Executive Summary of Dagstuhl Seminar 09471
15. - 20. November 2009

Computer-assisted proofs - tools, methods and applications

Organizers: B. Malcolm Brown — University of Wales, GB
Erich Kaltofen — North Carolina State University, US
Shin'ichi Oishi — Waseda University - Tokyo, JP
Siegfried M. Rump — TU Hamburg-Harburg, DE

Our seminars on computer-assisted proofs are intended to assemble a diverse group of scientists working on differing aspects of computer-assisted proofs and verification methods. The current one is the fifth initiated by Rump.

Computer-assisted proofs in general are characterized by the fact that part of a mathematical proof is assisted in an algorithmic way. This includes numerical calculations, taking account of all numerical errors, as well as symbolic computations.

This concept of computer-assisted proofs can be regarded as a special approach to constructive mathematics. In recent years, various mathematical problems have been solved by computer-assisted proofs, among then the Kepler conjecture (a 3 dimensional sphere packing problem), the existence of chaos, the existence of the Lorenz attractor, and more.

A major representative of computer-assisted proofs are so-called verification methods. These are algorithms verifying the correctness of the assumptions of mathematical theorems with rigor. These methods use solely floating-point arithmetic estimating all numerical errors. Therefore these methods are particularly fast. Besides the conference, a 163-page review article on verification methods by Rump was discussed which appeared in 2010 in Acta Numerica.

In our seminar various new and interesting verification methods were presented. For example, Tibor Csendes and his collaborators proved the chaotic behaviour of a double pendulum, a result which made it to large public media such as FAZ and TV programs. Moreover, a number of new and nontrivial problems related to existence, non-existence and behaviour of solutions of partial differential equations were presented. In particular the rigorous enclosure of sloshing frequencies (Behnke) and proof of photonic band gaps (Plum) attracted attention. Moreover, Nakao discussed the convergence speed of finite element smooth solutions on an L-shaped domain, Kobayashi presented a priori-error estimation for the approximate solution of a certain bi-harmonic equation to establish a verification method for the driven-cavity problem, Nagatou discussed how to establish a theory for verifying the stability of traveling wave solutions for a certain PDE, and Wieners presented an abstract framework for verified constrained minimization. Traditional verification methods for specific problems like Frommer's square root of a matrix were presented as well. The computational speed can be improved by optimized BLAS routines with verified results as presented by Ozaki.

The discipline of symbolic computation is also well-suited to computer-assisted proofs. In particular the interplay between approximate and exact algebraic number arithmetic has recently lead to irrefutable computer proofs of real optimization problems that were unachieved before. Several researchers from symbolic computation presented approaches that either used exact methods or hybrid symbolic-numeric methods.

Exact linear algebra algorithms as they are found in the LinBox library can assist in proving theorems in graph theory, such as graph isomorphism problems (Clement Pernet's talk). Exact methods in polynomial algebra, in particular singularity removal from algebraic varieties are deployed in Mohab Safey El Din's (with Hoon Hong) Variant Quantifier Elimination (QE) algorithm. By relaxing the I/O specifications in Tarski's QE problem, instances that are notoriously difficult to tackle by software, for example from control theory, have become doable by VQE.

Another way of turning numerical computations into exact symbolic proofs is to prove real polynomial inequalities. At task is to consider a sum-of-squares proof (Artin's theorem) and first to proceed inexactly by a numeric semidefinite program solver, and second to convert the SOS expression into an exact polynomial identity with rational coefficients. Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi with their students have successfully proved an instance of the monotone column permanent conjecture, given proofs for large degree for highly accurate factor coefficient bounds (known also as Siegfried Rump's model problem), and proved the positivity of polynomials arising in Voronoi diagram computations. Härter used the sums-of-squares approach in a verified optimization algorithm in pure floating-point.

In computer algebra a common tool is exact arithmetic. Operations in the field of rational numbers or algebraic extensions are performed exactly rather than approximating them. Another way to get rid of errors in floating-point operations are so-called error-free transformations. Here the result of an operation between floating-point numbers is represented exactly by a pair of floating-point numbers. These approaches produce results at tremendous speed because those pairs are computed themselves with few floating-point operations. Among others Graillat presented how to compute dot products over finite fields using error-free transformations in pure floating-point, or Ogita extended an algorithm by Rump to solve extremely ill-conditioned problems with condition number way over 10^100 in double precision floating-point arithmetic to calculate an LU- or Cholesky-decomposition.

Some of the basic algorithms using pure floating-point algorithms need very few operations, so that testing and comparing the quality of such algorithms becomes difficult. To overcome this, Langlois used detailed models of computer architectures for recent machines to model instruction-level parallelism. This technique explains why certain algorithms using error-free transformations are much faster than suggested by a pure flop count.

Finally, Arnold Neumaier allowed us to view the possible future of proofs in mathematics with his FMathL. In this ambitious project plain TeX-files of mathematical proofs shall be syntactically and semantically analyzed and transformed into formalized and computer- and human-readable proofs. Although it sounds pretty futuristic, detailed

plans suggest that it can be achieved some day.

The organizers refrained from presenting talks to give more space to the participants. As always, they and the 46 participants from 10 different countries of the seminar enjoyed the pleasant and stimulating atmosphere in Dagstuhl. Our own assessment is that computer-assisted proofs have several new exciting directions pursued by a number of established and young researchers, and we are already looking forward to the next seminar.