Elements of Mathematics in the digital age

Marc Bezem
Department of Informatics
University of Bergen [1]

Pomona, CA, May 2013
Belgrade, July 2014

[1] Research done with generous support from the IAS, Princeton.

A cultural change

- Proofs in mathematics are *social constructs* ...

  ... and will become fully formalized syntactic objects
- Absolute truth as ideal will further erode ...

  ... and will be replaced by full accountability
- Touchstone: formalized proof *required* for publication

Short history

- Euclid, Leibniz, Frege, Russell/Whitehead, Bourbaki
- Automath (1967, De Bruijn (1918-2012)
- Nuprl, 70's, Constable
- Mizar, 49.000 thm's
- QED, with manifesto :-)
  'The aim [...] is to build a [...] computerized repository that rigorously represents all [...] established mathematical knowledge.'

Scepticism

- ‘We have heard grand predictions before’ :
  - Marx, wrong ...?
  - Malthus, probably right ...
  - ... so, what is the time frame?
- ‘Utterly uninteresting, therefore not done yet’
- ‘Impossible’
- ‘Insights are more important than proofs’

Why formalize mathematics?

- Ask Euclid, Leibniz, Frege, ...

  ... eternal truths founded on social constructs?
- Independent verification (mechanical)
- Full accountability (informal explanation NOT obsolete)
- Elimination of errors (but ...)
- Uncovering hidden assumptions (cf. AC)
- Some proofs yield executable code (Curry-Howard)
- Interesting interaction with CS (AI, De Bruijn indices)

Why difficult?

- Designing a universal language
- Proof *search* is undecidable
- Proof *verification*: De Bruijn-factor
- Expressivity versus efficiency of processing
- Porting results between mathematical fields (univalence!)
- Colloquialisms: ‘by symmetry’, ‘without loss of generality’, ‘by induction on ...’

Signs of change

- New Scientist
- What in the Name of Euclid Is Going On Here?
- Formalized Mathematics, Archive of Formal Proofs, Journal of Formalized Reasoning
- Formal Proof — The Four-Color Theorem (Gonthier, NAMS, 2008)
- Dense Sphere Packings — A Blueprint for Formal Proofs (Hales, LMS, 2012)
- Odd Order Theorem in Coq (Gonthier e.a., announced)
- Univalent Foundations of Mathematics (Voevodsky, $\geq$2006)

Simply typed lambda calculus

- Two syntactic categories: types and terms
- Types, double role: sets and propositions
- Terms, double role: elements and proofs
- Proofs as first class citizens
- Typing relation: *term* : *type* (decidable)
- Examples:
  - $\lambda x{:}T.\, x : T \to T$
  - $\lambda x{:}T.\, \lambda y{:}T'.\, x : T \to T' \to T$
  - $\lambda f.\, \lambda g.\, \lambda a.\, g\,(f\,a) : (A \to B) \to (B \to C) \to (A \to C)$
- Pioneers: Russell, Church, Curry, Howard

Universes, inductive and dependent types

- Universe U of types (and hence of propositions)
- Polymorphy, f.e., $(\lambda T{:}U.\,\lambda x{:}T.\,x) : (\Pi T{:}U.\,(T \to T))$
- Inductive type, f.e., $\dfrac{}{0 : \mathbb{N}} \qquad \dfrac{n : \mathbb{N}}{S\,n : \mathbb{N}}$
- Dependent type, f.e., $P : \mathbb{N} \to U$ a unary predicate on $\mathbb{N}$
- Product type, f.e., $(\Pi x{:}\mathbb{N}.\,P\,x) : U$ (NB $\Pi = \forall$)
- Expressive power: higher-order predicate logic
- Pioneers: De Bruijn, Martin-Löf, Girard

Essential Problems

- $(\lambda n : \mathbb{N}.\, n) \not\equiv (\lambda n : \mathbb{N}.\, n + 0)$ with left recursive $+$
- Distinct terms may denote the ‘same’ function
- Undecidable: $f = g$ if $fn = gn$ for all $n : \mathbb{N}$
- Distinct types denote the ‘same’ set, proposition
- Even more ‘loose’ identifications are highly desirable: the natural numbers, the non-negative integers, lists over a singleton, etc.

Homotopy type theory

- Topological spaces modulo *homotopy* equivalence?
  - Geometry: shape
  - Topology: the essence of shape
  - Homotopy: continuous deformation (‘the essence of the essence of shape’)
  - Continuous map with continuous *quasi*-inverse
- Types, third role: topological spaces (homotopy types)
- Terms, third role: points in a topological space
- Identity types (equality): path spaces
- Book: Homotopy Type Theory (Special Year, IAS, 2012/13)

Univalence Axiom

- Type universe U: topological space of topological spaces
- UA: homotopy equivalent types in U can be identified
  - Extensionally equal functions can be identified
  - Also, $\mathbb{N}$ and $\mathbb{Z}^{\geq 0}$ can be identified, etc.
- Why not so in ZF? Since $12 \in 13$!
- Crucial: the language of type theory strikes a balance

Conclusion

- Cultural trend towards ever more formalization of mathematics
- Homotopy Type Theory addresses some essential problems of formalization
- Univalence is a new axiom about equality and could help

Thank You!

```
(* Examples with left recursive plus *)

Lemma foo1: forall (n: nat), plus 0 n = n.
Proof. intro. simpl. trivial. Qed.

Lemma foo2: forall (n: nat), plus n 0 = n.
Proof. induction n. trivial. simpl. replace (n+0)
with n. trivial. Qed.

Lemma transitivity_of_implication:
forall (A B C: Prop), (A->B) -> (B->C) -> (A->C).
Proof. intros. apply H0. apply H. assumption. Qed.

...
```