Homotopy Type Theory

Benno van den Berg

LoLaCo, 29 September 2014

What is homotopy type theory?

It introduces ideas from

HOMOTOPY THEORY

in

TYPE THEORY.

What is homotopy theory?

What is homotopy theory?

Homotopy is a branch of algebraic topology, so here we need to draw pictures and turn to the blackboard.

What is type theory?

What is type theory?

- It is a foundation for constructive mathematics.
- It is a functional programming language.
- It is the basis for proof assistants like Coq, Agda,. . .

I will mainly talk about the first aspect.

What is a constructive proof?

Theorem (Euclid)

There are infinitely many prime numbers.

Proof.

First of all, 2 is prime. Now suppose $p_1, \ldots, p_n$ is a list of prime numbers. Consider $u = p_1 \ldots p_n + 1$ and let v be the smallest divisor of u bigger than 1. Then v is prime and different from all p_i. □

Theorem

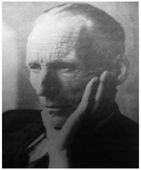
Either $e + \pi$ or $e - \pi$ is irrational.

Proof.

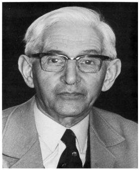
Suppose both $e + \pi$ and $e - \pi$ are rational. Then also $(e + \pi) + (e - \pi) = 2e$ is rational. Contradiction! □

Brouwer

Brouwer: No ineffective proofs!



In 1908 he realized that this means logic has to be revised (he wrote a paper "Over de onbetrouwbaarheid der logische principes"). He objected in particular to the Law of Excluded Middle ($\varphi \vee \neg\varphi$).



Heyting: constructive (or intuitionistic) logic.

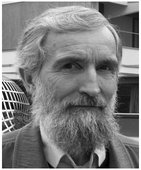
Customary foundation of mathematics

ZFC: Zermelo-Fraenkel set theory with the axiom of choice.

- Classical logic.
- Extensionality.
- Pairing.
- Union.
- Separation.
- Foundation.
- Infinity.
- Powerset.
- Replacement.
- Choice.

Martin-Löf Type theory

Type theory as an alternative foundation for constructive mathematics:



- There are *terms* and *types* and every term has a specific type ($t\colon A$).
- One may write $s = t$, but only if s and t have the same type ($s = t\colon A$).
- One can have parametrised (dependent) types $B(a)$, with $a\colon A$.
- Every type in inductively generated.

General shape of a judgement

$$\begin{array}{l}\Gamma \vdash B(x_0, \ldots, x_n)\,\mathrm{Type} \\ \Gamma \vdash B(x_0, \ldots, x_n) = C(x_0, \ldots, x_n) \\ \Gamma \vdash a(x_0, \ldots, x_n) \colon B(x_0, \ldots, x_n) \\ \Gamma \vdash a(x_0, \ldots, x_n) = b(x_0, \ldots, x_n) \colon B(x_0, \ldots, x_n)\end{array}$$

where

$$\Gamma = x_0 \colon A_0, x_1 \colon A_1(x_0), \ldots, x_n \colon A_n(x_0, \ldots, x_{n-1}),$$

is a context.

An example

Formation $\dfrac{}{\vdash \mathbb{N}\ \mathsf{Type}}$

Introduction $\dfrac{}{\vdash 0 \colon \mathbb{N}} \qquad \dfrac{\vdash n \colon \mathbb{N}}{\vdash s(n) \colon \mathbb{N}}$

Elimination
$$\frac{\begin{array}{c} n \colon \mathbb{N} \vdash P(n)\ \mathsf{Type} \\ \vdash c \colon P(0) \\ n \colon \mathbb{N}, x \colon P(n) \vdash g(x, n) \colon P(s(n)) \end{array}}{n \colon \mathbb{N} \vdash \mathsf{rec}(c, g, n) \colon P(n)}$$

Computation
$$\mathsf{rec}(c, g, 0) = c \colon P(0)$$
$$\mathsf{rec}(c, g, s(n)) = g(\mathsf{rec}(c, g, n), n) \colon P(s(n))$$

Another example

Formation $$\frac{A\ \mathsf{Type} \quad B\ \mathsf{Type}}{A \times B\ \mathsf{Type}}$$

Introduction $$\frac{\vdash a\colon A \quad \vdash b\colon B}{\vdash p(a,b)\colon A \times B}$$

Elimination $$\frac{\begin{array}{c} x\colon A \times B \vdash P(x)\ \mathsf{Type} \\ a\colon A, b\colon B \vdash f(a,b)\colon P(p(a,b)) \end{array}}{x\colon A \times B \vdash \mathsf{prodrec}(f,x)\colon P(x)}$$

Computation $$\mathsf{prodrec}(f, p(a,b)) = f(a,b)\colon P(p(a,b))$$

Yet another example

Formation
$$\frac{A\ \mathsf{Type} \quad B\ \mathsf{Type}}{A + B\ \mathsf{Type}}$$

Introduction
$$\frac{\vdash a \colon A}{\mathsf{inl}(a) \colon A + B} \qquad \frac{\vdash b \colon B}{\mathsf{inr}(b) \colon A + B}$$

Elimination
$$\frac{\begin{array}{c} x \colon A + B \vdash P(x)\ \mathsf{Type} \\ a \colon A \vdash f(a) \colon P(\mathsf{inl}(a)) \\ b \colon B \vdash g(b) \colon P(\mathsf{inr}(b)) \end{array}}{x \colon A + B \vdash \mathsf{sumrec}(f, g, x) \colon P(x)}$$

Computation
$$\mathsf{sumrec}(f, g, \mathsf{inl}(a)) = f(a) \colon P(\mathsf{inl}(a))$$
$$\mathsf{sumrec}(f, g, \mathsf{inr}(b)) = g(b) \colon P(\mathsf{inr}(b))$$

Where is logic?

According to Per Martin-Löf we already did logic! How is that possible?

- Proof-theoretic semantics: The meaning of a proposition is given by what counts as a proof of that proposition.
- In fact, we might as well identify a proposition with the collection/set/type of its proofs ("propositions as types").
- BHK-interpretation: A proof of $A \wedge B$ consists of a proof of A and a proof of B, a proof of $A \vee B$ consists either of a proof of A or a proof of B, ...
- So $A \times B$ is also conjunction and $A + B$ is also disjunction!

Towards an identity type

- There should also be a propositional equality, that is, a type $\mathrm{Id}_A(a, b)$ of proofs of the equality of a and b.
- Of course, it has to be inductively generated and the rules for it should conform to the general pattern.
- Idea: *equality is the least reflexive relation*.

Rules for the identity type

Formation $\dfrac{\vdash x\colon A, y\colon A}{\vdash \mathsf{Id}_A(x,y)\ \mathsf{Type}}$

Introduction $\dfrac{\vdash a\colon A}{\vdash r(a)\colon \mathsf{Id}_A(a,a)}$

Elimination $\dfrac{\begin{array}{l} x\colon A, y\colon A, z\colon \mathsf{Id}_A(x,y) \vdash C(x,y,z)\ \mathsf{Type} \\ x\colon A \vdash d(x)\colon C(x,x,r(x)) \end{array}}{x\colon A, y\colon A, z\colon \mathsf{Id}_A(x,y) \vdash J(x,y,z,d)\colon C(x,y,z)}$

Computation $J(x,x,r(x),d) = d(x)$

Not so easy

To complicate matters, the identity types can be nested:

$$\alpha\colon Id_{Id_A(x,y)}(f, g)$$

So there are proofs of the equality of certain equality proofs, and proofs of the equality of those, et cetera!

Quote from E. Cunningham

Professor Whitehead writes in his last book that if we begin to ask ourselves the meaning of the simple word "equal" we find ourselves plunged into abstruse modern speculations concerning the character of the universe.

Structure

Hoffmann and Streicher showed that every identity types $\mathsf{Id}_A(x, y)$ gives A the structure of a *groupoid*. Not strictly, but up to higher equality proofs.

Theorem (Lumsdaine, Garner, BvdB)

The identity types gives every type the structure of a (weak) ∞-groupoid.

New ideas from homotopy theory

- Simplicial model of type theory in which types are ∞-groupoids.
- Voevodsky's univalence axiom.
- Higher inductive types.
- Synthetic homotopy theory.
- New semantics.
- New (univalent) foundations of mathematics?

Main open question: computational meaning?

Some suggestions for further reading

- Per Martin-Löf – *Intuitionistic type theory*, Bibliopolis 1984.
- Bengt Nordstroem, Kent Petersson and Jan M. Smith – *Programming in Martin-Löf's type theory*. Oxford University Press, 1990.
- The Univalent Foundations Program – *Homotopy type theory: univalent foundations of mathematics*. Institute of Advanced Studies, 2013.

All these texts are freely available on-line. And, as this is 2014, there is a google group and a "Homotopy type theory" homepage. Also check out Michael Shulman's posts at the n-category cafe.