What does it mean to formalise and why do it

Riccardo Brasca

Atelier Lean 2023

May 2nd 2023

What is formalization of mathematics?

Formalization is a process that consists in using a computer to *raison*

What is formalization of mathematics?

Formalization is a process that consists in using a computer to *raison*

This is different from using tools as Pari, Sage, Maple. . .

What is formalization of mathematics?

Formalization is a process that consists in using a computer to *raison*

This is different from using tools as Pari, Sage, Maple. . .

Formalization is done using *proof assistants*

What is formalization of mathematics?

Formalization is a process that consists in using a computer to *raison*

This is different from using tools as Pari, Sage, Maple. . .

Formalization is done using *proof assistants*
There are several proof assistants

What is formalization of mathematics?

Formalization is a process that consists in using a computer to *raison*

This is different from using tools as Pari, Sage, Maple. . .

Formalization is done using *proof assistants*
There are several proof assistants
We will speak about Lean

Proof assistants

A proof assistants takes care of several aspects of the formalization process:

Proof assistants

A proof assistants takes care of several aspects of the formalization process:

- it translates something written by human beings to something totally precise

Proof assistants

A proof assistants takes care of several aspects of the formalization process:

- it translates something written by human beings to something totally precise
- it can do certain simple computations automatically

Proof assistants

A proof assistants takes care of several aspects of the formalization process:

- it translates something written by human beings to something totally precise
- it can do certain simple computations automatically
- it checks the correctness of the proofs, starting from the axioms

The first two parts are very complex

The first two parts are very complex, the goal for a user of the proof assistant is to write math as on a blackboard

The first two parts are very complex, the goal for a user of the proof assistant is to write math as on a blackboard
If x and y are real numbers, we write

$$x + y$$

The first two parts are very complex, the goal for a user of the proof assistant is to write math as on a blackboard
If x and y are real numbers, we write

$$x + y$$

$\mathbb{R}$ is endowed with several sums

The first two parts are very complex, the goal for a user of the proof assistant is to write math as on a blackboard
If x and y are real numbers, we write

$$x + y$$

$\mathbb{R}$ is endowed with several sums as a field, ring, group...

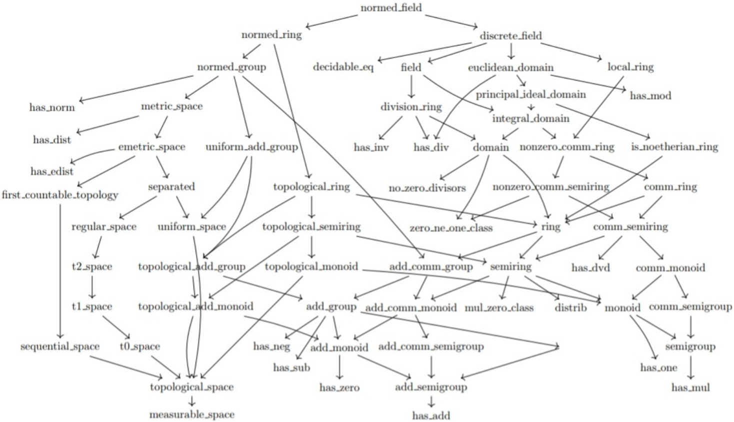


Image de Jeremy Avigad

Checking of correctness is done by the *kernel* of the proof assistant

Checking of correctness is done by the *kernel* of the proof assistant
It is a simple software

Checking of correctness is done by the *kernel* of the proof assistant
It is a simple software, easy to check

Checking of correctness is done by the *kernel* of the proof assistant

It is a simple software, easy to check and there are several independent versions

Checking of correctness is done by the *kernel* of the proof assistant
It is a simple software, easy to check and there are several independent versions

A bug in the kernel is very unlikely

Checking of correctness is done by the *kernel* of the proof assistant
It is a simple software, easy to check and there are several independent versions

A bug in the kernel is very unlikely

Bugs in the other parts of the proof assistant surely exist

Checking of correctness is done by the *kernel* of the proof assistant
It is a simple software, easy to check and there are several independent versions

A bug in the kernel is very unlikely

Bugs in the other parts of the proof assistant surely exist but this is less important

Lean

Lean has been developed by Leonardo de Moura at Microsoft Research in 2013

Lean

Lean has been developed by Leonardo de Moura at Microsoft Research in 2013

It is a *open source* software

Lean

Lean has been developed by Leonardo de Moura at Microsoft Research in 2013

It is a *open source* software

The current version is 3.50.3.

Lean

Lean has been developed by Leonardo de Moura at Microsoft Research in 2013

It is a *open source* software

The current version is 3.50.3. Lean 4 is ready and we are porting everything

Lean

Lean has been developed by Leonardo de Moura at Microsoft Research in 2013

It is a *open source* software

The current version is 3.50.3. Lean 4 is ready and we are porting everything

Mathlib is Lean's official mathematical library

Lean

Lean has been developed by Leonardo de Moura at Microsoft Research in 2013

It is a *open source* software

The current version is 3.50.3. Lean 4 is ready and we are porting everything

Mathlib is Lean's official mathematical library
It has the level of an advanced undergraduate or first year graduate student in mathematics (around 1.2 millions lines of code)

Why formalize mathematics

Why formalize mathematics

We're having fun

Why formalize mathematics

We're having fun

Formalization is challenging

Why formalize mathematics

We're having fun

Formalization is challenging

It invites us to rethink basic mathematical concepts from a different point of view

Checking correctness - LTE

Checking correctness - LTE

There are proofs are too big even for experts:

Checking correctness - LTE

There are proofs are too big even for experts:

- classification of finite simple groups

Checking correctness - LTE

There are proofs are too big even for experts:

- classification of finite simple groups
- a lot of results in number theory

Checking correctness - LTE

There are proofs are too big even for experts:

- classification of finite simple groups
- a lot of results in number theory

In December 2021 Scholze asked for a verification of the following theorem

Checking correctness - LTE

There are proofs are too big even for experts:

- classification of finite simple groups
- a lot of results in number theory

In December 2021 Scholze asked for a verification of the following theorem

Theorem (Clausen-Scholze)

Let $0 < p' < p \leq 1$ be real numbers, S a profinite set and V a p-Banach space.

Checking correctness - LTE

There are proofs are too big even for experts:

- classification of finite simple groups
- a lot of results in number theory

In December 2021 Scholze asked for a verification of the following theorem

Theorem (Clausen-Scholze)

Let $0 < p' < p \leq 1$ be real numbers, S a profinite set and V a p-Banach space. Then

$$\mathrm{Ext}^1_{\mathrm{Cond(Ab)}}(\mathcal{M}_{p'}(S), V) = 0.$$

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Why do I want a formalization?

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Why do I want a formalization?

- *... I think the theorem is of utmost foundational importance, so being 99.9 % sure is not enough*

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Why do I want a formalization?

- *... I think the theorem is of utmost foundational importance, so being 99.9 % sure is not enough*
- *... As it will be used as a black box, a mistake in this proof could remain uncaught*

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Why do I want a formalization?

- *... I think the theorem is of utmost foundational importance, so being 99.9 % sure is not enough*
- *... As it will be used as a black box, a mistake in this proof could remain uncaught*
- *... In the end, we were able to get an argument pinned down on paper, but I think nobody else has dared to look at the details of this, and so I still have some small lingering doubts*

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Why do I want a formalization?

- *... I think the theorem is of utmost foundational importance, so being 99.9 % sure is not enough*
- *... As it will be used as a black box, a mistake in this proof could remain uncaught*
- *... In the end, we were able to get an argument pinned down on paper, but I think nobody else has dared to look at the details of this, and so I still have some small lingering doubts*
- *... It is the kind of argument that needs to be closely inspected*

Here is Scholze on the *Xena project* blog (Kevin Buzzard's blog):

Why do I want a formalization?

- *... I think the theorem is of utmost foundational importance, so being 99.9 % sure is not enough*
- *... As it will be used as a black box, a mistake in this proof could remain uncaught*
- *... In the end, we were able to get an argument pinned down on paper, but I think nobody else has dared to look at the details of this, and so I still have some small lingering doubts*
- *... It is the kind of argument that needs to be closely inspected*
- *While I was very happy to see many study groups on condensed mathematics throughout the world, to my knowledge all of them have stopped short of this proof. (Yes, this proof is not much fun...)*

- *From what I hear, it sounds like the goal is not completely out of reach. ... If achieved, it would be a strong signal that a computer verification of current research in very abstract mathematics has become possible. I'll certainly be excited to watch any progress*

- *From what I hear, it sounds like the goal is not completely out of reach. ... If achieved, it would be a strong signal that a computer verification of current research in very abstract mathematics has become possible. I'll certainly be excited to watch any progress*
- *I think this may be my most important theorem to date*

- *From what I hear, it sounds like the goal is not completely out of reach. ... If achieved, it would be a strong signal that a computer verification of current research in very abstract mathematics has become possible. I'll certainly be excited to watch any progress*
- *I think this may be my most important theorem to date*
- *I didn't think I'd have the mental capacity to rebuild this in my head again*

- *From what I hear, it sounds like the goal is not completely out of reach. ... If achieved, it would be a strong signal that a computer verification of current research in very abstract mathematics has become possible. I'll certainly be excited to watch any progress*
- *I think this may be my most important theorem to date*
- *I didn't think I'd have the mental capacity to rebuild this in my head again*

In around six months we finished the most technical (and Scholze's main question) part of the theorem

Adam Topaz 7:58 PM

Yeah exactly. This is what I was worried about.

EDITED I *think* the order of the quantifiers can probably be reversed if one assumes completeness, because then for each epsilon you would get an element and eventually have to prove that those elements converge (I don't know if the details would actually work out). 8:01 PM

Riccardo Brasca 8:03 PM

I was thinking to it, but I am really sure this doesn't work for making the $\inf$ in the definition of the quotient norm a $\min$. Of course it can still work for our elements for some reasons but still, something has to be done

Peter Scholze 11:54 PM

Ah!

Sorry, indeed you caught something there. Let me think about this. 11:54 PM

One option might be to change the meaning of $\leq k$-exactness, to also include an inf 11:55 PM

Hmm. It should be possible to fix this by a small tweaking of some definition, but let me try to figure out a good global fix to this. I'll keep you posted. 11:59 PM

JAN 21, 2021 — JAN 22, 2021

Peter Scholze 12:50 AM

Probably this is just my mind making up a solution as I want to go to bed, but I think the following fix ought to work. Leave all the statements and definitions essentially unchanged, but replace all normed abelian groups with complete normed abelian groups. In particular, in 9.10, the quotient $N = M'/M$ is implicitly completed. Then I think 9.10 stays true as stated, except that one may have to replace $k^3 + k$ by something slightly different.

I'll try to update the file tomorrow 12:51 AM

The project was completed on July 14th, 2022

The project was completed on July 14th, 2022 by a team of around 15 people

The project was completed on July 14th, 2022 by a team of around 15 people

Joahn Commelin

The project was completed on July 14th, 2022 by a team of around 15 people

Joahn Commelin   Adam Topaz

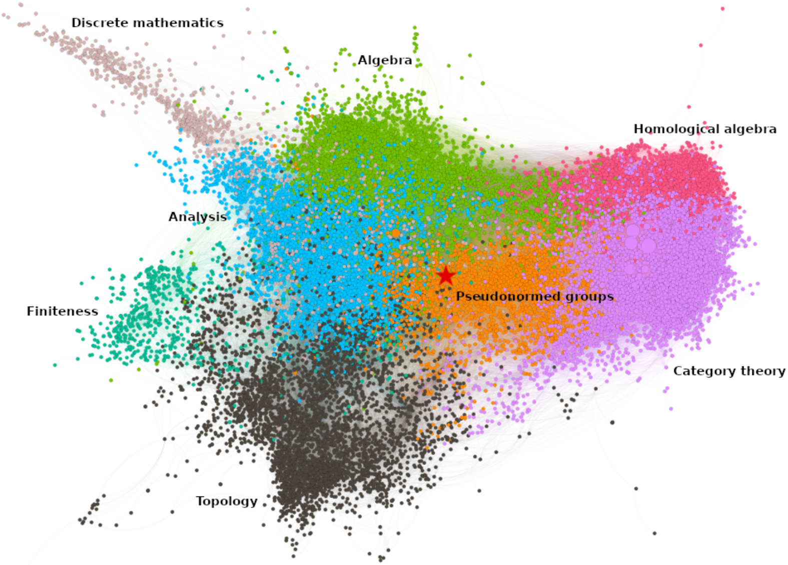
The project was completed on July 14th, 2022 by a team of around 15 people

Joahn Commelin	Adam Topaz
Riccardo Brasca	Kevin Buzzard
Mario Carneiro	Heather Macbeth
Patrick Massot	Bhavik Mehta
Scott Morrison	Filippo A.E. Nuccio
Joël Riou	Damiano Testa
Andrew Yang	many others

- *... I am excited to announce that the Experiment has verified the entire part of the argument that I was unsure about. I find it absolutely insane that interactive proof assistants are now at the level that within a very reasonable time span they can formally verify difficult original research*

- *... I am excited to announce that the Experiment has verified the entire part of the argument that I was unsure about. I find it absolutely insane that interactive proof assistants are now at the level that within a very reasonable time span they can formally verify difficult original research*
- *... When I wrote the blog post half a year ago, I did not understand why the argument worked*

- *... I am excited to announce that the Experiment has verified the entire part of the argument that I was unsure about. I find it absolutely insane that interactive proof assistants are now at the level that within a very reasonable time span they can formally verify difficult original research*
- *... When I wrote the blog post half a year ago, I did not understand why the argument worked*
- *The Lean Proof Assistant was really that: An assistant in navigating through the thick jungle that this proof is. Really, one key problem I had when I was trying to find this proof was that I was essentially unable to keep all the objects in my "RAM" ... So I think here we have witnessed an experiment where the proof assistant has actually assisted in understanding the proof*


Discrete mathematics
Algebra
Homological algebra
Analysis
Finiteness
Pseudonormed groups
Category theory
Topology

Formalization can help the working mathematician

Formalization can help the working mathematician

- The reader (and not the author) can choose the level of details

Formalization can help the working mathematician

- The reader (and not the author) can choose the level of details

- Database of *results* rather than database of papers

Formalization can help the working mathematician

- The reader (and not the author) can choose the level of details
- Database of *results* rather than database of papers
- Collaboration is sometimes easier

Formalization can help the working mathematician

- The reader (and not the author) can choose the level of details
- Database of *results* rather than database of papers
- Collaboration is sometimes easier
- Teaching

Mathematical gains

Mathematical gains

Formalization can help *understanding*

Mathematical gains

Formalization can help *understanding*

Consider the following easy lemma

Lemma

Let (u_n) *and* (v_n) *be sequences of real numbers and let* $\ell \in \mathbb{R}$. *If* $\lim u_n = \ell^+$ *and* $\lim v_n = -\infty$ *then*

$$\lim(u_n + v_n) = -\infty.$$

Mathematical gains

Formalization can help *understanding*
Consider the following easy lemma

Lemma

Let (u_n) *and* (v_n) *be sequences of real numbers and let* $\ell \in \mathbb{R}$*. If* $\lim u_n = \ell^+$ *and* $\lim v_n = -\infty$ *then*

$$\lim(u_n + v_n) = -\infty.$$

This is done in Lean (and in other proof assistants) using *filters*

Mathematical gains

Formalization can help *understanding*
Consider the following easy lemma

Lemma

Let (u_n) and (v_n) be sequences of real numbers and let $\ell \in \mathbb{R}$. If $\lim u_n = \ell^+$ and $\lim v_n = -\infty$ then

$$\lim(u_n + v_n) = -\infty.$$

This is done in Lean (and in other proof assistants) using *filters*.
Already done in Bourbaki.

Mathematical gains

Formalization can help *understanding*
Consider the following easy lemma

Lemma

Let (u_n) *and* (v_n) *be sequences of real numbers and let* $\ell \in \mathbb{R}$. *If* $\lim u_n = \ell^+$ *and* $\lim v_n = -\infty$ *then*

$$\lim(u_n + v_n) = -\infty.$$

This is done in Lean (and in other proof assistants) using *filters*.
Already done in Bourbaki.

Breen-Deligne resolution in LTE

Theorem

let $f : X \to Y$ be a continuous function, where X and Y are metric spaces with X compact. Then f is uniformly continuous.

Proof.

Let $\varepsilon > 0$ and let

$$K = \{(A, B) \in X \times X \mid \varepsilon \leq d(f(A), f(B))\}.$$

We have that K is closed and hence compact. Let $(P_1, P_2) \in K$ be a minimum of the distance function and let $\delta = d(P_1, P_2)$. If $A, B \in X$ are such that $d(A, B) < \delta$ but $d(f(A), f(B)) \geq \varepsilon$ then $(A, B) \in K$, so $\delta = d(P_1, P_2) \leq d(A, B)$, that is absurd. □