

Passages of Proof

C. S. Calude

(joint work with E. Calude
and S. Marcus)

*Depuis les Grecs, qui dit
Mathématique, dit démonstration.*

Bourbaki

Eight stages

1. Pre–Greek mathematics dominated by observation, intuition and experience.
2. Greek deductive mathematics based on theorems; Euclid’s geometry.
3. The mathematical language (Galilei, Descartes, Newton and Leibniz).
4. The epsilon rigour (Cauchy and Weierstras).
5. The challenge of the principle of non–contradiction and the logical crisis (Russell–Whitehead, Hilbert, Brouwer).
6. Gödel’s incompleteness theorem.
7. Reconciliation of empirical–experimental mathematics with deductive mathematics.
8. Quantization . . .

Knowledge is acquired through *reason* and by *experiment*.

For more than 2000 years, the Euclidean model of (mathematical) proof was based on reason only. In David Hilbert words:

The rules should be so clear, that if somebody gives you what they claim is a proof, there is a mechanical procedure that will check whether the proof is correct or not, whether it obeys the rules or not.

However, the Euclidean model of proof is not unanimously accepted as an “ideal”. For example,

Argument reaches a conclusion and compels us to admit it, but it neither makes us certain nor so it annihilates doubt that the mind rests calm in the intuition of truth, unless it finds this certitude by way of experience. (Roger Bacon)

Proofs are to mathematics what spelling (or even calligraphy) is to poetry. Mathematical works do consist of proofs, just as poems do consist of characters. (Vladimir Arnold)

Logical vs. computational

Classically, there are two equivalent ways to look at the mathematical notion of proof:

- *logical*, as a finite sequence of sentences strictly obeying some axioms and inference rules,
- *computational process*, as a specific type of computation.

Indeed,

from a proof given as a sequence of sentences one can easily construct a machine producing that sequence as the result of some finite computation and, conversely,

giving a machine computing a proof we can just print all sentences produced during the computation and arrange them in a sequence.

This gives mathematics an immense advantage over any science: any proof is an explicit sequence of reasoning steps that can be inspected at *leisure*.

In theory, if followed with care, such a sequence either reveals a gap or mistake, or can convince a skeptic of its conclusion, in which case the theorem *is considered proven*.

We said, *in theory*, because the “game” of mathematical proofs is ultimately a social experience, so it is contaminated to some degree by all “social maladies”.

**Digression: in real life proofs
may be different ...**

Proof by obviousness

“The proof is so clear that it need not be mentioned.”

Proof by general agreement

“All in favor? ...”

Proof by calculus

“This proof requires calculus, so we’ll skip it.”

Proof by lost reference

“I know I saw it somewhere ...”

Proof by necessity

“It had better be true, or the entire structure of mathematics would crumble to the ground.”

Proof by plausibility

“It sounds good, so it must be true.”

Artificial mathematicians

The equivalence between the logical and computational proofs has stimulated the construction of programs which perform like *artificial mathematicians*.

The “theorem provers” have been very successful in proving many results, from simple theorems of Euclidean geometry to the proof of the four-color theorem.

Artificial mathematicians are far less ingenious and subtle than human mathematicians, but they surpass their human counterparts by being infinitely more patient and diligent.

Of course, this was a good reason for sparking lots of controversies... For example,

- What about making errors? Are human mathematicians less prone to errors?
- What about “insight”?

If a conventional proof is replaced by a “quantum computational proof”, then the conversion from a computation to a sequence of sentences may be impossible, not because of its size but for reasons of physical law.

The quantum automaton would say “your conjecture is true”, but (due to quantum interference) there will be no way to exhibit all trajectories followed by the quantum automaton in reaching that conclusion.

The quantum automaton has the ability to check a proof, but it may fail to reveal a “trace” of the proof for the human being operating the quantum automaton.

Even worse, any attempt to *watch* the inner working of the quantum automaton (e.g. by “looking” at any information concerning the state of the on going proof) may compromise for ever the proof itself!

We seem to go back to Bertrand Russell:

*Thus mathematics may be defined as the subject
in which we never know what we are talking
about, nor whether what we are saying is true.*

...and even when it's true we might not know
why.

Digression: more real life proofs

Proof by intimidation

“Don’t be stupid; of course it’s true.”

Proof by terror

When intimidation fails . . .

Proof by lack of sufficient time

“Because of the time constraint, I’ll leave the proof to you.”

Proof by tessellation

“This proof is the same as the last.”

Proof by majority rule

Only to be used if general agreement is impossible

Proof by authority

“Well, Don Knuth says it’s true, so it must be!”

Proof by intuition

“I just have this gut feeling . . .”

We don't need to speculate too much to realise that any personal computer can compute functions no Turing machine can compute.

This is because physical computers have access to truly unpredictable numbers (as opposed to numbers produced by a pseudo-random number generator, which are predictable). For example, a radioactive source can be used to generate numbers that, at least as far as quantum mechanics can determine, are random, and by electronic means, random numbers can be made available to conventional digital computers.

Such a scenario has been actually realized already by Zeilinger and his colleagues in:

<http://xxx.lanl.gov/abs/quant-ph/9912118>.

Speculations about quantum proofs *may not affect* the essence of mathematical objects and constructions (which, many believe, have an autonomous reality quite independent of the physical reality), but they seem to *have an impact* on how we *learn/understand mathematics*, which is through the physical world.

Indeed, our glimpses of mathematics are revealed only through physical objects, human brains, silicon computers, quantum automata, etc., hence, according to David Deutsch, they have to obey not only the axioms and the inference rules of the theory, but the *laws of physics* as well.

To complete the picture we need to take into account also the *biological* dimension. No matter how precise the rules (logical and physical) are, we need human consciousness to apply the rules and to understand them and their consequences. Mathematics is a human activity.

Towards quasi-empirical mathematics?

A “proof is only one step in the direction of confidence” argued De Millo, Lipton and Perlis.

Written in the same spirit is Don Knuth’s warning: “Beware of bugs in the above code: I have only proved it correct, not tried it.”

“If one must choose between rigour and meaning, I shall unhesitatingly choose the latter” confessed R. Thom.

The above quotation turned slogan as “more rigour, less meaning”, or better still, “less rigour, more meaning” (Chaitin) points out the necessity to distinguish between the syntactic and the semantic aspects of proofs.

Points of reflection?

Should proofs belong exclusively to logic, according to the tradition started by Greeks such as Pythagoras and Euclid?

Or should they also be accepted as a cocktail of logical and empirical–experimental arguments, as in the proof of the four-color theorem (1976)?

Is the quasi-empirical view of mathematics (which sustains that although mathematics and physics are different, it is more a matter of degree than black and white) a viable alternative?

Are proofs losing their infallible and time-independence status?

