# NOTES

## COMPUTER THEOREM PROVING AND HoTT

*Joe Leslie-Hurd*[1] *and G.M*[c]*C. Haworth*[2]

Portland, Oregon, USA and Reading, UK

ABSTRACT

Theorem-proving is a one-player game. The history of computer programs being the players goes back to 1956 and the 'LT' LOGIC THEORY MACHINE of Newell, Shaw and Simon. In game-playing terms, the 'initial position' is the core set of axioms chosen for the particular logic and the 'moves' are the rules of inference. Now, the Univalent Foundations Program at IAS Princeton and the resulting 'HoTT' book on Homotopy Type Theory have demonstrated the success of a new kind of experimental mathematics using computer theorem proving.

The essence of mathematics is to prove theorems. The logicians do so within formal systems of symbolic logic and proceed from a chosen alphabet of symbols and initial set of axioms via a chosen set of rules of inference. In the language of game-playing, the axiom set is the initial position of a game and the inference rule set is the set of allowable moves of the game.

The first example of a computer program in the role of the player, the theorem prover, was the 'LT' LOGIC THEORY MACHINE of Newell, Shaw and Simon (1957). LT even found some novel proofs in proving 38 of the first 52 theorems of Whitehead and Russell's *Principia Mathematica* (1910), q.v. the appendix. The program, demonstrated at the 1956 Dartmouth Artificial Intelligence workshop, is one of the first true AI programs.[3]

*Principia Mathematica* was inspired by the earlier work of Gottlob Frege (1884, 1893), now regarded as one of the fathers of modern logic. Russell sought to repair the foundations of all mathematics after discovering that Frege's formulation of set theory allowed the existence of paradoxical sets, specifically 'the set *R* of sets which do not belong to themselves'. Gödel's Incompleteness Theorem (1931) proved that any formal logic system had its limits and that there will always be mathematical statements which can be either adopted or denied in new axioms without creating contradictions. Today, mathematics avoids the Russell set theory paradoxes by, for example, the adoption of 'ZFC' Zermelo-Fraenkel set theory with the Axiom of Choice.

Computers have now contributed more to mechanized proof (Mackenzie, 2001) than a few undiscovered elegancies in Propositional Calculus. They have assisted proofs of the '4CC' Four-Colour Conjecture (Appel et al., 1977a,b) and thereby raised questions about the nature of proof and verifiability (Hurd and Haworth, 2010) which had until then been assured by a social process (Lakatos, 1976). They have proved the Robbins conjecture with EQP (Mann, 2003; Sutcliffe, 2012), and generated formal proofs using the proof-assistant COQ of 4CC (Gonthier, 2008) and of the Feit-Thompson theorem (Gonthier, 2013). Today, computers are verifying aspects of the web and critical algorithms implemented in hardware and/or software.

The adoption of computer theorem proving has created a demand for machine-checked proofs of interesting theorems to be understandable by the mathematics community also. Further, there is a constant demand to improve interactive theorem-proving, analogous to Kasparov's Advanced Chess, where a human guides the search for a proof by invoking powerful automatic proof tactics. This suggests that the foundations of mathematics should be revisited, at least to create a cleaner base of concepts and notation for both man and machine.

There is an instructive parallel for such a revisit in the scientific world. Today's requirements to unify and advance the measurement of quantities have impelled the BIPM.CCU,[4] see Figure 1, to completely overhaul

[1] Intel Corporation, Portland, Oregon, USA. email: joe@gilith.com.
[2] The University of Reading, Berkshire, UK, RG6 6AH. email: guy.haworth@bnc.oxon.org.
[3] Davis' Presburger Arithmetic algorithm, and checkers programs by Strachey and Arthur Samuel were earlier.
[4] BIPM.CCU: the Bureau International des Poids et Mesures, Comité Consultatif des unités, http://www.bipm.org/

the definitions of the units of the Système International. The 'New SI' will be based exclusively on the fundamental constants of physics (Mills et al., 2011) rather than on a set of artifacts and prototypes. The latter have over time included the Earth (for its size and rotation), one litre of water (for its mass and triple point), the mètre des Archives, the 'IPM' International Prototype Metre,[5] the kilogramme des Archives and the 'IPK' International Prototype Kilogramme. Science, engineering and technology can be no better than the measurement system on which they are based, and a New SI requires the world's leading scientists to collaborate at the frontiers of science if new levels of measurement accuracy are to be achieved.[6]

**Figure 1.** The 20th meeting of the BIPM.CCU on the definitions of the units of the SI (2010).

For the last year, the 'IAS' Institute for Advanced Studies in Princeton has hosted, see Figure 2, over sixty mathematicians working together on the Univalent Foundations Program, an initiative to define a new foundation for mathematics. Remarkably, this has already resulted in the publication of a book (Shulman, 2013; UFP, 2013), its production being assisted by advanced software for collaboration and the checking of mathematical proofs. In this case, the answer to the question 'How many mathematicians does it take to write a 600 page book in less than half a year?' would appear to be in the region of 35 to 65.

Homotopy Type Theory (HoTT), introduced by Fields Medallist Vladimir Voevodsky, marries concepts from topology and logic to precisely define 'What is a mathematical proof?', a question which must be answered to uncover faulty proofs that threaten the consistency of mathematics. For this reason logic is sometimes rather unflatteringly called the hygiene of mathematics, but as Gödel and Turing showed, there are intrinsic limits which mean that no logic can provide a complete and consistent foundation for all mathematical truth.

The 20th century saw the development of ZFC set theory, which today is the standard foundation of mathematics. Sets are just unordered collections of elements $\{\boldsymbol{x}, \boldsymbol{y}, \ldots\}$, and all familiar mathematical objects such as integers or permutations have a representation in pure set form. The gold standard of a mathematical proof is that (in principle) it could be expressed entirely in the language of sets, reasoning using the ZFC axioms. These include the notorious Axiom of Choice, which can be used, among other paradoxes, to cut up a disc into five pieces and then reassemble those pieces into two discs that are the same size as the original (Banach and Tarski, 1924).

HoTT is an alternative foundation that is based on integrating concepts from topology into a typed logic which avoids the need for ZFC set theory and its troublesome axioms. In a nutshell, (i) types $\boldsymbol{T}$ and $\boldsymbol{U}$ are modelled as topological spaces; (ii) elements $\boldsymbol{a}$ and $\boldsymbol{b}$ of type $\boldsymbol{T}$ are considered identical if there is a continuous path in $\boldsymbol{T}$ from $\boldsymbol{a}$ to $\boldsymbol{b}$; and (iii) functions $\boldsymbol{f}$ and $\boldsymbol{g}$ from type $\boldsymbol{T}$ to $\boldsymbol{U}$ are continuous maps from $\boldsymbol{T}$ to $\boldsymbol{U}$. In topology a homotopy is a continuous morphing of one continuous map into another, and so in this context can be used to cleanly lift the notion of identity from elements $\boldsymbol{a}$ and $\boldsymbol{b}$ to functions $\boldsymbol{f}$ and $\boldsymbol{g}$.

[5] The metre, defined 1889-1960 as the distance between scratches on the IPM is now based on the speed of light.

[6] Mass will soon be measured with an accuracy of 1 part in $2\times10^8$, not possible relative to the IPK which is losing mass compared to the average of six near-identical copies of itself held in the same conditions.

**Figure 2.** Some of the authors of *Homotopy Type Theory* at the Institute for Advanced Studies, Princeton.

Naturally, HoTT comes with its own set of axioms, and during their development it was necessary for the authors to conduct reasoning experiments to check that the axioms were powerful enough to formalize mathematical concepts. Interestingly, the authors chose to use interactive theorem provers to carry out these experiments, with the human first asserting axioms and then guiding the computer to prove goal theorems by invoking automatic reasoning tactics. Often, this involves backing out of a line of reasoning which is going nowhere and sometimes even resetting the proof-goal when a counter-example is discovered en route.

The progress of the mathematicians was accelerated by their use of the GITHUB revision control system (Bauer, 2013a,b; GitHub, 2013) to facilitate collaboration on the development of both the book text and their formalized proofs. Note that while collaboration tools are extremely useful for multiple authors to write a book, they are even better for developing formalized mathematics, where as soon as a theorem is proved it can used as a lemma in other proofs. In the one-player game of interactive theorem proving, collaboration tools make it a consultation game allowing the players to work together efficiently and effectively to harvest the achievable goals.

Time will tell whether Homotopy Type Theory provides a cleaner foundation for mathematics than ZFC set theory, but this book represents a concrete success for a new kind of experimental mathematics and promises an exciting future for the 'HoTT' field of automated and interactive theorem proving.

## References

Appel, K. and Haken, W. (1977a). Every Planar Map is Four Colorable Part I: Discharging. *Illinois Journal of Mathematics* Vol. 21, pp. 429–490.

Appel, K., Haken, W. and Koch, J. (1977b). Every Planar Map is Four Colorable Part II: Reducibility. *Illinois Journal of Mathematics* Vol. 21, pp. 491–567.

Banach, S. and Tarski, A. (1924). Sur la décomposition des ensembles de points en parties respectivement congruentes. *Fundamenta Mathematicae* Vol. 6, pp. 244–277. ISSN: 0016-2736(p) 1730-6329(e).

Bauer, A. (2013a). The HoTT book: socio-technical aspects. http://math.andrej.com/2013/06/20/the-hott-book/.

Bauer, A. (2013b). A video rendition of the collaboration on the HoTT book. http://vimeo.com/68761218.

Frege, G. (1884). *Die Grundlagen der Arithmetik*. Breslau.

Frege, G. (1893). *Grundgesetze der Arithmetik*, Vol. 1. Jena.

GitHub (2013). A platform for collaborative projects. https://github.com/.

Gödel, (1931). Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I. *Monatshefte für Mathematik und Physik* 38: 173-98.

Gonthier, G. (2008). Formal Proof – the Four-Color Theorem. *Notices of the AMS*, Vol. 55, No. 11, pp. 1382-1393.

Gonthier (2013). Engineering Mathematics: The Odd Order Theorem Proof. *Proceedings of POPL'13*, pp. 1-2.

Hurd, J. and Haworth, G. M$^c$C. (2010). Data assurance in opaque computations. *Advances in Computer Games* 12 (ed. H. J. van den Herik and P. Spronck), LNCS Vol. 6048. pp. 221-231. ISSN 0302-9743, ISBN 978-3-642-12992-6, doi 10.1007/978-3-642-12993-3_20.

Lakatos, I. (1976). *Proofs and Refutations: the Logic of Mathematical Discovery* (ed. J. Worrall and E. Zahar). Cambridge University Press. ISBN 0-521-29038-4.

Mackenzie, D. (2001). *Mechanizing Proof*. The MIT Press. ISBN 0-262-13393-8.

Mann, A. (2003). A Case Study in Automated Theorem Proving: OTTER and EQP. Thesis, U. of Colorado.

Mills, I. M., Mohr, P. J., Quinn, T. J., Taylor, B. N. and Williams, E. R. (2011). Adapting the International System of Units to the twenty-first century. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 369, No. 1953, pp. 3907-3924. ISSN 1364-503X. doi: 10.1098/rsta.2011.0180.

Newell, A., Shaw, J.C. and Simon, H.A. (1957). Empirical Explorations of the Logic Theory Machine: A Case study in Heuristic. *Proceedings of the Western Joint Computer Conference*, pp. 218-240, esp. p219.

Shulman, G. (2013). The HoTT Book. http://golem.ph.utexas.edu/category/2013/06/the_hott_book.html.

Sutcliffe, G. (2012). Report on Automated Theorem Proving and the ATP competition. The Alan Turing Centenary conference. http://videolectures.net/turing100_sutcliffe_theorem_competition/ esp. at 2□ 45□.

The Univalent Foundations Program, IAS (2013a). The official announcement of the HoTT book. http://homotopytypetheory.org/2013/06/20/the-hott-book/.

The Univalent Foundations Program, IAS (2013b). *Homotopy Type Theory: Univalent Foundations of Mathematics*. http://homotopytypetheory.org/book/.

Whitehead, A.N. and Russell, B. (1910). *Principia Mathematica,* Vol. 1, esp. Chapter 2 and Theorem 2.01.

**Appendix:** LT's proofs of some *Principia Mathematica* theorems in Propositional Calculus

The text is closely based on Newell, Shaw and Simon (1957), p219, but for the connectives, $\vee$ substitutes for 'or', $\rightarrow$ for 'implies' and $\neg$ for 'not'.

Axioms with *Principia* numbering and *p*, *q* and *r* being propositions:

***a1.2***: $(p \vee p) \rightarrow p$ ***a1.3***: $p \rightarrow (q \vee p)$ ***a1.4***: $(p \vee q) \rightarrow (q \vee p)$
***a1.5***: $[p \vee (q \vee r)] \rightarrow [q \vee (p \vee r)]$ ***a1.6***: $(p \rightarrow q) \rightarrow [(r \vee p) \rightarrow (r \vee q)]$

Rules of Inference:

***ri1***: the rule of substitution: "Any expression may be substituted for any variable in any theorem, provided the substitution is made throughout the theorem wherever that variable appears."
***ri2***: the rule of replacement: "A logical connective can be replaced by its definition, and vice versa." Thus, in the logical system of the *Principia*, $p \rightarrow q$ means $(\neg p) \vee q$, and one of these expressions can be replaced by the other.
***ri3***: the rule of detachment (*modus ponens*): "If *A* and $A \rightarrow B$ are theorems, *B* is a theorem."

The proof of theorem 2.01, $(p \rightarrow \neg p) \rightarrow \neg p$, discovered by the 'British Library' breadth-first method:

***th1***: $(A \vee A) \rightarrow A$ (*a1.2*) … presumably LT was programmed to start with *A* rather than *p*
***th2***: $(\neg A \vee \neg A) \rightarrow \neg A$ (*th1* and *ri1*: substitution of $\neg A$ for *A*)
***th3***: $(A \rightarrow \neg A) \rightarrow \neg A$ (*th2* and *ri2*: replacement of '$\vee$' with '$\rightarrow$')
***th4***: $(p \rightarrow \neg p) \rightarrow \neg p$ (*th3* and *ri1*: substitution of *p* for *A* … QED).

LT's heuristics improved on basic 'breadth first' search. Building on proved theorems, it proved 17 theorems in one step, 19 in two steps and 2 in three steps. It was to some extent constrained by the 20KB memory of JOHNNIAC though at least one theorem (2.13: '$p \vee \neg\neg\neg p$') was provably beyond its ability.