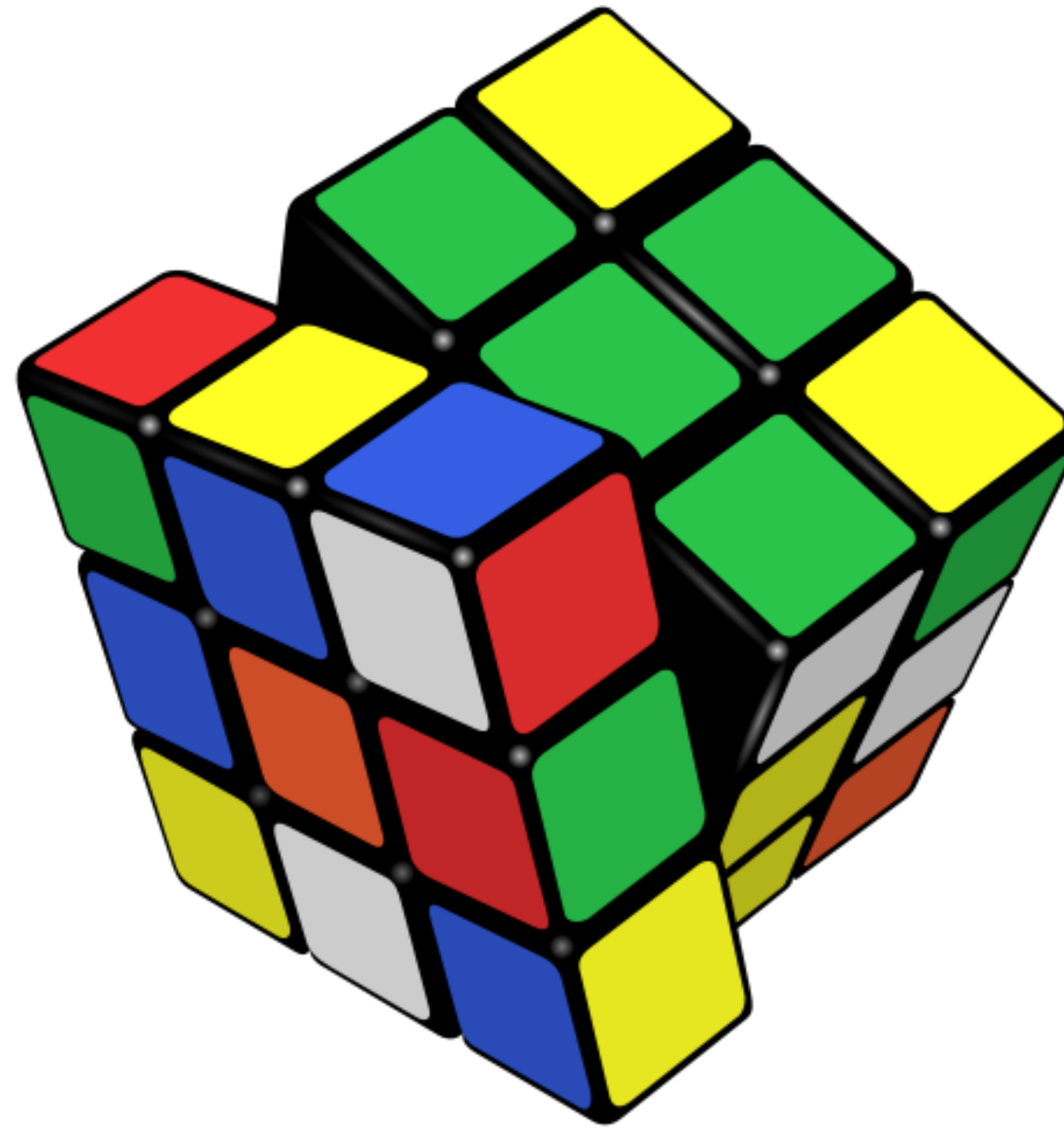
ASC 2014, Aug. 25, 2014, NTU, Singapore.

How I became interested in foundations of mathematics.

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

When I was 14 years I had a pneumonia and had to stay in bed at home. A friend of mine brought me the Rubik Cube. He said that it was not his and that he can only leave it with me for 24 hours.

Back then, in Soviet Union, there were no articles about the cube and no information on how to solve it was available. But when my friend came back I had the cube solved.



From http://en.wikipedia.org/wiki/Rubik's_Cube

I remember the effort it took and how I had to figure out that I need to record the positions of different colors and how I then invented several "operations" which were sufficient to assemble the cube.

And I remember how much fun it was, and how excited I was to have done it and how impressed was my friend.

BTW - The friend, Oleg Sheremetiev, who was 10 years older than I was, later became the person who introduced me to pure mathematics…

Many of us do mathematics that is a little like the Rubik Cube.

There is a problem. And there is the search for a solution. And when the solution is found it is certain that it is a solution.

But mathematics which earned me the Fields Medal at the International Congress of Mathematicians in Beijing in 2002 is very different.

There is a problem. And there is the search for a solution. But when the solution is found it is not certain at all that it is a solution.

The Fields Medal was awarded to me for the proof of Milnor’s Conjecture.

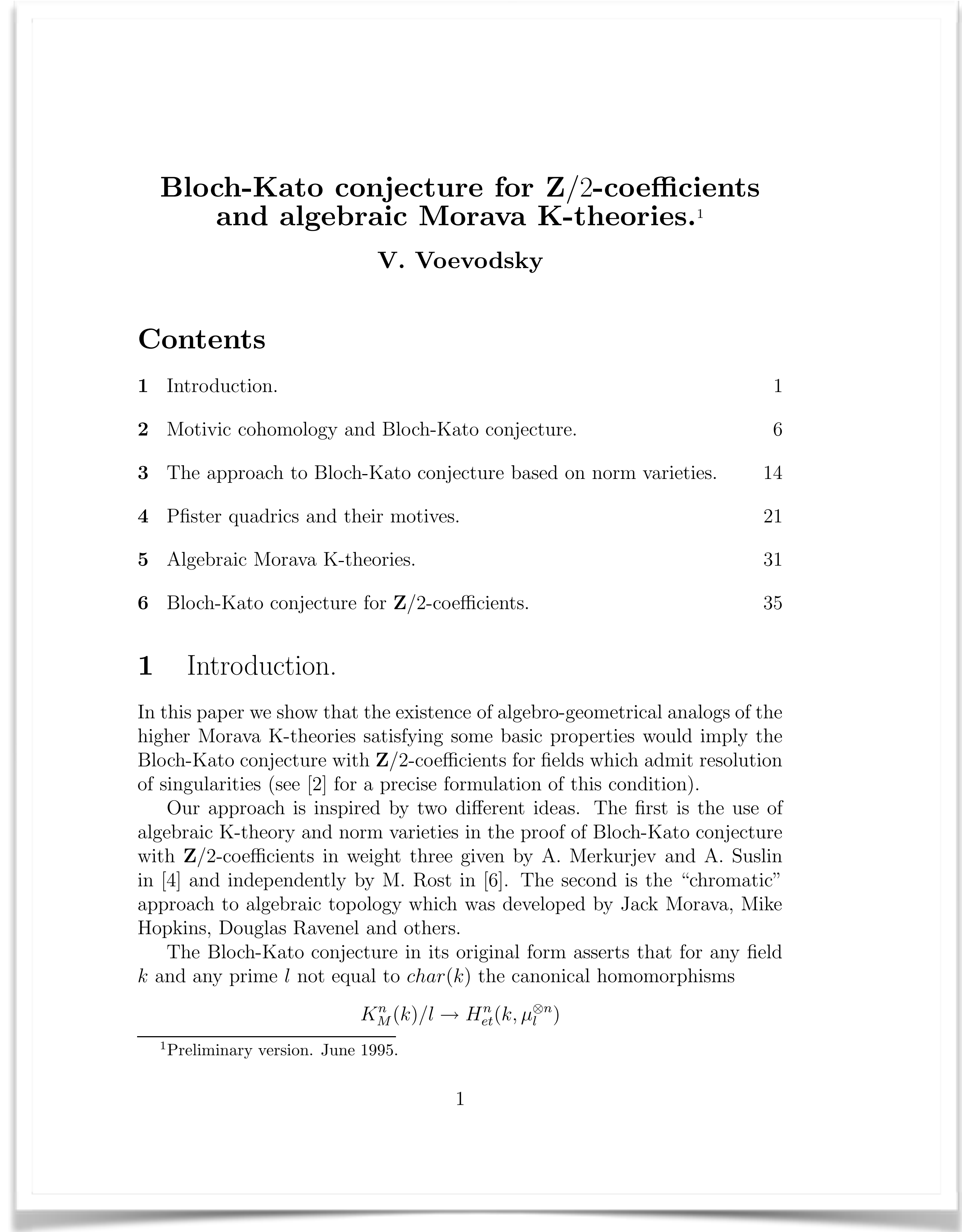
The problem was to find a proof of the conjecture.

The search for a solution took me about two years, from 1993 to 1995.

The solution was the proof.

In 1995 I started to work on “writing the proof down”. I had the first preprint available in June of 1995.

But it was only the beginning of the story of my proof of Milnor's Conjecture.



Bloch-Kato conjecture for $\mathbf{Z}/2$-coefficients and algebraic Morava K-theories.[1]

V. Voevodsky

Contents

1 Introduction.

In this paper we show that the existence of algebro-geometrical analogs of the higher Morava K-theories satisfying some basic properties would imply the Bloch-Kato conjecture with $\mathbf{Z}/2$-coefficients for fields which admit resolution of singularities (see [2] for a precise formulation of this condition).

Our approach is inspired by two different ideas. The first is the use of algebraic K-theory and norm varieties in the proof of Bloch-Kato conjecture with $\mathbf{Z}/2$-coefficients in weight three given by A. Merkurjev and A. Suslin in [4] and independently by M. Rost in [6]. The second is the “chromatic” approach to algebraic topology which was developed by Jack Morava, Mike Hopkins, Douglas Ravenel and others.

The Bloch-Kato conjecture in its original form asserts that for any field k and any prime l not equal to $char(k)$ the canonical homomorphisms

$$K_M^n(k)/l \to H_{et}^n(k, \mu_l^{\otimes n})$$

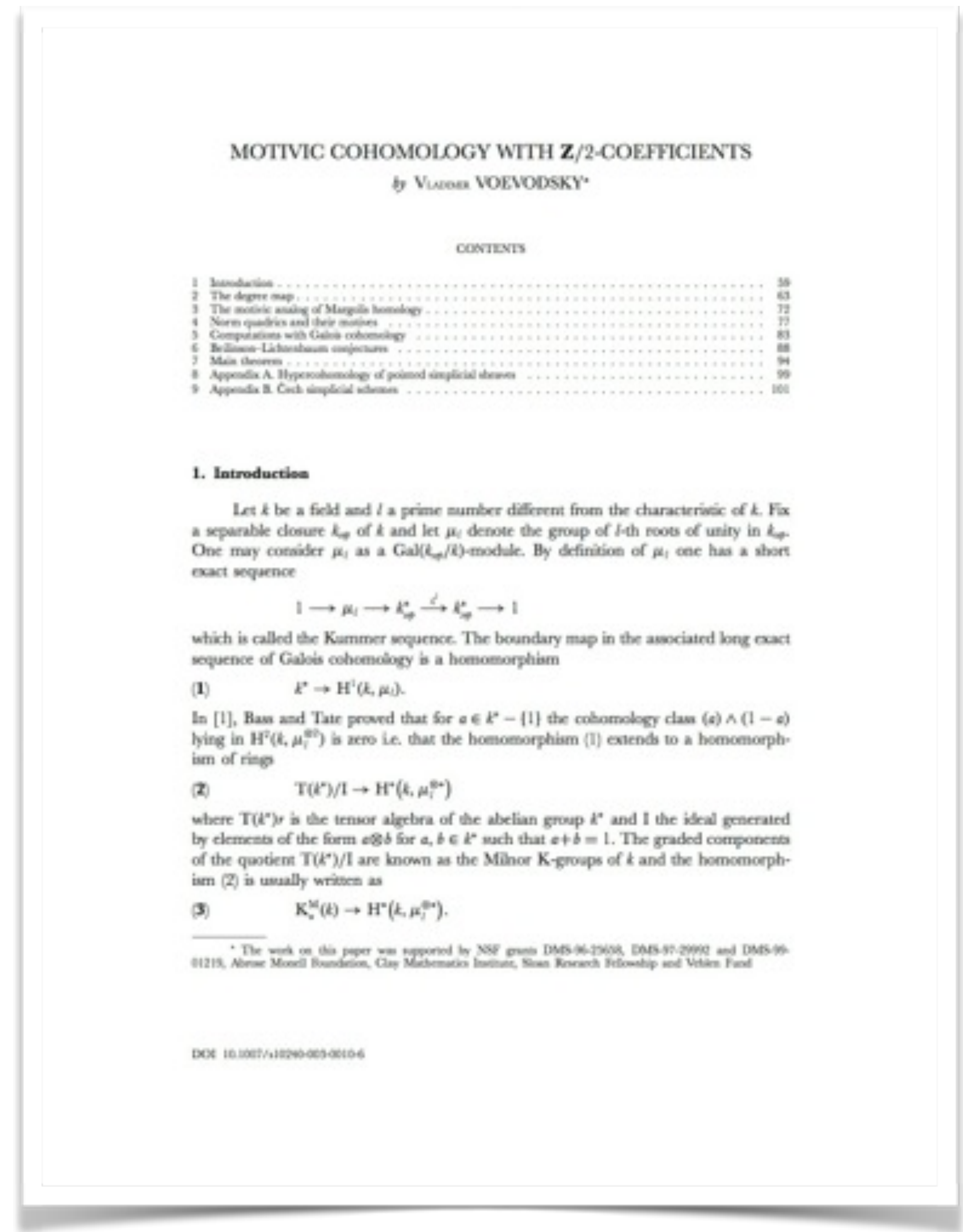
[1]Preliminary version. June 1995.

1

The proof that I found depended on another conjecture. That conjecture was in itself very cool and connected two areas of mathematics which were, at that time, very far apart. I was also sure that I know how to prove this conjecture, but that it will take a long time.

Then I started to look for a modification of the first proof which would not require proving this new conjecture and about a year later found it. I wrote a preprint with the new proof in December 1996. The proof in the preprint contained all of the main ideas but many details were left out.

And then it took me 7 hard years to work out these details and to publish a paper with a complete proof…



MOTIVIC COHOMOLOGY WITH $\mathbf{Z}/2$-COEFFICIENTS

by VLADIMIR VOEVODSKY*

CONTENTS

1. Introduction

Let k be a field and l a prime number different from the characteristic of k. Fix a separable closure k_{sep} of k and let μ_l denote the group of l-th roots of unity in k_{sep}. One may consider μ_l as a $Gal(k_{sep}/k)$-module. By definition of μ_l one has a short exact sequence

$$1 \longrightarrow \mu_l \longrightarrow k_{sep}^* \xrightarrow{l} k_{sep}^* \longrightarrow 1$$

which is called the Kummer sequence. The boundary map in the associated long exact sequence of Galois cohomology is a homomorphism

(1) $$k^* \to H^1(k, \mu_l).$$

In [1], Bass and Tate proved that for $a \in k^* - \{1\}$ the cohomology class $(a) \wedge (1-a)$ lying in $H^2(k, \mu_l^{\otimes 2})$ is zero i.e. that the homomorphism (1) extends to a homomorphism of rings

(2) $$T(k^*)/I \to H^*(k, \mu_l^{\otimes *})$$

where $T(k^*)$ is the tensor algebra of the abelian group k^* and I the ideal generated by elements of the form $a \otimes b$ for $a, b \in k^*$ such that $a+b=1$. The graded components of the quotient $T(k^*)/I$ are known as the Milnor K-groups of k and the homomorphism (2) is usually written as

(3) $$K_*^M(k) \to H^*(k, \mu_l^{\otimes *}).$$

* The work on this paper was supported by NSF grants DMS-96-25658, DMS-97-29992 and DMS-99-01219, Ambrose Monell Foundation, Clay Mathematics Institute, Sloan Research Fellowship and Veblen Fund

DOI 10.1007/s10240-003-0010-6

And I was lucky!

The ideas which the proof was based on turned out to be solid and the results of other people which I relied on turned out to be correct.

This is not always the case.

Let me tell you the story of another of my proofs which turned out very differently.

In 1987 I was introduced to Mikhail Kapranov. I was an undergrad at Moscow University and he was a graduate student.

We immediately discovered that we are both dreaming of developing new ‘higher dimensional’’ mathematics inspired by the concepts of higher category theory.

We started to work together. It was great fun. Doing mathematics with someone from whom you can learn, while discovering together things which are new both for you and for the world is an amazing and powerful experience.

And it was a great time to be growing up too…

In the late1989 the Berlin Wall fell. In the same year I received my first invitation to present at a conference in the West. It was still impossible to get a permission from the Soviet government to go to a western country so I did not go to the conference, but this was changing.

When in the summer of 1990, by recommendation of Kapranov, I was accepted to the graduate school at Harvard without having to apply I was able to get a tourist visa and in the Fall of 1990 I left the Soviet Union and the american period of my life began…

CAHIERS DE TOPOLOGIE
ET GÉOMÉTRIE DIFFÉRENTIELLE
CATÉGORIQUES

VOL. XXXII-1 (1991)

INTERNATIONAL CATEGORY THEORY MEETING
BANGOR, WALES, JULY 2-7 1989
CAMBRIDGE, ENGLAND, MARCH 23-25, 1990

The pair of meetings had a high international participation, notable for the presence of nine colleagues from Tbilisi, two from Moscow and five from Eastern Europe. The second part was organised in conjunction with a Peripatetic Seminar on Sheaves and Logic.
There were 41 talks at Bangor, and 12 at Cambridge. Also, on the first day at Bangor, four discussion groups were organised on:

Categorical Topology (chaired by G.L. Brummer)
Pure Category Theory (chaired by G.M. Kelly)
Computer Science (chaired by D. Rydeheard)
Sheaves and Homotopical Algebra (chaired by W.F. Lawvere)

The Chairmen reported back to a full meeting. This structure enabled the meeting to start with a broad picture of activity over the whole field, and contributed to the lively debate and friendly atmosphere.
We split up on a sunny afternoon for a walk to Aber Falls or a tour around the walled city and castle of Conway. The Conference Dinner was notable for the writer being reminded to keep his speech short by a clap of thunder.
The meeting was supported by the Science and Engineering Research Council and the British Council. The use of two venues enabled this support to be used effectively; it enhanced considerable the Scientific merit of the meeting, and broadened the scope of the Proceedings. The University of Wales, Bangor, also supported a reception.
Thanks are particularly due to Tim Porter for his organising efforts at Bangor, and Martin Hyland for his similar work at Cambridge.
Especial thanks go to Tim also for editing the Proceedings, and Pat Morrell for the typing.

R. Brown

I did not go to the conference but Kapranov and I submitted two papers to the proceedings of this conference.

The second of these two papers was about one of the key conjectures of the new "higher dimensional" mathematics that was due to the famous French mathematician Alexander Grothendieck.

In his mysterious "Esquisse d'un Programme" he wrote:

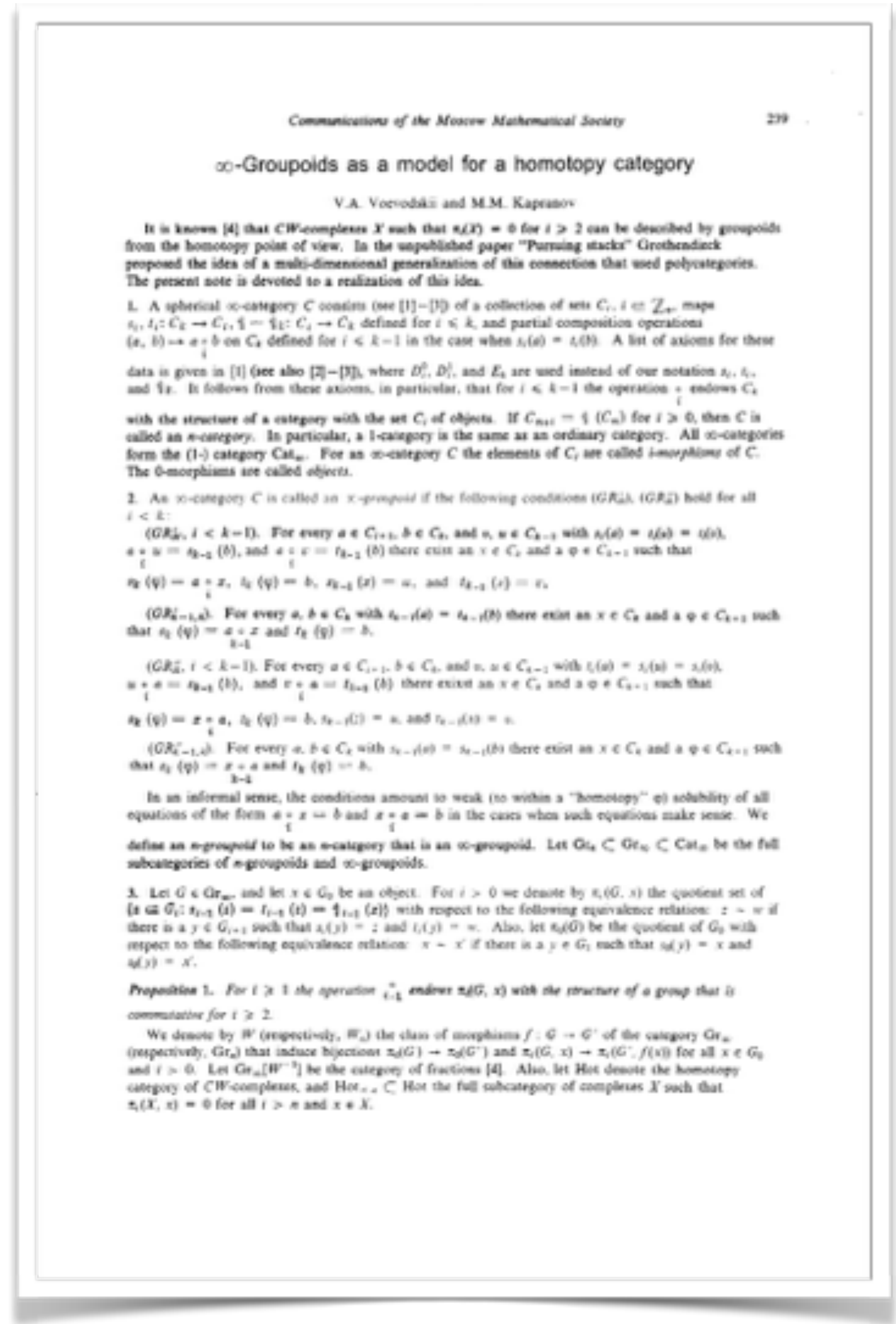
… *the intuition appeared that* **∞**-*groupoids should constitute particularly adequate models for homotopy types, the n-groupoids corresponding to truncated homotopy types (with* $\pi_i = 0$ *pour i > n).*

A. Grothendieck "Esquisse d'un Programme" 1984.

The conjecture was not a precise one since what should be the definition of an infinity groupoid remained open.

Kapranov and I decided that we know what the definition should be and how to prove the conjecture with this definition.

We wrote a paper with a sketch of the proof and published it in one of the best Russian mathematical journals and the paper with the complete proof was published in the proceedings of the conference that I have been invited to.



Communications of the Moscow Mathematical Society 239

∞-Groupoids as a model for a homotopy category

V.A. Voevodskii and M.M. Kapranov

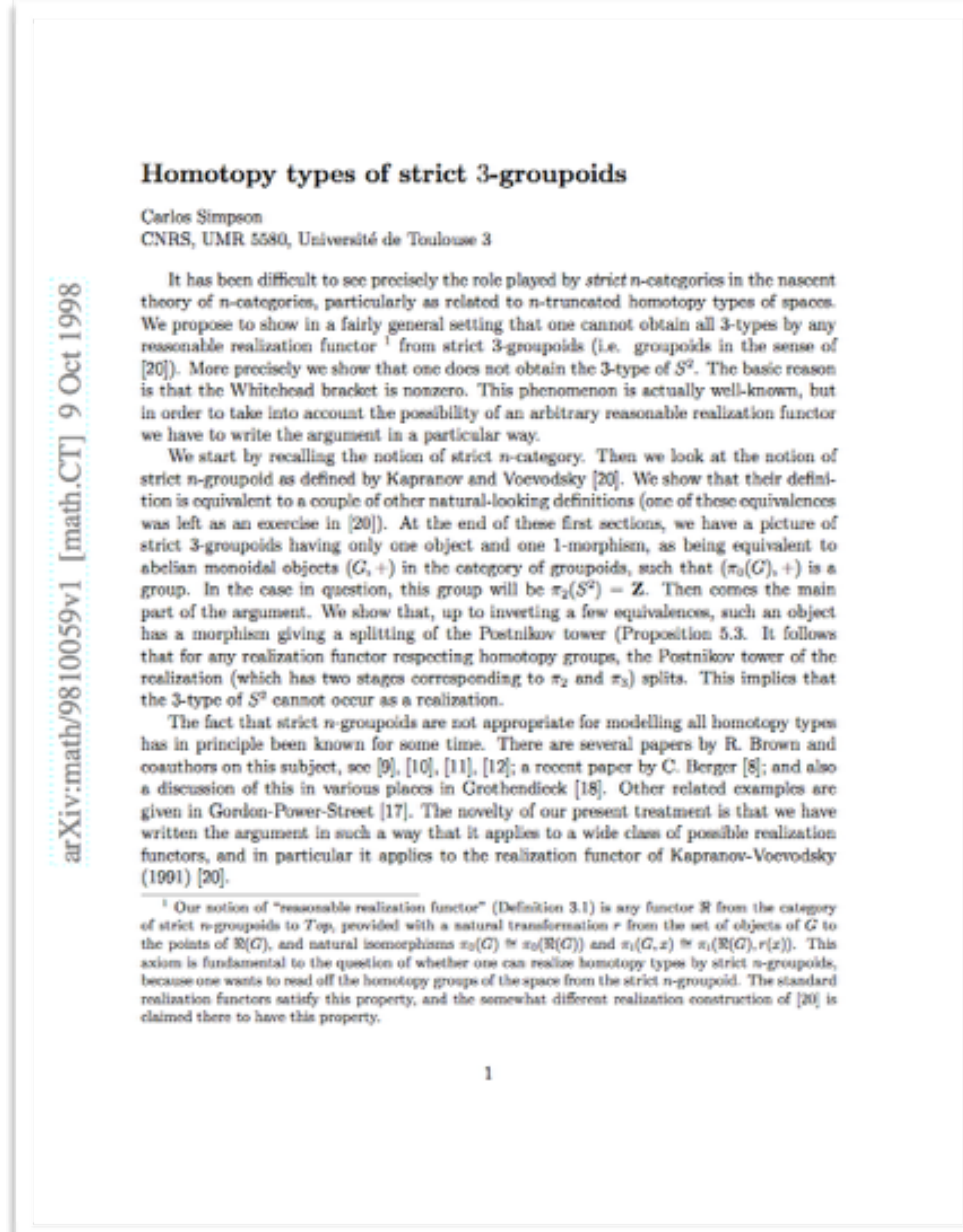
It is known [4] that *CW*-complexes X such that $\pi_i(X) = 0$ for $i > 2$ can be described by groupoids from the homotopy point of view. In the unpublished paper "Pursuing stacks" Grothendieck proposed the idea of a multi-dimensional generalization of this connection that used polycategories. The present note is devoted to a realization of this idea.

1. A spherical ∞-category C consists (see [1]–[3]) of a collection of sets C_i, $i \in \mathbb{Z}_+$, maps $s_i, t_i: C_k \to C_i$, $1 = 1_k: C_i \to C_k$ defined for $i \le k$, and partial composition operations $(a, b) \mapsto a \underset{i}{*} b$ on C_k defined for $i \le k-1$ in the case when $s_i(a) = t_i(b)$. A list of axioms for these data is given in [1] (see also [2]–[3]), where D_i^0, D_i^1, and E_k are used instead of our notation s_i, t_i, and 1_k. It follows from these axioms, in particular, that for $i \le k-1$ the operation $\underset{i}{*}$ endows C_k with the structure of a category with the set C_i of objects. If $C_{n+i} = 1(C_n)$ for $i > 0$, then C is called an *n-category*. In particular, a 1-category is the same as an ordinary category. All ∞-categories form the (1-) category Cat_∞. For an ∞-category C the elements of C_i are called *i-morphisms* of C. The 0-morphisms are called *objects*.

We felt that the issue with this conjecture is closed and that this important element of "higher dimensional" mathematics had been understood.

Then in 2003, twelve years after our proof was published in English, a preprint appeared on the web in which his author, Carlos Simpson, very politely claimed that he has constructed a counter-example to our theorem.

I was busy with the work on the motivic program and very sure that our proof is correct and ignored the preprint.



arXiv:math/9810059v1 [math.CT] 9 Oct 1998

Homotopy types of strict 3-groupoids

Carlos Simpson
CNRS, UMR 5580, Université de Toulouse 3

It has been difficult to see precisely the role played by *strict* n-categories in the nascent theory of n-categories, particularly as related to n-truncated homotopy types of spaces. We propose to show in a fairly general setting that one cannot obtain all 3-types by any reasonable realization functor [1] from strict 3-groupoids (i.e. groupoids in the sense of [20]). More precisely we show that one does not obtain the 3-type of S^2. The basic reason is that the Whitehead bracket is nonzero. This phenomenon is actually well-known, but in order to take into account the possibility of an arbitrary reasonable realization functor we have to write the argument in a particular way.

We start by recalling the notion of strict n-category. Then we look at the notion of strict n-groupoid as defined by Kapranov and Voevodsky [20]. We show that their definition is equivalent to a couple of other natural-looking definitions (one of these equivalences was left as an exercise in [20]). At the end of these first sections, we have a picture of strict 3-groupoids having only one object and one 1-morphism, as being equivalent to abelian monoidal objects $(G, +)$ in the category of groupoids, such that $(\pi_0(G), +)$ is a group. In the case in question, this group will be $\pi_2(S^2) = \mathbf{Z}$. Then comes the main part of the argument. We show that, up to inverting a few equivalences, such an object has a morphism giving a splitting of the Postnikov tower (Proposition 5.3. It follows that for any realization functor respecting homotopy groups, the Postnikov tower of the realization (which has two stages corresponding to π_2 and π_3) splits. This implies that the 3-type of S^2 cannot occur as a realization.

The fact that strict n-groupoids are not appropriate for modelling all homotopy types has in principle been known for some time. There are several papers by R. Brown and coauthors on this subject, see [9], [10], [11], [12]; a recent paper by C. Berger [8]; and also a discussion of this in various places in Grothendieck [18]. Other related examples are given in Gordon-Power-Street [17]. The novelty of our present treatment is that we have written the argument in such a way that it applies to a wide class of possible realization functors, and in particular it applies to the realization functor of Kapranov-Voevodsky (1991) [20].

[1] Our notion of "reasonable realization functor" (Definition 3.1) is any functor $\Re$ from the category of strict n-groupoids to Top, provided with a natural transformation r from the set of objects of G to the points of $\Re(G)$, and natural isomorphisms $\pi_0(G) \cong \pi_0(\Re(G))$ and $\pi_1(G, x) \cong \pi_1(\Re(G), r(x))$. This axiom is fundamental to the question of whether one can realize homotopy types by strict n-groupoids, because one wants to read off the homotopy groups of the space from the strict n-groupoid. The standard realization functors satisfy this property, and the somewhat different realization construction of [20] is claimed there to have this property.

1

Then the motivic period of my life was completed and I started to work on computer proof verification and new foundations of mathematics.

The correspondence between the infinity groupoids and homotopy types re-emerged as the cornerstone of the Univalent Foundations.

And then in the Fall of 2013, less than a year ago, some sort of a block in my mind collapsed and I suddenly understood that Carlos Simpson was correct and that the proof which Kapranov and I published in 1991 is wrong.

Not only the proof was wrong but the main theorem of that paper was false!

In this story I got lucky again.

The theorem was false with the particular definition of infinity groupoids which Kapranov and I have used. There were by now various other definitions with which the statement of the theorem became correct.

The use of the Grothendieck correspondence, as it became known, in the Univalent Foundations was not endangered.

But belief in the correctness of our false theorem played an important and negative role in how I perceived, for all these years, the subject area of multidimensional category theory.

When I recognized that the theorem of the paper is false I contacted Kapranov to tell him that we need to do something about the paper and then Carlos Simpson to tell him that his preprint from 2003 is correct.

An interesting feature of this story is that Carlos Simpson did point out where in the proof, which was about 10 pages long, the mistake was. He only showed that it can not be correct by building a counter-example to the final statement.

It took me several weeks to find which particular lemma in the paper is incorrect and to find counterexamples to that lemma.

There no ending to this story yet. The question that we originally wanted to answer - how to find an algebraic definition of infinity groupoids that would satisfy the Grothendieck correspondence, remains open…

Now let us look at this story again. Kapranov and I have found a solution to the problem which we worked on - the proof of the theorem.

If the problem was to solve an equation and we would have found a solution we would have checked that it is a solution before publishing it, right?

And if it were a complex equation we would probably have checked it on a computer.

So why can not we check a solution which is a proof of a theorem?

I started to ask myself this question more than 10 years ago when the solutions, proofs, which I was inventing were becoming more and more complex and I was getting more and more worried that they may contain mistakes.

And trying to answer this question led me to my current interest in Foundations of Mathematics.

Let me explain how.

A solution to an equation would probably be a number or a collection of numbers.

Verification in this case would consist in performing some computations with these numbers and comparing the result of these computations with some other numbers.

But what should we do when the solution is a proof of a statement?

A hint can be seen from looking at the case when the problem was to solve an equation in symbolic form. For example, to find a formula for solving a general equation of the form $x^3+ax+b=0$.

How would we check the solution in this case? We would probably use some software for symbolic computation which can compute not only with numbers but also with expressions which have variables in them.

So in order to check a solution which is a proof of a statement we need to write both the statement and the proof as some kind of symbolic expressions A and T and then use some software which can compute with these expressions in such a way as to check that A is indeed a proof of T.

Encoding of statements and proofs which exist in our thoughts into symbolic expressions is called **formalization**.

Formalization is, just like programming, first of all a tool that we can use to pass on to computers some of the mental tasks which we need to perform.

But at the moment it is much less developed than programming and when I started to search, in 2003, for a formalization system that I could use to help me check my proofs I could not find any.

I decided that I need to create such a system.

The first question to answer was what was it that prevented the creation of such a system earlier?

What is involved in the creation of a formalization systems for use in mathematics?

First of all we need to have a some knowledge about how to design formal deduction systems which are for formalization what programming languages are for programming.

The theory of formal deduction systems originated, as far as I could find, with an amazing paper by Gottlob Frege from 1879 which is called "A formula language, modeled upon that of arithmetic, for pure thought".

Today it is studied mainly in Computer Science "Theory B".

BTW - it is "Theory B" not because it is less important than "Theory A" but because of a Handbook of Theoretical Computer Science which was published in two volumes "A" and "B" and the theory of formal deduction systems was discussed in the second volume.

But the theory of formal deduction systems is only one part of what we need to formalize mathematical statements and proofs.

This theory studies all possible formal deduction and computation systems. Whether a given system formally represents some actual system of reasoning which is used in the world of thought is of no concern to this theory.

For proof verification we need to construct a *particular* formal deduction system and explain how it corresponds with the mathematical objects and forms of reasoning which exist in our thoughts.

Constructing such systems and correspondences between their formal components and objects and actions in the world of our mathematical thoughts is the main task of the field which is called Foundations of Mathematics.

A formal deduction system together with a correspondence between its components and objects and actions in the world of mathematical thoughts which can be used to formalize all subject areas of mathematics is called a foundational system for mathematics or "foundations of mathematics".

The mainstream foundation of classical pure mathematics is called Zermelo-Fraenkel Set Theory with the Axiom of Choice or ZFC, by the name of the axiomatic system of predicate logic which it uses.

It was created in the first decades of the 20th century before computers came into existence and the problem of formalization of actual complex proofs became relevant. In part because of this in part because it was designed to be used with mathematics of that time it is not well adapted to the mathematics of the 21st century.

To be able to check my proofs as one can check solutions to equations I needed new foundations of mathematics.

And this is how I became interested in foundations…

Since then the story developed as follows.

I came up with the main ideas of Univalent Foundations in 2006. Only one element was missing and it took me three years to find it.

In the Fall of 2009 I gave the first public lecture about the "univalent model" - a mathematical construction which connects Martin-Lof Type Theory to ZFC in a new, unexpected, way.

By the Spring of 2010 I have recognized that I had a working version of a new formalization system based on a new foundational system that I called Univalent Foundations.

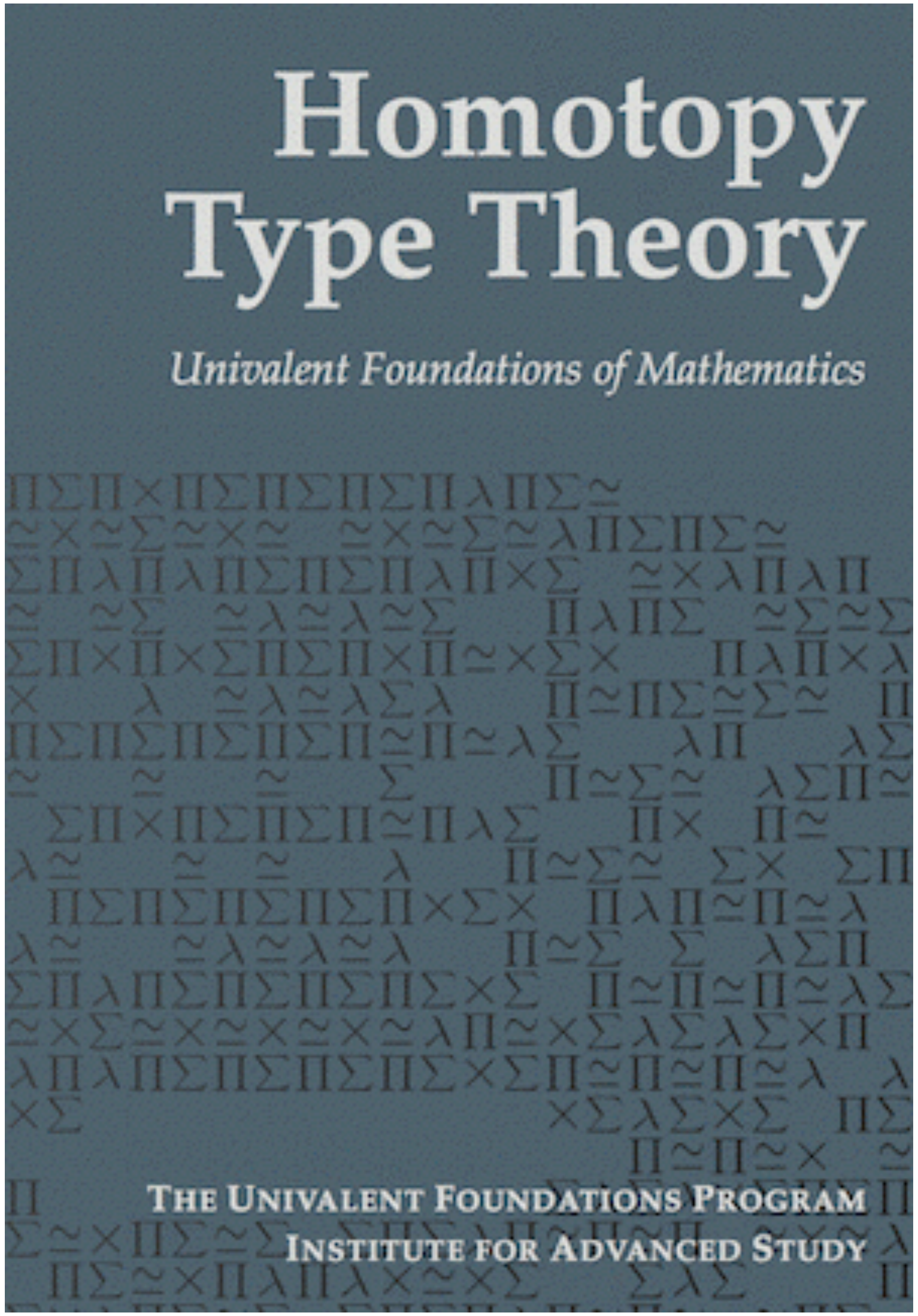
In the academic year 2012/13, Thierry Coquand, Steve Awodey and myself organized a special program at the Institute for Advanced Study in Princeton where I work.

Univalent Foundations Program, IAS, Princeton, Spring 2013.

During that year the participants of the program wrote, together, a book called "Homotopy Type Theory".

Type these words in Google and you will be directed to a website where you can learn more about this new subject and also download the book for free.

The book is a truly collective effort and as such it does not have an author. The person who did most to make this book happen and who continues to shape the content and the style of the book is Michael Schulman.



On June 21, 2014 Univalent Foundations passed another important milestone. Thierry Coquand gave a talk about Univalent Foundations at the Bourbaki Seminar in Paris. Being chosen for a presentation on this seminar is widely considered to be an important symbol of recognition in the world of pure mathematics.

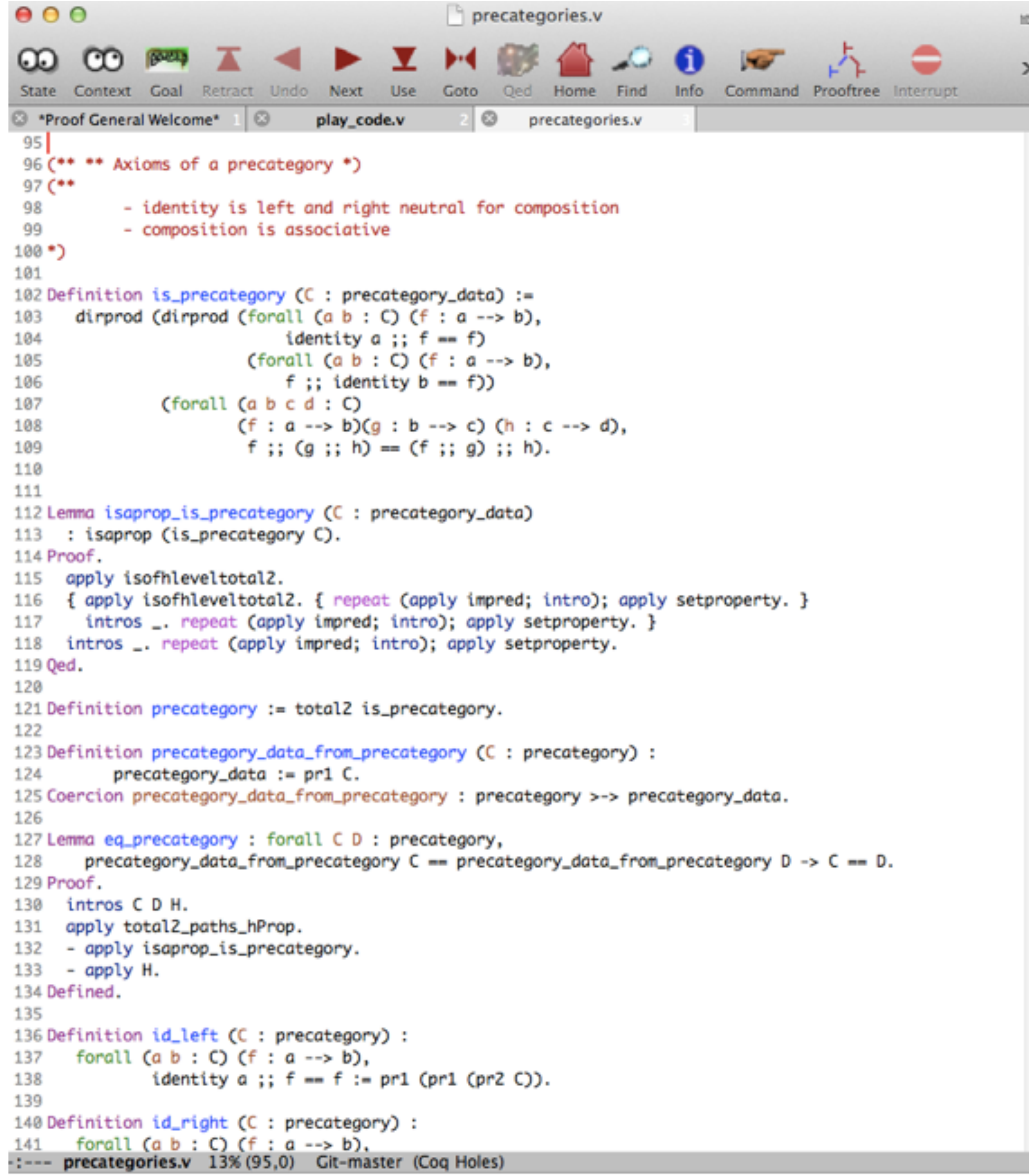
Thierry and his colleagues are also the authors of the most important advance in the mathematics of Univalent Foundations since their invention. They have constructed another model, similar to the original "univalent model" of 2009 but based on constructive mathematics.

This model opens up the way for wider Univalent Synthesis of classical and constructive mathematics…

Here is a screenshot of a session in proof assistant Coq with the code from one of the libraries of formalized mathematics that form UniMath and can be found on GitHub.

Another such group of libraries, based on a more experimental approach, is called HoTT.

More about Coq, GitHub, UniMath and HoTT can be easily found on the Web.



Such amazing stories as this one do not happen often. But little boring stories of small mistakes happen all the time.

They were happening in my life

These small mistakes waste our time and embarrass us when discovered by others.

As we get older and more established the fear of mistakes grows. We spend more time re-checking our results and become less daring in trying new things.

As I said, I am lucky that I don't have in my mathematical life a story of a mistake which destroyed an important part of my work.

I know people who are not so lucky.

And as mathematics becomes more complex the weight of mistakes of the fear of making a mistake is slowing the development of mathematics more.