Formal Proof-Verification and Mathematical Intuition

the case of Univalent Foundations

Andrei Rodin (IPRAS/HSE)

CLMPST 2019, Prague, August 5 -10, 2019

Hilbert & Bernays

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

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.

Aristotle on proofs

By demonstration I mean a syllogism productive of scientific knowledge, a syllogism, that is, the grasp of which is eo ipso such knowledge. . . . [T]he premisses of demonstrated knowledge must be [i] true, [ii] primary, [iii] immediate, [iv] better known than and [v] prior to the conclusion, which is further related to them as effect to cause. Unless these conditions are satisfied, the basic truths will not be appropriate to the conclusion. Syllogism there may indeed be without these conditions, but such syllogism, not being productive of scientific knowledge, will not be demonstration. (An. Post. Book 1, ch.2, transl. G.R.G. Mure)

Essenin-Volpin (1970) on proofs

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

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 . . . .

Ax. 1 and the projective duality

Axiom 1.1 : Two distinct points A, B always completely determine a straight line l.

("points" as straight lines and "straight lines" as points)

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

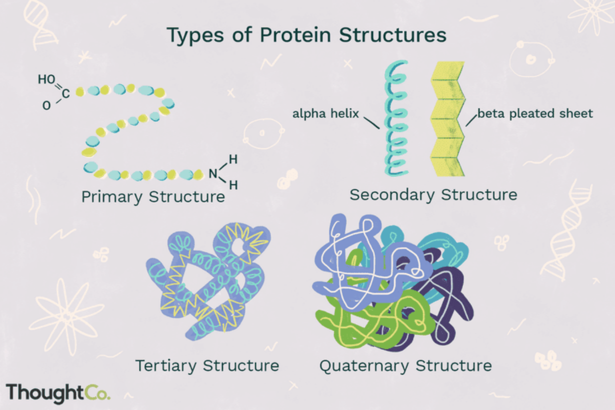
Does FSI provide all formal proofs with a sufficient evidential force ?

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.

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

Remark :

The homotopical intuition belongs to syntax (along with the symbolic intuition), not to semantics !

The Morning Star is The Evening Star

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

circle as higher inductive type (after Shulman)

$$b : S^1$$

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

$$\pi_1(S^1) \simeq \mathbb{Z}$$

Voevodsky 2010 on the purposes of automated proof-verification

Ideally, a paper submitted to a journal should contain text for human readers integrated with references to formalised 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 [2] the paper is interesting and [1] that the formalisations of the statements correspond to their intended meaning.

Remarks :

Unless the formalisations of the statements express a meaning they do not represent any mathematical contents (beyond the syntactic contents).

Remark :

Interesting mathematical contents are typically expressed with higher-level rather than lower-level syntactic structures.

Two kinds of APV

Two kinds of APV

- 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.

Two kinds of APV

- 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 APV of this latter sort.

Conclusion

A lot remains to be done !

Thank You !