From the universality of mathematical truth to the interoperability of proof systems

Gilles Dowek

I. Computerized proof systems

Mathematics before 1967

A: The perpendicular bisectors of the sides of a triangle meet at one point

A: Let ABC be a triangle… thus… therefore… hence… they meet at one point

B: The proof is correct (The text is a proof)

What is a correct proof?

A sequence of steps

At each step a new proposition is obtained from previously proven propositions using a deduction rule, for example

$$\frac{A \Rightarrow B \quad A}{B}$$

... thus $A \Rightarrow B$,

... thus A,

$A \Rightarrow B$ and A, thus B

... thus $A \Rightarrow B$,

... thus B,

$A \Rightarrow B$ and B, thus A

An easy, repetitive, and boring operation

A_1, ..., A_n, thus B

- check A_1, ..., A_n have indeed been proved before
- check there is indeed a deduction rule that produces B from A_1, ..., A_n

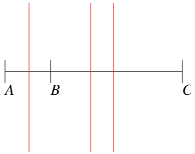
De Bruijn, Milner: Instead of doing it yourself, use a computer

Automath and LCF

Turing (1936): There is an algorithm to decide if a text is a proof of some statement (but no algorithm to decide if a statement has a proof)

Why did this change the world?

You thought the perpendicular bisectors of the sides of a triangle meet at one point?
The proof is wrong



- They meet at an infinite point (is the theorem about the projective plane?)
- It is not a triangle (did anyone told you that three colinear points were not a triangle?)
- It works for most triangles (is it a probabilistic theorem?)

If M is on the perpendicular bisectors of AB and BC then it is also on the perpendicular bisectors of AC
A new rigor standard

Why did this change the world?

Another wrong theorem

If

$$f(a) \leq 0$$

$$f(b) \geq 0$$

$$\forall x \; ((a \leq x \leq b) \Rightarrow f \text{ continuous at } x)$$

then

$$\exists y \; ((a \leq y \leq b) \wedge f(y) = 0)$$

Why did this change the world?

Mathematicians write proofs that are difficult to check

Classification of finite simple groups: the proof consists of tens of thousands of pages in several hundred journal articles written by about one hundred authors

Gonthier et al.: a Coq proof of the odd case

Why did this change the world?

Proof built using computers

The Kepler conjecture: Hales' proof is a proof by exhaustion involving the checking of many individual cases using complex computer calculations

Referees said that they were 99% certain of the correctness of Hales' proof, and the Kepler conjecture was accepted as a theorem

Hales et al.: a proof of the theorem mixing HOL Light and Isabelle/HOL

Why did this change the world?

Air traffic control: assign a velocity vector to each aircraft such that for all t, the function mapping each aircraft to its position is injective

Write a program
Hope the program does not have too many bugs

Prove the function injective
Nobody will check your proof (each time you update the program)

Prove your program correct in PVS

Leroy et al.: A Coq poof of a C compiler
seL4: an Isabelle/HOL proof of an OS Kernel

Why did this change the world?

The four milestones in the history of mathematical rigor

Euclide, Russell and Whitehead, Bourbaki, us

But...

Automath, LCF
Coq, Isabelle/HOL, PVS, HOL Light, Lean...

A Coq proof, an HOL Light proof, a Isabelle/HOL proof, a PVS proof...

Jeopardizes the universality of mathematical truth

A proof of Fermat's little theorem ⟶ a Coq proof of Fermat's little theorem, a PVS proofs of Fermat's little theorem...

Each proof system: its own language and its own truth conditions

An example of “informal statement”

$$\forall x \left(x \neq 0 \Rightarrow x \times \frac{1}{x} = 1\right)$$

An example of “informal statement”

$$\forall x\,(x \neq 0 \Rightarrow x \times \frac{1}{x} = 1)$$

$$0 \neq 0 \Rightarrow 0 \times \frac{1}{0} = 1$$

- $\frac{1}{0} = 42$
- $\frac{1}{0}$ undefined
- we must not substitute 0 for x
- there is no function application $f(t)$

$$\forall x\,(x \neq 0 \Rightarrow \forall y\,(div(1, x, y) \Rightarrow x \times y = 1))$$

- extra argument to function application: a proof that the argument is in the domain

A usual problem in computer science?

I thought I knew the addition algorithm
Add ones with ones, tens with tens, hundreds with hundreds... propagating the carry

But when I had to program it:

- arrays or lists
- loop or recursivity
- modifying the data or creating new ones
- add(n,p), n.add(p)
- ...

One natural language to express algorithms $\longrightarrow$ thousands of formal ones

But the unity of programming stands

Because we have compilers

II. Yet another crisis of the universality of mathematical truth

The universality of mathematical truth

The truth conditions of a mathematical statement must be the object of unanimous agreement

- Constitutive of the notion of mathematical truth itself
- Yet, constantly jeopardized
- When mathematicians disagree on the truth of some statements: a crisis of the universality of mathematical truth

In the past

- The incommensurability of the diagonal and side of a square

$$\exists x\,(x \textit{ is a number} \wedge x^2 = 2)$$

- The introduction of infinite series

$$\sum_n \frac{1}{2^n} = 2 \qquad \sum_n (-1)^n = 0$$

- $$\exists x\,(x \textit{ is a number} \wedge x^2 = -1)$$
- Infinitesimals
- The non-Euclidean geometries

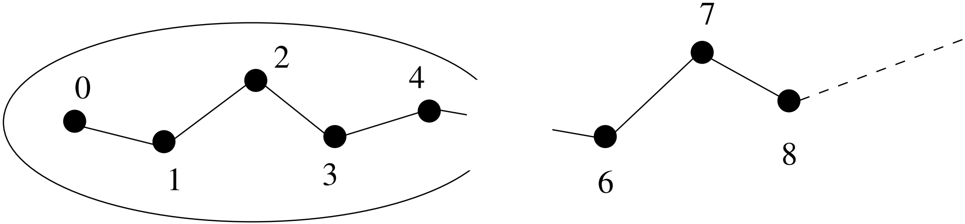
The sum of the angles in a triangle equals the straight angle

- The independence of the axiom of choice

Every vector space has a basis

- Constructivity

If $A \cup B$ infinite, then A infinite or B infinite


0
1
2
3
4
6
7
8

All these crises have been resolved

$\sqrt{2}$ and $\sqrt{-1}$: rational numbers, real numbers, complex numbers

Infinite series and infinitesimals: limit

Non-Euclidean geometries: several solutions

- Different spaces: truth of

  On a space of zero curvature, the sum of the angles in a triangle equals the straight angle

  but not of

  On a space of negative curvature, the sum of the angles in a triangle equals the straight angle

- Axiomatic theories: E and H, truth of

  $$E \vdash \textit{the sum of the angles in a triangle equals the straight angle}$$

  but not of

  $$H \vdash \textit{the sum of the angles in a triangle equals the straight angle}$$

Equivalent (soundness and completeness)

The second solution

- A true $\longrightarrow \Gamma \vdash A$ true
- Truth conditions: for the statements of geometry $\longrightarrow$ for arbitrary sequents
- Separation between the definition of the truth conditions of a sequent: the logical framework and the definition of the various geometries as theories
- A logical framework: Predicate logic
- The various geometries defined in this logical framework

The axiom of choice

First solution: truth of

In a model of ZFC, every vector space has a basis

but not of

In a model of ZF, every vector space has a basis

Second: *Every vector space has a basis* consequence of the axiom of choice

First solution does not work:
- Too far from the original formulation
- Problem of the “absolute” theory in which this should be proved

Thus, second chosen, paving the way to Reverse mathematics

Constructivity

First solution: truth of

> *In a model valued in a Boolean algebra, if $A \cup B$ infinite, then A infinite or B infinite*

but not of

> *In a model valued in a Heyting algebra, if $A \cup B$ infinite, then A infinite or B infinite*

Again, too far from the original formulation and question of the "absolute" theory

Second: *if $A \cup B$ infinite, then A infinite or B infinite* consequence of the excluded middle

A third solution: Ecumenism

Changing the axioms while keeping the same symbols?

Axioms express the meaning of the symbols:
different axioms $\longrightarrow$ different meanings $\longrightarrow$ different symbols (just like $\vee$ and $\oplus$)

The only "mistake" is not to accept or to reject the excluded middle, but to use the same symbol for $\vee$ and $\vee_c$

Nothing prevents from using them both

Truth of

$$\mathit{Infinite}(A \cup B) \Rightarrow_c \mathit{Infinite}(A) \vee_c \mathit{Infinite}(B)$$

but not of

$$\mathit{Infinite}(A \cup B) \Rightarrow \mathit{Infinite}(A) \vee \mathit{Infinite}(B)$$

$\sqrt{2}$: $\mathbb{Q}$ vs. $\mathbb{R}$ already Ecumenical (mass vs. weight...)

Past crises have been resolved

But... a new crisis: computerized proof systems to be resolved

III. A solution to our crisis: logical frameworks

A solution that (already) worked for several crises

Express the theories implemented in Coq, Isabelle/HOL, PVS, HOL Light, Lean... in Predicate logic

- (if we are lucky) many common axioms and few differentiating the theories
- (if we are lucky) mixing the axioms differentiating the symbols (Ecumenism)
- analyze which proof uses which axiom (just like for the axiom of choice)
- try to find better proofs using less axioms (just like constructivization, Reverse mathematics...)

A solution that (already) worked for several crises

Express the theories implemented in Coq, Isabelle/HOL, PVS, HOL Light, Lean... in a logical framework

- (if we are lucky) many common axioms and few differentiating the theories
- (if we are lucky) mixing the axioms differentiating the symbols (Ecumenism)
- analyze which proof uses which axiom (just like for the axiom of choice)
- try to find better proofs using less axioms (just like constructivization, Reverse mathematics...)

Beyond Predicate logic

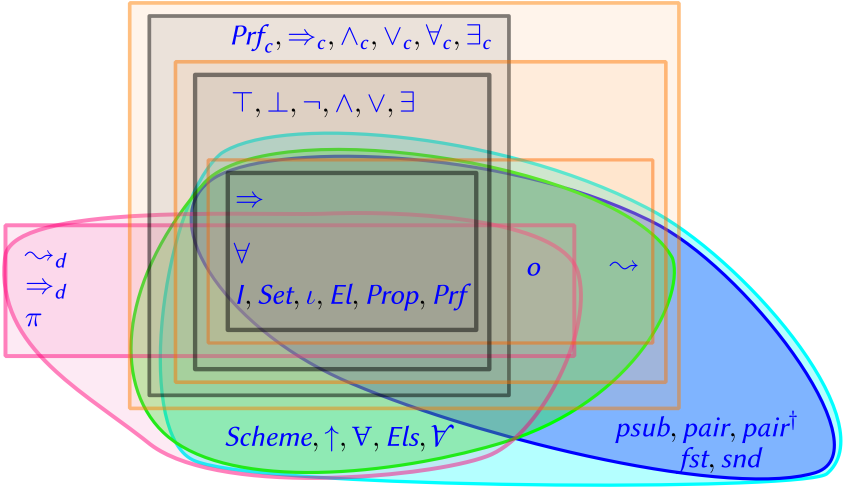
In a century: some limitations of Predicate logic

Other logical frameworks: λ-Prolog, Isabelle, the Edinburgh logical framework, Pure type systems, Deduction modulo theory, Ecumenical logic, Dedukti

In Dedukti

- Function symbols can bind variables (like in λ-Prolog, Isabelle, the Edinburgh logical framework)
- Proofs are terms (like in the Edinburgh logical framework)
- Deduction and computation are mixed (like in Deduction modulo theory)
- Both constructive and classical proofs can be expressed (like in Ecumenical logic)

Some axioms and theories in Dedukti



$Prf_c, \Rightarrow_c, \wedge_c, \vee_c, \forall_c, \exists_c$

$\top, \bot, \neg, \wedge, \vee, \exists$

$\Rightarrow$

$\forall$

$I, Set, \iota, El, Prop, Prf$

o

$\leadsto$

$\leadsto_d$

$\Rightarrow_d$

π

$Scheme, \uparrow, \forall, Els, \forall$

$psub, pair, pair^{\dagger}$

fst, snd

Enough to express Predicate logic, Simple type theory, Simple type theory with predicate subtyping, The Calculus of constructions...

IV. The benefits of universality

- Reverse engineering proofs
  First book of Euclide's Elements in Coq ⟶ in Predicate logic (Géran)
  Fermat's little theorem in Matita ⟶ in constructive Simple type theory (Thiré)
  Bertrand's postulate in Matita ⟶ in Predicative type theory (Felicíssimo)
- Interoperability
  The first book of Euclide's element in Isabelle/HOL, TSTP...
  Fermat's little theorem in Isabelle/HOL, HOL Light, Coq, Lean, PVS...
  Bertrand's postulate in Agda
- Cross-verification

A social motivation: mathematicians and industrials more likely to develop proofs in mathematics (possibly with some axioms they can debate) than in an exotic system

And a philosophical one: Universality has survived many crises: we ought not to give up on it (and we do not need to)

La mathématique est nécessairement toujours en crise, et toujours en train de la résoudre.

Michel Serres