Computers, mathematical proof, and the nature of the human mind

POMSIGMAA Keynote Address Philosophy of Mathematics

American Mathematical Society and Mathematical Association of America Joint Meetings

Jeff Buechner

Rutgers University-Newark and The Saul Kripke Center, CUNY, The Graduate Center

January 6th, 2017

1976 Appel and Haken prove the four-color theorem

- June, 1976 Wolfgang Haken and Kenneth Appel, with the aid of John Koch prove the Four-Color Theorem. Their proof was published in 1977 in the Illinois Journal of Mathematics

Their proof is implicitly recognized as valid by the United States Postal Authority

1979 Tymoczko on the Four-Color Theorem

- The first paper in the philosophy of mathematics on the philosophical importance of the four-color theorem: Thomas Tymoczko "The Four-Color Problem and Its Philosophical Significance," Journal of Philosophy, 1979

Tymoczko on mathematical proof

- Why are mathematical proofs convincing?
- “That proofs are surveyable and that they are formalizable are two such characterizations” Tymoczko, op. cit. p. 59

Paul Teller on Tymoczko

- “Surveyability is needed, not because without it a proof is in any sense not a proof, but because without surveyability we seem not to be able to verify that a proof is correct. So surveyability is not part of what it is to be a proof in our accustomed sense.” Paul Teller “Computer Proof,” Journal of Philosophy, 1980

The dispute between Teller and Tymoczko: the concept of mathematical proof

- Tymoczko: surveyability is an essential feature of the concept of a mathematical proof.
- Teller: surveyability is not an essential feature of the concept of a mathematical proof.
- Who is right? On what grounds are they right?

Detlefsen on Tymoczko

- Detlefsen provides several examples of mathematical proofs which are surveyable and in which computations are made. He argues that such computations necessarily utilize empirical premises (such as: the computing agent correctly executes the program required to make the computation).
- If his argument is sound, Detlefsen has shown that unsurveyability is not necessary for the presence of an empirical element in mathematical proofs. This refutes a major claim in Tymoczko’s paper.

Understanding Chisholm’s point

- a posteriori knowledge: knowledge which is arrived at on the basis of sense experiences or perceptual beliefs.
- a priori knowledge: knowledge which is arrived at on the basis of intellectual processes which do not involve reference to or reliance upon sense experiences.

Why is Chisholm’s point important?

- If Chisholm is right that long mathematical proofs require a premise about what we happen to remember—and thus are not either known or justified a priori—then it easily follows that those proofs are known or justified empirically. They rely upon or refer to sense experiences.
- Tymoczko is right about the epistemological status of the 4CT if we accept Chisholm’s point. But he is wrong that only unsurveyable mathematical proofs require (in whole or in part) empirical justification.

Burge on the use of computers in mathematical proofs

- Tyler Burge, 1998, sidesteps the need to understand what a mathematical proof is
- He argues that no empirical element need be added when computers are used in mathematical proofs.
- So the 4CT can be known a priori (to be true).

What have Detlefsen and Burge shown?

- Detlefsen has shown that unsurveyability is not necessary for the existence of an empirical element. Burge has shown it is not sufficient.
- Their results, if correct, show there is no conceptual connection between unsurveyability and the existence of an empirical element in proofs.

Three Problems for Burge

- First problem: his account makes it too easy to have gettiered “knowledge.”
- Gettier counterexamples : a subject S has a true, justified belief that p, but S does not know that p.

For example, suppose the 4CT is true, but the computer program for resolving the cases is fallacious. S is justified—according to Burge—in believing the 4CT true.

S has a true, justified belief in the 4CT, but does not know the 4CT.

Three Problems for Burge

- One of Burge’s assumptions is that “individual’s knowledge of pure mathematics, resting on specifically mathematical understanding or reasoning, is ordinarily a priori.”
- This contradicts Detlefsen—that empirical premises are used in surveyable (as well as unsurveyable) proofs.
- We defer our exposition of the third problem for Burge.

The dialectics of how things stand

- Tymoczko and Teller: stalemate
- Tymoczko and Detlefsen: If Detlefsen is correct, empirical premises occur in mathematical proofs that are both surveyable and unsurveyable. This puts pressure on getting clear on what we mean by a mathematical proof.
- Tymoczko and Burge: If Burge is correct, then the use of computers in mathematical proofs does not introduce an empirical element into those proofs (nor does the use of computations in mathematical proofs). Tymoczko and Detlefsen are both refuted.

A line of thought not taken

- We will now discuss a line of thought that is broached by Teller, Detlefsen, Davis, and Tymoczko, but not taken up by any of them.
- For example, Teller writes: “The computer proof of the combinatorial lemma is subject to error—computers can make mistakes. We cannot guard against this possibility of mechanical failure or error in programming in the traditional way because we cannot survey the proof.”

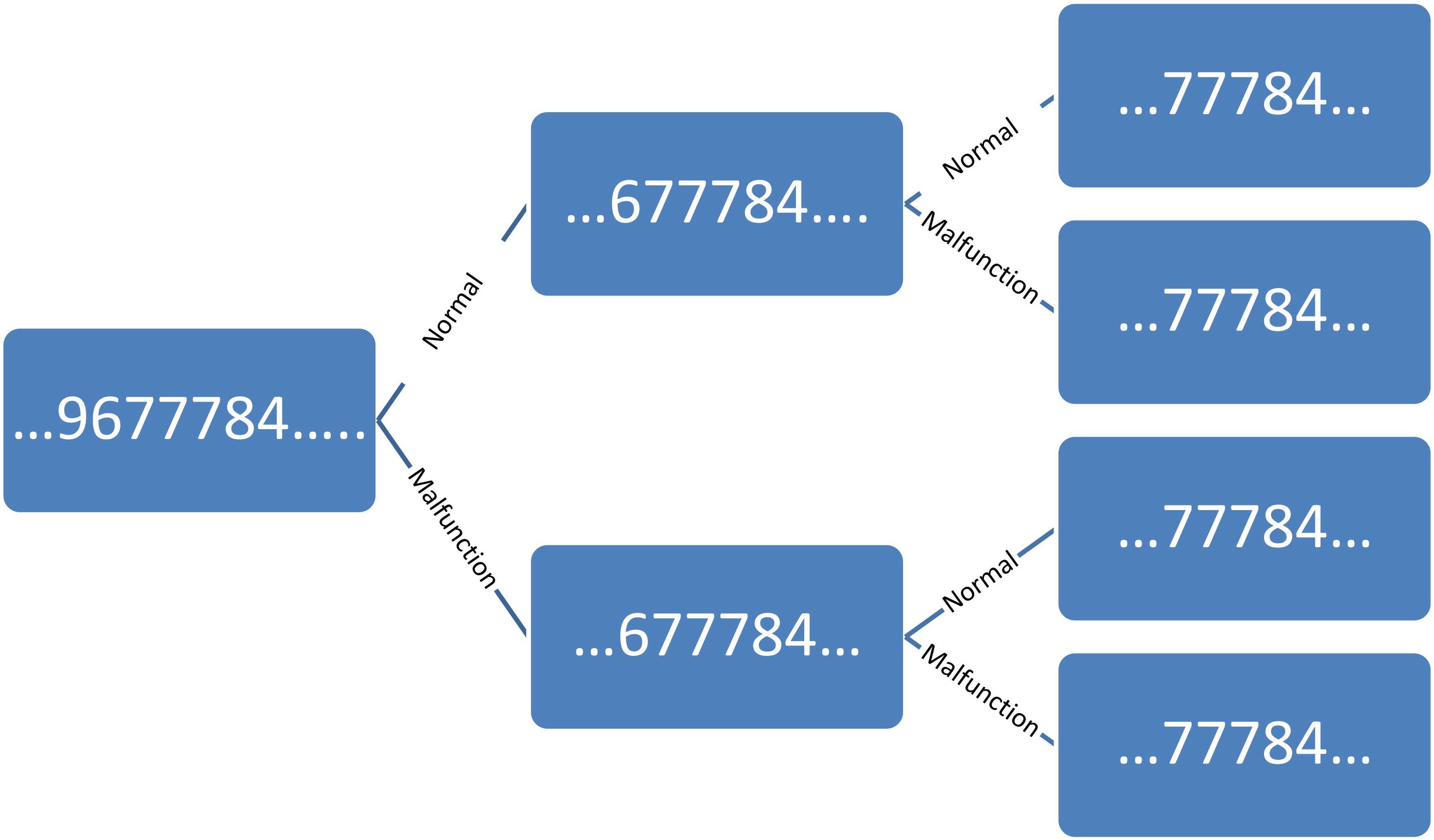
The basic idea

- Since physical computing machines—PCMs--can break down in various ways, how do we really know what function F a given PCM computes?
- One might think that is not a serious problem. If F is the square function, and the PCM computes F(2) = 4, the PCM is operating normally. IF the PCM computes F(2) = 8, then it has suffered a breakdown.

The basic idea

- That view is too naïve. There are many other functions (say, G) that PCM might be computing. Perhaps the output ‘4’ is when PCM suffers a breakdown in computing G. Perhaps the output ‘8’ is when PCM operates normally in computing G.
- Unless it is KNOWN that the PCM computes, say, F, it cannot be ruled out that, based on its behavior, it is computing, say, G.

How many distinct designers of the IBM 370-160A might there be?



A disturbing conclusion

- No mathematician is ever justified that a computing machine is computing F because there is no way, from the machine's program or output, to be certain that it's wired and programmed to do so.
- Nor do we have any way to be certain that the machine is not having a physical malfunction, because we cannot know that it is correctly wired and programmed.
- So we have no more reason to believe the computing machine is computing F than we have reason to believe that a fair flip of a fair coin will come up heads.

Third Problem for Burge

For Burge, relying on our short-term memory and relying on computers is simply part of cognitively accessing those sources.

But he notes there might be cases in which one needs to reason, using empirical evidence, to the conclusion that one can rely on some source of information.

I claim reliance on computers is such a case.

Where do we go from here?

There is much work to be done on developing a concept of mathematical proof and on proof assistants. But no matter what the development of these areas looks like in the future, unless we come to terms with the philosophical questions concerning the nature of the human mind, we will not be in a position to say whether a mathematical proof that uses computers (in the way the 4CT does) is a genuine mathematical proof.

Where do we go from here?

- We will not have an adequate view of machine computations until we have an adequate view of the nature of the human mind.
- Whether these views must respect the mathematical work on computation is an open question. It might be that, e.g., a new concept of computational complexity will be needed.
- This seems strange; indeed, it IS strange. But the arguments I have presented here today show that, although strange, it is (perhaps) necessary.

The End

- Thanks to Bonnie Gold for much helpful editorial advice and discussion.