ICMS 2018

A New Style of Mathematical Proof

William M. Farmer

Department of Computing and Software
McMaster University

25 July 2018

A Universal Digital Mathematics Library

- The holy grail of mathematical software systems is a universal digital mathematics library (UDML) in which essentially all public mathematical knowledge resides.
  - It will be highly distributed like the World Wide Web.
  - The knowledge in it will be extremely interconnected.
  - There will be a rich set of "laboratory" tools to explore, access, and extend its knowledge base.
- Mathematical proofs will play a crucial role in a UDML: they will be the threads that tie the knowledge in a UDML together.
- A UDML will be revolutionize mathematics practice!

Architecture for a UDML

- We believe that the best architecture for a UDML is a theory graph of axiomatic theories connected by theory morphisms.
- The theories serve as mathematical models at various levels of abstraction.
- The morphisms are meaning-preserving mappings from the formulas of one theory to those of another.
  - Serve as information conduits.
  - Provide an infrastructure for finding relevant concepts and facts.
- Supports the little theories method in which mathematics is:
  1. Formalized in the most convenient logic at the most convenient level of abstraction using the most convenient vocabulary.
  2. Then applied in many different contexts across the theory graph.

Styles of Mathematical Proof

- A proof is an argument that is intended to show that a statement is a logical consequence of a set of premises.
- There are many styles of proof such as:
  - A description of a deduction.
  - A prescription of how to produce a deduction.
  - A deduction presented in a two-column format.
  - A computation.
  - A construction.
  - A geometric proof.
  - A visual proof.
- Two important — and competing — styles are:
  1. The traditional proof style.
  2. The formal proof style.

Traditional Proof Style

- A traditional proof is an argument for some intended audience expressed in a stylized form of natural language.
- The terminology and notation may be ambiguous, assumptions may be unstated, and the argument may contain gaps.
- The reader is expected to be able to resolve the ambiguities, identify the unstated assumptions, and fill in the gaps.
- The writer has great freedom to express traditional proofs in whatever manner that is deemed to be most effective.
  - The main focus is usually on making key ideas understandable.
  - Low-level details are usually performed by computation or left to be verified by the reader.

Formal Proof Style

- A formal proof is a derivation in a proof system for a formal logic.
- Software systems can be used to interactively develop and mechanically check formal proofs.
- The writer is highly constrained by the logic, the proof system, and the fact that every detail must be verified.
- As a result, the meaning of the theorem and the key ideas of proof may not be readily apparent to the reader.
- But there is a very high assurance that the theorem is correct!

The Purposes of Mathematical Proofs

- Proofs are usually intended to serve several purposes that include:
  1. Communicating mathematical ideas.
  2. Certifying that mathematical results are correct.
  3. Discovering new mathematical facts.
  4. Learning mathematics.
  5. Showing the universality of mathematical results.
  6. Establishing coherency with a body of mathematical knowledge.
  7. Creating mathematical beauty.
- A UDML needs a style of proof that fulfills all of these purposes!
- Both traditional and formal proofs fall short.

Purpose 1: Communication

- The main purpose of a proof given in a textbook and scientific paper is to communicate to the reader why a theorem is true.
  - They are used to convey insight and to build intuition.
- The highly flexible style of traditional proofs is usually a much better vehicle for communication than the highly constrained style of formal proofs.
  - This is especially true when the key ideas are considered a bigger concern than the low-level details of the proof.

Purpose 2: Certification

- A proof is used to certify that a statement follows from a set of premises.
- The proof is a certificate that can be independently checked.
- A traditional proof can be checked by hand by members of the intended audience.
  - May be difficult to check by someone outside of the audience.
  - May contain mistakes that are not easily noticed.
- A formal proof can be mechanically checked by software alone.
  - Offers the highest level of certification.

Purpose 3: Discovery

- A proof is often formulated as a provisional argument that can be used to discover new theorems.
  - Imre Lakatos presents this idea in Proofs and Refutations.
- Example:
  1. A proof attempt of a conjecture leads to a subconjecture.
  2. A local counterexample to the subconjecture is discovered.
  3. The local counterexample is actually a global counterexample.
  4. The conjecture and the proof attempt are repaired.
  5. The process is continued.
- Traditional proofs are well suited for expressing provisional arguments that can be analyzed by humans.
- Formal proofs are too rigid to express provisional arguments.
- On the other hand, machines can be used to analyze the structure of a formal proof much easier than a traditional proof.

Purpose 4: Learning

- The most effective way to learn mathematics is to read and write proofs.
- Today traditional proofs are generally easier to read and write than formal proofs.
- With effective software support, reading and writing formal proofs can be made much easier than it is now.

Purpose 5: Universality

- A proof is universal if it is expressed without superfluous ideas.
  - It can thus be applied in every context in which the conditions of the proof hold.
- A traditional proof can be expressed in a universal manner, but its underlying logical foundation is usually implicit.
- A formal proof has a precise mathematical home, but the home is usually not connected to many other contexts in which the proof can be applied.

Aside: Cross Checks

- A cross check of a theorem compares the theorem or its proof with known facts.
  - Used to find contradictions or unexpected relationships.
  - Georg Kreisel has emphasized the importance of cross checks.
- Examples of cross checks:
  - A similar proof of a similar theorem.
  - An independently proved logical consequence of the theorem (e.g., a special case or a corollary) .
  - An independently proved instance of the theorem (e.g., a more concrete version of the theorem or a dual of the theorem).
- Cross checks establish valuable connections between mathematical knowledge.
- Cross checks are important and widely used but rarely written down and not considered part of a traditional or formal proof!

Purpose 6: Coherency

- A theorem is coherent with a body of mathematics if it fits into the body without any contradictions or unexpected relationships.
- A proof by itself does not establish that the theorem is coherent.
  - Most mathematicians are reluctant to accept a theorem on only the basis of its proof.
- Coherency is established by cross checks.

Purpose 7: Beauty

- Mathematics is a utilitarian art form like architecture and industrial design.
- The desire to create beauty (called "elegance") is one of the strongest driving forces in mathematics.
- Mathematicians seek to develop proofs that are elegant as well as correct.
- Some mathematicians will not accept a theorem until an elegant proof of the theorem has been found.
- It appears to be easier to write beautiful proofs with the highly flexible style of traditional proofs than with the highly constrained style of formal proofs.

Comparison Summary

	Traditional Proofs	Formal Proofs
Communication	●	◒
Certification	◒	●
Discovery (Human)	●	○
Discovery (Machine)	○	●
Learning (Reading)	◒	◒
Learning (Writing)	◒	◒
Universality	◒	◒
Coherency	○	○
Beauty	●	○

● : high; ◒ : medium high; ◒ : medium low; ○ : low.

A Proposed New Style of Proof [1/2]

- We propose a new style of proof having four components:
  1. A home theory **HT** consisting of:
     a. A formal logic **Log**.
     b. A language **Lang** in **Log**.
     c. A set **Axms** of formulas in **Lang** that are the axioms of **HT**.
  2. A theorem **Thm** that is a formula of **Lang** purported to be a logical consequence of **Axms**.
  3. An argument **Arg** showing **Thm** is a logical consequence of **Axms**.
  4. A set **CC** of cross checks that compare the argument with similar arguments and the theorem with related theorems.
- **HT** should be a node in a UDML chosen as the best mathematical home for **Thm** and **Arg**.
- **Thm** can be transported to other nodes in the UDML via appropriate morphisms in the UDML.

A Proposed New Style of Proof [2/2]

- **Arg** is a combination of traditional and formal proof.
  - It has a traditional component for communication, discovery, learning, and beauty.
  - It has a formal component in which all details are mechanically checked for certification, discovery, and learning.
  - The two components are tightly integrated.
  - The formal component may be incomplete and even empty.
- **Arg** should be as universal as possible.
- The set **CC** of cross checks should be carefully chosen to show that **Thm** is coherent with the established facts in the UDML.
  - The cross checks establish both formal and informal connections.
- **HT** and **Thm** are formal, but **Arg** and **CC** are flexiformal.

Conclusion

- In a future UDML, proofs will serve as the threads that tie the mathematical knowledge together.
- Proofs are intended to serve at least seven purposes.
  - A UDML needs a style of proof that fulfills all these purposes.
  - Both the traditional and formal styles of proof fall short.
- We have proposed a new style of proof in which:
  1. The home of the proof is expressed as a formal axiomatic theory.
  2. The theorem is a formal statement in the theory.
  3. The argument is a combination of traditional and formal proof that is as universal as possible.
  4. Cross checks are employed systematically.

Conclusion

- In a future UDML, proofs will serve as the threads that tie the mathematical knowledge together.
- Proofs are intended to serve at least seven purposes.
  - A UDML needs a style of proof that fulfills all these purposes.
  - Both the traditional and formal styles of proof fall short.
- We have proposed a new style of proof in which:
  1. The home of the proof is expressed as a formal axiomatic theory.
  2. The theorem is a formal statement in the theory.
  3. The argument is a combination of traditional and formal proof that is as universal as possible.
  4. Cross checks are employed systematically.

Thank You!