

THE FUTURE OF PROOF

by

Dana S. Scott
University Professor Emeritus
Carnegie Mellon University

LICS 2006

WARNING!

The quotations collected for these slides were assembled from many on-line sources and no record was kept of origin or attribution. Please do not recycle them without doing your own “research”! Their purpose in this talk was for entertainment by emphasizing the many differences of viewpoints.

Outline of Talk

- Background
- Examples
- A Proposal

The Gödel Earthquake

- 1929 The Completeness of First-Order Logic
(anticipated by Skolem)
- 1930 The Incompleteness of Higher-Order Logic
(*not* anticipated by Russell or Hilbert)

Another Surprise (1936)

Given any computable function ϕ and any integer n , there is a sentence provable in second-order arithmetic in n steps, and, though provable in first-order arithmetic, requires at least $\phi(n)$ steps.

(announced by Gödel, proved by Parikh and, later, by Statman)

Do We Need Proofs?

“Logic, Padoa says, is not in a particularly fortunate position. On the one hand, **philosophers** prefer to speak of it *without using it*, while on the other hand **mathematicians** prefer to use it *without speaking of it* — and even without desiring to *hear it spoken of*.”

— C.H. Langford (1937)

What is a Proof?

“Proofs really aren't there to convince you something is true — they're there to show you *why* it is true.”

— Andrew Gleason

Is Logic Good for You?

“When you question a man's logic, you question his taste!”

— J.L. Kelley (1954)

“A good notation sets the mind free to think about really important things.”

— Alfred North Whitehead

Are Proofs Good for You?

“There is a real conflict between the logician's goal and the educator's. The logician wants to minimize the variety of ideas and doesn't mind a long, thin path. The educator (rightly) wants to make paths short and doesn't mind — in fact, prefers — connections to many of other ideas. And he cares almost nothing about the direction of the link.”

— Marvin Minsky
“Form and Content in Computer Science” (1970)

Oh, Bury Me Not!

“Moreover, there are good reasons why Mathematicians do not usually present their proofs in **fully formal style**. It is because proofs are not only a means to certainty, but also a means to understanding. Behind each substantial formal proof there lies an idea, or perhaps several ideas. The idea, initially perhaps tenuous, explains why the result holds. The idea becomes Mathematics only when it can be formally expressed, but that expression must be so couched as to reveal the idea; it will not do **to bury the idea under the formalism**.”

— Saunders Mac Lane (1986)

Formal = Bad?

“Everybody who has worked in **formal logic** will confirm that it is one of the **technically most refractory** parts of mathematics. The reason for this is that it deals with rigid, all-or-none concepts, and has very little contact with the continuous concept of the real or the complex number, that is, with mathematical analysis. Yet analysis is the technically most successful and best elaborated part of mathematics.”

— John von Neumann (1948)

Do We Even Want Logic?

“**LOGIC**, n. the art of thinking and reasoning in strict accordance with the limitations and incapacities of the human misunderstanding”

— Abrose Bierce.

“If Mathematics had never been invented, physics would have been set back a week.”

— Richard Feynman

“Obviousness is always the enemy of correctness.”

— Bertrand Russell

Proof vs. Truth?

“It should be noticed that logical proof starts with premises, and that premises are based on evidence. Thus, evidence is presupposed by logic; at least, it is presupposed by the assumption that logic has any importance.”

— Alfred North Whitehead

“You can only find truth with logic if you have already found truth without it.”

— G. K. Chesterton
The Man Who was Orthodox

Automated Deduction?

“Despite the significant advances automated reasoning has seen over the past decades, the impact of automated reasoning on the practice of doing *mathematics* is small.”

— Bruno Buchberger (IJCAR 2006)

Logic and Computation?

“It is reasonable to hope that the relationship between computation and mathematical logic will be as fruitful in the next century as that between analysis and physics in the last. The development of this relationship demands a concern for both applications and for mathematical elegance.”

— John McCarthy

Too Much Math?

“With the enormous growth of results at well over 100,000 (new?) theorems every year ... the chance of a new piece of pure mathematics being spotted by you and also being at hand when you need it, and not have not be recreated when needed, is increasing small ... *Regeneration* is increasingly easier than *retrieval*.”

— Richard W. Hamming (1997)
Art of Doing Science and Engineering

Bad Predictions?

“I think there is a world market for maybe five computers.”

— Thomas J. Watson (1943)

“Computers in the future may weigh no more than 1.5 tons.”

— Popular Mechanics (1949)
forecasting the relentless march of science

“I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a *fad* that won't last out the year.”

— Prentice Hall business editor (1957)

Computer Proofs?

“In the early days (1960s) there was the idea that computers could replace mathematicians, and prove serious mathematical theorems entirely on their own. Even to this day, the success along these lines is extremely limited, and this idea has been all but abandoned. An exception is **plane geometry**, where beautiful things of interest to humans are done solely by computers. But this is still very far from general-purpose ordinary mathematics, and worthless for program verification.”

— Harvey Friedman (2005)

No Crystal Ball?

“But what ... is it good for?”

— IBM Engineer (1968)
commenting on the microchip

“There is no reason anyone would want a computer in their home.”

— Ken Olson, DEC founder (1977)

“640K ought to be enough for anybody.”

— Bill Gates (1981)

Is There Hope?

“In recent years there has been a flurry of interest in the development of verification tools that rely quite heavily on sophisticated decision procedures. The quality and efficiency of many of these decision procedures is impressive. The underlying theory is also advancing rapidly. Such theoretical advances will make it easier to construct correct decision procedures and integrate them more easily with other inference mechanisms. Contrary to the impression that decision procedures are black boxes, they need rich interfaces in order to be deployed most efficiently.”

— Natarajan Shankar (2002)

Doing Formal Verification

“Most successful automated formal verification tools are based on a bit-level model of computation. Using powerful inference engines, such as Binary Decision Diagrams (BDDs) and Boolean satisfiability (SAT) checkers, symbolic model checkers and similar tools can analyze all possible behaviors of very large, finite-state systems.”

— Randal E. Bryant (LICS 2006)
Formal Verification of Infinite State
Systems using Boolean Methods

Future Coming Soon?

“Today it is state of the art that hardware manufacturers have complete formal models of processors and verify much of their functionality. Thanks to theorem provers the same level of formality will in the future be applied to core software components like programming languages and compilers.”

— Tobias Nipkow (2006)

Model Checking Today

Model checking technology arguably ranges among the foremost applications of logic to computer science and computer engineering. In the 25 years since its invention, model checking has achieved multiple breakthroughs, bridging the gap between theoretical computer science, hardware and software engineering. Today, model checking is extensively used in the hardware industry, and has become feasible for verifying many types of software as well. Model checking has been introduced into computer science curricula at universities worldwide, and virtually has become a universal tool for the analysis of systems.

Proof-Carrying Code is dead.

Premises of PCC, 1997

- Too hard to prove source program correct
- Too hard to prove compiler correct
- Brilliant insight [Harper, Morrisett, Lee, Necula]:
Type-preserving compiler can output a safety proof

State of the art, 2006

- Success in proving nontrivial source programs correct
- Success in proving nontrivial compilers correct
- Don't need the “workaround” of PCC.

— Andrew W. Appel (2006)

Verifying the Verifiers?

The HOL Light prover is based on a logical kernel consisting of about 400 lines of mostly functional OCaml, whose complete formal verification seems to be quite feasible. We would like to formally verify

- (i) that the abstract logic HOL is supposed to implement is indeed correct, and
- (ii) that the OCaml code does correctly implement this logic.

— John Harrison (IJCAR 2006)
Towards self-verification of HOL Light

Paraconsistency?

“Large software systems are permeated with inconsistencies. Professional people deal with the pervasive inconsistency in large software systems on a daily basis. So how do they cope? They certainly don't use classical logic because by the rules of classical logic, every proposition (including, for example, that ***The moon is made of green cheese!***) follows from a contradiction. We need systems that don't blow up in the face of inconsistencies and have developed **Direct Logic** with this in mind.”

— Carl Hewitt (2006)

NASA: "Independent Verification and Validation"

The operative word here is "independent." The model of verification that they are interested in is one in which the code is taken as given, and verification is done by a different group than the group that developed the code.

Any avenues wherein we **change** the way that programmers work are off-the-table.

— Karl Cray (2006)
Report on NASA's Software Assurance Symposium

Are Contradictions Bad?

“No one has ever yet got into trouble from a contradiction in logic.”

— Ludwig Wittgenstein (ca. 1939)

“The real harm will not come in unless there is an application, in which case a bridge may fall down.”

— Alan Turing (ca. 1939)

Like a Nice Quantum PC?

“Silicon-based computing power is expected to reach its physical limits in 2015, when it becomes impossible to keep up with Moore's Law; squeezing more power past the silicon barrier requires a transition to **quantum computing**, which some of the world's top research agencies and technology companies are pursuing. The quantum phenomenon of superposition means that quantum bits (qubits) can encompass all values simultaneously, allowing quantum computers to rapidly calculate tough problems such as reliably forecasting **weather** or **traffic**.”

— Fortune Magazine (August 2006)

To Paraphrase Hilbert

We must prove.

We will prove!

(—if we are lucky)

Q: What is Needed for Great Computer Proofs?

A: Better *interfaces* to users, special purpose devices, and better *libraries*.

End Note

The first part of the talk was meant to indicate that there has been much progress in making computer-assisted proofs feasible and robust. That gives us hope for the future. The remainder of the talk (if time had permitted) was meant to give several examples of proofs where the strategy is to **add more structure** beyond what was implied in the statement of the theorem to be proved. And this is where human **insight** usually enters.

The author has a particular example of new structure he likes for **plane projective geometry**. This will have to be a topic of another presentation.