MLTT.

Theorem of MLTT. $\Pi(y : X), \text{isSingleton}(\Sigma(x : X), x = y)$.

Non-Theorem of MLTT. ~~$\Pi(x, y : X), \text{isSubsingleton}(x = y)$~~.

An even subtler, crucial example (Voevodsky)

Let $f : X \to Y$ be a function of two types X and Y.

1. The type

$$\text{isIsomorphism}(f) \equiv \Sigma(g : Y \to X), (g \circ f = \text{id}_X) \times (f \circ g = \text{id}_Y)$$

   need not be a proposition.

   Because of the potential presence, in MLTT, of higher-dimensional types.

2. However, the type

$$\text{isEquivalence}(f) \equiv \Pi(y : Y), \text{isSingleton}(\Sigma(x : X), f(x) = y)$$

   always is a proposition, assuming functional extensionality.

   (The latter is a **retract** of the former.)

A formulation of the univalence axiom, and consequences

1. $X \simeq Y \equiv \Sigma(f : X \to Y), \text{isEquivalence}(f)$.
2. $\text{UA} \equiv \Pi(X : \mathcal{U}), \text{isSingleton}(\Sigma(Y : \mathcal{U}), X \simeq Y)$.

   Not the original formulation of UA by Voevodsky.

   Chosen here because it requires a minimal amount of machinery to be formulated.

- Theorem of MLTT (Voevodsky). The type UA is a proposition.
- Metatheorem (Voevodsky). UA is consistent with MLTT. (Simplicial set model.)
- Theorem of MLTT+UA. $P(X)$ and $X \simeq Y$ imply $P(Y)$ for any $P : \mathcal{U} \to \mathcal{U}$.
- Theorem of spartan MLTT with two universes. The univalence axiom formulated with crude isomorphism rather than equivalence is false.

Logical consequences of univalence

- Functional and propositional extensionality.

  Which we already needed.

  Univalence is a generalized extensionality axiom for intensional MLTT.

Another example of when Curry–Howard goes wrong: image

Define the image of a function $f : X \to Y$ in the usual way, translated to Curry-Howard:

$$\text{image}\, f \equiv \Sigma(y : Y), \Sigma(x : X), f(x) = y.$$

- This is the type of points $y : Y$ for which we have some $x : X$ with $f(x) = y$.
- Trouble: $\text{image}\, f \simeq X$.

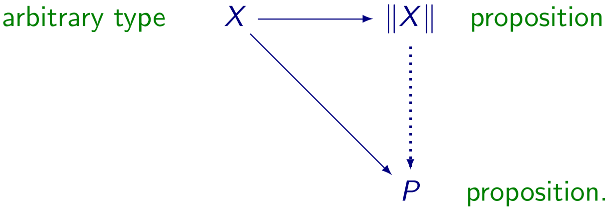
  This is not what we expect.
- Example. We don't expect the image of the unique function $\mathbb{2} \to \mathbb{1}$ to be isomorphic to $\mathbb{2}$.

  We expect the image to be a subtype of $\mathbb{1}$.

Univalent logic fixes such things in the same way as topos logic.

Propositional truncation (or reflection)

1. A propositional truncation of a type X, if it exists, is the universal solution to the problem of mapping X to a proposition:



   $\|X\|$ is required to be the smallest proposition X maps into.

2. Several kinds of types can be shown to have truncations in MLTT.

3. There are a number of ways to extend MLTT to get truncations for *all* types.
   (Such as resizing + funext, or higher inductive types.)

Theorem (impredicative characterization of propositional truncation)

(Independently of how it is defined concretely, from the universal property alone.)

$$\underbrace{\|X\|}_{\text{small type}} \iff \underbrace{\Pi(P : \mathcal{U}), \mathsf{isProp}(P) \to (X \to P) \to P}_{\text{large type}}$$

Moreover, the rhs is a proposition assuming funext.

Univalent logic

Like Curry-Howard logic, with two differences only:

- $A \vee B \equiv \|A + B\|$.
- $\exists(x : X), A(x) \equiv \|\Sigma(x : X), A(x)\|$.

This turns out to give exactly the same disjunction and existence as topos logic and higher order intuitionistic logic.

In Cubical type theory, they satisfy the disjunction and existence properties (Huber).

(Like in the free topos.)

Example concluded: univalent image

The image of a function $f : X \to Y$ is

$$\text{image}\, f \equiv \Sigma(y : Y), \|\Sigma(x : X), f(x) = y\|.$$

Theorem (impredicative characterization of univalent logic)

We get the usual intuitionistic higher-order logic, which reduces everything to *implication* $\to$ and *universal quantification* Π:

- $\bot \iff \Pi(R : Prop), R.$
- $P \wedge Q \iff \Pi(R : \mathrm{Prop}), (P \to Q \to R) \to R.$
- $P \vee Q \iff \Pi(R : \mathrm{Prop}), (P \to R) \to (Q \to R) \to R.$
- $\exists(x : X), P(x) \iff \Pi(R : \mathrm{Prop}), (\Pi(x : X), P(x) \to R) \to R.$
- $\|x = y\| \iff \Pi(P : X \to \mathrm{Prop}), P(x) \to P(y).$ (Leibniz principle.)

(Again, the lhs types are small and the rhs types are large.)

Curry–Howard "excluded middle"

Theorem of MLTT+$\| - \|$. The following are logically equivalent:

1. $\Pi(X : \mathcal{U}), X + \neg X$.
2. $\Pi(X : \mathcal{U}), \neg\neg X \to X$.
3. $\Pi(X : \mathcal{U}), \|X\| \to X$.
4. $\Pi(X : \mathcal{U}), \Sigma(f : X \to X), \Pi(x, y : X), f(x) = f(y)$.

- This is more like global choice than excluded middle.

  We can pick a point of every non-empty type.
- It implies that all types are sets, making univalent type theory trivial.
- False in the presence of two univalent universes.

Univalent excluded middle

The following are equivalent:

1. $\Pi(P : \mathcal{U}), \text{isProp}(P) \to P + \neg P$.
2. $\Pi(P : \mathcal{U}), \text{isProp}(P) \to \neg\neg P \to P$.

They imply $\Pi(X : \mathcal{U}), \|X\| \iff \neg\neg X$.

Which is consistent with univalent type theory.

Myth: propositional truncation erases information

It doesn't. E.g.:

Theorem of MLTT+$\|-\|$. For any $f : \mathbb{N} \to \mathbb{N}$,

$$\|\Sigma(n : \mathbb{N}), f(n) = 0\| \to \Sigma(n : \mathbb{N}), f(n) = 0.$$

If there is a root of f, we can find one.

Correct formulation of unique existence

- Not $(\Sigma(x : X), A(x)) \times (\Pi(x, y : X), A(x) \times A(y) \to x = y)$.
- Instead $\mathrm{isSingleton}(\Sigma(x : X), A(x))$.

  Especially when formulating universal properties.
- A unique $x : X$ such that $A(x)$ is not enough.
- What is really needed is a unique *pair* (x, a) with $x : X$ and $a : A(x)$.

  Like in category theory again.

  Unless all types are sets.

Choice just holds in Curry–Howard logic

Let $X, Y : \mathcal{U}$ be types and $R : X \times Y \to \mathcal{U}$ be a relation.

$$(\Pi(x : X), \Sigma(y : Y), R(x, y)) \to \Sigma(f : X \to Y), \Pi(x : X), R(x, f(x)).$$

Moreover, the implication can be strengthened to a type equivalence.

However, univalent choice implies univalent excluded middle

$$(\Pi(x : X), \|\Sigma(y : Y(x)), R(x, y)\|) \to \|\Sigma(f : \Pi(x : X), Y(x)), \Pi(x : X), R(x, f(x))\|.$$

The assumptions are that $\mathrm{isSet}\, X$ and $\mathrm{isSet}\, Y(x)$ for all $x : X$, and we are given $R : (\Sigma(x : X), Y(x)) \to \mathrm{Prop}$.

This form of choice is consistent with univalent type theory.

But we do get unique choice

“Moral”

1. Σ is used to express given structure or data in general.

   Cf. the type of groups.

2. Truncated Σ is used to express existence. (Still constructive.)

   - But, even better, in practice, one is encouraged to use Σ so that it produces univalent propositions without the need of truncation (if we can).
   - A crucial example is Voevodsky’s primary notion of equivalence.

     (But we have seen additional examples.)

3. At the moment, it seems to be an art to decide whether particular mathematical statements should be formulated as giving structure/data or propositions.

4. But the main point is that our mathematical language allows the distinction.

   (A distinction that is obliterated by the axiom of choice.)