Univalent Foundations

Talk by Vladimir Voevodsky
from Institute for Advanced Study in Princeton, NJ.

September 21 , 2011

Introduction

After Goedel's famous results there developed a "schism" in mathematics when abstract mathematics and constructive mathematics became largely isolated from each other with the "abstract" steam growing into what we call "pure mathematics" and the "constructive stream" into what we call theory of computation and theory of programming languages.

Univalent Foundations is a new area of research which aims to help to reconnect these streams with a particular focus on the development of software for building rigorously verified constructive proofs and models using abstract mathematical concepts.

This is of course a very long term project and we can not see today how its end points will look like. I will concentrate instead its recent history, current stage and some of the short term future plans.

Elemental, set-theoretic and higher level mathematics

1. Element-level mathematics works with elements of "fundamental" mathematical sets mostly numbers of different kinds.

2. Set-level mathematics works with structures on sets.

3. What we usually call "category-level" mathematics in fact works with structures on groupoids. It is easy to see that a category is a groupoid level analog of a partially ordered set.

4. Mathematics on "higher levels" can be seen as working with structures on higher groupoids.

To reconnect abstract and constructive mathematics we need new foundations of mathematics.

The "official" foundations of mathematics based on Zermelo-Fraenkel set theory with the Axiom of Choice (ZFC) make reasoning about objects for which the natural notion of equivalence is more complex than the notion of isomorphism of sets with structures either very laborious or too informal to be reliable.

More importantly to formalize *constructive* arguments about higher level objects in ZFC one is forced to use inherently *non-constructive* parts of ZFC such as Axiom of Choice. This means that large parts of abstract mathematics which are in fact constructive can not be constructively formalized using ZFC.

Because of these issues ZFC is not usable for constructive formalization of abstract mathematics.

Homotopy theory enters the picture

1. New foundations must provide a way to work constructively not only with sets but also with higher analogs of sets.
2. The objects of set-theoretic mathematics which most closely correspond to "higher sets" are higher groupoids. By Grothendieck's insight groupoids of all levels may be considered as homotopy types.
3. We conclude that in order to build constructive foundations for contemporary abstract mathematics we need to have a formal deduction system which can be used to work constructively with homotopy types.

Here a little miracle happens - a whole class of such deduction systems has been known since 1970-ies and moreover systems of this class are being widely used in theoretic computer science to reason about programs. However, it was not recognized until very recently that they can be used to work with homotopy types and homotopy types with structures.

Martin-Lof type theories

Deduction systems of this class are called Martin-Lof type theories. The first such theory was introduced by Per Martin-Lof in the 70-ies as a basis for new foundations of constructive mathematics. Two most important for us features of his theory are:

1. Identity types or types of "intensional equality", together with the associated "induction principle" and "computation rules" which are defined for any pair of terms of a given type X,
2. A universe U which is used to quantify over types.

Martin-Lof type theories (cont.)

It was originally assumed that Martin-Lof theory is something like a constructive set theory. Types were interpreted as sets and constructions on types as corresponding constructions on sets.

It was soon observed however that it is not a very good formalization of the world of sets because many of the natural properties expected from sets were not provable in the Martin-Lof theory. Adding axioms which made the objects of his theory to behave more like sets led to the deterioration of its constructive nature.

Consequently it has not become popular with mathematicians or even with constructive mathematicians.

Martin-Lof type theories (cont.)

Instead, the ideas of Martin-Lof found their way into theoretical computer science in part through Thierry Coquand's Calculus of Constructions and its extension - Calculus of Inductive Constructions .

This later variant of Martin-Lof type theory , more complex and more convenient for practical use because of its sophisticated machinery of inductive definitions became the basis for proof assistant Coq - the proof assistant which is now used to teach courses on the theory of programming languages in many leading universities.

Martin-Lof theory and homotopy theory

The first hint that Martin-Lof type theory may have something to do with homotopy types appeared in 1996 when Martin Hofmann and Thomas Streicher constructed a new semantics for a version of this theory which interpreted types not as sets but as groupoids.

In 2005 Steve Awodey discovered the connection between the Martin-Lof "induction principle" for the identity types and factorization axioms of the abstract homotopy theory. This led to the interpretation of identity types as path spaces.

At about the same time I understood that the universe U is to be interpreted as the base of a universal univalent fibration.

It all came together in the fall of 2009. Combining the ideas of Steve Awodey on the interpretation of the identity types with my ideas on the interpretation of the universes I have constructed the *univalent model* of the calculus of inductive constructions.

This model provides a semantics for the Calculus which allows one to use it to do exactly what was needed from the hypothetical language for new foundations of mathematics which was discussed above.

Some of the key univalent concepts

1. There is a filtration on types , or rather on type expressions, by their "h-level".
   (a) Types of h-level 0 are equivalent to the one point type.
   (b) Types of h-level 1 correspond to propositions.
   (c) Types of h-level 2 correspond to sets.
   (d) Types of h-level 3 correspond to groupoids.
   (e) Types of higher levels correspond to higher groupoids or, equivalently, to more general homotopy types.

Some of the key univalent concepts (cont.)

2. Types with decidable equality such as natural numbers, trees etc. have level ≤ 2 e.g. the usual inductive types are sets.
3. Typical examples of types of level > 2 are universes.
4. Constructions translated into CIC using univalent semantics are invariant under *weak equivalences* between types.
5. The univalent model satisfies a new axiom which is called the univalence axiom. It imposes the condition that the identity type between two types is naturally weakly equivalent to the type of weak equivalences between these types.

Some of the key univalent concepts (cont.)

6. The univalence axiom implies the functional extensionality both for "straight" functions and for dependent functions. It also implies that two logically equivalent "propositions" (types of h-level 1) are equal.

7. The univalence axiom implies that the universe of types of h-level n has h-level $n+1$. In particular, the type of "propositions" is a "set" and the type of "sets" is a "groupoid".

8. The univalence axiom implies similar statements for types with structures e.g. one can prove using the univalence axiom that the identity type between two groups is equivalent to the type of isomorphisms between these groups.

Some of the key univalent concepts (cont.)

9. Unlike many other axioms (e.g. the axiom of excluded middle), the univalence axiom is expected "to have computational content". In other words decidable normalization should be extendable in a certain sense to terms which involve the univalence axiom. For example there is the following precise:

   Conjecture 1. There exists a terminating algorithm which for any term expression t of type [nat] (natural numbers) constructed using the univalence axiom returns a term expression t' of type [nat] which does not use univalence axiom and a term expression of the identity type [Id nat t t'] which may use the univalence axiom.

In February 2010 I started to write a Coq library of formalized mathematics based on the univalent model.

See `http://github.com/vladimirias/Foundations/` .

There is also an HTML version of the library which can be found at my web-page `http://www.math.ias.edu/~vladimir`

Currently the basic properties of types and functions such as contractibility, h-levels, weak equivalences and their behavior relative to the main constructions of type theory are formalized. I also formalized some basic algebra culminating at the moment in the formal construction of localization for commutative rings.

In addition there are files with basic natural and integer arithmetic and basic theory of finite sets developed as particular cases of general constructions.

There will be a full year program on Univalent Foundations topic at the Institute for Advanced Study in 2012-2013 co-organized by Steve Awodey, Thierry Coquand and myself. For information on the program see `http://www.math.ias.edu`.

Some idea of the near future the Univalent Foundations can be obtained from the list of topics which we plan to address during the program:

1. Practical formalization of set-level mathematics in Coq based on the univalent approach.

   Goals: developing skills for collective work on libraries of formalized mathematics, locating the points of "tension" between constructive and non-constructive approaches especially in the formalization of analysis, creating libraries for future use.

2. Computational issues in constructive type theory related to the univalence axiom.

   Goals: looking for approaches to the proof of the "main computational conjecture" of the univalent approach with a special focus on looking for practical algorithms for automatic construction of fully constructive terms from terms build with the help of extensionality axioms.

3. Formalization of advanced homotopy-theoretic structures in constructive type theory.

   Goals: looking for approaches to formalize higher coherence structures (simplicial types, H-types, n-1-categories and n-1-functors etc.). Looking for possible syntax and computation rules for higher inductive definitions. Looking for the constructions of elements in homotopy groups of spheres as mappings between the corresponding loop "functors".

4. Relation of constructive type theory to set-theoretic foundations.

   Goals: formalizations of type theories and known constructions of their models in ZFC and related theories. Looking for new models of constructive type theories, especially for non-standard models of the univalence axiom.