# Are there True Grand Mathematical Challenges in Mechanized Mathematics?

Jacques Calmet *

Institut für Algorithmen und Kognitive Systeme (IAKS)
University of Karlsruhe (TH)
calmet@ira.uka.de

**Abstract.** Grand mathematical challenges do exist in pure mathematics. Are some of the acute mathematical problems that we face when mechanizing mathematics true challenges? This short paper tries to assess through a few examples that they are indeed so.

## 1 Introduction

The quest for mathematically challenging problem is present in any field of science. A very recent example is from material science (Taylor 2003). However, the most famous challenges concern Mathematics itself. A puzzling one was the proof of Fermat's theorem. It is barely necessary to cite the landmark presentation of David Hilbert at the 1900 Paris Conference. His list of problems for the 20th century was then extended to the well-known set of the 21 Hilbert's problems. On the eve of the 21th century, the International Mathematical Union asked a selected number of top mathematicians to contribute a similar list for the coming century. The contribution of Steve Smale has been widely distributed. It appeared first in the Mathematical Intelligencer (Smale 1998). Two years later a version in French (Smale 2000) appeared in the January issue of the Bulletin of the French Mathematical Society. It looks like Smale's list got a wide agreement and no other list of challenge problems has, apparently, been published. The three greatest open problems of mathematics are: the Riemann Hypothesis (Hilberth's 16th), Poincaré conjecture and "Does P=NP?". The latter is already tightly linked to our domain. One of the remaining challenging mathematical problems is very relevant to this community. It amounts to answer the question "What are the limits of (artificial or natural) intelligence?". This simple, apparently philosophical question leads in fact to very difficult mathematical problems such as the decidability of the Mandelbrot set. Besides, it is not obvious whether or not there is a link to the implications of the Gödel incompleteness theorem.

To propose a definition of a mathematical challenge in theorem proving or in computer algebra that can be acknowledged by mathematicians is always touchy and sometimes impossible. However, if we introduce either of the words

* Work partially supported by the Calculemus Reserach Training Network, HPRN-CT-2000-00102

"mechanized" or "constructible" to qualify the part of Mathematics we deal with, we can then open a few tracks along the following directions.

(i) Mechanize new areas of Mathematics such as algebraic topology or better Grothendieck's theory when also including geometry. Indefinite symbolic integration is a well-known example where a problem in analysis was turned into an algebraic problem. The methodology is constructive since Risch's algorithm decides whether or not integrability exists. It is also mechanized since the solution, when it does exist is constructed,

(ii) Identify and master new representations of mathematical objects. This is well understood when designing algebraic algorithms for computer algebra systems. A certainly challenging task is to investigate how algebraic fields (Laumon 1999) could be introduced in mechanizing algebraic geometry problems. Also relevant are proof techniques in algebraic topology. This is a domain where the infinity plays a very special part compared to algebra, analysis, geometry of algebraic geometry. In these domains, the infinity is not really a challenge since proofs do not have to namely address this concept. In algebraic topology, the concept of infinity is very important when designing proofs,

(iii) Devise new proof techniques for domains where the amount of computation, not the theoretical difficulties is the challenge. An example is to prove some theorems on p-groups that would take a lifetime by hand calculation,

(iv) Space and time complexity issues when designing proofs and algorithms. Besides the "P=NP ?" problem already quoted, a prototypical example is the factorization of integer numbers. More practical examples arise when trying to improve doubly exponential algorithms such as the Gröbner bases algorithm, which play an important part in theorem proving in geometry, or when dealing with parameters as in constraint programming, which concerns any computing problem

(v) What means to prove? This looks like a silly question but a domain as demanding and "theoretical" as provable security sheds some light on this question.

The remaining part of this abstract is devoted to the presentation of some specific problems.

## 2 Provable security and proofs

The deduction community is much concerned by designing proof techniques for security protocols and there are many publications in this domain. It may be worthwhile to restrict the question to the simpler one "what is provable security?" and then to assess the part played by proofs in the answer. This is a domain of standard cryptography and a very nice state of the art is available in (Stern 2003). Provable cryptography is an attempt to mathematically establish security. This is indeed very difficult and as a result, what is available is a form of "practical" provable security. It is possible to decompose provable security into 5 steps:

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 remark is that we are in engineering, not in mathematics but concepts are expressed mathematically. A second one is that provable security does not necessary yield proofs that are sound. What really matters, is that public key encryption cannot be broken. As a consequence it is not that surprising to notice that the 4th point on checking proofs may assert that a proof for an encryption mechanism is false. In fact "this does not matter so much". Indeed, there is usually enough time left, before the encryption is broken, to come out with a right proof. An open but difficult problem is to extend provable security to security protocols. One may guess that this task implies to introduce a concept of randomness in the date structures and of probability in the proof techniques.

## 3 Involutive bases

Systems of polynomial equations are solved using Gröbner bases and the related Buchberger's algorithm. Involutive bases are a special kind of Gröbner bases with additional combinatorial properties that make them very useful for many applications (Calmet 2001). They were first introduced by Janet a very long time ago and almost forgotten for many years.They exist in many polynomial algebras (also non-commutative ones) including ordinary polynomials and linear differential or difference operators. They are thus a possible approach to investigate symbolic solutions to system of (partial) differential equations. This is a domain where we need to find a suitable representation for differential objects. An overview is given in the final report of an INTAS project (Calmet 2002). On the theoretical side, numerous results on the relations between different kinds of involutive bases, Gröbner bases and characteristic sets have been obtained both for ordinary and for differential ideals. Several characterisation theorems for involutive bases have been proved and the computation of (differential) dimension polynomials has been studied. We have thoroughly investigated the homological approach to involution via Spencer cohomology. An algebraic algorithm for the geometric completion to involution was developed (including a constructive solution of the problem of the so-called delta-regularity).

## 4 Global integrability

Given a system of non-linear partial differential equations, can we decide of its integrability? A first answer is that we have tools, such as the Cartan-Kuranishi theorem, to decide of the local integrability but none to assess the global integrability. Physicists and mathematicians are investigating this problem for around 50 and 100 years respectively and no satisfactory solution is yet found.

A possible approach is to investigate the impact of involutive techniques outlined in the previous section in field theory, a domain of Physics. Most, if not all, physical models are represented by systems of partial differential equations. Among such systems are the well-known Yang-Mills or Einstein equations for instance. Without aiming at doing better than what the very many expert physicists of string theory are doing, it is possible to study whether some systems are integrable or not. What is challenging is to solve symbolically over- or under-determined systems of polynomial or differential equations or in simpler terms to extend the concept of Gröbner bases to such systems. This is again an old, well-known problem that was much earlier investigated by Cartan and his co-workers before being put aside. The need to design constructive methods in mechanized mathematics was at the origin of a revival. But, we still need to find out the proper representations in which to better formulate involutive bases. Again in very simple words, we are in a situation where we can get some information on local solutions of non-linear systems and we aim at extending them to some kind of non-local neighborhood. At this stage it is worthwhile to assess whether algebraic topology can be the key tool leading to a breakthrough in this domain. Physics texbooks such as (Weinberg 2002) report that algebraic topology is already playing a role in obtaining approximate solutions to physical systems. This is a truly challenging problem where the chaleenge is to design constructive proofs and decision methods. This is a task better suited for computer scientists.

## 5 An example in group theory

This is a prototypical domain where problems are more tedious and repetitive than dificult. Some open proof problems could take a lifetime to be completed by hand calculation. This area reminds of the beginning of computer algebra. The first successes that established the field were obtained in high energy particle physics, celestial mechanics or general relativity where repetitive, very long and tedious computations were required. Besides exceeding the human capability, they were also error prone when done on paper.

A test problem is as follows, where the word suitable is used to avoid a too long presentation of the problem:

> *Given a "suitable" infinite collection of p-groups, give a formula for the least n such that the i-th group in the collection can be embedded in* $S_n$*, not in* $S_{n-1}$.

This is, according to the experts, a very long term project even when coupling DSs and CASs. However, when analyzing the problem, it is possible to identify sub-problems. Many of them are purely computational ones. For instance, one must compute determinants of matrices. Depending on the size of these matrices, a very thorough management of the computation is required. There are deduction problems as well. One of them is supposed to be simple and can be seen as a test of feasibility.

*Can we prove, by machine, that every subgroup of $Q_{n^2}$, the quaternion group of order $2^n$, is normal?*

Solving such problems would bring fame in the group theory community.

## 6 Conclusion

This selection of a few computational domains where a need for new proof techniques looks pretty obvious shows, hopefully, that we are facing some very challenging mathematical problems. Some may be qualified to be grand. The list here, as said by Smale in his paper, is only taken from problems where the author has some experience. This is a further proof that it ought to be easely enlarged. It is not explicitely mentioned in the section on global integrability that the required tools belong to algebraic topology. This is a domain where contacts to computer science are rather limited. Two pieces of works are worth citing. A first one is by Jesus Aransay at the University of La Rioja in Spain. It is on progress and performed within Calculemus. It deals with proving theorems in algebraic topology. A second one is the KENZO computer algebra system of F. Sergeraert at the Fourier Institute in Grenoble. It is the only computer algebra system enabling to perform computations in algebraic topology. A last word is that a true grand mathematical challenge is possibly to solve a problem leading to fame in the domain, Mathematics or Physics, rather than in Computer Science.

## References


J. E. Taylor: Bulletin of the AMS, Vol. 40, No. 1, January 2003

S. Smale: Mathematical Problems for the Next Century, Mathematical Intelligencer Vol 20 No. 2, 7-15, 1998

S. Smale: Problèmes mathématiques pour le prochain siècle, Gazette des mathématiques, SMF, Janvier 2000.

G. Laumon and L. Moret-Bailly: "Champ algébriques",Vol. 39 in A Series of Modern Surveys in Mathematics, Springer, 1999

J. Calmet, M. Hausdorf and W. Seiler: A Constructive Introduction to Involution. Proceedings of ISACA2000 "Applications of Computer Algebra", R. Akerkar ed., Allied Publishers Limited, pp. 33-50, 2001

J. Calmet et al.: "INTAS - Final report", http://iaks-www.ira.uka.de/iaks-calmet/intas.htlm, 2002

J. Stern: Why Provable Security Matters?, In "Advances in Cryptology ", Proceedings of Eurocrypt 2003, Warsaw, May 2003, Biham E., Ed., LNCS 2656 , Springer, 2003

S. Weinberg: The Quantum Theory of Fields, Volume II, Chapter 23, Cambridge University Press, 1996