

Computer-Assisted Proofs and Human Understanding

the case of Univalent Foundations

Andrei Rodin (IPRAS/SPBU)

Intellectual Systems and Computer Science, MSU, November
29 - December 3, 2021

Automated Proof-Verification

Example : 4CT

What is a proof?

Homotopical intuition in UF

Conclusion and Future Work

Automated Proof-Verification : Timeline

Automated Proof-Verification : Timeline

- ▶ Prehistory : Leibniz (17 c.), Hilbert (early 20 c.)

Automated Proof-Verification : Timeline

- ▶ Prehistory : Leibniz (17 c.), Hilbert (early 20 c.)
- ▶ 1967 (release) : Automath (Peter De Bruijn)

Automated Proof-Verification : Timeline

- ▶ Prehistory : Leibniz (17 c.), Hilbert (early 20 c.)
- ▶ 1967 (release) : Automath (Peter De Bruijn)
- ▶ since 1986 : NuPrl (released in 1986), ALF, Agda, LF, Lego, Isabelle, Coq : all (ML)TT-based.

Automated Proof-Verification : Timeline

- ▶ Prehistory : Leibniz (17 c.), Hilbert (early 20 c.)
- ▶ 1967 (release) : Automath (Peter De Bruijn)
- ▶ since 1986 : NuPrl (released in 1986), ALF, Agda, LF, Lego, Isabelle, Coq : all (ML)TT-based.
- ▶ [List of verification and synthesis tools](#) (Filippidis), overviews : Geuvers 2009, Avigad 2018 (UniMath missing)

Automated Proof-Verification : Timeline

- ▶ Prehistory : Leibniz (17 c.), Hilbert (early 20 c.)
- ▶ 1967 (release) : Automath (Peter De Bruijn)
- ▶ since 1986 : NuPrl (released in 1986), ALF, Agda, LF, Lego, Isabelle, Coq : all (ML)TT-based.
- ▶ [List of verification and synthesis tools](#) (Filippidis), overviews : Geuvers 2009, Avigad 2018 (UniMath missing)
- ▶ since 2014 : [UniMath](#)

General observation

The mainstream development in automated proofs (proof-verification) did **not** follow in Hilbert's steps :

General observation

The mainstream development in automated proofs (proof-verification) did **not** follow in Hilbert's steps :

- ▶ Typed systems instead of untyped systems ;

General observation

The mainstream development in automated proofs (proof-verification) did **not** follow in Hilbert's steps :

- ▶ Typed systems instead of untyped systems ;
- ▶ Gentzen-style (rule-based) systems instead of Hilbert-style (axiom-based) systems.

4CT : 1977

Appel, Haken and Koch 1977 : informal argument followed by 1482 special cases (configurations) checked by (and checkable only by) computer.

Gonthier 2005 : Coq version

Appel 1979 : “ [The public] clearly divided into two groups : people with more than 40 years that 'could not be convinced that a proof by computer could be correct' and 'people under forty [who] could not be convinced that a proof that took 700 pages of hand calculations could be correct ”

Philosophical discussion on 4CT (1)

Tymoczko 1979 : The computer-assisted proof of 4CT does not qualify as a mathematical proof in anything like the usual sense of the word because the computer part of this proof cannot be surveyed and verified in detail by a human mathematician, or even a group of human mathematicians. The 4CT theorem and its existing proof represents a wholly new kind of *experimental* mathematics akin to experimental natural sciences, where the computer plays the role of experimental equipment.

Philosophical discussion on 4CT (3)

Teller 1980 : Tymoczko misconceives of the concept of mathematical proof by confusing the epistemic notion of verification that something is a proof of a given statement with this proof itself. If Appel&Haken&Koch's alleged proof of 4CT is indeed a proof, this proof is unusual only in how one gets epistemic access (if any) to it but, contra Tymoczko, there is nothing unusual in the involved concept of mathematical proof itself.

Comment : According to Teller's a (formal and rigorous) mathematical proof has no *epistemic* content.

Philosophical discussion on 4CT (4)

Prawitz 2006 Teller's distinction between a proof and its verification is correct. However an epistemic access to a proof is a proper element of this proof. Hence Tymoczko is right that Appel&Haken&Koch's proof of 4CT comprises a crucial piece of empirical evidence provided by computer and is thus not deductive.

What is a proof? Hilbert & Bernays

Formal derivation in a Hilbert-style deductive system (a syntactic proof-object).

Semantic requirement : the preservice of truth (in all models).

Model-theoretic logical semantics (Hilbert-Tarski)

Under the assumption that truth pertains of existence (truth-maker realism) the model-theoretic logical semantics provides formal proofs with some *ontic content*. However it does *not* provide Hilbert's concept of formal proof with any epistemic content.

Prawitz (1979) on formal proofs

[A] valid argument must preserve truth. But the preservance of truth is clearly not a sufficient condition for validity; [...] It is not enough that the steps of a proof happen to follow from the preceding ones, it must also be seen that they follow. Nobody would consider e.g. Peano's axioms followed by Fermat's last theorem as a proof, even if in fact Fermat's last theorem follows [is formally derivable] from these axioms.

Essenin-Volpin (1970) on proofs

By proof of a judgement I mean a honest procedure making this judgement inarguable.

Artemov (2020) on Provability of Consistency

$\text{Con}(\text{PA})$ is not the best formal representation of proof of consistency of PA in PA.

Proof-theoretic logical semantics (Gentzen, Prawitz et al.)

The preservance of truth is a necessary but not sufficient condition that allows one to qualify a given formal derivation as proof. In order to qualify a formal derivation as proof some further requirements of epistemic nature (transparency, surveyability, evidential force, etc.) need to be met.

The standard notion of (formal) proof, which is devoid of any epistemic meaning, is ill-formed. The concept of proof is epistemic par excellence.

Remark (contra Vavilov)

The task of bridging the existing gap between epistemically strong mathematically proofs and typical formal proofs is not hopeless.

Local and Global Surveyability

Bassler 2006 : one should distinguish between the *local* and the *global* surveyability of mathematical proofs. The local surveyability of proof p is the property of p that makes it possible for a human to follow each elementary step of p . The local surveyability of p does not, by itself, make p epistemically transparent or surveyable in the usual intended sense. The *global* surveyability is required, which allows one to see that all steps of p taken together provide p with a sufficient epistemic force that warrants its conclusion on the basis of its premises.

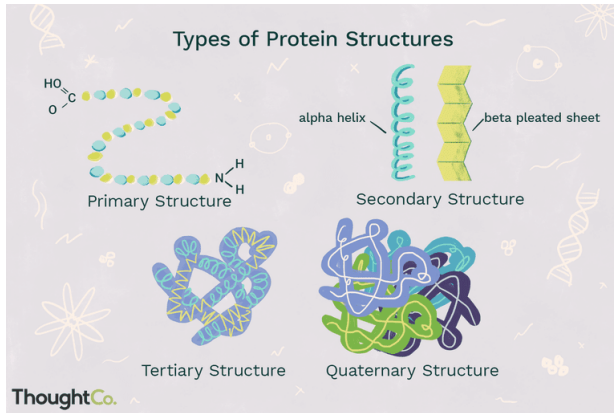
My claim in Bassler's line

Appel&Haken&Koch computer-assisted proof of 4CT is both globally surveyable (since it provides reasons why the computer-assisted verification, if successful, completes the proof) and locally surveyable (since every short piece of the computer code is written by human and can provide a full understanding of each elementary computational step)(Bassler) but (me) still lacks the surveyability at the crucial mesoscopic level, which could allow one to synthesise local syntactic steps into a global picture and thus follow the computation ignoring minute syntactic details.

Biochemical analogy : proteins

- ▶ Primary structure : the linear sequence of amino acids ;
- ▶ Secondary structure : the three-dimensional form of local fragments of proteins ;
- ▶ Tertiary structure : the global spatial shape ;
- ▶ Quaternary structure ...

Biochemical analogy : proteins



Higher Identity Types in MLTT

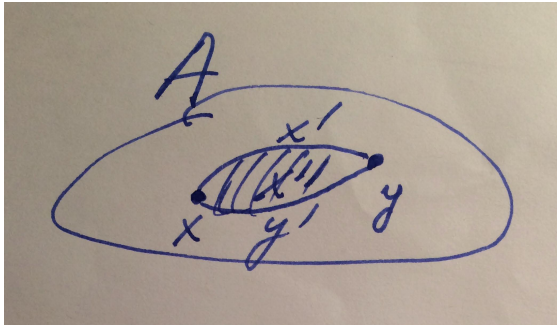
- ▶ $x', y' : x =_A y$
- ▶ $x'', y'' : x' =_{x=Ay} y'$
- ▶ ...

Homotopical interpretation of Intensional MLTT

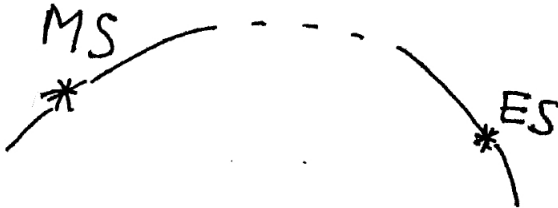
- ▶ $x, y : A$
 x, y are points in space A
- ▶ $x', y' : x =_A y$
 x', y' are paths between points x, y ; $x =_A y$ is the space of all such paths
- ▶ $x'', y'' : x' =_{x=Ay} y'$
 x'', y'' are homotopies between paths x', y' ; $x' =_{x=Ay} y'$ is the space of all such homotopies
- ▶ ...

Homotopical intuition

helps to identify a higher-level syntactic structure.



The Morning Star is The Evening Star



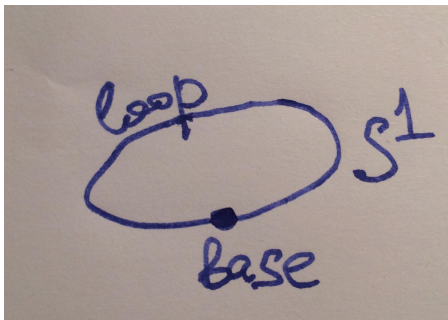
Remark :

The homotopical intuition belongs to syntax, not to semantics !
The homotopical interpretation of MLTT is on equal footing with the intuitive grasp of its symbols, not with semantic interpretation of these symbols !

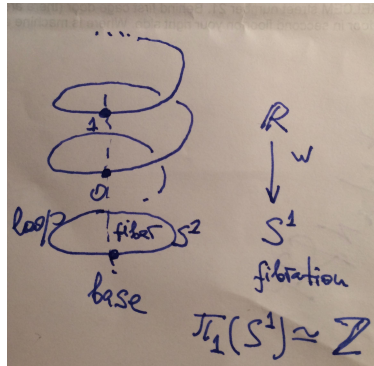
circle as higher inductive type

$$b : S^1$$

$$\text{loop} : b =_{S^1} b$$



Coq proof of $\pi_1(S^1) \simeq \mathbb{Z}$ (after Licata&Shulman 2013)



universal cover of the circle

Remark :

In this example each step of the formal proof is represented with a spatial-like (to wit homotopical) intuitive construction ; the corresponding computer code preserves this intuitive interpretation and becomes readable (at the intermediate scale) like a traditional Euclid-style geometric proof. So one can *understand* the programming code and hence the computation performed by machine.

Conclusion : Two kinds of automated proofs

Conclusion : Two kinds of automated proofs

- ▶ Computer as a magic box : Only assumptions (including axioms) and conclusions express a mathematical meaning. No meaningful proof. No meaningful reasoning.

Conclusion : Two kinds of automated proofs

- ▶ Computer as a magic box : Only assumptions (including axioms) and conclusions express a mathematical meaning. No meaningful proof. No meaningful reasoning.
- ▶ Computer as a tool extending human intuitive constructive capacities on all levels of structure (imagery, VR, ...).
Meaningful proofs and reasoning. UF supports automated of this latter sort.

Conclusion : Epistemic features of UF-based proofs

(judged against other conceptual and foundational frameworks for automated proofs)

UF supports a representation of mathematical reasoning which is :

Conclusion : Epistemic features of UF-based proofs

(judged against other conceptual and foundational frameworks for automated proofs)

UF supports a representation of mathematical reasoning which is :

- ▶ fully formal in the sense that it uses a symbolic calculus with an explicit rigorous syntax ;

Conclusion : Epistemic features of UF-based proofs

(judged against other conceptual and foundational frameworks for automated proofs)

UF supports a representation of mathematical reasoning which is :

- ▶ fully formal in the sense that it uses a symbolic calculus with an explicit rigorous syntax ;
- ▶ computer-checkable ;

Conclusion : Epistemic features of UF-based proofs

(judged against other conceptual and foundational frameworks for automated proofs)

UF supports a representation of mathematical reasoning which is :

- ▶ fully formal in the sense that it uses a symbolic calculus with an explicit rigorous syntax ;
- ▶ computer-checkable ;
- ▶ supported by a spatial (homotopical) intuition that balances local and global aspects of mathematical intuition in the traditional way (the unique feature).

Open Problems :






The UF project aims at extending the homotopical intuition over all areas of mathematics and beyond. This goal has not been achieved so far.

The above example belongs to (synthetic) Homotopy theory. It is far from being obvious that the homotopical intuition may be relevant in other areas of mathematics.

A Research Proposal :

Rewriting Euclid's *Elements* once again, this time in the UF style.

References I

-  S. Artemov, *The Provability of Consistency*, arXiv :1902.07404
-  J. Avigad and al., *Introduction to milestones in interactive theorem proving*, Journal of Automated Reasoning **61** (2018), no. 1, 1–8.
-  K. Appel and W. Haken, *Every planar map is four colorable*, Illinois Journal of Mathematics **21** (1977), no. 3, 429–567.
-  O. Bradley Bassler, *The surveyability of mathematical proof : A historical perspective*, Synthese **148** (2006), no. 1, 99–133.
-  H. Geuvers, *Proof assistants : History, ideas and future*, Sadhana **34** (2009), no. 1, 3–25.

References II



G. Gonthier, *A computer-checked proof of the four colour theorem*, 2005, [http : //research.microsoft.com/gonthier/4colproof.pdf](http://research.microsoft.com/gonthier/4colproof.pdf).



D. Hilbert and W. Ackermann, *Principles of mathematical logic*, New York : Chelsea Publishing Company, 1950.



D. Hilbert and P. Bernays, *Grundlagen der Mathematik*, Springer, 1934-1939.



D. Hilbert, *Foundations of mathematics*, J. van Heijenoort (ed.), *From Frege to Gödel : A Source Book in the Mathematical Logic* **2** (1967), 464–480.

References III



D.R. Licata and M. Shulman, *Calculating the fundamental group of the circle in homotopy type theory*,
<https://arxiv.org/abs/1301.3443>, 2013.



D. Prawitz, *Proofs and the meaning and completeness of the logical constants*, J. Hintikka, I. Niiniluoto and E. Saarinen (eds.) *Essays on Mathematical and Philosophical Logic*, Proceedings of the Fourth Scandinavian Logic Symposium and the First Soviet-Finnish Logic Conference, Jyväskylä, Finland, June 29-July 6, 1976 (Synthese Library v. 122 **1** (1979), 25–40.

References IV



———, *Proofs verifying programs and programs producing proofs : A conceptual analysis*, Deduction, Computation, Experiment : Exploring the Effectiveness of Proof (R. Lupacchini and G. Corsi, eds.), Springer, 2008, pp. 81–94.



M. Bickford R. Constable and A. Kellison, *Implementing Euclid's straightedge and compass constructions in type theory*, Annals of Mathematics and Artificial Intelligence **85** (2019), 175–192.



A. Rodin, *On constructive axiomatic method*, Logique et Analyse **61** (2018), no. 242, 201–231.

References V



———, *Two styles of axiomatization : Rules versus axioms. a modern perspective*, Bulletin of Symbolic Logic **24** (2018), no. 2, 263–264.



P. Teller, *Computer proof*, The Journal of Philosophy **77** (1980), no. 12, 797–803.



Th. Tymoczko, *The four-color problem and its philosophical significance*, The Journal of Philosophy **76** (1979), no. 2, 57–83.

Thank You !