Some Grand Mathematical Challenges in Mechanized Mathematics?

Jacques Calmet

University of Karlsruhe (TH)

- Pure Mathematics
- Mechanized Mathematics

Pure Mathematics

- Hilbert‘s 23 (+1) problems for the 20th century

- Smale‘s 18 problems for the 21st century
  - P = NP ?
  - Limits of (human or artificial) intelligence

Clay Mathematics Institute
7 Millenium problems

- **Birch and Swinnerton-Dyer Conjecture**
- **Hodge Conjecture**
- **Navier-Stokes Equations**
- **P vs NP**
- **Poincaré Conjecture**
- **Riemann Hypothesis**
- **Yang-Mills Theory**

3 leading problems

- 1. The Riemann hypothesis
- 2. The Poincaré conjecture
- 3. Does P = NP ?

Some comments on P=NP

- Probabilistic algorithms
- DNA computing
- Quantum Computing

  software without hardware

  „plenty of proofs“ but useless?

Hilbert´s Problems

- Thierry Coquand´s talk: „Hilbert´s program“
- Problem 10: Is there a universal algorithm to solve Diophantine equations? Solution in 1970 □
- Richardson´s theorem: for a class of expressions there is no solution to the zero equivalence problem.
- A problem in logic: Suggestion: mechanize this kind of proof to other classes.

Mechanized Mathematics

- Constructive mathematics
- A proof is an algorithm. An algorithm is a proof (OMSCS)
- Mechanize new areas of Mathematics such as algebraic or differential topology
- New representations of mathematical objects
- Domains where the amount of computation, not the theoretical difficulties is the challenge
- Space and time complexity issues
- Meaning of „to prove“ (probabilistic proofs?)

On the meaning of proofs

D. Ruelle „Mathematical Platonism Reconsidered“ Bernouilli Lecture, Groningen, 1999)

Example from Oscar Lanford leads to look at the concept of proof and proofs on arithmetics.

My motivation: extend OMSCS to arithmetics hon-trivial (talk of Laurent Théry)

Article in New York Times: the world (and the origin of life) is probably not „Einsteinian“.

Contributions from physicists and mathematicians. Why do not we join in based on the contribution from Shannon?

In both cases: entropy concept (statistical mechanics)

Some selected problems

Involutive Bases

- Polynomial systems
  - Groebner bases
  - algebraic geometry
  - ideal/affine variety
  - Solutions
- Differential systems
  - involutive bases
  - algebra and geometry
  - topology (algebraic or differential)?
  - jet bundles
  - No solutions

Global integrability of differential systems

- How many solutions to a differential system ?
- A very old problem in Math and Physics
  - Yang-Mills equations,
  - Einstein‘s equation,
  - Navier-Stokes equation (plasma physics, fluid mechanics ..)
- Algorithms on local integrability (Cartan-Kuranishi)
- Global: more than a first integral plus special case solutions. No Cauchy conditions.
- Is it possible to duplicate successes for indefinite integration and closed form solutions of some ODEs?

Provable security and security protocols - 1

- Provable security (J. Stern at Eurocrypt 2003) is an attempt to mathematically establish security.
- Security protocols (SAT ...)
- Problem: to go from provable security to security protocols is a challenge by itself. This, most probably requires probabilistic facets in proofs.
- Claim based upon security of mobile agents (it is enough that 2/3 of the agents are „secure“)

Provable security - 2 (from Stern)

- 1 - define the goal of the adversary,
- 2 - define a security model,
- 3 - provide a proof by reduction,
- 4 - check the proof,
- 5 - interpret the proof.
  - a „first“ proof may be incorrect,
  - another proof is provided.

- **Other examples:**
  - **p-groups, where the amount of computation is enormous**
  - **Proofs in algebraic topology (group at La Rioja)**
  - **Computations + proofs + contexts tutoring mathematical systems.**

Conclusion

- We ought to learn more mathematics. When we build models (we always do that) can we learn from R. Thom (Morphogenesis book written in 1972)? Could we use concepts from algebraic fields or schemes to design new algebraic algorithms/proofs?
- Computer scientists rather than computers ought to contribute more to Mathematics.
- Despite OMSCS: when we turn an algebraic problem into a logic formulation this leads to more efficient algorithms. Do we understand why?

- a challenge is to make Calculemus successful and to prove John McCarthy was right in his 1963 citation.