

Computer-Assisted Proofs and Mathematical Understanding

the case of Univalent Foundations

Andrei Rodin (IPRAS/HSE)

HoTT/ UF Workshop, Internet, 5-7 July, 2020

Automated Proof-Verification

Example : 4CT

What is a proof?

Role of intuition in mathematical proofs

Homotopical intuition in UF

Conclusion and Future Work

Automated Proof-Verification : Timeline

- ▶ Prehistory : Leibniz (17 c.), Hilbert (early 20 c.)
- ▶ 1967 : Automath (N.G. De Bruijn)
- ▶ 1973 : Mizar (Andrzej Trybulec) : QED
- ▶ since mid-1980ies : NuPrl (R.L. Constable 1986), ALF, Agda, LF, Lego, Isabelle, Coq, Lean.
- ▶ since 2014 : [UniMath](#), Cubical Agda, Arend (JetBrains)

[List of verification and synthesis tools](#) (Filippidis),

Overviews : [[Gau09](#)], [[Aa18](#)] (UniMath missing)

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
(Carlo Angiuli : “Type theory is a kind of *sorcery*”);

General observation

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

- ▶ Typed systems instead of untyped systems (Carlo Angiuli : “Type theory is a kind of *sorcery*”);
- ▶ Gentzen-style (rule-based) systems instead of Hilbert-style (axiom-based) systems.

A new dimension of *axiomatic freedom* : playing with rules (both in syntax and semantics), not only with propositional axioms.

Axiomatic Method

The received concepts of axiomatic method and axiomatic theory stemming from Hilbert need, once again, a deep revision, see [Rod18b], [Rod18a].

The key idea (illuminated by HoTT/UF but also based on a historical analysis of older mathematical works including Euclid's *Elements*) :

A mathematical theory does not reduce to a system of props, (higher-order) mathematical *structures* are equally essential ! This general view does not commit one to the received *mathematical structuralism*. Cf. theorems and problems in Euclid.

4CT : 1977

Appel, Haken and Koch 1977 [[AH77](#)] : informal argument followed by 1482 special cases (configurations) checked by (and checkable only by) computer.

Gonthier 2005 [[Gon05](#)] : 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 ” (cit. by [[SP17](#)]).

Philosophical discussion on 4CT (1)

Tymoczko 1979 [[Tym79](#)] :

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 (2)

Teller 1980 [[Tel80](#)] :

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 (3)

Prawitz 2008 [[Pra08](#)] :

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 1934-39 [HB39]

Formal derivation in a Hilbert-style deductive system (a syntactic object). Semantic requirement : the preservance of truth (in all models).

Prawitz (1979) on formal proofs

[A] valid argument must preserve truth. But the preservice of truth is clearly not a sufficient condition for validity. [...]. As every examiner stresses, 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. [Pra79, p. 26]

Model-theoretic logical semantics (Tarski)

does *not* provide Hilbert's concept of formal proof with any epistemic content. Under the assumption that truth pertains of existence this semantics provides formal proofs with an unspecified *ontic content*.

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

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.

Essenin-Volpin (1970) on proofs

“By proof of a judgement I mean a honest procedure making this judgement inarguable. ” Cf. Martin-Löf 2019 at the PTS conference in Tübingen.

Intuition Expelled : Hilbert 1899

“Let us consider three distinct systems of things. The things composing the first system, we will call points ... ; those of the second, we will call straight lines ...”.

tables, chairs, and beer mugs

Intuition Vindicated : Hilbert after 1918

“The purpose of the symbolic language in mathematical logic is to achieve in logic what it has achieved in mathematics, namely, an exact scientific treatment of its subject-matter. . . . [L]ogical thinking is reflected in a [symbolic] logical calculus.” [HA50, p.1]

Intuition (partly) Vindicated : Hilbert after 1918

“No more than any other science can mathematics be founded by logic alone ; [...], certain extralogical concrete objects that are intuitively present as immediate experience prior to all thought. If logical inference is to be reliable, it must be possible to survey these objects completely [...]; the fact that they occur, that they differ from one another, and that they follow each other, or are concatenated, is immediately given intuitively [...]. [I]n mathematics [...] what we consider [as such extralogical objects] is the concrete signs themselves.” [Hil67, pp. 464-465]

Finitary Symbolic Intuition

FSI : the intuition that supports finitary manipulations with letter-like symbols.

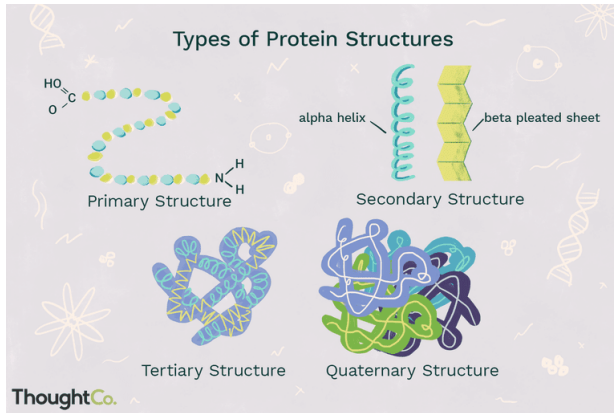
Claim (after Hilbert) : Mathematical Logic in its modern form is essentially empowered by FSI.

Finitary Symbolic Intuition : Syntax

Does FSI provide all formal proofs with a sufficient evidential force?

No, because FSI makes evident only the microscopic syntactic structure of formal proofs (that involve separate symbols and small combinations of symbols) but leaves their larger-scale macroscopic structures obscure. As a result the evidential force of long formal (symbolic) proof is typically poor (except the case when the proof is long but has very little structure of larger scales) — even if the evidential force of the corresponding informal proof is strong.

Biochemical analogy : proteins



Philosophical discussion on 4CT (4)

O. Bradley Bassler 2006 :

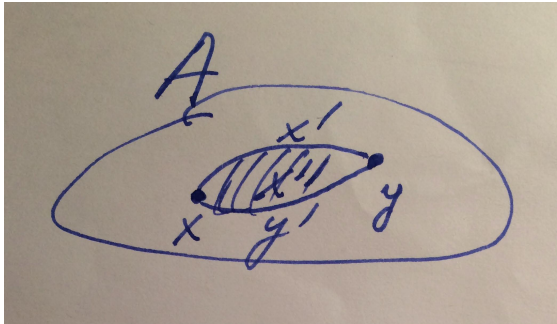
one should distinguish between the *local* and the *global* surveyability of mathematical proofs. The local surveyability of proof p is the property of p that makes it possible for a human to follow each elementary step of p . The local surveyability of p does not, by itself, make p epistemically transparent 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. [Bas06]

My claim in Bassler's line

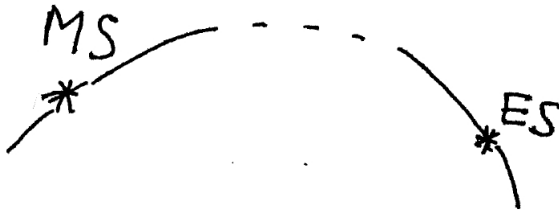
Appel&Haken&Koch computer-assisted proof of 4CT is both globally surveyable (since it explains why the computer-assisted verification, if successful, completes the proof) and locally surveyable (since every short piece of the computer code is written by human and can provide a full understanding of each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

Homotopical intuition

helps to identify and conceive of higher-level structures.



The Morning Star is The Evening Star



Venus Homotopically <http://philsci-archive.pitt.edu/12116/>

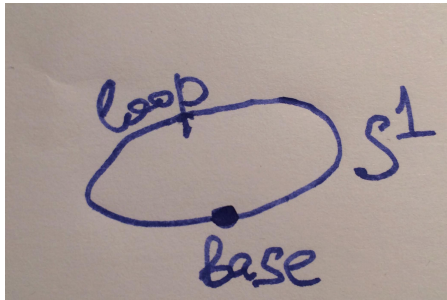
Remark :

The homotopical interpretation of MLTT is on equal footing with fixed logical semantics of CPL and CFOL syntax, not with various models of Hilbert-style formal theories such as Hilbert's axiomatic theory of Euclidean geometry ! HoTT supports Lawvere's view according to which "Logic is a special case of geometry" (Lawvere 1970).

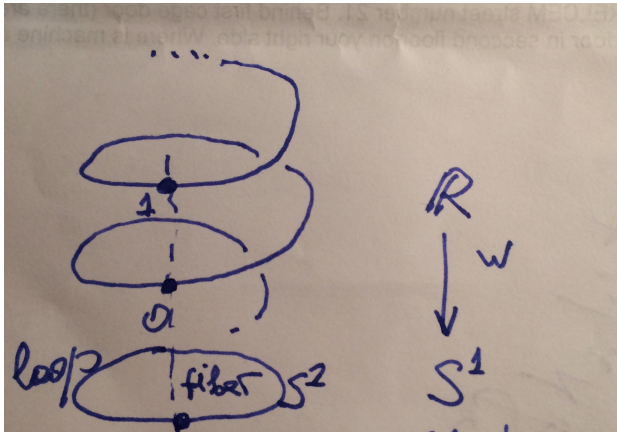
circle as higher inductive type

$$b : S^1$$

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



Coq proof of $\pi_1(S^1) \simeq \mathbb{Z}$ (after Licata&Shulman 2013)
 [LS13]



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 preserve this intuitive interpretation (beyond FSI) and becomes readable (at the intermediate scale) like a traditional Euclid-style geometric proof.

Automated Proof-Verification

Example : 4CT

What is a proof?

Role of intuition in mathematical proofs

Homotopical intuition in UF

Conclusion and Future Work

Conclusion : Two kinds of automated proofs

Conclusion : Two kinds of automated proofs

- ▶ Computer as a magic box : Hilbert-style deductive systems. 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 : Hilbert-style deductive systems. 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 (or related intuition : cf. Directed TT) over all areas of mathematics and beyond. This goal has not been achieved so far.

The above example belongs to Homotopy theory. It is far from being obvious that the homotopical intuition may be relevant in other areas of mathematics. The expressive power of MLTT and its descendents appears to be sufficient for expressing all contents of interest. Can the homotopical intuition go along with all relevant MLTT-based formal representations or it needs and upgrade or replacement ?

Automated Proof-Verification

Example : 4CT

What is a proof?

Role of intuition in mathematical proofs

Homotopical intuition in UF

Conclusion and Future Work

Research Proposals :





Research Proposals :

- ▶ Rewriting Euclid's *Elements* (once again), this time in the UF style. Cf. the attempt by Mark Bickford and co-authors [RCK19].





Research Proposals :

- ▶ Rewriting Euclid's *Elements* (once again), this time in the UF style. Cf. the attempt by Mark Bickford and co-authors [RCK19].
- ▶ Developing a software that supports a visualisation of UF-based constructions (inferences).



References : I

-  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 Bessler, *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.
-  G. D. Secco and L.C. Pereira, *Proofs versus experiments : Wittgensteinian themes surrounding the four-color theorem*, How Colours Matter to Philosophy (Marcos Silva, ed.), Springer, 2017, pp. 289–307.
-  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 !