Macalester Journal of Philosophy

Volume 20 | Issue 1 Article 10

6-21-2012

Epistemic Justification and the Possibility of Computer Proof

Drew Van Denover
Macalester College

EPISTEMIC JUSTIFICATION AND THE POSSIBILITY OF COMPUTER PROOF

Drew Van Denover

Abstract Some mathematical theorems can be proven only with the help of computer programs. Does this reliance on computers introduce empirics into math, and thereby change the nature of proof? I argue *no*. We must distinguish between the warrant the proof gives for its conclusion, and our knowledge of that warrant. A proof is a priori if and only if the conclusion follows deductively from the premises without empirical justification. I start by defending this definition, and proceed to demonstrate that computer-generated proofs meet its criterion.

For more than one hundred years, mathematicians tried and failed to produce a valid mathematical proof of the "Four Color Theorem", or 4TC. First proposed in 1852, the 4TC conjecture remained unproven until Kenneth Appel and Wolfgang Haken published their solution in 1976. Debate immediately erupted about the legitimacy of their methods. Unlike every previous proof, Appel and Haken's work made ineliminable use of a computer program. Their knowledge of the 4TC depended on the operations of a physical machine—apparently introducing empirical elements into mathematics, the purest a priori science. Thomas Tymoczko soon emerged as a chief critic of the possibility of a "computer-assisted proof." These CAPs, he alleged, incorporate contingent facts about the world, whereas mathematical proofs require a priori certainty. On his account, we should reject the 4TC as a true “theorem” lest we fundamentally alter the nature of mathematical truth. He writes:

> [The] use of computers, as in the 4CT, introduces empirical experiments into mathematics. Whether or not we choose to regard the 4CT as proved, we must admit that the current proof is no traditional proof, no a priori deduction of a statement from premises …. I will suggest that, if we accept the 4CT as a theorem, we are committed to changing the sense of “theorem”, or, more to the point, to changing the sense of the underlying concept of “proof.”[1]

I disagree with Tymoczko; CAPs *can* be a priori in the requisite sense. Something is a priori if it has a non-empirical justification—regardless of whether humans have a priori knowledge of that justification. We must distinguish between the warrant the proof gives for its conclusion and *our knowledge of that warrant*. I contend CAPs provide excellent, a posteriori reasons for thinking that Appel’s proof has an a priori justification.

Most of the debate turns on what we mean by “a priori proof.” I begin by discussing competing definitions, and then offer an account of how computer-generated proofs satisfy the best one. I conclude that we need not choose between CAPs’ legitimacy and the aprioricity of mathematics.

[1] Tymoczko, Thomas. 1979. "The Four-Color Problem and Its Philosophical Significance". *The Journal of Philosophy.* 76 (2): 58

Assumptions

I want to make explicit some of the background assumptions underlying my thesis. First, I assume that normal mathematical reasoning, such as we find in ordinary human-produced proofs, counts as a priori. Following Frege, this is not to say that we discover arithmetic truths without reference to sense experience, but rather that their *ultimate justification* makes no use of it. Contemporary philosophers of mathematics seem largely to accept this thesis, and anyone denying it would see no epistemic difference between computer-derived proofs and the more natural kind. For the purposes of this paper, we shall therefore bracket objections to the aprioricity of mathematics in general.

Second, we need to outline our general conception of "proof." I agree with Rota that a mathematical proof is fundamentally an *argument*—a "sequence of steps which leads to the desired conclusion."[2] Like any other argument, proofs proceed from a set of premises to a conclusion, which we call a mathematical theorem. I see at least two necessary conditions for proof-hood (although more may exist). An argument is a mathematical proof only if (1) the argument is deductively valid and (2) it is in some sense a priori. These are distinct criteria. Heuristic arguments are increasingly common in the field, and indeed they can provide legitimate a priori mathematical knowledge—however, "The proposition was true for all of the 10^6 cases we tested" does not amount to a *proof* of that proposition. Observe that Goldbach's Conjecture, for all its inductive support,

[2] Rota, Gian Carlo. 1997. "The Phenomenology of Mathematical Proof". *Synthese.* 111 (2): 183

has yet to achieve the status of "theorem." Similarly, many arguments deductively entail their conclusions, but because their premises are fundamentally empirical claims, they do not enjoy a priori status. Tymoczko's argument denies the second condition that CAPs are a priori, but we will seek to reaffirm it.

Defining "A Priori Proof"

We must clarify what we mean by "a priori." In this section I reject the definition Tymoczko uses, which requires proofs necessarily to generate a priori knowledge. Instead, I offer my own definition which does not refer to any particular individual's knowledge at all.

Recall that aprioricity is an epistemological concept. It primarily concerns *knowledge*—that is, justified true beliefs.[3] Specifically, it concerns the "justified" part of knowledge. A given belief is a priori when its justification does not depend on sense experience. I agree with Kripke that, strictly speaking, the predicate "… is a priori" applies to *knowledge* and *belief* exclusively, for they are the only bearers of justification.[4] We know something a priori when we know it on the basis of strictly non-empirical evidence.

As such, calling a proof "a priori" involves a little sleight of hand. Proofs are neither beliefs nor knowledge. They are arguments—abstract mathematical constructions consisting of a set of premises, a conclusion, and the inferential relations between them. An argument is a proof whether or not any particular person

[3] Where the justification and the belief are related in the right way, of course.

[4] Kripke, Saul A. 1980. *Naming and Necessity*. (Cambridge, Mass: Harvard University Press.), 35

knows it is a proof, and whether or not anyone *believes* it is a proof. We need to stipulate what "a priori" means when applied to mathematical arguments.

Before presenting my own definition, I want to discuss what I take to be the received definition of "a priori proof":

(1) An argument is an "a priori proof" if and only if it is capable of providing a priori knowledge of its conclusion to people with sufficient mathematical ability and knowledge of the involved concepts.

Intuitively, I find this view highly plausible. As mathematical apriorists by assumption, we think that all mathematical truth can be known without sense experience. Naturally, proofs should provide exactly that knowledge. This definition paints the following picture: When a mathematician reads the proof of a theorem, he mentally internalizes each proceeding step. He holds the entire proof in his mind, and can *see* why it is true. Because he knows the workings of the proof, he believes the theorem it underpins. If asked, he can rely on his understanding alone to justify that belief without recourse to experiential propositions. His knowledge of the theorem is completely a priori.

On definition (1), CAPs are not a priori because they are not surveyable. Since no one mathematician can read the proof in its entirety, no one person can truly *know* it. Appel presumably understands the concepts involved in his proof of 4CT, but when he justifies the results step by step, he must refer to empirical work done by computers. For this reason, Tymoczko denies that CAPs are truly "proofs"—they cannot actually provide a priori knowledge:

> The mathematician surveys the proof in its entirety, and thereby comes to know the conclusion …. The proof relates the mathematical known to the mathematical knower, and the surveyability of the proof enables it to be comprehended by the pure power of the intellect—surveyed by the mind's eye, as it were. Because of surveyability, mathematical theorems are credited by some philosophers with a kind of certainty unobtainable in the other sciences. Mathematical theorems are known a priori.[5]

I agree with Tymoczko that CAPs are not surveyable in the sense he requires, and if we accept (1), CAPs are not truly proofs. However, I think we have good reason to reject (1) as the criterion for a priori proofs: requiring that proofs be capable of generating a priori knowledge indexes what counts as "proof" to particular, individual minds. On (1), whether a given argument is a proof depends on facts about the person attempting to understand it.

Because knowledge is a species of belief, it belongs to individuals. When Jones and Smith witness the same event, they form their own separate beliefs about it, which then count as knowledge if and only if they are true. So "Jones' knowledge" and "Smith's knowledge" are distinct entities. Further, what is sufficient to provide Jones with "knowledge of x" may not be sufficient to provide Smith with "knowledge of x." What actually *will* generate knowledge in a person depends on facts about that

[5] Tymoczko, *The Four-Color Problem*, 60.

person's perception and reasoning processes, and such contingencies are unacceptable for a good definition of proof.

Imagine an argument that requires hundreds of billions of pages to write down on paper (for example, suppose we somehow printed the results from every computation performed during Appel's the proof of the 4CT). That argument would be unsurveyable in a very real way. The time required to read and absorb it would exceed the human lifespan several times over. By (1), the argument is not a proof. But suppose now that modern technology increases human life expectancy tenfold, and cognitive enhancements permit us to read quickly enough to digest the argument and know its contents. The same definition dictates that now, the argument *is* a proof. Its proof-status changed because of strictly empirical facts which had nothing to do with the argument itself! Suppose further that an environmental disaster destroys the technology, but leaves record of the argument intact. Has it now ceased being a proof?

Mathematicians and philosophers often assert that "false proof" is a contradiction in terms.[6] Proofs are certain and timeless. If Euclid proved a proposition in 300 B.C., that same proof remains equally valid today. Definition (1) does not capture this character of mathematical proofs. We do not want our criteria for proof-hood to depend on any one person's a priori knowledge, because what is a priori knowable in practice will always be contingent. We need a different concept of "a priori proof."

A better definition of "a priori proof" will determine the argument's epistemic status using only features of the argument

[6] Rota, *The Phenomenology of Mathematical Proof*, 183.

itself—not features of the entities reading it. Remember, to call something a priori is to say that its *ultimate justification* does not depend on empirical propositions; whether any one person's knowledge of that justification is also a priori is irrelevant. Hence, I offer a counter-definition:

> (2) An argument is an "a priori proof" if and only if:
> (a) none of its premises depend on empirical evidence for justification; and
> (b) the conclusion follows from the premises using only rules of inference with non-empirical justification.

Unlike (1), (2) does not depend upon contingent facts unrelated to the argument itself. The argument will be a priori or not regardless of whom or what is reading it. Moreover, (2) best captures the spirit of a priori as a feature of justifications, rather than genesis. (1) seems dependent on the "context of discovery"—it asks, "How, in practice, did some mathematician come to know the theorem in question?" (2) cares only about how we might, in principle, *justify* that theorem. If we can do so independently of sense experience, our theorem has achieved a priori status. On (2), "a priori proofs" are arguments guaranteed to generate a priori justifications, which is precisely what proofs ought to do.

Given our assumption that "normal" mathematical knowledge is a priori, we can derive the following:

(2*) An argument is an “a priori proof” if:

(a) all its premises are mathematical axioms or theorems; and

(b) the conclusion follows from the premises using only rules of logic.

Deciding whether computer-assisted proofs are legitimately a priori requires only determining whether they meet our two sufficient conditions. Do the computers assisting us employ only mathematically warranted inferences? We have excellent reason for believing they do.

Do CAPs Meet Our Definition?

Consider Appel and Haken’s proof of the 4CT, for example. Exactly what role did computers play? We should remember that one hundred percent of the conceptual work for the proof was developed by *humans*. Stated roughly,[7] Appel and Hanken developed an *algorithm*—a mechanical procedure for applying a finite number of mathematical operations to some input, terminating in some output. The algorithm—like any valid algorithm—involves only mathematically warranted steps. The mathematicians proved, using tried-and-true human-generated methods, that when the algorithm takes a graph as input, a certain output results if and only if the graph has the property of being

[7] The description that follows oversimplifies a complicated and technical mathematical process, but I believe it accurately portrays the philosophical elements involved.

"reducible".[8] They further proved that if every one of a particular set of graphs *is* reducible, the 4CT must necessarily be correct. No suspect "computer-proof" has been invoked thus far.

Applying the algorithm by hand, however, is simply impracticable. The procedure requires "analysis of about ten thousand neighborhoods of vertices" for each of about fifteen hundred graphs.[9] Given the computational nature of an algorithm, the only reasonable way forward involves outsourcing these calculations to a machine. To do so, they wrote a machine-language program—another series of mechanical instructions that, in theory, cause the machine to run through the algorithm precisely as Appel and Hanken described it, storing its data in bits of RAM. On the hypothesis that the computer functions properly, it executes the algorithm using only inferences with a priori justification.

Three things in this process are of note. First, the work done by computer in CAPs remains purely combinatorial—different in scope, but not kind, from the role that calculators and even abaci serve in "normal" mathematics. That role comes nowhere near the creative artificial intelligence Tymoczko imagines:

> Suppose that advances in computer science lead to the following circumstances. We can program a computer to initiate a search through various proof procedures, with subprograms to modify

[8] I will not discuss here what "reducibility" means as a property of graphs. For details of the proof, see Appel and Hanken, 2002.

[9] Appel, Kenneth and Wolfgang Haken. "The Four Color Problem," in *Philosophy of Mathematics: An Anthology*, ed. Dale Jacquette (Oxford: Blackwell Publishing, 2002), 207

> and combine procedures in appropriate circumstances, until it finds a proof of statement A. After a long time, the computer reports a proof of A, although we can't reconstruct the general shape of the proof beyond the bare minimum…. [T]he question is whether mathematicians would have sufficient faith in the reliability of computers to accept this result.[10]

The kind of method Tymoczko describes goes far beyond a computer-assisted proof—it represents a computer-*generated* proof. Specifically, Tymoczko hypothesizes a scenario in which a computer creates a "proof" of Peano arithmetic's inconsistency. Surely, he says, logicians would find this result "hard to swallow." I agree; we should be very skeptical of such a hypothetical proof—but that hesitation does not indicate that mathematicians lack confidence in the *basic calculations* computers perform. Again, CAPs require only this latter kind of combinatorial computation.

Second, we see that computers might introduce error into proof results in two ways: through flaws in their programming (a software bug), or malfunctions in the physical processes underlying their data storage systems (a hardware bug). Both are real possibilities, but neither differs substantially from the errors commonly found in flawed attempts at proof by humans. We misuse notation and make similar syntactical mistakes with regularity, and our calculations are exponentially more error-prone than those of machines. If I ask a mathematician for even a (relatively) simple combinatorial result—say, the rational

[10] Tymoczko, *The Four-Color Problem*, 74.

representation of $\left(\frac{32497}{8237}\right)^{234} - \sum_{i=1}^{73^7} \frac{587i^{13}}{7}$, he will immediately reach for a calculator or (even more likely thirty years after Tymoczko published his paper) a computer. Why? Because empirically, computers are simply more reliable than humans. Appel, in his philosophical defense of his work, observes:

> When proofs are long and highly computational, it may be argued that even when hand checking is possible, the probability of human error is considerably higher than that of machine error; moreover, if the computations are sufficiently routine, the validity of programs themselves is easier to verify than the correctness of hand computations.[11]

His last comment raises the final, most important point of how computer-derivations function in practice: they are subject to easy and repeated *verification*. Certainly, it is possible for a single processor or a single program to malfunction in some way and thereby produce a false result. But CAPs like that of the 4TC have been reproduced on hundreds of individual computers, and their results agreed upon by numerous independently-coded programs. In fact, new implementations for deriving the 4CT proof continue to appear even in the 21st century. Granted, these results should not give us complete, absolute confidence in its validity (as philosophers, we regard very few things as *certain beyond a doubt*). But given the rigor and frequency of their verification, we can be just about as confident that Appel and Haken's algorithm

[11] Appel, *The Four Color Problem*, 207.

indeed generates the desired output as we can be about any empirical fact.

I say “empirical” without concern, though Tymoczko and his sympathizers would balk at such an admission. They grant that computers are almost always reliable, but argue that when assessing their capacity to prove theorems, we are exclusively concerned with a priori evidence. Tymoczko says as much:

> [T]here is a great deal of accumulated evidence for the reliability of computers in [CAP] operations, and the work of the original computers was checked by other computers....The reliability of the 4CT, however, is not of the same degree as that guaranteed by traditional proofs, for this reliability rests on the assessment of a complex set of empirical factors.[12]

In my estimation, this common argument misses the crucial distinction between the proof’s a priori justification for its conclusion, and our knowledge of that justification. As per our definition, proof-hood requires that arguments begin from a priori premises, and proceed along a priori methods; our belief that it does so needn’t be similarly a priori. We have overwhelming a posteriori evidence that the computer’s methodology follows strict a priori guidelines, and therefore meets our criteria for an “a priori proof.”

[12] Tymoczko, *The Four-Color Problem*, 74.

Conclusion

Tymoczko and I start from fundamentally different conceptions of what “a priori” means in the context of mathematical results. He roots his entire project in the idea that that “mathematical theorems are known a priori.”[13] Are they always? Remember that knowledge is proprietary to individuals. One person can have a priori knowledge of a fact another person knows only empirically, and this principle does not change when applied to mathematical knowledge. Much (dare I say, *most*) mathematical knowledge exists on an a posteriori basis. For example, I have no graduate training in mathematics, but when a Fields medalist informs me she has proven an extremely high-level theorem, I believe her. Is my belief justified? I say *yes*. This woman is likely the most knowledgeable expert on the planet. She has nothing to gain from lying, but everything to lose if caught. If I cannot trust her opinion, I can trust no one’s. Is my belief true? If she really has proven the theorem, it must be. In such a case, my belief constitutes a posteriori knowledge of a mathematical theorem. I expect that most undergraduates accept their professors’ word about theorems prima facie, and thereby create knowledge of a similar kind. Asserting that theorems are necessarily known a priori seems simply unrealistic.

We better capture the aprioricity of theorems with reference not to how particular individuals *actually* know them, but how those theorems are *justified*. For this, we must look to the proofs’ methods. As per (2*), mathematical arguments follow a priori methods when neither their premises nor inferences depend upon

[13] Ibid., 60

sense experience for justification. This certainly seems to be the case for Appel and Haken's proof of the 4TC, and for other CAPs like it.

Tymoczko rightly asserts that *mathematicians' knowledge* of CAPs is necessarily empirical. That fact is difficult to deny. However, it does not speak to the internal operations of the proof, which (in my estimation) are the sole determinants of the proof's a priori status. As long the proof offers an a priori justification for its conclusion, it does not matter whether humans know of that justification in an a priori way. In essence: *we need not know a priori that the proof's warrant is a priori.* Insofar as we trust our belief that hundreds of tests run on hundreds of thousands of combinations of software and hardware platforms cannot *all* be completely mistaken, we should trust our belief that CAPs justify their conclusion without reliance on empirics. Anyone suggesting that CAPs are not sufficient "proofs" for lack of a priori justification cannot ignore this result.

Bibliography

Appel, Kenneth and Wolfgang Haken. “The Four Color Problem,” in *Philosophy of Mathematics: An Anthology*, ed. Dale Jacquette (Oxford: Blackwell Publishing, 2002)

Kripke, Saul A. 1980. *Naming and Necessity*. Cambridge, Mass: Harvard University Press.

Rota, Gian Carlo. 1997. "The Phenomenology of Mathematical Proof". *Synthese.* 111 (2): 183-196.

Tymoczko, Thomas. 1979. "The Four-Color Problem and Its Philosophical Significance". *The Journal of Philosophy.* 76 (2): 57-83.