WIKIPEDIA

Computer-assisted proof

A **computer-assisted proof** is a mathematical proof that has been at least partially generated by computer.

Most computer-aided proofs to date have been implementations of large proofs-by-exhaustion of a mathematical theorem. The idea is to use a computer program to perform lengthy computations, and to provide a proof that the result of these computations implies the given theorem. In 1976, the four color theorem was the first major theorem to be verified using a computer program.

Attempts have also been made in the area of artificial intelligence research to create smaller, explicit, new proofs of mathematical theorems from the bottom up using machine reasoning techniques such as heuristic search. Such automated theorem provers have proved a number of new results and found new proofs for known theorems. Additionally, interactive proof assistants allow mathematicians to develop human-readable proofs which are nonetheless formally verified for correctness. Since these proofs are generally human-surveyable (albeit with difficulty, as with the proof of the Robbins conjecture) they do not share the controversial implications of computer-aided proofs-by-exhaustion.

Contents

Methods

One method for using computers in mathematical proofs is by means of so-called validated numerics or rigorous numerics. This means computing numerically yet with mathematical rigour. One uses set-valued arithmetic and inclusion principle in order to ensure that the set-valued output of a numerical program encloses the solution of the original mathematical problem. This is done by controlling, enclosing and propagating round-off and truncation errors using for example interval arithmetic. More precisely, one reduces the computation to a sequence of elementary operations, say $(+,-,*,/)$. In a computer, the result of each elementary operation is rounded off by the computer precision. However, one can construct an interval provided by upper and lower bounds on the result of an elementary operation. Then one proceeds by replacing numbers with intervals and performing elementary operations between such intervals of representable numbers.

Philosophical objections

Computer-assisted proofs are the subject of some controversy in the mathematical world, with Thomas Tymoczko first to articulate objections. Those who adhere to Tymoczko's arguments believe that lengthy computer-assisted proofs are not, in some sense, 'real' mathematical proofs because they involve so many logical steps that they are not practically verifiable by human beings, and that mathematicians are effectively being asked to replace logical deduction from assumed axioms with trust in an empirical computational process, which is potentially affected by errors in the computer program, as well as defects in the runtime environment and hardware.[1]

Other mathematicians believe that lengthy computer-assisted proofs should be regarded as *calculations*, rather than *proofs*: the proof algorithm itself should be proved valid, so that its use can then be regarded as a mere "verification". Arguments that computer-assisted proofs are subject to errors in their source programs, compilers, and hardware can be resolved by providing a formal proof of correctness for the computer program (an approach which was successfully applied to the four-color theorem in 2005) as well as replicating the result using different programming languages, different compilers, and different computer hardware.

Another possible way of verifying computer-aided proofs is to generate their reasoning steps in a machine-readable form, and then use an automated theorem prover to demonstrate their correctness. This approach of using a computer program to prove another program correct does not appeal to computer proof skeptics, who see it as adding another layer of complexity without addressing the perceived need for human understanding.

Another argument against computer-aided proofs is that they lack mathematical elegance—that they provide no insights or new and useful concepts. In fact, this is an argument that could be advanced against any lengthy proof by exhaustion.

An additional philosophical issue raised by computer-aided proofs is whether they make mathematics into a quasi-empirical science, where the scientific method becomes more important than the application of pure reason in the area of abstract mathematical concepts. This directly relates to the argument within mathematics as to whether mathematics is based on ideas, or "merely" an exercise in formal symbol manipulation. It also raises the question whether, if according to the Platonist view, all possible mathematical objects in some sense "already exist", whether computer-aided mathematics is an observational science like astronomy, rather than an experimental one like physics or chemistry. This controversy within mathematics is occurring at the same time as questions are being asked in the physics community about whether twenty-first century theoretical physics is becoming too mathematical, and leaving behind its experimental roots.

The emerging field of experimental mathematics is confronting this debate head-on by focusing on numerical experiments as its main tool for mathematical exploration.

Theorems for sale

In 2010, academics at The University of Edinburgh offered people the chance to "buy their own theorem" created through a computer-assisted proof. This new theorem would be named after the purchaser.[2][3]

List of theorems proved with the help of computer programs

Inclusion in this list does not imply that a formal computer-checked proof exists, but rather, that a computer program has been involved in some way. See the main articles for details.

- Four color theorem, 1976
- Mitchell Feigenbaum's universality conjecture in non-linear dynamics. Proven by O. E. Lanford using rigorous computer arithmetic, 1982
- Connect Four, 1988 – a solved game
- Non-existence of a finite projective plane of order 10, 1989
- Robbins conjecture, 1996
- Kepler conjecture, 1998 – the problem of optimal sphere packing in a box
- Lorenz attractor, 2002 – 14th of Smale's problems proved by W. Tucker using interval arithmetic
- 17-point case of the Happy Ending problem, 2006
- NP-hardness of minimum-weight triangulation, 2008
- Optimal solutions for Rubik's Cube can be obtained in at most 20 face moves, 2010
- Minimum number of clues for a solvable Sudoku puzzle is 17, 2012
- In 2014 a special case of the Erdős discrepancy problem was solved using a SAT-solver. The full conjecture was later solved by Terence Tao without computer assistance.[4]
- Boolean Pythagorean triples problem solved using 200 terabytes of data in May 2016.[5]

See also

- Mathematical proof
- Model checking
- Proof checking
- Symbolic computation
- Automated reasoning
- Formal verification
- Seventeen or Bust
- Metamath

References

1. Tymoczko, Thomas (1979), "The Four-Color Problem and its Mathematical Significance", *The Journal of Philosophy*, **76** (2): 57–83, doi:10.2307/2025976 (https://doi.org/10.2307%2F2025976)
2. "Herald Gazette article on buying your own theorem" (https://web.archive.org/web/20101121000707/http://www.heraldscotland.com/news/education/your-own-maths-theorem-for-15-1.1068654). *Herald Gazette Scotland*. November 2010. Archived from the original (http://www.heraldscotland.com/news/education/your-own-maths-theorem-for-15-1.1068654) on 2010-11-21.
3. "School of Informatics, Univ of Edinburgh website" (http://www.ed.ac.uk/informatics/news-events/recentnews/theorem). *School of Informatics, Univ of Edinburgh*. April 2015.
4. Cesare, Chris (1 October 2015). "Maths whizz solves a master's riddle" (http://www.nature.com/news/maths-whizz-solves-a-master-s-riddle-1.18441). *Nature*. pp. 19–20. doi:10.1038/nature.2015.18441 (https://doi.org/10.1038%2Fnature.2015.18441).
5. Lamb, Evelyn (26 May 2016). "Two-hundred-terabyte maths proof is largest ever" (http://www.nature.com/news/two-hundred-terabyte-maths-proof-is-largest-ever-1.19990). *Nature*. **534**: 17–18. doi:10.1038/nature.2016.19990 (https://doi.org/10.1038%2Fnature.2016.19990). PMID 27251254 (https://www.ncbi.nlm.nih.gov/pubmed/27251254).

Further reading

- Lenat, D.B., (1976), AM: An artificial intelligence approach to discovery in mathematics as heuristic search, Ph.D. Thesis, STAN-CS-76-570, and Heuristic Programming Project Report HPP-76-8, Stanford University, AI Lab., Stanford, CA.

External links

- Oscar E. Lanford; A computer-assisted proof of the Feigenbaum conjectures, "Bull. Amer. Math. Soc.", 1982
- Edmund Furse; Why did AM run out of steam?
- Number proofs done by computer might err
- "A Special Issue on Formal Proof". *Notices of the American Mathematical Society* December 2008.