

Foundations of proof assistants: impact on student perception of proof

Iro Bartzia Emmanuel Beffara Antoine Meyer
Julien Narboux

ThEdu 2023 - Roma

Table of contents

- 1 Epistemology of proof and proof assistants
- 2 Epistemology of proof and foundations of proof assistants

Motivations for teaching proof and proving using proof assistants

- 1 student understanding of the concept of proof
 - “getting students to recognize the logical form of a mathematical statement”
 - “provide a robust understanding of mathematical proof”

Avigad¹
- 2 feedback
 - “give instant feedback without compromising student autonomy”

Hanna²

¹Jeremy Avigad (2019). “Automated reasoning for the working mathematician”.
In: *Frontiers of Combining Systems (FroCoS)*

²Gila Hanna, Brendan Larvor, and Xiaoheng (Kitty) Yan (Feb. 2023).
“Human-Machine Collaboration in the Teaching of Proof”. In: *Journal of Humanistic Mathematics* 13.1

Previous work

In previous work³, we studied an exercise using several proof assistants (Coq, Deaduction, Edukera, Lean (Verbose), Lurch) and provided an a priori analysis of potential impact of some features.

Exercise

Given three sets A , B and C such that $C \subseteq A$ and a function $f: A \rightarrow B$, show that if f is injective then $f^{-1}(f(C)) = C$.



³Evmorfia Bartzia, Antoine Meyer, and Julien Narboux (Oct. 2022). “Proof assistants for undergraduate mathematics and computer science education: elements of a priori analysis”. In: *INDRUM 2022: Fourth conference of the International Network for Didactic Research in University Mathematics*

Our focus today

In this talk, we focus on motivation 1 for using proof assistants in the classroom: understanding proofs.

We provide some thoughts about the **potential** links between teacher/student conception of proof and the use/design of proof assistants.

This should be considered as an *a priori* analysis to prepare the design of lectures and tools or further studies about the impact of the use of these tools.

Table of contents

1 Epistemology of proof and proof assistants

2 Epistemology of proof and foundations of proof assistants

Epistemology of proof

Maths educators agree that teachers/researchers perception of proof is not unique.

David Reid⁴ distinguishes two trends:

- ① “traditional concept of proof” : derivations providing absolute validity
- ② “proof as part of a quasi-empirical process, in which proofs operate to clarify and make the detection of errors easier” (Lakatos “Proofs and Refutations”, ...)

This second vision emphasizes other purposes of proof: to explore, to communicate or to explain.

⁴David A. Reid (2005). “The meaning of proof in mathematics education”. In: *CERME 4*

David Reid (reviewing work by Godino, Recio, and Balacheff) identified five dimensions in which the meaning of proof and proving differ.

the concept of proof what counts as a proof is different in formal logic, mainstream mathematics, and schools

the purpose of teaching proof for transfer to other contexts / better understanding of the nature of mathematics

the kinds of reasoning proving is seen to involve only deductive reasoning or including other modes of reasoning

the needs that proving is seen to address verification only or also exploration, explanation, systematisation, communication and social acceptance (see Villiers, Hanna)

the relationship seen between proof and language diagrammatic proofs / semantics vs syntax

Proof vs proving

Types of reasoning involved in proofs:

- ① deductive

Types of reasoning involved in proving:

- ① deductive
- ② abductive
- ③ inductive
- ④ conceptualization
- ⑤ counterexample finding
- ⑥ ...

Different points of view on proof can lead to different choices:

Pure validation Proof assistant using tactic languages (Coq/SSReflect, Lean...)

Validation and communication Proof assistant with declarative or controlled natural language (Mizar, Isabelle/Isar, Lean Verbose, Coq Waterproof, Lurch...)

Conceptualization/Conjectures/Counterexamples HRL (Alison Pease and Simon Colton), QED-Tutrix (Philip Richard)

Proving/Proof assistants

Do we need systems which

- allow statements “detached” from hypothesis and goal ? or restrict to backward/forward reasoning ?
- allow incorrect reasoning ?
- asks for or provides counterexamples ?
- help studying examples ? or generic examples (sketches) ?
- help visualizing the proofs ?
- help visualizing the semantics of the statements ?
- allow modifying the definitions ?
- provide examples outside maths (transfer) ?

Impact of using proof assistants

“what counts as a proof” is what is what is accepted by the system
This leads to tensions between informal and formal proofs:

automation of proof steps non alignment between what the system can prove, and what the teacher would accept:

- students or teachers are frustrated when the system does not accept something they consider as trivial,
- but some exercises can be solved completely automatically by the proof assistant.

automation of unfolding of definitions the system knows the definitions and can unfold perfectly

- wrong impression of success which can lead to difficulties on paper (\rightarrow Lean Verbose / Coq Waterproof)
- real success, since we obtained a proof ?

interaction mode undo and automatic application of logical rules can lead to a strategy: proving by trial and error

Experience report in the classroom

Context: Course about interactive and automatic reasoning in geometry, M1 (Fourth year) at University of Strasbourg.

I proposed two activities:

- 1 Prove some high-school exercises based on a precise formalization of geometry (axioms and theorems of the GeoCoq library)
- 2 Choose one of the numerous proofs of Pythagorean theorem and propose a (partial) formalization.

The second activity lead to very interesting discussions about:

- nature of the statement
- validity of the proofs
- other purpose of the proof: explanation
- simplicity
- validity of visual proofs
- circularity of proofs
- generality of the statement (proof in a model vs proof in every model)

Table of contents

1 Epistemology of proof and proof assistants

2 Epistemology of proof and foundations of proof assistants

Foundations of proof assistants

Proof assistants are built on different foundations:

- Type theory (Coq, Lean, Matita, Agda),
- Set theory (Mizar, Isabelle/ZFC),
- Higher-order logic (HOL-Light, Isabelle/HOL)

Foundations of proof assistants and classroom use

Two strategies wrt. foundations⁵:

- 1 Try to hide the foundations
 - ▶ Example: Distinction between the introduction rule for \Rightarrow (“Assume that n is even”) and introduction rule for \forall (“Fix n / Take n ”) in Lean Verbose and CoqWaterProof.
- 2 Explicitly teach the proof assistant and its foundations

⁵M. Kerjean et al. (Oct. 2022). “Utilisation des assistants de preuves pour l’enseignement en L1 - Retours d’expériences”. French. In: *La Gazette de la Société Mathématique de France* 174

But foundations of proof assistants are difficult to hide

- In HOL every type is inhabited, whereas in Lean/Coq not all types are inhabited. $\forall x P(x) \Rightarrow \exists x P(x)$ is provable in Isabelle, and false in Coq.
- Meta-theory is explicit in Isabelle:

$$\bigwedge x_1 \dots x_p. \llbracket A_1; \dots ; A_n \rrbracket \Longrightarrow B$$

where as in Coq/Lean meta conjunction forall is not displayed.

Computations

In Coq:

- Extensionality is not always taken for granted:

$$(\forall x, f(x) = g(x)) \Rightarrow f = g$$

- $a + 0$ does not behave the same way as $0 + a$
- functions are total

Meta-theory in Mizar

Mizar is based on first-order logic, so higher order axioms/theorem require a different syntax for schemes.

```
scheme :: NAT_1:sch 1
Ind { P[Nat] } :
for k being Nat holds P[k]
provided
P[0]
and
for k being Nat st P[k] holds P[k + 1];
```

Foundations also appear in standard libraries:

- two versions of the same lemma using meta-quantifiers or quantifiers in Isabelle
- proof terms in Lean or Coq
- ...

Brouwer-Heyting-Kolmogorov semantics

Brouwer-Heyting-Kolmogorov semantics consist in viewing proof as functions.

- A proof of $A \rightarrow B$ is a *function* which takes as argument a proof of A and returns a proof of B .
- A proof of $A \wedge B$ is a *pair* composed of a proof of A and a proof of B .
- A proof of $A \vee B$ is a pair (i, p) with ($i = 0$ and p a proof of A) or ($i = 1$ and p a proof of B).
- A proof of $\forall x.A$ is a function which, for each object t constructs an object of type $A[x := t]$.

Foundations also appear in proof languages

In the tactic language: one can apply lemma to argument to instantiate universally quantified variables and assumptions using the SAME syntax.

“ apply H1 in H2. ”

In the standard library:

```
theorem subset_preimage_image {f : a → b} (s : set a) :  
  s ⊆ f ⁻¹ (f '' s) :=  
  x hx, x, hx, rfl
```

```
theorem preimage_image_subset {f : a → b} (s : set a) :  
  function.injective f → f ⁻¹ (f '' s) ⊆ s :=  
  hf x y, hys, hxy, hf hxy |> hys
```

```
theorem eq_preimage_image {f : a → b} (s : set a) :  
  function.injective f → f ⁻¹ (f '' s) = s :=  
  hf, set.subset.antisymm  
    (preimage_image_subset s hf)  
    (subset_preimage_image s)
```

Proof by reflection

a proof of the prover + computation = proof

Conclusion

- Teachers' perceptions of the concept proof are diverse.
- Should tools take into account all aspects of the process of proving (not only validation) ?
- Mode of interaction with the proof assistant can have an impact on the vision of what is a proof and how to find proofs.
- Foundations of proof assistants are visible to the user and can have an impact on its perception

Thank you

If you are interested in making experiments with your students, please contact me.

Bibliography



Avigad, Jeremy (2019). “Automated reasoning for the working mathematician”. In: *Frontiers of Combining Systems (FroCoS)*. Invited Talk. London.



Bartzia, Evmorfia, Antoine Meyer, and Julien Narboux (Oct. 2022). “Proof assistants for undergraduate mathematics and computer science education: elements of a priori analysis”. In: *INDRUM 2022: Fourth conference of the International Network for Didactic Research in University Mathematics*. Ed. by María Trigueros. Hanovre, Germany: Reinhard Hochmuth.



Hanna, Gila, Brendan Larvor, and Xiaoheng (Kitty) Yan (Feb. 2023). “Human-Machine Collaboration in the Teaching of Proof”. In: *Journal of Humanistic Mathematics* 13.1, pp. 99–117.



Kerjean, M. et al. (Oct. 2022). “Utilisation des assistants de preuves pour l’enseignement en L1 - Retours d’expériences”. French. In: *La Gazette de la Société Mathématique de France* 174.



Reid, David A. (2005). “The meaning of proof in mathematics education”. In: *CERME 4*.