

Re: What is a proof, exactly?

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-12/4091.html>

From: Jasper Stein (*J.J.Stein.Stein_at_cs.cs.ru.ru.nl.nl*)

Date: 12/02/04

Date: Thu, 02 Dec 2004 14:45:44 +0000

J.E. wrote:

>> – *Does the extremely simple theorem "5=5" need a proof? Why (not)?*

>

> *Yes, even more you need a definition of "5" "=" and a standard of proof. Why? Because that's what proving things is all about. If you*

Exactly. I believe that's what I'm after. You say we need a standard of proof – I'm trying to get to know what that standard looks like. As I've said, I come from the automated reasoning community, and I believe our own standard of proof is skewed. So I want to know what the 'standard' standard of proof is.

People have answered that there is a difference between formal proof and informal proof, and that the informal proof should convince the reader that there is a formal proof, being a sequence of statements following from axioms or from rules of inference. But no one seems to bother actually carrying out this transition. 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?

> *define "x=y" as "Az (zex <=> zey)" then there IS a provable theorem*
> *"Ax x=x",*

Nice to see the defined equality boil down to a logical one in this case (after all, for all predicates P we have "Az P(z)<=>P(z)")

> *so then as long as "5" is a set (usually*
> *{ {}, {{}}, {{{}}, {{{{}}}, {{{{{{}}}}} }*

I thought usually it something else, but never mind :-)

```
{ {},
  {{}},
  { {}, {{}} },
  { {}, {{}}, { {}, {{}} } },
  { {}, {{}}, { {}, {{}} } }, { {}, {{}}, { {}, {{}} } } }
}
```

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

- > then "5=5" is a theorem too, the
- > proof of the more general theorem already covers when x happens to be
- > 5 assuming you defined 5 to be a set.

So you assume everything to be a set. It is said that this 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 vector spaces, 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.

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.

- >> – How is a proof different from just an explanation? Is there a
- >> difference
- >> at all?
- >
- > The usual standard is that a proof (of T relative to A) is a
- > demonstration that if T were false then A would be false too. So if

??? That can't possibly be true. Deriving $A \rightarrow T$ from $\sim T \rightarrow \sim A$ isn't even possible if you haven't got the law of excluded middle (ie. forall P, P or $\sim P$) or equivalently double negation (forall P, $\sim\sim P \rightarrow P$).

But even if you do have them, this is only one means of inference, certainly not the only one.

- > the assumption is "A", then "A" is a theorem, in the usual standard.
- > I'm assuming the is an ordinary first order logic system.

This raises another interesting question: 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.

- >> – Suppose we defined an object X. Then we state a theorem Thm. about X,
- >> which we subsequently prove by a proof prf. According to the main
- >> school(s) of mathematics, 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?
- >
- > I'm not sure you meant this as written, just defining something
- > doesn't entail proving that it exists, so the ontological status of X
- > is undetermined at this point.

Okay, that's true. But if we can prove the existence of X, then what's your opinion? If you need an example, let's take this one:

$X := \{ \{ \} \}$

Thm := (forall a,b: (aeX and beX) \rightarrow a=b) (ie. "X has 1 element")

Re: What is a proof, exactly?

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

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

- >> – *Once we defined X as above, we can make additional definitions Y, Z,*
- >> ...
- >> *depending on X. Can we also make definitions depending on Thm? On prf?*
- >> *Can you comment on the definition of the reciprocal ($\frac{1}{x}$ to*
- >> *$\frac{1}{x}$), which seems to depend not only on x but also on a*
- >> *'theorem' stating that $x \neq 0$? Does it also depend on a proof of such*
- >> *a theorem? How?*

[...skipping "definition == shorthand", with which I agree mostly – in type theory you ARE doing something: making a definition means extending the context, unfolding a definition is doing a delta reduction...]

- > *the point is*
- > *that there is a function f that takes each non-zero real to it's*
- > *reciprocal, so $1/x$ can be thought of as $f(x)$ and checking that $x=0$ is*
- > *just like checking that a number is in the domain of a function and*
- > *then finding the value of the function.*

My point in this question is exactly that: how do you check whether x is in the domain of the function? In general that's undecidable. If you're a classical mathematician (ie. believing in classical logic) then decidability isn't an issue in principle, but in practice it is. The prime example would be the number (let's call it "a") defined by decimal expansion, where digit n is 1 if a sequence of 99 9's has occurred prior to position n in the expansion of π , and 0 otherwise. So (classically speaking) a is either 0 or 0.000...01111... Now how does one check whether $1/a$ makes sense? For this we need a proof that actually $a \neq 0$, ie. a proof that π has a series of 99 9's somewhere in its expansion. (And as of today this is unproved.)

- > *so why should I trust a proof by that is checked only by a computer?*

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. (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? Why (not)?

- >> – *This code calculated and checked a few thousands of 'configurations'.*
- >> *If*
- >> *these calculations and the checking were done by mathematicians, would*
- >> *the proof be still as controversial? Why (not)?*
- >
- > *It's not one mathematician versus one computer, it's the fact that so*
- > *few independant minds would actually go through the bother of checking*
- > *it. It's just not as trustworthy, because it's been checked a smaller*
- > *number of both quality and independant times.*

Re: What is a proof, exactly?

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

Allow me to play the devil's advocate: in the middle ages, everyone thought the earth was flat. Today everyone thinks the theorem is true, that this—and–this reasoning is sound.

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

> *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)

> *so why should I trust a proof by that is checked only by a computer?*

By the way, thanks for having taken so much time already to answer my questions. (And this goes for others who responded as well!) I hope you and others can find the time to answer my further questions too – they're quite important to me, because they bear on what I'm doing for my job every day, and I'm doubtful (as you may have noticed)...

Jasper

--

The problem with having an open mind is that people toss in garbage