Computer-Assisted Proofs and Mathematical Understanding: the case of Univalent Foundations

Andrei Rodin (andrei@philomatica.org)

Institute of Philosophy, Russian Academy of Sciences and Higher School of Economics, Moscow

The computer-assisted proof of Four Colour Map theorem (4CT) published by Kenneth Appel, Wolfgang Haken and John Koch back in 1977 [1] prompted a continuing philosophical discussion on the epistemic value of computer-assisted mathematical proofs [8],[7],[3],[2],[6]. We briefly overview this discussion and then show how the Univalent Foundations of Mathematics (UF) meet some earlier risen epistemological concerns about computer-assisted proofs and offer new possibilities for filling the gap between computer-assisted and traditional mathematical proofs. We illustrate the argument with a proof of basic theorem in Algebraic Topology formalised in UF and implemented in AGDA [5].

1 Overview

In their proof of 4CT Appel and his co-authors used a low-level computer code written specifically for this purpose in order to check one by one 1482 different cases (configurations), which was not feasible by hand. More recently a fully formalised version of Appel&Haken&Koch's proof has been implemented with Coq [4]. A philosophical discussion on this proof has been started by Thomas Tymoczko [8] who argued that the computer-assisted proof of 4CT did not qualify as mathematical proof in anything like the usual sense of the word because the computer part of this proof could not be surveyed and verified by a human mathematician.

Paul Teller in his response to Tymoczko [7] argues that 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, which under Teller's general conception of mathematical proof has no intrinsic epistemic content.

Commenting on Teller's analysis in 2008 Dag Prawitz [6] approves on Teller's distinction between a proof and its verification. However since Prawitz's conception of proof unlike Teller's is essentially epistemic, Prawitz comes to a different conclusion. Contra Teller and in accordance with Tymoczko Prawitz argues that *if* Appel&Haken&Koch's alleged proof is indeed a proof then it comprises a crucial empirical evidence provided by computer and thus is not deductive.

Mic Detlefsen and Mark Luker in their response to Tymoczko [3] quite convincingly show that the difference between the computer-assisted proof of 4CT and traditional mathematical proofs is less dramatic than Tymoczko says. How much a given symbolic calculation is epistemically transparent or blind, is, according to Detlefsen&Luker, a matter of degree rather than a matter of principle.

2 Local and Global Surveyability of Mathematical Proofs

O. Bradley Bassler [2] makes a valuable distinction between *local* and *global* surveyability of mathematical proofs. By local surveyability of proof p Bassler understands the property of p that makes it possible for a human to follow each elementary step of p. Bassler argues that local surveyability of p does not, by itself, make p epistemically transparent or surveyable in the usual intended sense because on the top of local surveyability it requires at least a minimal *global* surveyability, 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.

When one applies the distinction between local and global surveyability in the analysis of Appel&Haken&Koch's proof of 4CT the resulting picture is more complex than one suggested by Tymoczko [8]. The computer part of the proof is fully locally surveyable in the sense that each piece of the computer code can be checked and interpreted by human (since it is written by human). Informal arguments explaining why the computation so encoded, if performed correctly, completes the proof of the theorem, provide a global survey of this proof. What this proof still lacks is rather an expected surveyability and traceability at the intermediate scale between the general understanding of what the given computation computes and the low-level computational steps expressed with the program code.

3 Univalent Foundations and Spatial Intuition

Homotopy Type theory (HoTT) allows one to think of formal derivations in Martin-Löf Type theory (MLTT) as homotopical spatial constructions . When this base calculus or its fragment is implemented in the form of programming code then the same homotopical interpretation along with the associated spatial intuition applies to the code. This spatial (homotopical) intuition makes formal symbolic derivations and the corresponding programming code humanly surveyable in a new way: on the top of the *local* surveyability that allows one to control elementary steps of the process, and in addition to the high-scale *global* surveyability that provides one with a general understanding of the resulting construction, the homotopical spatial intuition provides an epistemic access to the intermediate mesoscopic level of this construction, which allows one to follow and control all significant steps of formal reasoning ignoring its minute details. Such an intuitive reading of the formalism bridges the gap between the rigour formal representation of mathematical reasoning with a logical calculus, on the one hand, and the conventional representations of mathematical reasoning, which typically heavily use various symbolic means of expression without strict syntactic rules, on the other hand. Thus HoTT supports a representation of mathematical reasoning in general and mathematical proof in particular, 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 (syntactic) and global (conceptual) aspects of mathematical proofs in the traditional way.

A simple (but not trivial) example of mathematical proof represented in this way is found in [5]. It is a proof of basic theorem in Algebraic Topology according to which the fundamental group $\pi_1(S^1)$ of (topological) circle is S^1 (isomorphic to) the infinite cyclic group $\mathbb{Z}$, which is canonically represented as the additive group of integers.

Let *base* be a point of given circle S^1 (the base point). This judgement is formally reproduced with the MLTT syntax as formula

$$b : S^1$$

Then loops associated with this base point are terms of form:

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

The resulting formal proof and its implementation in a programming code are interpretable in terms of such intuitive spatial (homotopical) constructions all the way through. This feature allows a human to follow this proof without paying attention to tedious syntactic details verified by computer.

4 Conclusion

Computer-assisted mathematical proofs designed with the UF-based approach, unlike other computer-assisted proofs, do not appear as "black box proofs" where significant parts of the argument remain epistemically opaque and are replaced by non-deductive empirical evidences. This feature makes UF-based proofs similar to traditional mathematical proofs in accordance with the general line of Detlefsen&Luker's argument [3].

References

[1] K. Appel and W. Haken. Every planar map is four colorable. *Illinois Journal of Mathematics*, 21(3):429–567, 1977.

[2] O. Bradley Bassler. The surveyability of mathematical proof: A historical perspective. *Synthese*, 148(1):99–133, 2006.

[3] M. Detlefsen and M. Luker. The four-color theorem and mathematical proof. *Journal of Philosophy*, 77(12):803–820, 1980.

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

[5] D.R. Licata and M. Shulman. *Calculating the Fundamental Group of the Circle in Homotopy Type Theory*. https://https://arxiv.org/abs/1301.3443, 2013.

[6] D. Prawitz. Proofs verifying programs and programs producing proofs: A conceptual analysis. In R. Lupacchini and G. Corsi, editors, *Deduction, Computation, Experiment : Exploring the Effectiveness of Proof*, pages 81–94. Springer, 2008.

[7] P. Teller. Computer proof. *The Journal of Philosophy*, 77(12):797–803, 1980.

[8] Th. Tymoczko. The four-color problem and its philosophical significance. *The Journal of Philosophy*, 76(2):57–83, 1979.