Formal Mathematics and Mathematical Practice

Peter Koepke, Mathematical Institute, University of Bonn, Germany

14th Congress of Logic, Methodology, and Philosophy of Science
Special Symposium: Mathematics and the New Technologies
Nancy, July 22, 2011

Formal mathematics

1. Formal mathematics has become an established research area.

2. Formal mathematics is already covering substantial mathematical results.

3. Formal mathematics is beginning to interact with research mathematics.

4. Formal mathematics could become part of mathematical practice.

5. The acceptance of formal mathematics in mathematical practice will depend on the naturalness of its use.

6. The naturalness of formal mathematics can be increased considerably.

7. Formal mathematics will become an everyday tool in mathematical practice (?)

Foundations of formal mathematics

Kurt Gödel: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.

Die Entwicklung der Mathematik in der Richtung zu größerer Exaktheit hat bekanntlich dazu geführt, daß weite Gebiete von ihr formalisiert wurden, in der Art, daß das Beweisen nach einigen wenigen mechanischen Regeln vollzogen werden kann. Die umfassendsten derzeit aufgestellten formalen Systeme sind das System der Principia Mathematica (PM) einerseits, das Zermelo-Fraenkelsche (von J. v. Neumann weiter ausgebildete) Axiomensystem der Mengenlehre andererseits. Diese beiden Systeme sind so weit, daß alle heute in der Mathematik angewendeten Beweismethoden in ihnen formalisiert, d.h. auf einige wenige Axiome und Schlußregeln zurückgeführt sind.

Foundations of formal mathematics

Kurt Gödel: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.

As is well-known the development of mathematics towards greater exactness has lead to the point that large areas were formalised in a way that proofs can be carried out according to a small number of mechanical rules. [...] These two systems are sufficiently developed so that all proof methods currently applied in mathematics can be formalised in them, [...].

Foundations of formal mathematics

Kurt Gödel: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.

As is well-known the development of mathematics towards greater exactness has lead to the point that large areas were formalised in a way that proofs can be carried out according to a small number of mechanical rules. [...] These two systems are sufficiently developed so that all proof methods currently applied in mathematics can be formalised in them, [...].

Foundations of formal mathematics: modeling mathematics by mathematical logic

Mathematics			**Mathematical logic**	
Language -	basic notions statements proofs	$\leftrightarrow$	symbols formulas formal derivations ($\vdash$)	- Syntax
Ontology -	structures truth implication ...		sets, relations, etc satisfaction relation logical implication ($\models$)	- Set theoretic semantics

Foundations of formal mathematics: modeling mathematics by formal logic

- excellent agreement between ontology and semantics: a *group* is a *set* such that ...
- complete agreement between syntax and semantics: Gödel completeness theorem: $\vdash = \models$
- hence: every proof can be replaced by a formal derivation
- formal mathematics: to actually produce formal derivations from informal proofs

On the feasability of formal mathematics

N. Bourbaki:

[...] such a project is absolutely unrealizable: the tiniest proof at the beginnings of the Theory of Sets would already require several hundreds of signs for its complete formalization. [...] formalized mathematics cannot in practice be written down in full, [...]

J. McCarthy:

Proofs to be checked by computer may be briefer and easier to write than the informal proofs acceptable to mathematicians. This is because the computer can be asked to do much more work to check each step than a human is willing to do, and this permits longer and fewer steps.

The development of formal mathematics systems

- Automath, de Bruijn, ~1967
- Mizar, Trybulec, ~1973
- **Isabelle/Isar**, Paulson, Nipkow, Wenzel, ~2002
- **Coq**
- **HOL Light**, Harrison
- many other systems

Substantial mathematics in Automath

van Benthem Jutting, 1977

Checking Edmund Landau, Grundlagen der Analysis

Substantial mathematics in Mizar

Banach Fixed Point Theorem for compact spaces, the Brouwer Fixed Point Theorem, the Birkhoff Variety Theorem for manysorted algebras, Fermat's Little Theorem, the Fundamental Theorem of Algebra, the Fundamental Theorem of Arithmetic, the Gödel Completeness Theorem, the Hahn-Banach Theorem for complex and real spaces, the Jordan Curve Theorem for special polygons, ...

Substantial mathematics in Isabelle/Isar

largest ... is the formalization of Gödel's proof of the relative consistency of the axiom of choice

Substantial mathematics in Coq

Fundamental Theorem of Algebra by Herman Geuvers, Freek Wiedijk, Jan Zwanenburg, Randy Pollack, Henk Barendregt

Proof of Buchberger's algorithm by Laurent Thery, Henrik Persson

...

Substantial mathematics in HOL Light

Fundamental theorem of calculus, fundamental theorem of algebra, inverse function theorem, Brouwer's fixpoint theorem, Jordan curve theorem, compactness and Löwenheim-Skolem theorem, Gödel's first incompleteness theorem, ...

Big theorems in Isabelle/Isar

Prime Number Theorem, elementary proof, by J. Avigad et al.

Big theorems in HOL Light

Prime Number Theorem, analytical proof, by J. Harrison

Big theorems in Coq

Four Colour Theorem, by G. Gonthier

The flyspeck project

Formal proof of the Kepler conjecture (T. Hales et al.), using various systems.

Why is formal mathematics not yet widely used?

- Wiedijk: The other reason that there has not been much progress on the vision from the QED manifesto is that currently formalized mathematics does not resemble real mathematics at all. Formal proofs look like computer program source code.

- So far, formal mathematics does not fit common mathematical practice(s).

Naturalness in formal mathematics

- input and output languages and formats
- user interfaces
- logics
- background theories
- automation
- ...

Natural language

- mathematical language = natural language + formulas
- use computational linguistics to parse input language
- formal grammars define controlled natural languages for mathematics
- discourse representation theory can handle mathematical texts as discourses (like stories)
- use natural language to describe/steer Coq or HOL style proofs?

User interfaces

- use LaTeX-style language for mathematical typesetting
- merge existing formal mathematics interfaces with LaTeX editors
- use LaTeX quality wysiwyg editors like TeXmacs

Logics

- classical logic
- rich (dependent) type system
- declarative proof style
- many figures of proof / argumentation

Automation

- use strong general or special purpose automatic theorem provers to derive statements in proofs from preceding premises

- use ‘‘reasoner’’ modules for straightforward inferences and substitutions, before invoking automatic theorem provers

- premise selection according to natural language cues and text structure

The SAD project: System for Automated Deduction

- A. Lyaletski, A. Paskevich, K. Verchinine
- ForTheL: Formula Theory Language, a combination of controlled English with mathematical notation
- Reasoner performing “obvious” inferences
- generic interface to first-order provers

The SAD project: System for Automated Deduction

Theorem Main.

For all nonzero natural numbers n,m,p if p * (m * m) = (n * n) then p is compound.

Proof by induction. Let n,m,p be nonzero natural numbers. Assume that p * (m * m) = (n * n). Assume that p is prime. Hence p divides n * n and p divides n. Take q = n / p.
Then m * m = p * (q * q). Indeed p * (m * m) = p * (p * (q * q)).
m < n. Indeed n <= m => n * n <= m * m.

Hence p is compound.

qed.

The Naproche project: Natural language proof checking

- studies the syntax and semantics of the language of mathematical proofs, emphasizing natural language and natural argumentation, relating them to formal mathematics

- models natural language proofs using computer-supported methods of formal linguistics (natural language processing) and formal logic (automatic theorem provers)

E. Landau, *Grundlagen der Analysis*, 1930

Theorem 30: For all $x, y, z, x * (y + z) = (x * y) + (x * z)$.

Proof: Fix x, y. $x * (y + 1) = x * y' = x * y + x = (x * y) + (x * 1)$.

Now suppose $x * (y + z) = (x * y) + (x * z)$. Then $x * (y + z') = x * ((y + z)') = (x * (y + z)) + x = ((x * y) + (x * z)) + x = (x * y) + ((x * z) + x) = (x * y) + (x * z')$.

Thus by induction, for all z, $x * (y + z) = (x * y) + (x * z)$. Qed.

Combining SAD with natural language

Theorem 1. (Fuerstenberg) *Let* $S = \{\mathrm{Arseq}(0,\ r) \mid r\ \textit{is prime}\}$. *Then* S *is infinite.*

Proof. We have $-\bigcup S = \{1, -1\}$, indeed n belongs to $\bigcup S$ iff n has a prime divisor.

Assume that S is finite. Then $\bigcup S$ is closed and $-\bigcup S$ is open. Take p such that $\mathrm{ArSeq}(1, p) \subseteq -\bigcup S$.

Claim. $\mathrm{ArSeq}(1, p)$ has an element that does not belong to $\{1, -1\}$.
Proof. $1 + p$ and $1 - p$ are elements of $\mathrm{ArSeq}(1, p)$. $1 + p \neq 1 \wedge 1 - p \neq 1$. $1 + p \neq -1 \vee 1 - p \neq -1$. *qed.*

Contradiction. □

Outlook

- Combine best practices from various formal mathematics systems to obtain naturalness and power
- will this achieve acceptance by mathematical practioneers
- Jeremy Avigad: *On a personal note, I am entirely convinced that formal verification of mathematics will eventually become commonplace.*
- What would be the implications of a widespread use of formal mathematics for the methodology, practice, and philosophy of mathematics?

Thank You!