Univalent Type Theory

Thierry Coquand

Logic in Computer Science, Oxford, July 2018

Plan of the talk

First part: try to explain how issues of

modularisation of proofs/programs

might have to do with

homotopy theory

Second part: survey of recent results on constructive presheaf semantics of the univalence axiom

Close to what will appear in the semantic column of the SIGLOG Newsletter issue, July 2018

Collections and identifications

Any formalism for representing mathematical reasoning should address the questions of

collections and *identifications*

of mathematical objects

Equality of objects has an intuitive meaning

Question: when should we *identify* two *collections* of mathematical objects?

Collections and identifications

What are the logical laws of the notion of identifications

This should be closely connected to/generalize the laws of *equality*

Leibniz's law *identity of indiscernibles*

Discours de métaphysique Section 9, 1686

Two *new* Laws

-P. Martin-Löf (1973)

-Voevdosky (2006) univalence axiom, strong form of extensionality principle

Algebraic and ordered structures

Basic examples of collections: algebraic and ordered structures

E.g. groups, rings, lattices

Set equipped with some operations and/or relations satisfying some properties

Mathematical abstraction: to realize that two isomorphic structures can be considered to be the "same"

What matters is the *structure* and not the nature of the elements

Algebraic and ordered structures

This is the level considered by Bourbaki in his *théorie des structures*

Very useful for *modularisation*

Any abstract reasoning for groups can be applied in different concrete situations

Cf. *Types, abstraction and parametric polymorphism*, J.R. Reynolds and works of Morris, Liskove and Zilles, ... on the importance of

representation independence results

for modular development of programs

Algebraic and ordered structures

To realize that two structures are isomorphic can be a key mathematical step

One can transfer intuitions from one field to another

One can solve a problem by transforming it to another one which is isomorphic

Example: Galois correspondance normal subfields/normal subgroups

Description of mathematical objects

Two isomorphic groups G and H satisfy the same “structural “ properties

If G is abelian, so is H

If G is solvable, so is H

But we can have $0 \in G$ and $0 \notin H$

Transportable properties (Bourbaki)

“When two relations have the same structure, their logical properties are identical, except such as depend upon the membership of their fields”

Russell (1959) *My philosophical development*

Description of mathematical objects

Bourbaki has a characterisation of transportable properties for his notion of structure

Voevodsky's guiding principle for the design of a formal system for mathematics

It should be impossible to formulate a statement which is not invariant with respect to isomorphisms/equivalences

Strong form of extensionality/modularity principle

Identification

This notion of identification has recently be generalized in mathematics

Next level: collection of all groups, or all sets (in a fixed universe)

When are two such collections considered to be the "same"?

Let B be a given set

For a mathematician the two collections SET^B and SET/B are "identical"

They satisfy the same "structural"/transportables properties

SET^B contains families of sets $X_b,\ b \in B$

SET/B contains "sets over B", i.e. $Y, f : Y \to B$, functions of codomain B

Identification

We have two canonical maps $F : \mathsf{SET}^B \rightarrow \mathsf{SET}/B$ and $G : \mathsf{SET}/B \rightarrow \mathsf{SET}^B$

$F(X) = \Sigma(b : B)X_b, \pi_1$

$G(Y, f) = (f^{-1}(b))_{b \in X}$

$G(F(X))$ and X are only isomorphic (and not equal as sets in general)

$G(F(X))_b = \{b\} \times X_b$

The two collections (groupoids) SET^B and SET/B are *equivalent*

F and G do *not* define an isomorphism

Equivalence as identification

We get a *new* way to identify collections

Another example: the collection $\mathbb{L}_{27}$ of all linear orders with 27 elements

This is a large collection; in set theory, it forms a class and not a set

We have an *identification* to the groupoid with one object and one morphism

$$\mathbb{L}_n \simeq 1$$

Equivalence as identification

In *computer algebra* such equivalences are used for computations

Equivalence between the category of coherent sheaves over projective space $\mathbb{P}^n$ and Serre quotient of the category of graded modules over $k[X_0, \ldots, X_n]$

System CAP (Categories, Algorithms, Programming), developped by M. Barakat

Based on constructive category theory

Some double exponential computation can be replaced by a polynomial computation with a transport via an equivalence

Description of mathematical objects

At the next level we have 2-*groupoids*

We have new laws of identification

Vertical and horizontal compositions, with the exchange law

Then n-groupoids, then ∞-groupoids

More and more complex notions of equivalences

Indeed these laws are connected to the higher homotopy groups of spheres which are very mysterious objects; e.g. the fact that the exchange law is not strict is connected to the equality $\pi_3(S^2) = \mathbb{Z}$

Description of mathematical objects

Less and less clear when a property is transportable along equivalences

The notion of equivalence should generalize the notion of isomorphism

Can one describe what is a general notion of equivalence?

What is surprising is that it can be done in an uniform way

Two *new* laws for equality (Martin-Löf 1973, Voevodsky 2006)

Laws of identifications

There may be several possible identifications between two collections

E.g. two isomorphic structures

So we should have a collection of identifications Id A a_0 a_1 which may have more than one element

Collections of structures form a *groupoid*

Id A a_0 a_1 has itself a notion of identification

Some Laws of identifications

We have an identification 1_a in $\mathsf{Id}\ A\ a\ a$

Given $\alpha : \mathsf{Id}\ A\ a_0\ a_1$ and $P(x)$ a family of collections for x in A

We can use α to build a transport function $P(a_0) \rightarrow P(a_1)$

Some Laws of identifications

$1_a : \mathsf{Id}\ A\ a\ a$

$\mathsf{transp} : \mathsf{Id}\ A\ a_0\ a_1 \to P(a_0) \to P(a_1)$

Dependent Type Theory

The language of *dependent* type theory is well suited for expressing these laws

We want to express that we have transport, not only for properties but also for structures

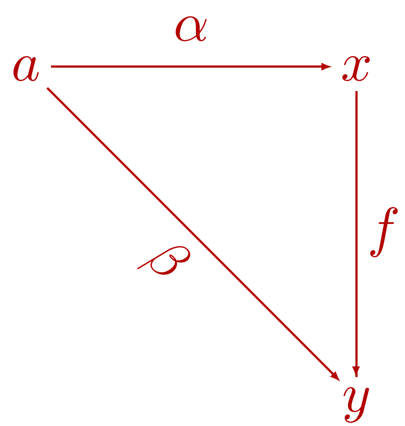
E.g. A collection of sets and $P(a)$ is the collection of group structures on a

$\mathsf{Id}\ A\ a\ b \rightarrow P(a) \rightarrow P(b)$ expresses the notion of *transport of structure*

A New Law of identifications

Given a in A we can form the groupoid $\Sigma(x : A)\mathsf{Id}\ A\ a\ x$

Element x, α and maps $f : (x, \alpha) \simeq (y, \beta)$ if $f : x \simeq y$ and $f\alpha = \beta$



A New Law of identifications

So the groupoid $S = \Sigma(x : A)\mathsf{Id}\ A\ a\ x$ is always *trivial*

$\Pi(x : A)\Pi(\omega : \mathsf{Id}\ A\ a\ x)\ \mathsf{Id}\ S\ (a, 1_a)\ (x, \omega)$

where $S = \Sigma(x : A)\mathsf{Id}\ A\ a\ x$

This is a *law* of identification, like reflexivity and composition of identifications

The type theoretic formulation

$\Pi(x : A)\Pi(\omega : \mathsf{Id}\ A\ a\ x)\ \mathsf{Id}\ S\ (a, 1_a)\ (x, \omega)$

generalizes the law for groupoids that $\Sigma(x : A)\mathsf{Id}\ A\ a\ x$ is trivial (exactly one morphism between two objects)

A New Law of identifications

Martin-Löf introduced this law for purely formal reasons

Systematic way of expressing elimination rules with dependent types

This law/principle has a *lot* of consequences

E.g. one can show from it the groupoid laws for composition of identifications

This was noticed by M. Hofmann and Th. Streicher around 91

It was first formulated by P. Martin-Löf 1973

In another context, it was also formulated by J.P. Serre's thesis 1951

Stratification

Stratify collections following the complexity of their notion of identification

A collection is a *set* if each identification has at most one element

A collection is a *groupoid* if each identification is a set

A collection is a *proposition* if each identification has exactly one element (subsingleton)

Equivalence

It is possible to formulate *uniformly* the notion of equivalence

A map $f : A \to B$ is an equivalence whenever each fiber $\Sigma(x : A)\mathsf{Id}\ B\ (f\ x)\ y$ has exactly one element

This captures uniformly the notion of logical equivalence, of bijection between sets, of categorical equivalence between groupoids, $\ldots$

This can be formulated as

$$\mathsf{isEquiv}\ f \ = \ \Pi(y : B)\mathsf{isContr}(\Sigma(x : A)\mathsf{Id}\ B\ (f\ x)\ y)$$

$$\mathsf{isContr}\ T \ = \ \Sigma(u : T)\Pi(v : T)\mathsf{Id}\ T\ u\ v$$

Equivalence

Surprising that one can capture in such a simple way the notion of equivalence

This illustrates how well suited is the formalism of dependent types

This was discovered by Voevodsky 2009, who furthermore formalised all arguments in a proof assistant based on dependent type theory

Univalence states that the canonical map

$\mathsf{Id}\ U\ A\ B \rightarrow \mathsf{Equiv}\ A\ B$

is an equivalence

The Laws of Identifications

$1_a : \mathsf{Id}\ A\ a\ a$

$\mathsf{transp} : \mathsf{Id}\ A\ a_0\ a_1 \to P(a_0) \to P(a_1)$

$\Sigma(x : A)\mathsf{Id}\ A\ a\ x$ has exactly one element $(a, 1_a)$

$\mathsf{Equiv}\ (\mathsf{Id}\ U\ A\ B)\ (\mathsf{Equiv}\ A\ B)$

Homotopy types/groupoids versus categories

One of the things that made the "categories" versus "groupoids" choice so difficult for me is that I remember it being emphasized by people I learned mathematics from that the great Grothendieck in his wisdom broke with the old-schoolers and insisted on the importance of considering all morphisms and not only isomorphisms and that this was one of the things that made his approach to algebraic geometry so successful.

It was overcoming the appeal of category theory as a candidate for new foundation of mathematics that was for me personally most difficult.

Homotopy types/groupoids versus categories

The successes of category theory inspired the idea that categories are "sets in the next dimension" and that the foundation of mathematics should be based on category theory or on its higher dimensional analogs.

It is the idea that categories are "sets in the next dimension" that was the most difficult roadblock for me. I clearly recall the feeling of a breakthrough, which I experienced when I understood that this idea is wrong. Categories are not "sets in the next dimension". They are "partially ordered sets in the next dimension," and "sets in the next dimension" are groupoids.

Semantics?

Voevodsky extended the formalism of dependent type theory with these laws for identifications

He could check that this gives a proper basis to express mathematical notions

Really unexpected that the axioms are so formally simple

See *Notes on homotopy* λ*-calculus*, March 2006

Notes for a talk at Standford (available at V. Voevodsky gitub repository)

Is this a *consistent* system?

Models?

Semantics?

"the intuition appeared that ∞-groupoids should constitute particularly adequate models for homotopy types, the n-groupoids corresponding to truncated homotopy types (with $\pi_i = 0$ for $i > n$)"

Grothendieck, *Sketch of a program*, 1984

A given ∞-groupoid should be considered to be a "space up to homotopy"

The idea of Voevodsky was to use this connection in the *reverse* direction

We represent a collection as a homotopy type

Semantics?

There exists in mathematics a “combinatorial” way to represent homotopy types, due to Kan 1958, as so-called Kan simplicial sets

Voevodsky could use this representation and show that these Kan simplicial sets form a model of dependent type theory

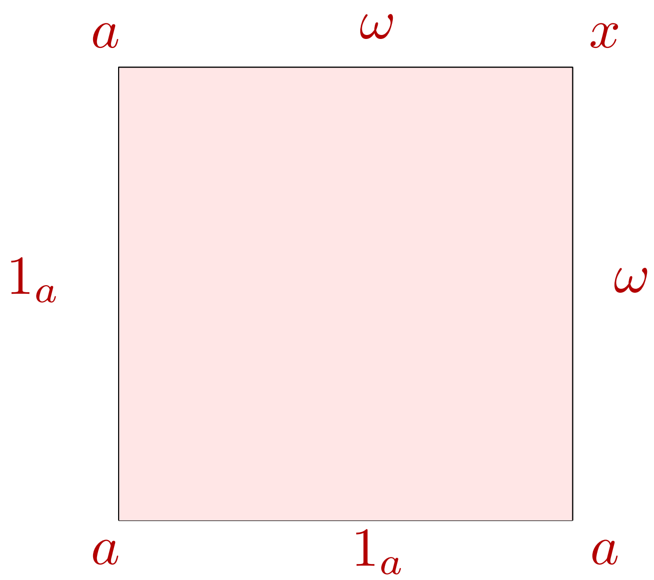
Furthermore this model satisfies the univalence axiom

Semantics?

Intuitively, one can think of a collection as a space

An identification between two elements of this collection is like a *path*

Singleton types are contractible



Any element (x, ω) in the type $\Sigma(x : A)\mathsf{Id}\ A\ a\ x$ is equal to $(a, 1_a)$

Loop space

Indeed, to apply Leray's theory I needed to construct fibre spaces which did not exist if one used the standard definition. Namely, for every space A, *I needed a fibre space* E *with base* A *and with trivial homotopy (for instance contractible). But how to get such a space? One night in 1950, on the train bringing me back from our summer vacation, I saw it in a flash: just take for* E *the space of paths on* A *(with fixed origin* a*), the projection* $E \to A$ *being the evaluation map: path* $\to$ *extremity of the path. The fibre is then the loop space of* (A, a). *I had no doubt: this was it!* ... It is strange that such a simple construction had so many consequences.

J.-P. Serre, describing the "loop space method" introduced in his thesis (1951)

Semantics?

Univalence holds in this model

See letter from Bousfield, May 1, 2006

Posted by D. Grayson, homotopy type theory newsgroup, 10/11/2017

Use *minimal* complexes, which are highy non canonical objects

Constructive presheaf models

Voevodsky's simplicial set model is quite sophisticated

Furthermore it uses intrinsically non effective principles

Also it requires ZFC together with a hierarchy of inaccessible cardinals which is a much stronger systems than dependent type theory with universes

Constructive presheaf models

What is the proof theoretic strength of the univalence axiom?

Can we justify this axiom in a constructive way?

These two questions have been recently completely elucidated

Furthermore all this is developped in a constructive framework

And most of it has been actually formalised in proof systems

Constructive presheaf models

I want to explain why the notion of *presheaf* model is relevant

The relevance of presheaf models for semantics is elegantly described in

D. Scott *Relating models of λ-calculus*, 1980

Uses some “vivid” terminology from Lawvere

Constructive presheaf models

These models can be seen as generalized *Kripke* models

The object $X, Y, \ldots$ in the base category are "stages"

A presheaf A is given by a collection of sets $A(X)$

$f : Y \rightarrow X$ gives us transititions between stages X and "later" stages Y

Each such transition "restricts" elements of $A(X)$ to elements of $A(Y)$ "along" the map f

The intuition is *temporal*

Constructive presheaf models

One early use of presheaves by Eilenberg and Zilber relies on a *spatial* intuition

The objects $X, Y, \ldots$ now represent basic "shapes"

A presheaf A is thought of as a collection of basic shapes $A(X)$ that are connected via transition maps

1950 Eilenberg and Zilber 1956 Beth 1958 Kripke

Constructive presheaf models

It turns out that all basic notions about presheaf semantics are naturally expressed in a constructive setting

M. Hofmann *Syntax and semantics of dependent type theory*, 1997

The internal language of presheaf models, presented in D. Scott 1980's paper, can be generalized to dependent types

Constructive presheaf models

Two parameters: a type $\mathbb{I}$ representing the unit interval

A property Cofib of so-called cofibrant propositions

Some axioms, listed in

Axioms for Modelling Cubical Type Theory in a Topos, 2017
I. Orton and A. Pitts.

E.g. the class of cofibrant propositions should define a dominance

Constructive presheaf models

Using $\mathbb{I}$ we define a notion of path

Using Cofib we define a notion of "good subpolyhedra"

E.g. $\forall(i : \mathbb{I})\mathsf{Cofib}(i = 0)$ expresses that the faces of a cube are cofibrant

Constructive presheaf models

We can then express a condition that was extracted by Eilenberg (1939) as a key property for homotopy theory

If A subpolyhedra of B

Proposition: *Given two homotopic functions* $f_0\ f_1 : A \rightarrow X$ *and an extension* $f_0' : B \rightarrow X$ *of* f_0 *there is an extension* f_1' *of* f_1 *homotopic to* f_0

Proofs of basic results about homotopy "can be obtained quite neatly by repeated, and sometimes tricky, use of this general lemma" (Bourbaki's notes on homotopy by Eilenberg, 1951)

Constructive presheaf models

We get a class of models of dependent type theory with an univalent universe

There is a technical condition on the interval

One axiom states that $\mathbb{I}$ has to be "tiny"

$X \mapsto X^{\mathbb{I}}$ has a right adjoint

This does *not* hold for the category Δ and the interval Δ^1

This is satisfied if the base category has finite products and $\mathbb{I}$ representable

Application 0: extension of dependent type theory

This is satisfied if the base category has finite products and $\mathbb{I}$ representable

E.g. the base category is the Lawvere theory of *distributive lattices*

One can then design a type theory based on this model, e.g.

Cubical Type Theory: a constructive interpretation of univalence
C. Cohen, Th. C., S. Huber, A. Mörtberg, 2015

Cf. Voevodsky's talk at the Big Proof Meeting, 2017, explaining the relevance of having a Lawvere theory for the base category

Canonicity results (S. Huber, 2016)

Application 1: consistency strength

The metatheory can be CZF extended with a hierarchy of universes as in

Aczel
On Relating Type Theory and Set Theory, 1998

or it can be NuPrl, as done formally by Bickford

In both cases, these systems are known to have the same proof theoretic strength as dependent type theory with Π, Σ, W and a hieararchy of universes

The axiom of univalence and propositional truncation does not add any proof theoretic strength to type theory

E.g. provably total functions $\mathbb{N} \to \mathbb{N}$ are the same

Application 2: impredicative universe

Uemuara
Cubical Assemblies and the Independence of the propositional resizing axiom 2018

We work in an *extensional* type theory with an impredicative universe

We get a model of type theory with a *univalent impredicative universe*

Awodey, Frey, Speight
Impredicative Encodings of (Higher) Inductive Types, LICS 2018

Application 3: consistency with uniform continuity

These models can be relativized in any presheaf topos

We can generalize the notion of Lawvere-Tierney topology

Rijke, Shulman, Spitters
Modalities in homotopy type theory, 2017

The objects modal for all these modalities form a model ("stack" model) of type theory with univalence

Application 4: countable choice

Similarly we can adapt the usual sheaf models to show that countable choice is not provable in type theory with univalence and propositional truncation

Application 5: model of higher inductive types

Elegant combination of ideas coming from computer science (data types, constructor) and homotopy theory

Characterisation of spheres, suspension via universal operations

Some potential applications to homotopy theory

A Generalized Blakers-Massey Theorem
M. Anel, G. Biedermann, E. Finster, A. Joyal, 2017

A model of this notion is described in

On Higher Inductive Types in Cubical Type Theory
Th. C., S. Huber, A. Mörtberg, LICS 2018

Questions/Summary

For the first part: do we get a good system for representing mathematics?

System *UniMath*, starting from Voevodsky's 2010 library with representations of abelian categories, triangulated categories

Voevodsky's library contains incredibly elegant proofs

Proofs by M. Escardo, e.g.
Injective types and searchable types in univalent mathematics
HoTT/Univalent Foundation workshop, 2018

Questions/Summary

For the second part: new kind of *nominal* computations

Extension of λ-calculus with dimensions/names

We compute higher-dimensional objects

Connections with the simplicial set model?

Recently we have just shown (j.w.w. C. Sattler) that homotopy groups of CW-complex are correctly represented for higher inductive types in the cubical set model based on distributive lattices

Questions/Summary

Intuitions coming from λ-calculus, semantics of programming languages and homotopy theory

Some references

Cisinski
Les préfaisceaux comme modèles des types d'homotopie 2006

Licata, Orton, Pitts, Spitters
Internal Universes in Models of Homotopy Type Theory 2018

Orton, Pitts
Axioms for Modelling Cubical Type Theory in a Topos 2017

Uemuara
Cubical Assemblies and the Independence of the propositional resizing axiom 2018

Some references

Awodey, Frey, Speight
Impredicative Encodings of (Higher) Inductive Types 2018

Cohen, C., Huber, Mörtberg
Cubical type theory: a constructive interpretation of the univalence axiom, 2015

C., Huber, Mörtberg
On higher inductive types in cubical type theory 2018

Angiuli, Brunerie, C. Favonia, Harper, Licata
Cartesian cubical type theory, 2017

Angiuli, Harper, Wilson
Computational Higher-Dimensional Type Theory, 2017

Some references

Aczel
On Relating Type Theory and Set Theory, 1998

Schreiber
Some thoughts on the future of modal homotopy type theory, 2015

Gambino, Sattler
The Frobenius Condition, Right Properness, and Uniform Fibrations, 2015

Sattler
The Equivalence Extension Property and Model Structures, 2017

Sattler
Idempotent completion of cubes in posets, 2018

Some references

Kapulkin, Voevodsky
Cubical approach to straightening, 2018

Swan
An Algebraic Weak Factorisation System on 01-Substitution Sets: A Constructive Proof, 2016