Prove It: Mathematics and Certainty

STSC 278

Final Paper

Proofs and Technology:

Which Drives Which?

Author:

Emmett Neyman

Professor:

Dr. Stephanie Dick

December 21, 2018

Think for a minute about the following question. Do new technologies drive new types of mathematics or do new types of mathematics drive new technologies? There is not a clear answer. On the one hand, the advent of powerful computers have opened the door to new types of math. Research in machine learning and big data are constantly producing new mathematical results. New virtual reality projects are creating new fields of geometry. And the possibility of quantum computers are spurring new advances in a variety of different mathematical fields. On the other hand though, none of these technological advancements would be possible without mathematics first laying the groundwork. From Alan Turing's original work on Turing machines to the linear algebra concepts behind those new buzz-wordy machine learning algorithms, mathematics completely permeates the field of technology. It is a true chicken and egg problem. If we restrict the question to the relationship between technology and proofs, the answer seems to get easier. Automated theorem provers and interactive proof assistants instantly jump to mind as examples of technology driving new advances in the study of proofs. But is this always the case or is it ever the other way around? Can new types of proofs drive the development of new technology. In this paper, I will argue that yes, not only is this possible but it has happened before throughout history, dating as far back as the ancient Greeks and stretching as far forward as the twentieth century.

In the history of mathematics, the first civilization studied is usually ancient Greece. This course stuck to that pattern, starting by studying how the Greeks developed their concept of the proof. In a chapter from his book *Demystifying Mentalities*, historian G.E.R Lloyd explores how the Greeks' concept of mathematical proof was created from other parts of society, including legal and political rhetoric and ancient philosophy. He argues that, although other civilizations may have understood the concept of a mathematical proof, the

Greeks were the first to formalize the notion and use it in a rigorous manner in practice. Aristotle, in particular, was the first to give a formal analysis of the mathematical proof. His works on logic, which include the study and formalization of deduction, syllogism, and premises, were the first to analyze explicitly what counts as a proof. Lloyd argues that the development of formal mathematical proofs in ancient Greece was partly driven by the desire to separate formal, demonstrative proofs from informal rhetorical arguments. Scholars such as Plato and Aristotle believed that rhetoric and other informal methods had no place in mathematics and these new ideas were a giant step forward for mathematicians who wished to separate their arguments from the rhetorical and persuasive methods used by lawyers and politicians at the time. Lloyd argues that even though Aristotle was the first to formally define and use these new techniques, it was Euclid who provides the most famous example of these techniques in practice in his *Elements*.[1]

Reviel Netz, in his piece *Linguistic Formula as Cognitive Tools*, expands on the new technologies (although he uses the more specific term "cognitive tools") Euclid uses in his proofs. He argues that the type of deductive proofs found in *Elements* evolved from linguistic techniques used in ancient Greek Homeric poetry. In both this type of story telling and Euclid's deductive proofs, formulas were used in order to simplify the overall process, whether it be telling a story or proving a theorem. Repetition, substitution, and types were each major components of this formula system. Netz claims that the entirety of *Elements* II consists of only 71 different formulas, repeated various number of times each. He characterizes these formulas into five types: *object formulas* which describe geometric entities, *construction formulas* which describe how to change or add to a geometric entity, *predicate formulas*

[1] G.E.R Lloyd, *Demystifying Mentalities*

which describe the properties of geometric entities, *argumentation formulas* which describe arguments made by the prover, and *second order formulas* which describe second-order arguments about other formulas. By restricting the anatomy of a proof to only certain types of strings, phrases, and symbols, proofs became more rigorous than they had ever been before. The other new technology employed by Greek mathematicians was the lettered diagram.This technology fit nicely with the above mentioned formula system since object formulas could use label names to easily and accurately identify specific geometric entities. Like the formula system, these labeled diagrams had structure and provided the mathematician with a formal system in which to work.[2] Along with the formal definitions and analysis provided by Aristotle in his groundbreaking work on logic, these two new technologies opened the door for rigorous and formal deductive proofs. Without these technologies, the advent of proof as we know it today would not have been possible. Aristotle developed a set of rules and standards to which all proofs must adhere and Euclid popularized several tools that made following these rules easier. It is important to note that these new tools developed by Euclid would not have been needed, and thus would never have been created, had Aristotle not developed a new style and standard of proof. This is the first example of proof driving the development of new technology.

The next great shift in the meaning of proof came thousands of years later, at the end of the nineteenth century. New fields of mathematics, such as set theory and non-Euclidean geometry, and the paradoxes that accompanied them, had introduced a sense of anxiety into mathematics. With that anxiety came the worry that many mathematical proofs did not stand on strong foundations. In fact, the very concept of what counted as

[2] Reviel Netz, *Linguistic Formula as Cognitive Tools*

a proof was thrown into turmoil. As new mathematical fields were created, proofs had to evolve to fit inside these new fields. And as proofs evolved, so too did the discussions around them. No longer was it clear what a "good" proof was; assumptions had to be made and often proofs heavily relied on these assumptions. It was during this period of anxiety that mathematicians started to realize that proofs were just as much social objects as they were mathematical ones. Jeremy Gray writes that mathematicians "could put their trust, too, in the social aspect of proving theorems, the shared agreement that such-and-such an argument was indeed a proof."[3] For other mathematicians, such as Gottlob Frege, David Hilbert, Bertrand Russell, and Alfred North Whitehead, this social definition of a proof did not suffice. These mathematicians, known as logicists, believed that a new type of proof system, based in formal logical systems was required in order to truly prove a theorem and save mathematics from unstable foundations. Russell wrote that their goal was "to show that all pure mathematics follows from purely logical premises and uses only concepts definable in logical terms".[4]

Frege set out to create such a system, hoping to dispel the anxiety that worried so many throughout the mathematical field. His work aimed to translate everyday mathematics such as arithmetic into an axiomatic logical system so that every theorem could be rewritten inside a strict, rule-based framework, thereby ensuring its correctness and consistency. Every step in his proofs would be accompanied by a corresponding inference rule or axiom to formally show that all proofs were correct.[5] After Russell uncovered serious flaws in Frege's work in the form of Russell's paradox, he and Whitehead took up the mantle of creating a new

[3] Jeremy Gray, *Anxiety and Abstraction in Nineteenth-Century Mathematics*
[4] Bertrand Russell, *My Philosophical Developments*
[5] Edward Zalta, "Gottlob Frege", *Stanford Encyclopedia of Philosophy*

formal system. Their work, *Principia Mathematica*, was inspired by Frege's and introduced a brand new logical system inside which they wanted to derive all of mathematics. Although the specifics of Russell and Whitehead's formal system was different that Frege's their goals and methods remained remarkably similar. Like Frege, they believed that by embedding all of mathematics inside a strict formal system and by proving everything using a rigorous set of rules and axioms, they could finally put mathematics on a solid foundation. They also believed that their style of proof should and would become the industry standard for modern mathematicians.[6] Although this last hope never came to be, *Principia Mathematica* is still regarded as one of the most influential books on logic ever written. Russell and Whitehead's work, along with Frege's, set the standard for what a logicist program should look like, laying the groundwork for Hilbert's Program later in the twentieth century.

Hilbert's Program was the name given to a lofty goal posed by Hilbert in the early twentieth century. He proposed that *all* of mathematics could be and should be reworked into an entirely formal and axiomatic system. Additionally, he proposed that all known theorems should be reproved inside this formal system. What set apart Hilbert's Program from earlier logicist efforts such as *Principia Mathematica* was its final goal. Not only did Hilbert want to solidify all of mathematics in a axiomatic system, he wanted to prove the consistency of this axiomatic system, dispelling the possibility of any paradoxes.[7] In a 1927 address, Hilbert spells out his goals explicitly:

> ... I pursue a significant goal, for I should like to eliminate once and for all the questions regarding the foundations of mathematics, in the form in which they are now posed, by turning every mathematical proposition into a formula that can be concretely exhibited and strictly derived, thus recasting mathematical

[6] Andrew David Irvine, "Principia Mathematica", *The Stanford Encyclopedia of Philosophy*
[7] Richard Zach, "Hilbert's Program", *The Stanford Encyclopedia of Philosophy*

> definitions and inferences in such a way that they are unshakable and yet provide an adequate picture of the whole science. I believe that I can attain this goal completely with my proof theory, even if a great deal of work must still be done before it is fully developed.[8]

Even earlier, in 1917, he was clear how his goals differed from those of Russell and Whitehead:

> The chief requirement of the theory of axioms must go farther [than merely avoiding known paradoxes], namely, to show that within every field of knowledge contradictions based on the underlying axiom-system are absolutely impossible.[9]

Although Kurt Gödel later proved that Hilbert's ultimate goal was impossible, Hilbert's Program was an important continuation of the work of earlier logicists. Like *Principia Mathematica*, it continued to redefine what a proof could, and to some, should, look like.

The new style of proof introduced by the logicists and put into practice in *Principia Mathematica* and Hilbert's Program represented the biggest shift in proof technique since the ancient Greeks first formally defined the deductive proof. For hundreds of years, mathematicians had been doing proofs in roughly the same style: deductively but relatively informally. That is, they made sure to use deductive arguments in the style of Aristotle and Euclid, but they did not necessarily take care to avoid paradoxes or inconsistencies; assumptions were a common component of many proofs. In order to resolve the worries and errors in mathematics during the nineteenth century, the logicists wanted to fundamentally change the way mathematicians proved things. This, however, required new technology: formal, axiomatic logical systems and new concepts like the consistency of a formal system. Without these new formal systems, mathematicians like Frege, Russell, Whitehead, and Hilbert would not have been able to develop their new ultra-formalized style of proof. In this case, like with

[8]David Hilbert, *The foundations of mathematics*
[9]David Hilbert, "Axiomatisches Denken"

the ancient Greeks, the need for a new type of proofs drove the development of new technology. With Aristotle and Euclid, it was the desire to dispel informal rhetorical methods from mathematics that led to the formulation of the deductive proof. And it was this formulation that led to the advent and use of lettered diagrams and linguistic formula systems within Aristotelian demonstrative, deductive proofs. In the late nineteenth century, the paradoxes of set theory and the growing unease throughout mathematics led to the development of a new standard of proof. And this new standard led to the creation of formal, axiomatic logical systems and new concepts like consistency proofs. Both scenarios are strikingly similar. In each, a problem led to a new standard of proof which, in turn, led to a new technology.

We now turn our attention to perhaps the most obvious case where technology and proof go hand in hand: automated theorem proving and other types of computer-assisted proofs. The advent of computer-based methods in proofs was the next drastic shift in the definition of a proof after the advent of formal axiomatic proof systems at the beginning of the twentieth century. At first glance, it may seems like these types of proof are clear examples of technology driving new proof methods: without computers, these proofs would not have been possible. And while that is certainly true, I will argue that it is not the whole truth. The most famous example of a computer-assisted proof is the proof of the Four-Color Theorem in graph theory produced in 1977 by Kenneth Appel, Wolfgang Haken, and John Koch. I claim that the success of this new proof method for this famous, long-open conjecture, along with the success of several other related fields, was the impetus that drove future research in automated theorem proving, interactive proof assistants, and software verification. In this way, it is also true that this new proof method drove the development of new types of technology. Before Appel, Haken, and Koch's result in the late 1970s, substantial work in automated theorem proving had already been carried out. Starting as early as the 1950s, computer scientists, logicians, and mathematicians had been working on software that could reason on its own, proving theorems via "artificial intelligence" (AI). Although many different flavors of automated theorem provers were being developed, "resolution" theorem provers, introduced in the 1960s, soon became regarded as the most successful and most promising. However, by the early 1970s, "resolution" theorem provers were seen as too inefficient to be practical and overall sentiment toward automated theorem proving was turning towards disappointment. In his piece *The Automation of Proof*, Donald MacKenzie writes that "the combination of ideological reaction and practical disappointment meant a rapid decline in the 1970s in the salience of automated theorem proof as a topic in artificial intelligence."[10]

As the field of automated theorem proving was on the decline in the 1970s, other related fields were starting to bloom. As mentioned above, the computer-assisted proof of the Four-Color Theorem is one of the most famous examples. Other fields, such as software and hardware verification and interactive theorem proving, were also experiencing success. Software verification became increasingly popular among computer scientists as interest in AI and automated theorem proving was on the decline and military software use was increasing. Interactive theorem provers were developed in conjunction with these verification projects in order to give programmers better tools to use for formal verification. Eventually, entire programming languages were developed with formal verification in mind, shrinking even more the gap between programming and proving. While verification projects were not all success stories, they had a better overall outcome than the mostly failed experiments in automated

[10]Donald MacKenzie, *The Automation of Proof*

theorem proving.[11] This is evident from looking at the state of the field currently. Many of the new technologies developed for verification in the 1970s and 180s, such as ML and HOL, are still widely used today. Additionally, because of the success of these early tools, many more technologies for verification and theorem proving such as Coq, Isabelle, and Agda have been developed since.

Clearly, the success of early computer-assisted proofs and formal verification projects impacted the development of new technology. But it still remains to be shown that these early computer-assisted proofs were really a new type of proof in the sense that the formal, axiomatic, symbol-based proofs of the logicists were in the early twentieth century. To make this argument we need look no further than Thomas Tymoczko's piece *The Four-Color Problem and Its Philosophical Significance*. In this piece, the author argues that the Appel, Haken, and Kroch's proof of the Four-Color Theorem is not a real mathematical proof in the traditional sense of the word. Tymoczko claims that proofs need to be three things: convincing, surveyable, and formalizable. He makes the observation that a proof cannot be known to be formalizable unless it is surveyable or there exists another surveyable proof that asserts the original proof is formalizable. Then he raises the question: If the computer-assisted proof of the Four-Color Theorem is not surveyable, how can we know if it is formalizable? Because the proof is not surveyable, and maybe not even formalizable as well, Tymoczko asserts that this proof is something radically different than any mathematical proof seen before.[12] Based on Tymoczko's argument and the more obvious, less philosophical facets about the proof of the Four-Color Theorem, it is safe to say that it is a significantly

[11] Donald MacKenzie, *The Automation of Proof*
[12] Thomas Tymoczko, *The Four-Color Problem and Its Philosophical Significance*

new type of proof.

In summary, we have seen three different types of proof methods throughout the course of history: the original deductive proof developed by Aristotle, the highly-formalized, axiomatic proof of the turn-of-the-century logicists, and the computer-assisted proofs of the late twentieth century. Each type of proof method has been accompanied by a new type of technology, developed solely because of the new proof method. For the ancient Greek demonstrative proofs, the lettered diagram and the structured linguistic formula were developed to make it easier to create a proof. When proofs transitioned to being more rigorous and logic-based, formal, axiomatized symbol systems were developed in order to give these proofs their own language. And lastly, when computers started to enter the game of proving, new verification frameworks, interactive theorem provers, and even entirely new programming languages were invented to keep up with the budding field. These three examples show that it is indeed possible for a new proof method to drive what types of technologies are developed. This means the answer to the question about the relationship between proofs and technology is no less clear cut than the question about mathematics and technology. Perhaps the answer is that proofs and technology continually push each other to new advances, each one trying to outdo and catch up to the other.

Works Cited

Gray, Jeremy J. "Anxiety and Abstraction in Nineteenth-Century Mathematics." *Science in Context* 17.1-2 (2004): 23–47. Print.

Hilbert, David. "Axiomatisches Denken." *Mathematische Annalen* 78 (1917): 405–415. Web.

——."Hilbert (1927) The foundations of mathematics." *From Frege To Godel*. Harvard University Press, 1967. 464–479. Print.

Irvine, Andrew David. "Principia Mathematica." *The Stanford Encyclopedia of Philosophy*. Edited by Edward N. Zalta. Winter 2016. Metaphysics Research Lab, Stanford University, 2016. https://plato.stanford.edu/archives/win2016/entries/principia-mathematica/.

Lloyd, Geoffrey Ernest Richard. *Demystifying Mentalities*. Cambridge University Press, 1990. Print. Themes in the Social Sciences.

MacKenzie, Donald. "The Automation of Proof: A Historical and Sociological Exploration." *IEEE Ann. Hist. Comput.* 17.3 (Sept. 1995): 7–29. Web.

Netz, Reviel. "Linguistic Formulae as Cognitive Tools." *Pragmatics and Cognitionpragmatics and Cognition* 7.1 (1999): 147–176. Print.

Russell, Bertrand. "My Philosophical Development." *Les Etudes Philosophiques* 14.4 (1959): 558–558. Print.

Tymoczko, Thomas. "The Four-Color Problem and Its Philosophical Significance." *The Journal of Philosophy* 76.2 (1979): 57–83. Web.

Zach, Richard. "Hilbert's Program." *The Stanford Encyclopedia of Philosophy*. Edited by Edward N. Zalta. Spring 2016. Metaphysics Research Lab, Stanford University, 2016. https://plato.stanford.edu/archives/spr2016/entries/hilbert-program/.

Zalta, Edward N. "Gottlob Frege." *The Stanford Encyclopedia of Philosophy*. Edited by Edward N. Zalta. Summer 2018. Metaphysics Research Lab, Stanford University, 2018. https://plato.stanford.edu/archives/sum2018/entries/frege/.