Voevodsky's Univalent Foundation of Mathematics

Thierry Coquand

Bonn, May 15, 2018

Univalent Foundations

Voevodsky's program to express mathematics in

type theory

instead of

set theory

Univalent Foundations

Voevodsky "had a special talent for bringing techniques from homotopy theory to bear on concrete problems in other fields"

1996: proof of the Milnor Conjecture

2011: proof of the Bloch-Kato conjecture

He founded the field of motivic homotopy theory

In memoriam: Vladimir Voevodsky (1966-2017) Dan Grayson (BSL, to appear)

Univalent Foundations

What does "univalent" mean?

Russian word used as a translation of "faithful"

"These foundations seem to be faithful to the way in which I think about mathematical objects in my head"

(from a Talk at IHP, Paris 2014)

Univalent foundations

Started in 2002 to look into formalization of mathematics

Notes on homotopy λ-calculus, March 2006

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

Univalent Foundations

«nowadays it is known to be possible, logically speaking, to derive practically the whole of known mathematics from a single source, the Theory of Sets . . . By so doing we do not claim to legislate for all time. It may happen at some future date that mathematicians will agree to use modes of reasoning which cannot be formalized in the language described here; according to some, the recent evolutation of axiomatic homology theory would be a sign that this date is not so far. It would then be necessary, if not to change the language completely, at least to enlarge its rules of syntax. But this is for the future to decide.»

Bourbaki, Introduction of Theory of Sets

Dependent type theory

Any formal system for mathematics should address the two questions

-representation of the notion of *functions* and of *collections* of mathematical objects: algebraic, ordered mathematical structures (Bourbaki), then collections of such structures (categories), then collections of such collections (2-categories), and so on . . .

-laws of *identification* of mathematical objects

Description of mathematical objects

First level: algebraic structure, ordered structure

E.g. groups, rings, lattices

Set with operations and/or relations satisfying some properties

Uniqueness up to isomorphisms

It is the level considered by Bourbaki in his *theory of structures*

Description of mathematical objects

The next level is usually described as the level of *categories*

Actually the next level is the level of *groupoid with structures*

(A category will be like a poset at the level of groupoids)

The notion of isomorphism becomes at this level the notion of *equivalences*

Description of mathematical objects

The collection of all sets is an object at the next level

If B is a set the collections (groupoids) Set^B and Set/B are *equivalent*

Set^B collection of families of sets (X_b)

Set/B collection of pairs $Y,\ f : Y \to B$

If (X_b) is a family, we define $Y = \Sigma(b \in B)X_b$ and $f : (b, x) \mapsto b$

If $Y,\ f : Y \to B$ we define $X_b = \{y \in Y \mid f(y) = b\}$

Description of mathematical objects

We have canonical maps $F : \mathrm{Set}^B \to \mathrm{Set}/B$ and $G : \mathrm{Set}/B \to \mathrm{Set}^B$

F and G are *not* isomorphisms

$Y = G(F(X))$ is the family $Y_b = \{b\} \times X_b$

Y_b is only isomorphic (and not equal) to X_b

For a mathematician, the collections Set^B and Set/B can be identified

In the same way, two isomorphic groups can be identified

Collapsing

We get a *new* way to identify collections

This refines the identification of isomorphic structures

The collection of all linear orders with 27 elements in a given Grothendieck universe $\mathcal{U}$ can be *identified* with the groupoid with one object and one morphism!

Note that this is a large collection (not even an element of $\mathcal{U}$)

So a large collection is identified with a small collection

Univalent foundations

Starting point: *First of all I want to suggest a modification of the usual thesis stating that categories are higher level analogs of sets. We will take a slightly different position. We will consider groupoids to be the next level analogs of sets*

The key argument for this modification of the basic thesis is the following observation - not all interesting constructions on sets are functorial with respect to maps but they are all functorial with respect to isomorphisms.

Laws of identification

Mathematics is the art of giving the same name to different things. It is enough that these things, though differing in matter, should be similar in form, to permit of their being, so to speak, run in the same mould. When language has been well chosen, one is astonished to find that all demonstrations made for a known object apply immediately to many new objects: nothing requires to be changed, not even the terms, since the names have become the same.

Poincaré, *Science et Méthode*

Description of mathematical objects

At the next level we have structures on 2-*groupoids*

And so on, n-groupoids and then ∞-groupoids

«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)

The notion of *homotopy type* generalizes the notion of *set*

The notion of (homotopical) equivalence generalizes the notion of bijection

Univalent foundations

Once the modification of the basic thesis is accepted the connection between foundations and the homotopy theory becomes obvious since we know that n-groupoids are the same as homotopy n-types.

Design a calculus where all constructions are by design homotopy invariant and hence invariant under equivalences

Important principle that two isomorphic or otherwise appropriate equivalent objects are interchangeable

Set theory and type theory

1908 Zermelo *Untersuchungen über die Grundlagen der Mengenlehre*

1908 Russell *Mathematical Logic as Based on the Theory of Types*

«Simple» type theory

1940 Church *A Formulation of the Simple Theory of Types*

Extremely simple and natural

A type $bool$ as a type of «propositions»

A type I for «individuals»

Function type $A \to B$

Natural semantics of *types* as *sets*

Functions in simple type theory

In set theory, a function is a *functional graph*

In type theory, a function is given by an *explicit definition*

If $t : B$, we can introduce f of type $A \to B$ by the definition

$$f(x) = t$$

$f(a)$ «reduces» to $(a/x)t$ if a is of type A

Functions in simple type theory

We have two notions of function

-*functional graph*

-*function explicitly defined* by a term

What is the connection between these two notions?

Church introduces a special operation $\iota x.P(x)$ and the «axiom of description»

If $\exists! x : A.P(x)$ then $P(\iota x.P(x))$

Functions in simple type theory

We can then define a function from a functional graph

$\forall x.\exists! y.R(x,y) \to \exists f.\forall x.R(x,f(x))$

by taking $f(x) = \iota y.R(x,y)$

By contrast, Hilbert's operation $\epsilon x.P(x)$ (also used by Bourbaki) satisfies

if $\exists x : A.P(x)$ then $P(\epsilon x.P(x))$

To use $\exists! x : A.\varphi$ presupposes a notion of equality on the type A

Rules of identification

Identification can be specified by the following purely logical rules

(1) $a =_A a$

(2) if $a_0 =_A a_1$ and $P(a_0)$ then $P(a_1)$

Identification in mathematics

The first axiom of set theory is the axiom of *extensionality* stating that two sets are equal if they have the same element

In Church's system we have two form of the axiom of extensionality

(1) two equivalent propositions are equal

$$(P \equiv Q) \ \rightarrow \ P =_{bool} Q$$

(2) two pointwise equal functions are equal (law of identification of functions)

$$(\forall x : A. f(x) =_B g(x)) \quad \rightarrow \quad f =_{A \rightarrow B} g$$

The axiom of univalence will be a generalization of (1)

Dependent types

The basic notion is the one of *family of types* $B(x),\ x : A$

We have some *primitive* operations

$\Pi(x : A)B(x)$	$f \quad \text{where } f(x) = b$
$\Sigma(x : A)B(x)$	(a, b)
$A + B$	$\mathsf{i}(a), \mathsf{j}(b)$

which are *derived* operations in set theory

Dependent types

Logical operations are reduced to constructions on types by the following dictionnary

$A \wedge B$	$A \times B = \Sigma(x : A)B$
$A \vee B$	$A + B$
$A \to B$	$A \to B = \Pi(x : A)B$
$(\forall x : A)B(x)$	$\Pi(x : A)B(x)$
$(\exists x : A)B(x)$	$\Sigma(x : A)B(x)$

Dependent types

de Bruijn (1967) notices that this approach is suitable for representation of mathematical proofs on a computer (AUTOMATH)

Proving a proposition is reduced to building an element of a given type

«This reminds me of the very interesting language AUTOMATH, invented by Dijkstra's colleague (and next-door neighbor) N. G. de Bruijn. AUTOMATH is not a programming language, it is a language for expressing proofs of mathematical theorems. The interesting thing is that AUTOMATH works entirely by type declarations, without any need for traditional logic! I urge you to spend a couple of days looking at AUTOMATH, since it is the epitome of the concept of type.»

D. Knuth (1973, letter to Hoare)

Dependent types

This is the approach followed for the formalization of Feit-Thompson's theorem

Voevodsky's program precises this representation by characterizing which types correspond to mathematical propositions

Universes

A universe is a type the element of which are types, and which is closed by the operations

$$\Pi(x : A)B(x) \qquad \Sigma(x : A)B(x) \qquad A + B$$

Russell's paradox does not apply directly since one *cannot* express $X : X$ as a *type*

However, Girard (1971) shows how to represent Burali-Forti paradox if one introduces a type of all types

Univers

Martin-Löf (1973), following Grothendieck, introduces of hierarchy of universe

$$U_0 : U_1 : U_2 : \dots$$

Each universe U_n is closed by the operations

$$\Pi(x : A)B(x) \qquad \Sigma(x : A)B(x) \qquad A + B$$

Universes and dependent sums

We can formally represent the notion of structure

$\Sigma(X : U_0)((X \times X \to X) \times X)$

collection of types with a binary operation and a constant

$(X \times X \to X) \times X$ family of types for $X : U_0$

This kind of representation is used by Girard for expressing Burali-Forti paradox

New laws for identification

Martin-Löf introduces (1973) a primitive notion of identification in dependent type theory

The ⟪proposition⟫ expressing the identification of a_0 and a_1 of type A is represented by a family of type Id A a_0 a_1. In general there might be different ways to identify a_0 and a_1.

Since Id A a_0 a_1 is itself a type, one can iterate this construction

$$\mathsf{Id}\ (\mathsf{Id}\ A\ a_0\ a_1)\ p\ q$$

This is the core of the connection with ∞-groupoid

New laws for identification

What are the rules of identification?

(1) Any element is equal to itself $1_a : \mathsf{Id}\ A\ a\ a$

(2) $C(a)$ implies $C(x)$ if we have $p : \mathsf{Id}\ A\ a\ x$

A given identification p of a and x allows us to transport any property/structure of a to a property/structure of x

New laws for identification

The *new* law discovered by Martin-Löf (1973) can be expressed as the fact that in the type

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

which contains the special element

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

any element (x, ω) can actually *be identified* to this special element $(a, 1_a)$

New laws for identification

For instance if we take the collection of all rings (in a given universe)

Given a ring R_0 we can form the (groupoid) of pairs

(R, u)

where R is a ring and $u : R_0 \simeq R$ an isomorphism

This is a *trivial* groupoid: given (R, u) and (S, v) there is a *unique* map $(R, u) \simeq (S, v)$ given by $vu^{-1} : R \simeq S$

So: a lot of objects but *unique* isomorphism between them

New laws for identification

We get three laws of identification in type theory

It follows from these laws that any type has a ∞-groupoid structure

For instance, composition corresponds to transitivity of identification

The fact that identification is symmetric corresponds to the inverse operation

Hoffman-Streicher (1993)

S. Awodey, M. Warren (2009), P. Lumsdaine (2010), B. van den Berg, R. Garner

New laws for identification

These laws were discovered in 1973

Should identification be extensional?

Actually, how to express the extensionality axioms in this context?

An answer to this question is given by Voevodsky (2009)

Stratification

Stratification of *collections* following the complexity of *identifications*

A type A is a *proposition*

$\Pi(x_0 : A)\Pi(x_1 : A)\mathsf{Id}\ A\ x_0\ x_1$

A type A is a *set*

$\Pi(x_0 : A)\Pi(x_1 : A)\mathsf{isProp}(\mathsf{Id}\ A\ x_0\ x_1)$

A type A is a *groupoid*

$\Pi(x_0 : A)\Pi(x_1 : A)\mathsf{isSet}(\mathsf{Id}\ A\ x_0\ x_1)$

Stratification

The notions of *propositions*, *sets*, *groupoids* have now aquired a precise meaning

They are descrined formally as types

They will be used with this meaning in the rest of this talk

Type theory appears as a generalization *of set theory*

Equivalence

Voevodsky gives a simple and uniform definition of the notion of *equivalence* for $f : A \to B$

If A and B are *sets* we get back the notion of *bijection* between sets

If A and B are *propositions* we get back the notion of *logical equivalence* between propositions

If A and B are *groupoids* we get back the notion of *categorical equivalence* between groupoids

Equivalence

If $f : A \to B$ the *fiber* of f at $b : B$ is the type

$F(b) = \Sigma(x : A)\mathsf{Id}\ B\ b\ (f(x))$

f is an *equivalence* if this fiber is *contractible* for each b

$\Pi(b : B)(F(b) \times \mathsf{isProp}(F(b)))$

$A \simeq B$ is defined to be $\Sigma(f : A \to B)\mathsf{Equiv}(f)$

For instance, the identity function is an equivalence using the new law of identification discovered by Martin-Löf and hence we have $A \simeq A$

The axiom of univalence

The *axiom of univalence* states roughly that if $f : A \to B$ is an equivalence then A and B can be identified

More precisely, since $A \simeq A$ we have a map $\mathsf{Id}\ U\ A\ B \to A \simeq B$

the canonical map $\mathsf{Id}\ U\ A\ B \to A \simeq B$ *is an equivalence*

This generalizes Church's axiom of extensionality for *propositions*

Voevodsky has shown that this axiom implies *function extensionality*

The axiom of univalence

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

$\mathsf{Id}\ U\ (A \times (B \times C))\ ((A \times B) \times C)$

Any property satisfied by $A \times B$ that can be expressed in type theory is also satisfied by $B \times A$

This is not the case in set theory (Bourbaki, theory of structures)

$(1, -1) \in \mathbb{N} \times \mathbb{Z}$ $\qquad$ $(1, -1) \notin \mathbb{Z} \times \mathbb{N}$

The axiom of univalence

This also entails

-two isomorphic sets can be identified

-two isomorphic algebraic structures can be identified

-two (categorically) equivalent groupoids can be identified

-two equivalent categories can be identified

Given an identification of a and b: any property of a is also a property of b

Transport de structures

Soit $\mathsf{Grp}(A)$ le type qui donne une structure de groupe sur A

$\mathsf{Grp}(A) = \Sigma(f : A \to A \to A)\Sigma(a : A) \dots$

The collection of all groups is $\Sigma(X : U_0)\mathsf{isSet}(X) \times \mathsf{Grp}(X)$

This type is a groupoid

Transport of structures

If A and B are two isomorphic sets we have a proof of

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

by the axiom of univalence and hence a proof of

$$\mathsf{Grp}(A) \to \mathsf{Grp}(B)$$

This expresses the notion of *transport of structure* (Bourbaki) along the given isomorphism between A and B

Differences with set theory

Any property is transportable

No need of «critères de transportabilité» as in set theory

«Only practice can teach us in what measure the identification of two sets, with or without additional structures, presents more advantage than inconvenient. It is necessary in any case, when applying it, that we are not lead to describe non transportable relations.» Bourbaki, Théorie des Ensembles, Chapitre 4, Structures (1957)

«$0 \in A$ » is a non transportable property of a group A

«to be solvable» is a transportable property

Semantics

It is natural to represent a type as a *homotopy type*

D. Kan *A Combinatorial Definition of Homotopy Groups*, 1958

A type is interpreted as a Kan simplicial set

A family of type $B(x),\ x : A$ is interpreted as a *Kan fibration*

The type Id $A\ a_0\ a_1$ becomes the space of *paths* joining a_0 and a_1

This model satisfies the axiom of univalence (Voevodsky, 2009)

Semantics

What happens to the new law for identification discovered by Martin-Löf in this interpretation?

Any element of $\Sigma(x : A)\mathsf{Id}\ A\ a\ x$ can be identified to $(a, 1_a)$

It expresses the fact that the total space of the fibration defined by the space of paths having a given origin is *contractible*

This is exactly this fact which was the starting point of the loop-space method in algebraic topology (J.P. Serre)

Semantics

«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 X, I needed a fibre space E with base X 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 X (with fixed origin a), the projection $E \to X$ being the evaluation map: path $\to$ extremity of the path. The fibre is then the loop space of (X, a). I had no doubt: this was it! ... It is strange that such a simple construction had so many consequences.»

Posets and categories

In this approach

the notion of groupoid is more fondamental than the notion of category

A groupoid is defined as a type satisfying a property

Voevodsky insists strongly on this point

It is a very natural idea and it took me a lot of effort to understand that it is wrong and that the universe of the new foundations of mathematics should not be the ∞-category of ∞-categories but instead the ∞-groupoid of ∞-groupoids and their equivalences.

Actual formal examples

In a few weeks, Voevodsky could write these ideas formally in type theory

See

"'Experimental library of univalent foundation of mathematics" V. Voevodsky

Objects uniquely determined by universal properties

T. Pannila, abelian categories, category of complexes, triangulated categories

Differences with set theory

The collection of all groups/rings/posets form a *groupoid*

U_0 is *not* a set (at least a groupoid)

U_1 is *not* a groupoid (at least a 2-groupoid)

Complexity of identification of a type versus set theoretic ⟪size⟫

Posets and categories

A *preorder* is a *set* A with a relation $R(x, y)$ satisfying

$$\Pi(x : A)\Pi(y : A)\mathsf{isProp}(R(x, y))$$

which is reflexive and transitive

A *poset* is a preorder such that the canonical implication

$$\mathsf{Id}\ A\ x\ y \to R(x, y) \times R(y, x)$$

is a logical equivalence

Posets and categories

A *category* is a *groupoid* A with a relation $\mathsf{Hom}(x, y)$ satisfying

$$\Pi(x : A)\Pi(y : A)\mathsf{isSet}(\mathsf{Hom}(x, y))$$

This family of sets is «transitive» (associative composition operation) and «reflexive» (we have a neutral element)

This corresponds to the notion of *preorder*

Posets and categories

One can define $\mathsf{Iso}(x, y)$ which is a *set* and show $\mathsf{Iso}(x, x)$

This defines a canonical map

$$\mathsf{Id}\ A\ x\ y \to \mathsf{Iso}(x, y)$$

For being a *category* we require this map to be an equivalence (bijection) between the sets $\mathsf{Id}\ A\ x\ y$ and $\mathsf{Iso}(x, y)$

The axiom of univalence implies that the groupoid of rings, for instance, has a categorical structure

Existence

Voevodsky also introduces a new *modal* operation

$$\mathsf{isInh}(A)$$

which is a *proposition* expressing that A is inhabited

A is an arbitrary type

Existence

(1) $\mathsf{isProp}(\mathsf{isInh}(A))$

(2) $A \to \mathsf{isInh}(A)$

(3) $\mathsf{isInh}(A) \to \mathsf{isProp}(X) \to (A \to X) \to X$

Functions and graphs

We define $(\exists x : A)B$ to be $\mathsf{isInh}(\Sigma(x : A)B)$

This is a *new* operation on types suggested by this approach

We *cannot* in general extract a witness from a proof of $(\exists x : A)B$, contrary to $\Sigma(x : A)B$

However this extraction is possible whenever $\Sigma(x : A)B$ is a *proposition*

Graphs and functions

In particular if $B(x)$ is a proposition and

$B(x_0) \to B(x_1) \to \mathsf{Id}\ A\ x_0\ x_1$

In this case $\Sigma(x : A)B(x)$ is a proposition and we have

$(\exists x : A)B(x) \to \Sigma(x : A)B(x)$

This *justifies* Church's description axiom

But this applies to more general situation

Torsors

Let G be a group

A torsor is a set X with a G-action such that

(1) for any u in X the map $n \longmapsto ug,\ G \to X$ is an equivalence

(2) *and* isInh(X)

If X is a torsor we cannot in general exhibit one element of X

The collection of all torsors for a groupoid which is the classifying space of G

cf. D. Grayson Foundations.Ktheory

Torsors

If X is a $\mathbb{Z}$-torsor we have

$\Pi(u_0\ u_1 : X)(\exists! n : \mathbb{Z})\mathsf{Id}\ X\ (u_0 + n)\ u_1$

and so, by *unique choice* we have an application

$X \times X \to \mathbb{Z}$

$(u_0, u_1) \longmapsto u_1 - u_0$

such that $\mathsf{Id}\ X\ (u_0 + u_1 - u_0)\ u_1$

An example in analysis

If we define the type of real numbers R as a quotient of the set of Cauchy sequences of rationals

We can define $x\#y$ as meaning $(\exists r > 0) r \leqslant |x - y|$

We can define the inverse function $\Pi(x : R) x\#0 \to R$

This is because the inverse is *uniquely* determined

Category theory

The previous definition of category solves some foundational issues that are somewhat disturbing when category theory is formulated in set theory

For instance, what should be a category with binary product?

Should the product of two objects given explicitely as an operation?

We have two notions (if we don't assume choice)

Category theory

In the univalent foundation, there is no problem since the product of two objects is uniquely determined up to isomorphism

And hence *up to identification* by definition of category

Since we have unique choice, we have an explicit product function on objects

Graphs and functions

For instance one can show *without using the axiom of choice* that a fully faithful and essentially surjective functor is an equivalence of categories

If $F : A \to B$ is fully faithful then for each object b of B the groupoid $\Sigma(x : A)\mathsf{Iso}(F(x), b)$ is a *proposition*

If F is also essentially surjective we can define (effectively) its «inverse»

Existence is effective if it is unique up to isomorphism

Complexity of identification

In the definition of category, $\mathsf{Hom}(x_0, x_1)$ has to be a set

This is formally similar to the definition of a *locally small* category

But here what is crucial is the

complexity of identification

of the type $\mathsf{Hom}(x_0, x_1)$ and not its

set theoretic ⟪size⟫