Making Math More Rigorous

Leslie Lamport

23 January 2022
error corrected 6 January 2024

Appeared as Section 4 of *Mathematical Proof Between Generations* by Jonas Bayer, Christoph Benzmller, Kevin Buzzard, Marco David, Leslie Lamport, Yuri Matiyasevich, Lawrence Paulson, Dierk Schleicher, Benedikt Stock, and Efim Zelmanov in *Notices of the American Mathematical Society*, Volume 71, No. 1 (January 2024)

Mathematics, as practiced by most mathematicians, is not very rigorous. There is evidence that about 1/3 of all published, refereed math papers contain significant errors—incorrect proofs or theorems that their authors believed to be correcct. (The evidence is described in [1].) Math can be made more rigorous, and mathematicians can make fewer errors, by replacing archaic customs with more sensible practices. Here is how.

Formulas

A few hundred years ago, formulas were written in prose. Today, mathematicians recognize the advantages of writing formulas with modern mathematical notation: they're shorter, easier to understand, and easier to manipulate. Replacing prose by mathematics must have reduced errors.

Mathematicians think they've stopped using prose to write formulas. They're wrong. They've replaced only some of the prose in their formulas by math. Consider this definition of what it means for $\lim_{x \to a} f(x)$ to equal b.

(1) For all $\epsilon > 0$ there exists $\delta > 0$ such that, for all x, if $0 < |a - x| < \delta$ then $|b - f(x)| < \epsilon$.

A mathematician would find (1) perfectly normal, even though it's a mathematical formula written with many words. Here is that formula written without words:

$$(2) \quad \forall\, \epsilon > 0 \,:\, \exists\, \delta > 0 \,:\, \forall\, x \,:\, (0 < |a - x| < \delta) \;\Rightarrow\; (|b - f(x)| < \epsilon)$$

I believe most mathematicians would find (2) harder to understand and uglier than (1). I expect mathematicians a few hundred years ago would have found $0 < |a - x| < \delta$ hard to understand and ugly.

Why write (2) rather than (1)? For the same reason we don't write *0 is less than the absolute value of*...: It's shorter, easier to understand (when you become comfortable with the notation), and easier to manipulate. And it will reduce errors. Show elementary calculus students the definition (1) and ask them to write what it means for $\lim_{x \to a} f(x)$ equals b to be false. I doubt if many of them would get it right. Teach them a little elementary logic and they could easily compute the negation of (2). The most obvious use of words in formulas is to express logical operations; but they are also used in other ways, such as describing sets and functions.

Formulas written without words can now be manipulated by computer programs. Programs can easily compute the negation of (2). They can't

compute the negation of (1).[1] Those programs can help students become comfortable with mathematical concepts, if the concepts are described with math rather than prose.

Mathematicians think it's difficult to write formulas completely mathematically, without words. I have asked a number of mathematicians how long a completely rigorous, wordless definition of the Riemann integral would be—assuming definitions of the set of real numbers and its arithmetic operations, as well as simple set theory. I've received answers ranging from 50 lines to 50 pages. They're wrong.

I've developed a language called TLA$^+$ that engineers use to write completely formal mathematical descriptions of computer systems. It has tools for checking the correctness of their mathematics. The Riemann integral can be defined in TLA$^+$ in about a dozen lines.

Proofs

A few hundred years ago, proofs were written in prose. They still are. Mathematicians haven't even begun to change the way they write proofs. They think their proofs express rigorous logical reasoning. They're wrong. Their prose proofs are written in a literary style that obscures the logic of the proof. Consider the following opening sentence of a proof from an elementary calculus book by Michael Spivak [4, page 170]—a book that is considered to be very rigorous.

> Let a and b be two points in the interval with $a < b$.

It is obviously wrong because the interval in question could consist of a single point, so it might be impossible to choose a and b. That sentence is actually part of a correct proof, but the reader must discover for herself the proof hidden inside Spivak's prose.

Writing proofs with prose leads to errors. How can those errors be avoided? Most mathematicians and computer scientists believe that the only way is to write machine-checked proofs. This requires writing formulas in a formal language. TLA$^+$ is simple enough that mathematically unsophisticated engineers can use it, and it is enough like everyday math that mathematicians should find it fairly natural. But it's too simple to be adequate

[1] Restricted, unnatural languages have been proposed for writing formulas approximately like (1) so they can be understood by a computer program. Such languages are of little or no use to people not afraid of mathematics.

for writing the kinds of proofs found in most math journal articles. Formalizing such proofs requires a language too complicated for most engineers to learn—one that I believe most mathematicians would find quite obscure. Few mathematicians would go to the effort of learning such a language unless it made writing their proofs significantly easier. Today, it makes writing most proofs much more difficult. Routine machine-checked proofs are now practical in just a few situations, including some safety-critical applications. I don't expect this to change in the next couple of decades.

Fortunately, there is a simple method that anyone can use now to write proofs with fewer errors. It can't eliminate all errors, but it can make them much less likely to occur. Its basic idea is to replace the linear order of ordinary prose by a hierarchical structure, and to name hypotheses and proved facts so they can be referred to later in the proof. Here is a brief explanation of the method; a complete description has appeared elsewhere [2, 3].

A theorem consists of a statement together with its proof. A proof is either a short paragraph or a sequence of statements and their proofs. At each point in a proof, there is a current goal and a set of usable facts that can be assumed in proving that goal. Statements can be written in prose or in math. When written in math, the logical structure of the statement often determines the hierarchical decomposition of its proof. Figure 1 shows the structure of part of a proof containing the statement $A \wedge B \Rightarrow C$, in which C is proved by first proving statements D and E. Usually, those two statements would easily imply C, making the proof of QED step $\langle 3 \rangle 4$ simple. The number $\langle 2 \rangle 3$ indicates that it is the third statement in the level-2 proof of a level-1 statement.

This is a straightforward proof, and presented in this way there seems no reason to structure it. But suppose it were a small part of a large proof, and the proofs of D and E were each half a page long. If the proof were written as prose, how could the reader keep track of where the scope of the hypotheses A and B ended, and where it was no longer valid to use D? Mathematicians try to handle complexity by using Lemmas; but that just provides one level of hierarchy, which doesn't get you very far.

Making a proof more rigorous requires filling in all the gaps that could conceal errors. This means making it longer. Making a prose proof longer makes it harder to read. But with hierarchical structure, the extra length makes the proof easier to read. The additional explanation appears at lower levels of the hierarchy, so it doesn't obscure the structure of the proof. This will be especially true when mathematicians stop producing pictures of print on dead trees and start using hypertext, so lower levels of the proof can be hidden when not being read.

⟨2⟩3. $A \wedge B \Rightarrow C$

Current goal set to $A \wedge B \Rightarrow C$

⟨3⟩1. SUFFICES ASSUME $A,\ B$
PROVE C

Proof: By simple logic. Trivial proof that assuming A and B, then proving C, proves the current goal.

Current goal set to C; and A and B added to usable facts.

⟨3⟩2. D

Proof of D

D added to usable facts.

⟨3⟩3. E

Proof of E

E added to usable facts.

⟨3⟩4. QED

Proof of C

Current goal and usable facts same as before ⟨2⟩3 except with fact $A \wedge B \Rightarrow C$ added.

⟨2⟩4. ...

Figure 1: A statement and its structured proof.

Avoiding errors requires more detailed proofs than are currently found in journals. Until journals use hypertext, this means writing a detailed proof to catch errors, then shortening it for publication. That's easy to do with structured proofs: you just replace the lower levels of the hierarchy with short proof sketches. (One can even write LaTeX macros so a single file can produce either version by changing a few characters.)

Students can learn to write structured proofs by teaching them to write very simple machine-checked proofs in some field. Any good proof system should allow hierarchical structuring of proofs. The language for writing theorems should be simple—not the kind of complicated language needed for serious math. TLA$^+$ and its proof system are not ideal, but they could be used if nothing better is available.

Students should understand that the facts they learn in their math classes can, in principle, be formally proved from simple axioms and proof rules. In practice, we only carry proofs down to the level where we believe the reader will find the steps to be obviously true. That level rises with education and experience. We also sometimes take shortcuts by writing formulas with words. But students and mathematicians should have the confidence that they could make their proofs completely rigorous and carry them down as close as they want to basic axioms.

Writing hierarchically structured proofs can help you avoid errors; it can't guarantee that you will. You have to be honest with yourself about what's obvious and what should be proved. My advice is to write the proof down to a level at which you think everything is obvious, and then go one level deeper. But if you don't care whether your proofs are correct, nothing short of having to write a machine-checked proof will keep you from making errors.

What Should You Do Now?

If you agree that writing formulas with words or that writing proofs with prose is silly, just stop doing it. You don't have to wait for others to change.

Formulas

You needn't remove all the words from your formulas. Start by using the quantifiers $\forall$ and $\exists$. Then try eliminating "...", which is not a mathematical operator. The sequence $x_1, \ldots, x_n$ is just a function x with domain $1 \,..\, n$ that maps each i in its domain to x_i.[2] Often, though not always, the math becomes simpler and more elegant if you eliminate the "..." and instead use the function x. Give it a try. Be aware of when you're using words and sloppy notation instead of being rigorous. If you're open to change, you will find that the mathematically rigorous approach is often the simplest.

If you're a teacher, your students should have learned, or should be learning, the basic math needed to write formulas with fewer words than they now use. Help them to become more comfortable with proper mathematical notation by using it in your classes.

Proofs

There is no reason not to start writing structured proofs now. It takes only a sentence or two to explain to readers how to read them. I've been doing it for about 30 years, and no editor or referee has complained about my proofs. Start by reading how I write structured proofs, but feel free to modify my style as you see fit. There are just two features that should be preserved: hierarchical structuring and the ability to name and refer to hypotheses and already proved statements.

[2] "$..$" is a mathematical operator, defined by $i \,..\, j \triangleq \{k \in \mathbf{Z} : i \leq k \leq j\}$, where $\mathbf{Z}$ is the set of all integers.

If you're a professor, teach your students to structure their proofs the way you do. They're not yet set in their ways, and they'll appreciate how the structure makes your proofs easier to understand. Encourage them to write structured proofs in all their courses. Other professors are unlikely to complain that the proofs are too rigorous; and they might even be inspired to write them themselves.

References

[1] Leslie Lamport. Errors in proofs - a correction and further data. Web page. `https://lamport.azurewebsites.net/tla/proof-statistics.html`.

[2] Leslie Lamport. How to write a proof. In Karen Uhlenbeck, editor, *Global Analysis in Modern Mathematics*, Houston, 1992. Publish or Perish Press. Also appeared in *American Mathematical Monthly 102*, 7 (August-September 1995), 348–369.

[3] Leslie Lamport. How to write a 21st century proof. *Journal of Fixed Point Theory and Applications*, March 2012. DOI: 10.1007/s11784-012-0071-6.

[4] Michael Spivak. *Calculus*. W. A. Benjamin, Inc., New York, 1967.