Univalent Foundations of Mathematics and automated proof checking

in memoriam of Vladimir Voevodsky (1966-2017)

Andrei Rodin (andrei@philomatica.org)

Steklov Mathematical Institute, 28 December 2017

The Origins and Motivations of Univalent Foundations

A Personal Mission to Develop Computer Proof Verification to Avoid Mathematical Mistakes

(The Institute Letter Summer 2014)

History of one mathematical mistake

- 1990: joint paper in Russian with M. Kapranov motivated by the *Esquisse d'un Programme* by A. Grothendieck (1984): "∞-Groupoids as a Model for a Homotopy Category" first publsihed in УМН in Russian;
- 1998: Carlos Simpson (Laboratoire Dieudonné) claims a counter-example to the main theorem of Kapranov&Voevodsky 1990 (arXiv: 9810059). Voevodsky and Kapranov check their proofs but do not find mistakes in it. Simpson's paper is not published, the community suspects a mistake in the alleged counter-example
- 2013: Voevodsky finally finds a (uncorrectable) mistake in the original proof: the main theorem of the 1990 paper is a non-theorem!

Purpose of APC

The present situation when new alleged mathematical proofs can be checked by a few experts in the given field is hardly tolerable. The strong reliance on authority in mathematics blurs its objective character and rational nature. It makes research mathematics publicly indistinguishable from an esoteric sect led by a group of distinguished gurus and it makes it difficult to find applications of new mathematical results outside the Pure Mathematics.

APC solves the problem if

- Mathematical proofs are written in the form of computer code and the content of this code is conceptually transparent for all its competent users:
- The code is computationally effective and does not require computational resources .
- Epistemic transparency: users understand how the machine works and can reasonably evaluate the probability of error.

2006 IAS Lecture

"Ideally, a paper submitted to a journal should contain text for human readers integrated with references to formalized proofs of all the results. Before being send to a referee the publisher runs all these proofs through a proof checker which verifies their validity. What remains for a referee is to check that the paper is interesting and that the formalizations of the statements correspond to their intended meaning."

History of the Idea:

- Descartes: Symbolic Algebra and Analytic Geometry;
- Leibniz: Geometrical Characteristics;
- Hilbert : Formal Axiomatic Method as "the basic instrument of all research"
- AUTOMATH (de Bruijn 1967), MIZAR (since 1973), HOL, Lego, Isabelle, Nuprl, Nqthm, AC2L, Elf, Plastic, Phox, PVS, IMPS, QED, ...

What has been achieved by 2000?:

Mostly *meta-mathematical* rusults such as Gödel's Incompleteness theorems. However important these results may be they have no direct relevance to the issue of formal proof checking.

Why formalization of mathematical reasoning did not become a common practice so far?

Because the existing principles and instances of formalization are NOT adequate!

Problems of set-theoretic formalization:

- Lack of invariance with respect to isomorphisms and higher equivalences (Benacerraf problem);
- The identification of proofs with formal deductions when a formal distinction between proof-supporting and not proof-supporting deductions is missing; (Prawitz, Martin-Löf);
- Formal deduction in ZFC, generally, is not algorithmic.

Isomorphism-Invariance :

For any proposition P about object X and any isomorphism $X \cong X'$ there exists proposition P' about object X' such as P' is true if and only if P is true.

Breaking of II in the ZFC-coding:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

where

- $i \in \mathbb{N}$;
- $i \in \mathbb{Z}$

In ZFC whole numbers are encoded as ordered pairs of natural numbers. So in ZFC the two versions of the formula (for natural and whole numbers) are not logically equivalent.

Solution: a combination of the following

- Homotopy theory;
- theory of ∞-groupoids (Grothendieck);
- Martin-Löf Constructive Type theory (MLTT);
- prover COQ (after Thierry Coquand).

+ Univalence Axiom.

Main Features:

- Internal Logic
- Rules instead of Axioms (consider QTT);

Logic in Foundations: External and Internal

- A theory is a system of formal sentences (= sentential forms), which are satisfied in a model;
- Semantics of *logical* terms is rigidly fixed: interpretation concerns only *non-logical* terms. Hence the standard (Bourbaki) notion of signature as the list of non-logical terms of the given theory.

Two distinct points of a straight line completely determine that line

If different points A,B belong to straight line a and to straight line b then a is identical to b.

External and Internal Logic: Lawvere 1970

The unity of opposites in the title [Quantifiers and Sheaves] is essentially that between logic and geometry, and there are compelling reasons for maintaining that geometry is the leading aspect. . . . [A] Grothendieck "topology" appears most naturally as a modal operator, of the nature "it is locally the case that", the usual logical operators, such as $\forall$, $\exists$, $\Rightarrow$ have natural analogues which apply to families of geometrical objects rather than to propositional functions. . . . We first sum up the principle contradictions of the Grothendieck-Giraud-Verdier theory of topos in terms of four or five adjoint functors [..] enabling one to claim that in a sense *logic is a special case of geometry*.

Logical and Extra-Logical Rules

Rules in UF qualify as logical insofar they are applied to propositional types. Types in UF are, generally, non-propositional (propositions-as-*some*-types. Axioms are distinguished propositional types. UF may not need any fixed distinguished types, propositional or not.

MLTT: Syntax

- 4 basic forms of judgement:
  (i) $A : TYPE$;
  (ii) $A \equiv_{TYPE} B$;
  (iii) $a : A$;
  (iv) $a \equiv_A a'$
- Context : $\Gamma \vdash$ judgement (of one of the above forms)
- no axioms (!)
- rules for contextual judgements; Ex.: dependent product :
  If $\Gamma, x : X \vdash A(x) : TYPE$, then $\Gamma \vdash (\Pi x : X)A(x) : TYPE$

MLTT: Semantics of $t : T$ (Martin-Löf 1983)

- t is an element of set T
- t is a proof (construction) of proposition T ("propositions-as-types")
- t is a method of fulfilling (realizing) the intention (expectation) T
- t is a method of solving the problem (doing the task) T (BHK-style semantics)

Sets and Propositions Are the Same

If we take seriously the idea that a proposition is defined by lying down how its canonical proofs are formed [...] and accept that a set is defined by prescribing how its canonical elements are formed, then it is clear that it would only lead to an unnecessary duplication to keep the notions of proposition and set [...] apart. Instead we simply identify them, that is, treat them as one and the same notion. (Martin-Löf 1983)

MLTT: Definitional aka judgmental equality/identity

$x, y : A$ (in words: x, y are of type A)

$x \equiv_A y$ (in words: x is y by definition)

MLTT: Propositional equality/identity

$p : x =_A y$ (in words: x, y are (propositionally) equal as this is evidenced by proof p)

Definitional eq. entails Propositional eq.

$$\frac{x \equiv_A y}{p : x =_A y}$$

where $p \equiv_{x=_A y} \mathit{refl}_x$ is built canonically

Equality Reflection Rule (ER)

$$\frac{p : x =_A y}{x \equiv_A y}$$

ER is not a theorem in the (intensional) MLTT (Streicher 1993).

Extension and Intension in MLTT

- MLTT + ER is called *extensional* MLTT
- MLTT w/out ER is called *intensional*
  (notice that according to this definition intensionality is a negative property!)

Higher Identity Types

- $x', y' : x =_A y$
- $x'', y'' : x' =_{x=_A y} y'$
- $\ldots$

HoTT: the Idea

Types in MLTT are (informally!) modeled by spaces (up to homotopy equivalence) in Homotopy theory, or equivalently, by higher-dimensional groupoids in Category theory (in which case one thinks of n-groupoids as higher homotopy groupoids of an appropriate topological space).

Homotopical interpretation of Intensional MLTT

- $x, y : A$
  x, y are points in space A
- $x', y' : x =_A y$
  x', y' are paths between points x, y; $x =_A y$ is the space of all such paths
- $x'', y'' : x' =_{x=_A y} y'$
  x'', y'' are homotopies between paths x', y'; $x' =_{x=_A y} y'$ is the space of all such homotopies
- ...

Point

Definition

Space S is called contractible or space of h-level (-2) when there is point $p : S$ connected by a path with each point $x : A$ in such a way that all these paths are homotopic (i.e., there exists a homotopy between any two such paths).

Homotopy Levels

Definition

We say that S is a space of h-level $n+1$ if for all its points x, y path spaces $x =_S y$ are of h-level n.

Cummulative Hierarchy of Homotopy Types

- -2-type: single point pt;
- -1-type: the empty space $\emptyset$ and the point pt: truth-values aka (mere) propositions
- 0-type: sets: points in space with no (non-trivial) paths
- 1-type: flat groupoids: points and paths in space with no (non-trivial) homotopies
- 2-type: 2-groupoids: points and paths and homotopies of paths in space with no (non-trivial) 2-homotopies
- ...

Propositions-as-**Some**-Types !

Which types are propositions?

Def.: Type P is a *mere proposition* if $x, y : P$ implies $x = y$ (definitionally).

Truncation

Each type is transformed into a (mere) proposition when one ceases to distinguish between its terms, i.e., *truncates* its higher-order homotopical structure.

Interpretation: Truncation reduces the higher-order structure to a single element, which is **truth-value**: for any non-empty type this value is **true** and for an empty type it is **false**.
The reduced structure is the structure of **proofs** of the corresponding proposition.
To treat a type as a proposition is to ask whether or not this type is instantiated without asking for more.

- Thus in HoTT "merely logical" rules (i.e. rules for handling propositions) are instances of more general formal rules, which equally apply to non-propositional types.
- These general rules work as rules of building models of the given theory from certain basic elements which interpret primitive terms (= basic types) of this given theory.
- Thus HoTT qualify as *constructive* theory in the sense that besides of propositions it comprises non-propositional objects (on equal footing with propositions rather than "packed into" propositions as usual!) and formal rules for managing such objects (in particular, for constructing new objects from given ones). In fact, HoTT comprises rules with apply *both* to propositional and non-propositional types.

Univalence

$$(A =_{TYPE} B) \simeq (A \simeq B)$$

In words: equivalnce of types is equivalent to their equality.

For PROPs: $(p = q) \leftrightarrow (p \leftrightarrow q)$ (propositional extensionality)

For SETs: Propositions on isomorphic sets are logically equivalent (isomorphism-invariance)

Univalence implies *functional extensionality*: if for all x X one has $fx =_Y gx$ then $f =_{X \to Y} g$ (the property holds at all h-levels).

Open Problem: the Initiality Conjecture

Build a category of models for MLTT (or its replacement) where the *term model* is the initial object. Solved only for Calculus of Constructions (CoC, after Th. Coquand) by Th. Streicher in 1991. CoC is a small fragment of MLTT. Cf. Lawvere's conception of theory as a "generic model".

Contributions to Philosophy/ Foundations/ UF

- 2003: Lecture in the Wuhan University (China): What is most important for mathematics in the near future?. :
  - Computerized version of Bourbaki;
  - Connecting pure and applied mathematics.
- 2003: Bangalore (India) Lecture: Mathematics and the Outside World;
- 2006: Inagural Lecture in IAS: Foundations of Mathematics and Homotopy Theory;
- 2006: A Very Short Note on Homotopy λ-Calculus;

Contributions to Philosophy/ Foundations/ UF

- 2010: Lecture at the 80 anniversary of IAS: What if the current foundations of mathematics are inconsistent?;
- 2011 - 2013: Many talks on Univalent Foundations in Universities of America, Europe and Asia;
- 2012-2017 Series of preprints on C-systems;
- 2013: Collective project in IAS ob HoTT and UF resulting in the HoTT Book. In 2015 V.V. requires to remove his name from the list of authors.

Contributions to Philosophy/ Foundations/ UF

- 2014: Paul Bernays Lectures in the ETH Zurich: Foundations of mathematics - their past, present and future.
- 2016: Invited Lecture and the 7th European Mathematical Congress: UniMath - a library of mathematics formalized in the univalent style.
- 2017 (August): Invited Lecture at the Logical Colloquium in Stockholm.
- Planned but later canceled contribution to the upcoming Springer volume "Reflections on the Foundations of Mathematics".