Computer-Assisted Proofs and Mathematical Understanding

the case of Univalent Foundations

Andrei Rodin (IPRAS/HSE)

Constructive Knowledge 12, Internet, July 3, 2020

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.

Hilbert style :

Hilbert style :

- A minimal set of syntactic rules : substitution, modus ponens (enough for CPL), additional rules for quantifier (for CFOL) ;

Hilbert style :

- A minimal set of syntactic rules : substitution, modus ponens (enough for CPL), additional rules for quantifier (for CFOL) ;
- "Logical axioms" aka tautologies that generate all other tautologies (via the above rules) ; special axioms, e.g. ZFC axioms.

Remark

The idea behind the Hilbert-style formal representation of theories is to represent a given theory T as a set of true sentences with a distinguished subset of *axioms* s.t. other T-sentences are syntactically derived from the axioms ; the intended semantics of this derivation is that of *logical inference*. In short, the idea is to distinguish in T a small set of T-truths called axioms s.t. all other T-truths would *logically* follow from the axioms. The meaning of word "logically" in this context will be explained in what follows.

Gentzen style :

Gentzen style :

- A large set of syntactic rules and no axioms : Natural Deduction, Sequent Calculus, MLTT, CTT, . . . ;

Gentzen style :

- A large set of syntactic rules and no axioms : Natural Deduction, Sequent Calculus, MLTT, CTT, . . . ;
- ND, SC and MLTT have an intended *logical* semantics (albeit not the same as in the above case) ; MLTT and CTT also admit extra-logical semantics via HoTT.

Remarks :

Remarks :

- The representation of specific non-logical theories in Gentzen style (via syntactic rules with non-logical semantics) is underdeveloped in mathematics and in philosophical logic but is routinely used in CS and its applications ("expert systems" of older generations).

Remarks :

- The representation of specific non-logical theories in Gentzen style (via syntactic rules with non-logical semantics) is underdeveloped in mathematics and in philosophical logic but is routinely used in CS and its applications ("expert systems" of older generations).
- Gentzen argued that the rule-based formal presentation of logical principles is more "natural" (better approximates the current practice ?). Gentzen-style formal systems are easier (to wit more straightforwardly) are implemented computationally, i.e., translated into a program code.

4CT : 1977

Appel, Haken and Koch 1977 : informal argument followed by1482 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 (2)

Detlefsen&Luker 1980 : The difference between the computer-assisted proof of 4CT by Appel&Haken&Koch and traditional mathematical proofs is less dramatic than Tymoczko thinks. For traditional mathematical proofs quite often, and perhaps even typically, comprise some "blind" symbolic calculations, like one that is needed in order to compute the product $50 \times 101 = 5050$. The extent to which a given symbolic calculation is epistemically transparent or blind, is a matter of degree, not a matter of principle.

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 object). Semantic requirement : the preservance of truth (in all models, more below).

Prawitz (1979) on formal proofs

[A] valid argument must preserve truth. But the preservance of truth is clearly not a sufficient condition for validity ; 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 from these axioms. 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.

Essenin-Volpin (1970) on proofs

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

Model-theoretic logical semantics (Hilbert-Tarski)

DEF (Tarski) :

$A_1 \ldots A_n \models B$ (read "B is a logical consequence of $A_1 \ldots A_n$") just in case all models of $A_1 \ldots A_n$ (= all interpretations under which $A_1 \ldots A_n$ are true) are also models of B (the "preservance of truth").

soundness : if $A_1 \ldots A_n \vdash B$ then $A_1 \ldots A_n \models B$ (every syntactic derivation represents some logical inference) ;

semantic completeness : if $A_1 \ldots A_n \models B$ then $A_1 \ldots A_n \vdash B$ (every logical inference is represented by some syntactic derivation).

Remark

Tarski's model-theoretic logical semantics (semantics of syntactic derivations) 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.)

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, surveyablitiy, 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.

Proof-theoretic logical semantics (cntd)

Ex : MLTT and its intended semantics ("meaning explanation").

Remark (contra Vavilov) : The task of bridging the existing gap between epistemically strong mathematically proofs and typical formal proofs is not hopeless. Cf. Euclid, UF.

Axiomatic styles and logical semantics

Hilbert-style formal systems more naturally admit a model-theoretic semantics ; Gentzen-style formal systems more naturally admit a proof-theoretic semantics. This is because $A_1 \ldots A_n \models B$ is a (meta-theoretical) sentence ; it provides no semantics for syntactic *rules* stricto sensu. By contrast PTS prescribes to these rules certain epistemic meaning.

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.

Intuition (partly) Vindicated : Hilbert after 1918

No more than any other science can mathematics be founded by logic alone ; rather, as a condition for the use of logical inferences and the performance of logical operations, something must already be given to us in our faculty of representation, 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.

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

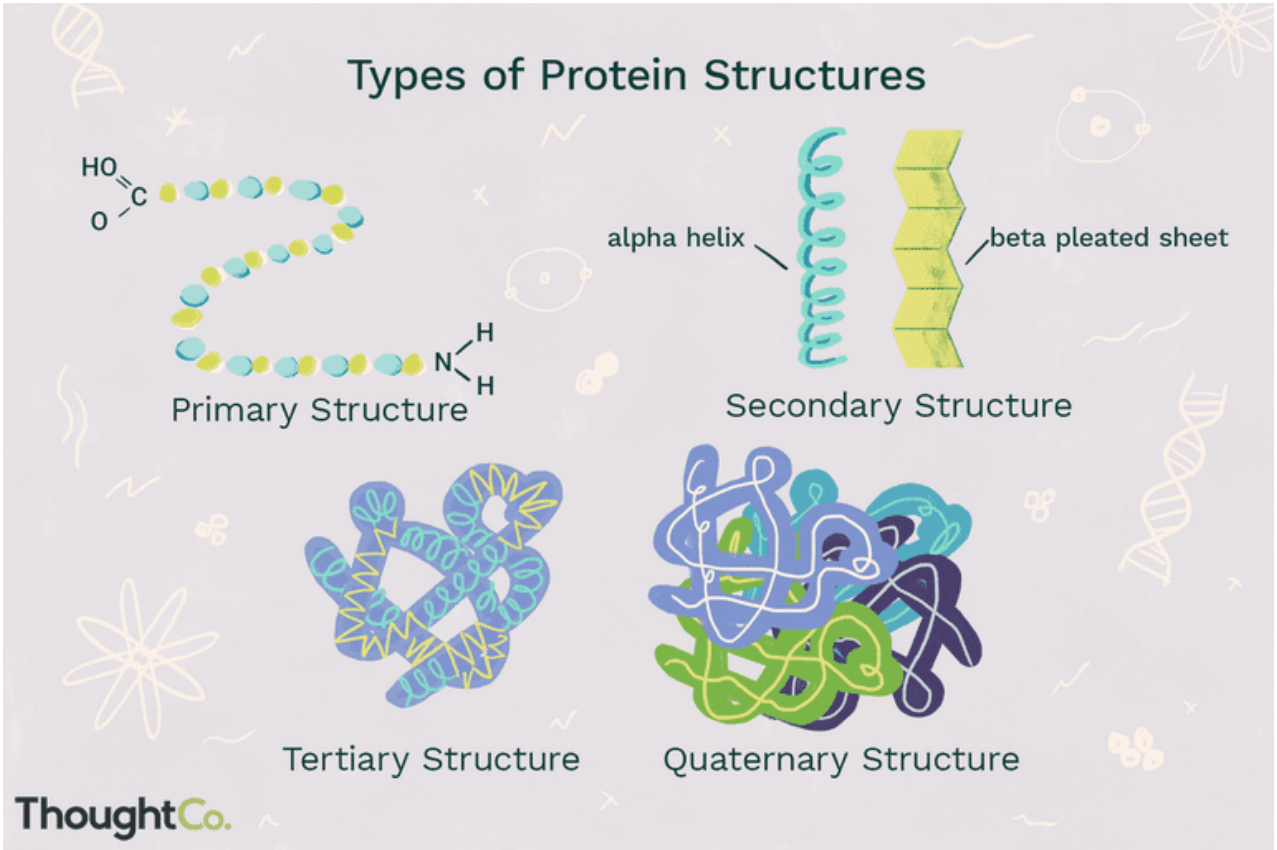
Does FSI provide all formal proofs with a sufficient evidential force ?

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

- 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



Finitary Symbolic Intuition : Semantics

Accordingly, FSI facilitates semantic interpretation of the microscopic syntactic structures (meaning of logical and non-logical constants, meaning of short symbolic expressions such as axioms of ZFC) but not semantic interpretation of larger syntactic structures, which typically are present in non-trivial mathematical proofs.

Proof structures

The macroscopic proof structures can be made evident via other kinds of mathematical intuition including geometrical, algebraic and other varieties of intuition (UF below).

Proof structures

The macroscopic proof structures can be made evident via other kinds of mathematical intuition including geometrical, algebraic and other varieties of intuition (UF below).

The macroscopic proof structures not only help to discover new knowledge (heuristically relevance) but also help to justify it. Therefore these proof structures make part of the knowledge proper but not only of the context of its discovery.

Philosophical discussion on 4CT (5)

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 serveyability 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 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.

Higher Identity Types in MLTT

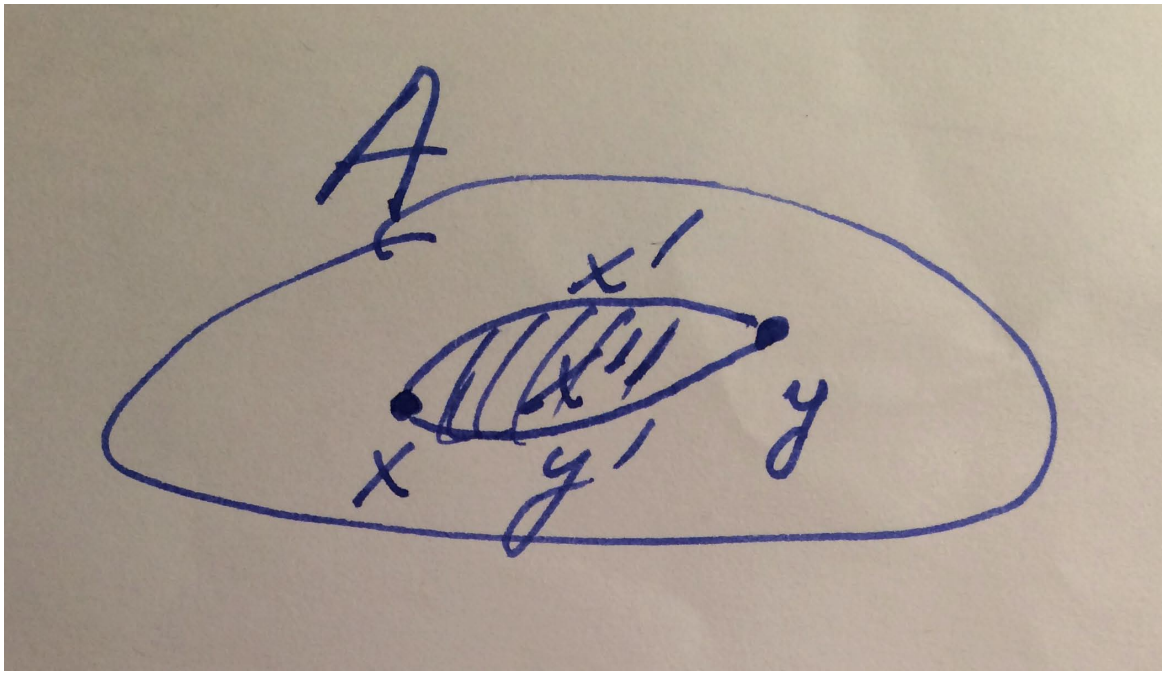
- $x', y' : x =_A y$
- $x'', y'' : x' =_{x=_A y} y'$
- $\ldots$

Homotopical interpretation of Intensional MLTT

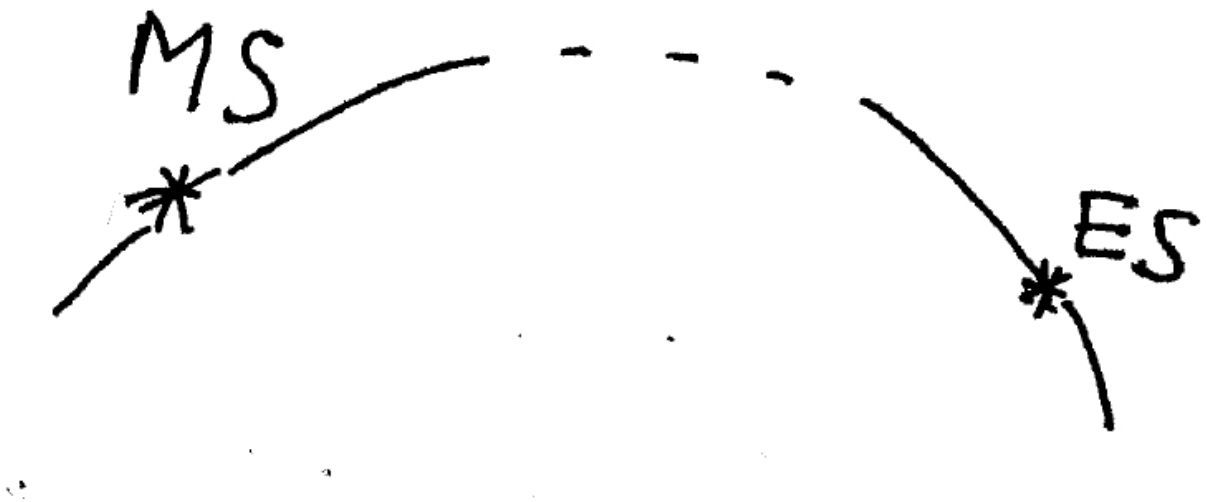
- $x, y : A$
  x, y are points in space A
- $x', y' : x =_A y$
  x', y' are paths between points x, y ; $x =_A y$ is the space of all such paths
- $x'', y'' : x' =_{x=_A y} y'$
  x'', y'' are homotopies between paths x', y' ; $x' =_{x=_A y} y'$ is the space of all such homotopies
- ...

Homotopical intuition

helps to identify a higher-level syntactic structure.

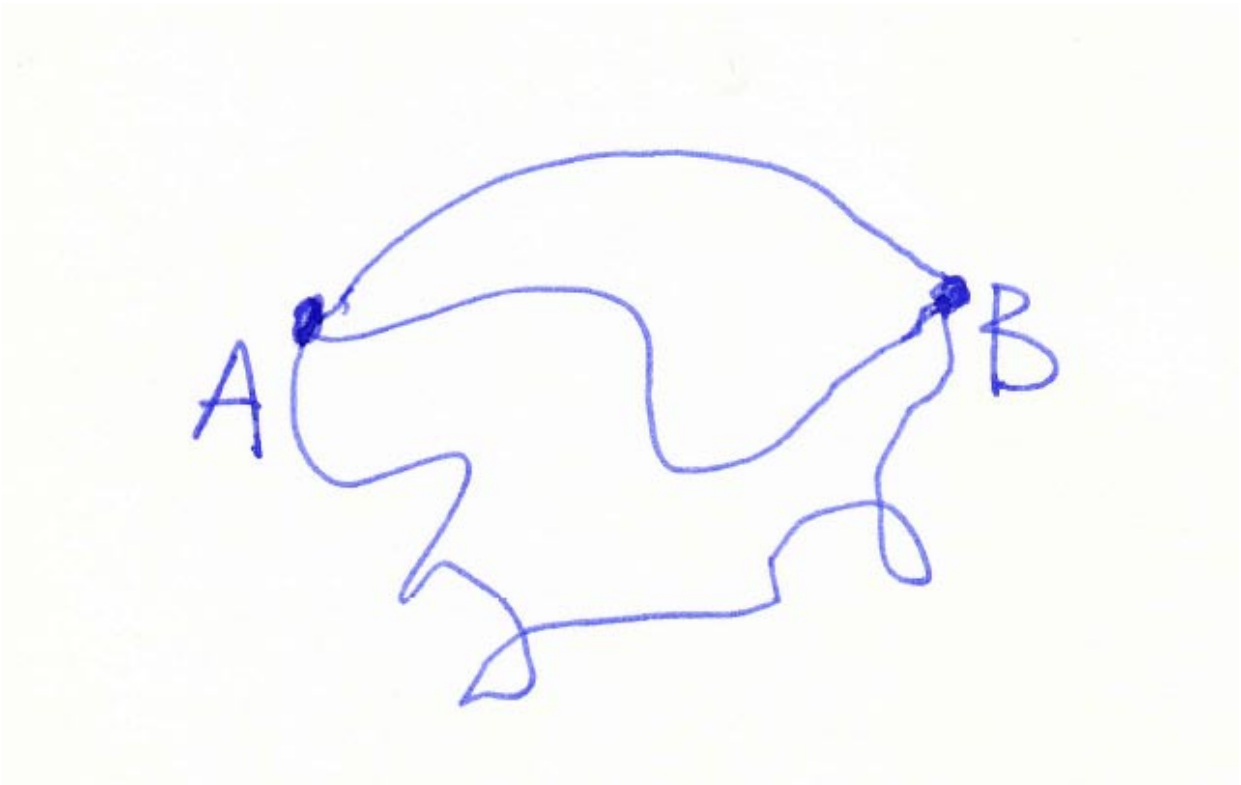


The Morning Star is The Evening Star



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

Quantum paths



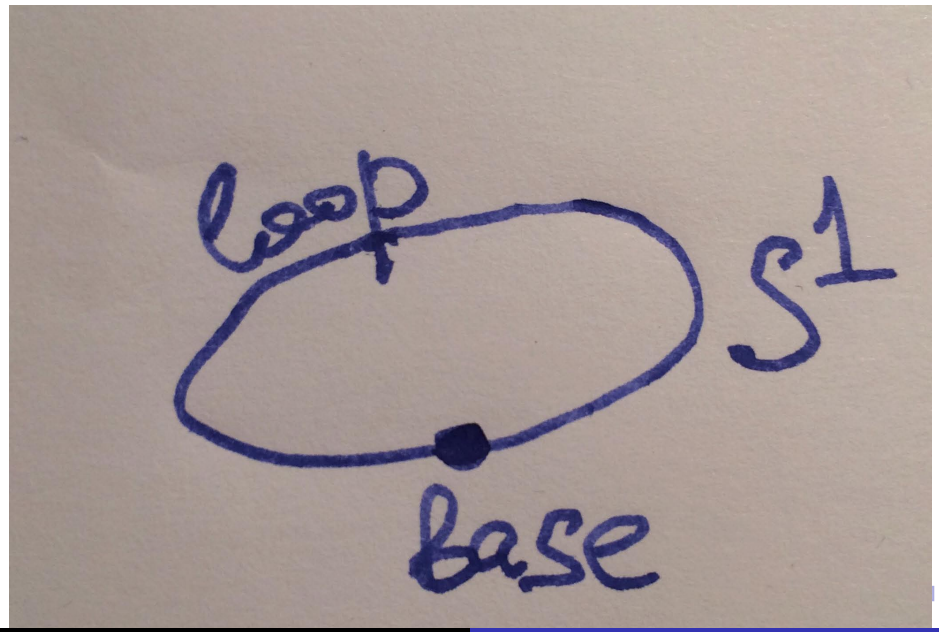
Remark :

The homotopical intuition belongs to syntax (along with the symbolic intuition), not to semantics ! The homotopical interpretation of MLTT is on equal footing with logical interpretation of CPL and CFOL syntax, not with the interpretation of of Hilbert-styles formal axioms for geometry ! Thus HoTT supports a very different on the relationships between logic and geometry. “Logic is a special case of geometry” (Lawvere 1970).

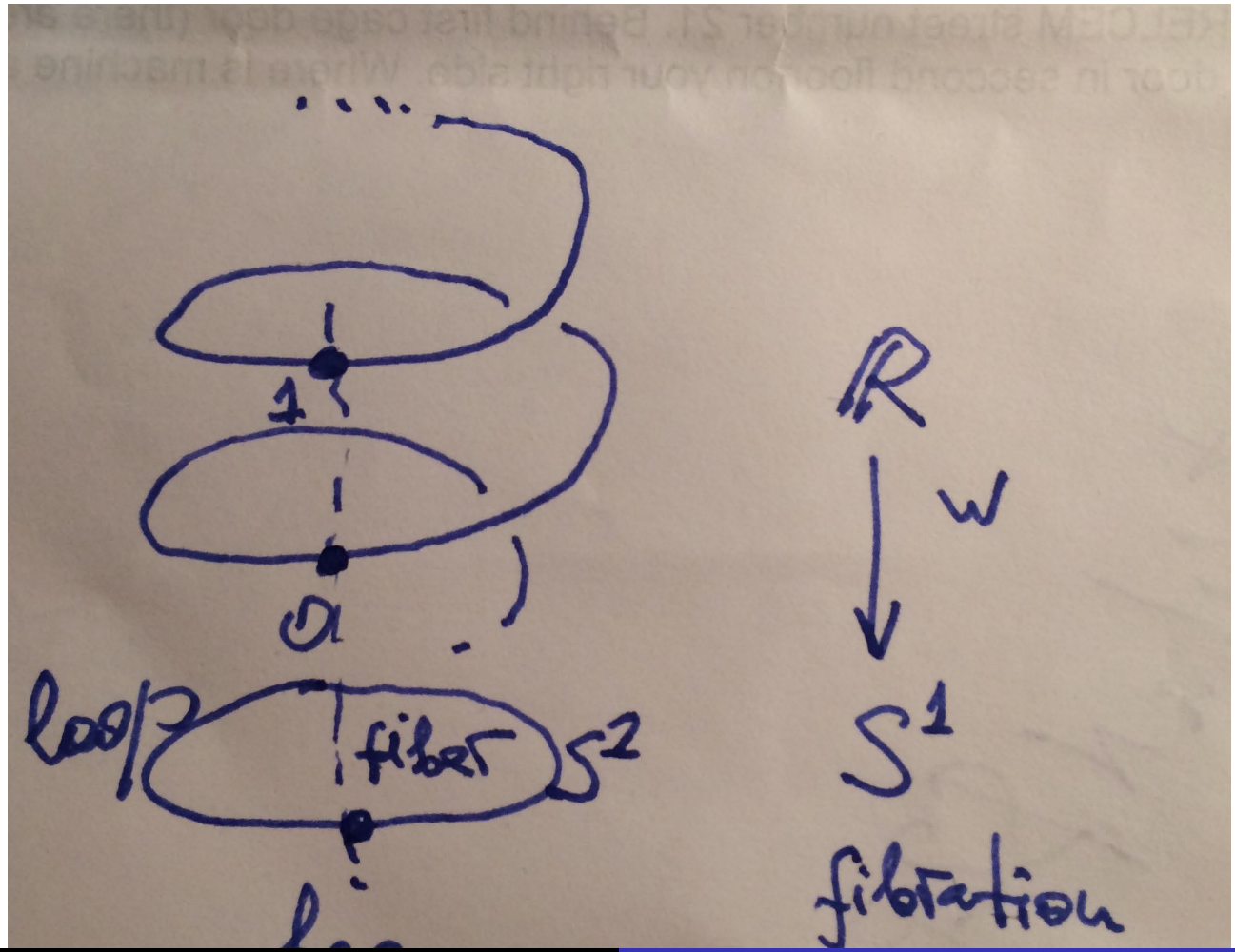
circle as higher inductive type

$$b : S^1$$

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



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



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.

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 an 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 an 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 an 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 an 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 descenders 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 ?

A Research Proposal :

What about rewriting Euclid's *Elements* once again, this time in the UF style ?

Thank You !