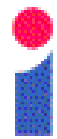
A Crisis in Mathematics?

Alan Bundy

School of informatics

University of Edinburgh



Mathematical Proofs

- **Ideal; short, simple and elegant.**
- **Social process:**
  - **understanding of argument;**
  - **community agreement.**
- **Formalization informal.**
- **Tolerance of non-fatal error.**

However, there are now pressures for change.

Inevitability of Enormous Proofs

- **Turing proved predicate calculus provability undecidable.**
  - **i.e. no algorithm to determine provability.**
  - **Nearly all areas of maths undecidable.**
- **Therefore, no limit to size of proofs of some simple theorems.**
  - **Otherwise, an algorithm could enumerate all candidate proofs.**
  - **Thereby guarantee to generate proof of conjecture, if it exists.**

Enormous Proofs Actually Occur

- **Several examples in last half century:**
  - **classification of finite simple groups;**
  - **four colour theorem;**
  - **Kepler's conjecture.**
- **Essential use of computers.**
- **Proofs not human understandable.**
- **Highly controversial.**

The Dilemma

- **Insist that proofs are human understandable.**
  - **accept that some simple theorems are forever unprovable.**
- **Accept computer-generated proofs.**
  - **abandon the traditional ‘social process’ in some cases.**

Classification of Finite, Simple Groups

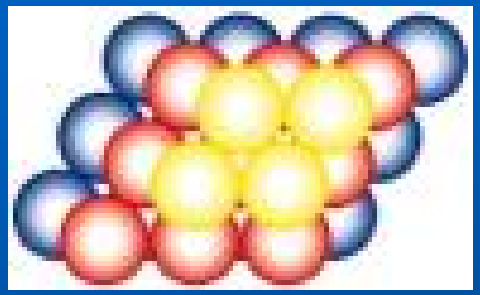
- **“10,000 pages in hundreds of papers” (Aschbacher’s estimate).**
- **“The probability of error is one” (Aschbacher).**
- **Use of computers to prove existence and/or uniqueness of sporadic groups.**
  - **Now mostly eliminated.**
  - **Why is such elimination considered a Good Thing?**

Four Colour Theorem

Can we colour any map with no more than four colours?

- **Long history of erroneous proofs.**
- **Appel and Haken 1976 proof used computer to analyse 1,936 cases.**
- **Many mathematicians reject proof.**

Kepler's Conjecture



What is the most efficient way to pack spheres?

- **Hales 1998 computer-assisted proof of 4-century old conjecture.**
- **Annals of Mathematics 12-person referee team fail to verify computer part.**
  - **Published with disclaimer.**

Objections to Computer Proof

- **Cannot be sure of correctness.**
  - **Programs notoriously buggy.**
- **May be impossible to understand.**
  - **Thousands of cases.**
  - **“Thus proofs are …. a vehicle for arriving at a deeper understanding of mathematical reality” (Aschbacher).**
  - **“Social process” denied.**

Computer Algebra Systems

- **Started in 1960s with symbolic integration systems.**
  - **Since expanded to algebra, matrices, groups, …..**
- **Many popular systems: Maple, Mathematica, GAP.**
  - **Widely used and taught in mathematics.**
  - **Nearly all known to be unsound.**
- **Used, for instance, in classification of finite simple groups.**
  - **Experimental mathematics – "Death of Proof" (Horgan).**

Automated Theorem Provers

- **Based on work in logic.**
  - **e.g. Frege, Hilbert, Herbrand, Gentzen,…**
- **Manipulation of formulae by valid rules.**
  - **“LCF” style guarantees correctness.**
    - **Rule application core small and verifiable.**
    - **Proof object can be 3rd party checked.**
- **Both automated and interactive.**
  - **Many mature systems: Isabelle, PVS, Coq, …**
  - **Usage highly skilled and time-consuming.**
- **Not widely used by mathematicians.**
  - **But see later …**

Error Detection by ATP

- **Fleuriot's Isabelle proof of Newton's proof of Kepler's Laws of planetary motion.**
  - **Formalization of infinitesimals.**
  - **Error undiscovered for 3 centuries.**
    - $\varepsilon^2 \sim \varepsilon \rightarrow \varepsilon \sim 1$ **--- detected and corrected.**
- **Meikle's formalization of Hilbert's Grundlagen der Geometrie.**
  - **Appeal to geometric intuition despite intention not to.**
  - **Hilbert's original intention now realised.**

Gonthier's ATP Proof of 4CT

- **Coq proof of four colour theorem.**
- **LCF style guarantees correctness.**
- **Proof still consists of many cases.**
- **Proof still hard to understand.**

Hale's FlysPecK project

- **Formal Proof of the Kepler's conjecture using ATP.**
  - **Reaction to Annals' decision.**
- **Computer proof with correctness guarantee.**
- **Widespread engagement of ATP community.**
  - **HOL-Light, Coq, Isabelle, … (Babel problem?)**
  - **http://www.math.pitt.edu/~thales/flyspeck/**
- **Hales' estimate 20 person-years.**
- **Initial success: Jordan Curve Theorem.**
  - **Proof not easy to understand.**

Are Computers Necessary?

- **Classification of finite simple groups largely human executed.**
  - **Use of CAS largely eliminated.**
- **Probability of error high.**
  - **p=1 says Aschbacher.**
- **No human understands in detail.**
  - **No published outline.**
- **So problems similar to computer proofs.**

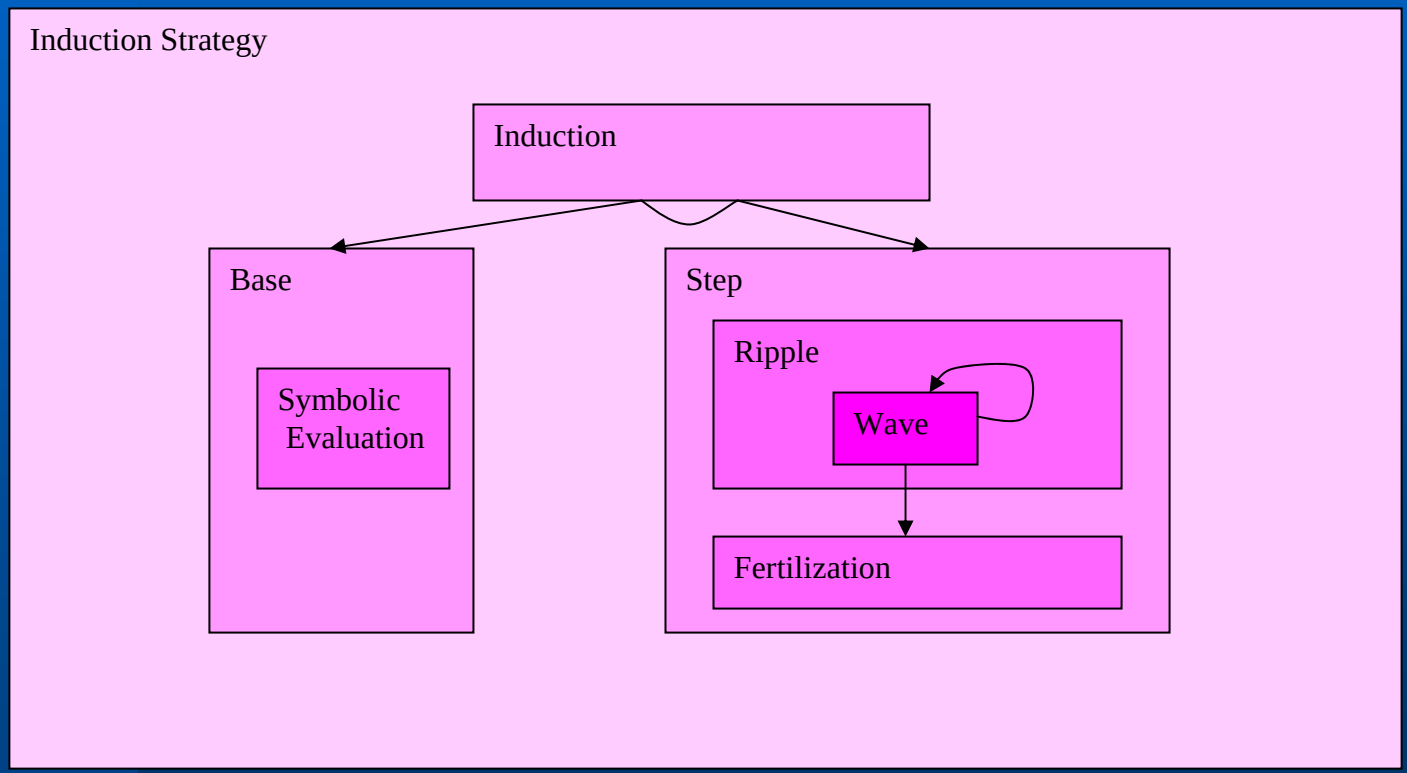
Can ATP Solve the Problems?

- **LCF style guarantees correctness.**
  - **But mathematicians tolerant of non-fatal error.**
- **Computer proofs typically inaccessible.**
  - **Understandability very important to mathematicians.**
- **Can computers aid understanding of large proofs?**
  - **We look at proof plans.**

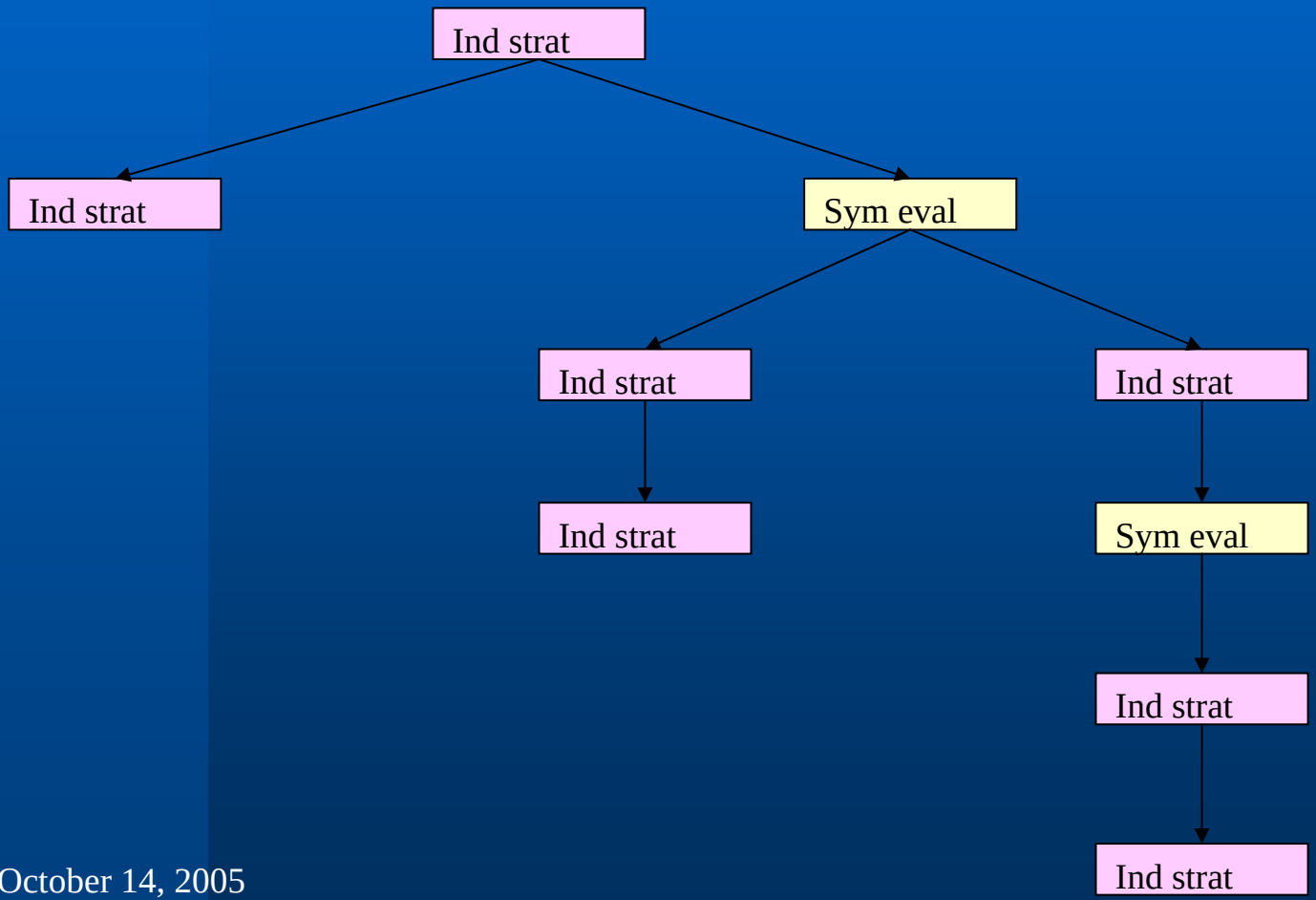
Proof Planning

- **LCF tactics guide application of logical rules.**
- **Proof methods specify tactics to explain how and why they fit together.**
- **Proof critics anticipate and patch proof failures.**
- **Hiproofs provide picture of proof structure.**

Proof Plan for Induction



Plan for n-Bit Multiplier



Conclusion

- **Large proofs of simple theorems are inevitable.**
  - **Either cope with this or abandon large tracts of mathematics.**
- **Computers have helped *produce* such large proofs.**
- **Computers can ensure *correctness* of large proofs.**
- **Can computers make large proofs more *accessible*?**