

## Re: What is a proof, exactly?

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2004-12/6599.html>

---

**From:** J.E. (*troubled6man\_at\_yahoo.com*)

**Date:** 12/09/04

Date: 9 Dec 2004 10:18:00 -0800

"Moreover, I expect that if I write a paper containing only formal proofs, it'd be (1)huge (2)too hard to follow even for relatively simple informal proofs (3)unpublishable in any regular math journal. So why do we care about formal proof?" Because it's the standard we use when people disagree. A formal proof couldn't even technically use theorems. The point is that mathematicians in practise use their own opinions about what is "formalizable" but as long as the standard is there, then if two mathematicians have different "opinions" then the opinions can be tested in a sense. That's what makes it science.

About the number 5, yes my cut-and-paste went wrong, terribly wrong, I was experimenting with some different axioms and didn't realize I was using the "new" macros.

"It is said that [everything being a set] can be done in principle, although personally I'd like to rephrase it as 'everything can be modeled using sets' since when I talk about numbers or graphs or vectorspaces, I don't think of these things as sets at all. They're more like urelements; a primitive notion that doesn't decompose into sets, although we can model them in pure set theory."

Grr (:>), an ur-element \*is\* a set. It contains only itself. I'm not sure one can have more than one urelement if you don't have an equality relation, or maybe even irregular sets of all kinds fall apart without equality, I'd have to think about it. I do think of all numbers, graphs, and vectorspaces as sets myself, I'm slowly learning from usenet that not everyone else does.

"I've been wondering: since math is all in the mind and on paper, wouldn't it be possible to actually have a foundation for mathematics based purely on non-sets? I'm thinking of a term model like kind of thing." Sure you can have "the things" be integers, or even formulas on paper themselves, as long as you have enough of them (an unbounded amount of binary numbers is sufficient) but then you have to "interpret" the relation "x belongs to y" on top of them, which means

## sci.math: Re: What is a proof, exactly?

you end up "thinking of them as sets" anyway.

"But even if you do have them, this is only one means of inference, certainly not the only one." I think you are confusing the "means of inference" with the "meaning of inference", they are different. Inference is silly IMO, validity is more primary and sufficient. Instead of assuming "A is true" and inferring that "T is true", just say "It is true in all possible worlds that either T or not A".

My standard was that rather than saying "T is true" one should STATE the assumptions that FORCE T to be true and just make a universally valid claim like "either it is not the case that A or it is the case that T". Just saying "T is a theorem" is a bit misleading to me, but apparently not to very many other people, though I don't know why.

"is informal maths formalisable using FOL only? I think we use higher order logic, actually. FOL might be enough if you say everything is a set, but if you don't think that's true then FOL seems rather restrictive." Can you give an example where you are proving things that aren't about sets, remember that vector spaces and numbers and such can be sets.

"what is the ontological status of X, Thm, and prf?":

"Does Thm 'exist' in the same sense as X 'exists'? Does prf 'exist' in the same sense as Thm?"

IMO, no thm is a sentence and X is .... well you assumed a proof that X exists, which means that you proved a sentence like "There exists an X, such that S[X]" is true if some other sentences A are true. So I'd consider the sentence "In all possible worlds either (There exists an X, such that S[X]) or it is not the case that all the sentences A are true" to be a universally valid sentence, but the letter X is clearly a variable, a placeholder. Sure placeholders exist, they live in sentences, but you probably mean "the thing that X refers to when S[X] is true", but we don't KNOW that S[X] is EVER true EVEN THOUGH you have a "proof" that says "if all the sentences A are true, then it is true that There exists an X, such that S[X]" because we don't know if the sentences are true. We don't know if X exists, EVEN WITH the proof.

*>If you need an example, let's take this one:"*

*>X := { {} }*

*>Thm := (forall a,b: (aeX and beX) -> a=b) (ie. "X has 1 element")*

*>prf := (take any proof you like, there must be lots)*

What if I interpret "Y = {}" to mean "Y contains everything" and in general "aeX" to mean "a is not in X" and therefore "X:= { {} }" to mean "X is the set that contains all sets except the set that contains everything", then "forall a,b: (aeX and beX) -> a=b" means that "X contains all but one element". So sentences and proofs don't "mean" what one "intended" them to mean when one wrote it. I'm pretty sure

Re: What is a proof, exactly?

sci.math: Re: What is a proof, exactly?

it's impossible to do that.

>My point in this question is exactly that: how do you check  
>whether  $x$  is in the domain of the function?

What do you mean "check"? The only point of math I know of is to make universally valid claims. If someone says "Either it is not the case that all  $A$  are true or it is the case that there exists an  $f$  such (that for all  $x$  either  $x$  is not a real number or  $(x+x=x$  or there is a  $y$  such that either  $y$  is not a real number or  $(x*y=1$  and  $\{\{x\},\{x,y\}\}ef$ )) and (if  $sef$  then there exists and  $x$  and a  $y$  such that  $\{\{x\},\{x,y\}\}ef$ ) and (for all  $x, y, z$ , it is either it is not the case ( $\{\{x\},\{x,y\}\}ef$  and  $\{\{x\},\{x,z\}\}ef$ ) or  $y=z$ ) )" or something similar in case I made a mistake, it's either a validity or it isn't, that they only "checking" required.

>Good answer. The main automated–reasoning response is that (1) we have the  
>de Bruijn criterion: the computer program code must be small enough that it  
>can be checked by hand.

The circuits too? The keyboards? The monitor/printer hardware? The OS source code? The source code of the compiler used to compile the OS source code? The source code of the OS that the compiler that compiled the OS that compiler that program code" was compiled on? The compiler that compiled the compiler that compiled the program code? Binary and circuits, doesn't sound like fun, you'd probably be better off making dedicated hardware.

>(2) we can let the computer emit a 'proof object' that contains the reasoning it followed in >proving the theorem. This proof object can then be checked independently. Does this >influence your opinion?

If a computer wrote a proof readable by a human and it was valid, it would be irrational to deny it's validity. If I human can't, then the next best thing is to have a an proof output that anyone can apply arbitrary automated proof checkers to, but it's not the same, not as good.

>Allow me to play the devil's advocate: in the middle ages, everyone  
>thought the earth was flat.

I don't believe that. The ancient Greeks measured the size of the earth, and the earth casts a shadow on the moon, it's roundness has been obvious to thinking people for a long time and I find these kinds of tales apocraphal, IMO.

>Today everyone thinks the theorem is true, that this–and–this reasoning is sound.

Re: What is a proof, exactly?

sci.math: Re: What is a proof, exactly?

Again I disagree. I haven't ever met a theorem I thought was true. A validity is a truth, but a theorem is usually only the consequent of a validity, not a validity itself.

>You sound like you think maths is a sociological enterprise. Is that true?

Validities are validities regardless of whether anyone has even stated them. If we consider the validities people state, that is sociological, but that's not math anymore.

>> *If we could understand the symbols, then we could make a machine (from*

>> *scratch) to check the proof. More likely I would expect that*

>> *mathematicians would prefer to make a machine that attempted to*

>> *\*simplify\* the proof. Then you can just read the simpler proof, a*

>> *much better case.*

>

>Now for 'pack of paper' substitute 'my computer's proof object', which is

>indeed a string of symbols that my computer has checked. How does this hold

>with your remark (see above)

One computer and one program checked it, but you couldn't simplify it. I wouldn't trust it as is. I think one might be able to make a circuit based on a formal proof that lights for correct proofs and doesn't for incorrect ones, the point is how do you know the circuit was made correctly. It's better to program the computer to make the new concepts and definitions that make the proof readable to a human, that's better in the long run because it means that humans can BUILD on the proof's methods not just the results.