05391 – Executive Summary
Numerical and Algebraic Algorithms and Computer-assisted Proofs
— Dagstuhl Seminar —
26.–30. September 2005

Bruno Buchberger[1], Christian Jansson[2⋆], Shin'ichi Oishi[3], Michael Plum[4], Siegfried M. Rump[2,3]

[1] Johannes Kepler University, Linz, Austria
[2] Hamburg University of Technology, Germany
[3] Waseda University, Tokyo, Japan
[4] University of Karlsruhe, Germany

Abstract. The common goal of self-validating methods and computer algebra methods is to solve mathematical problems with complete rigor and with the aid of computers. The seminar focused on several aspects of such methods for computer-assisted proofs.

Keywords. Self-validating methods, computer algebra, computer-assisted proofs, real number algorithms

1 Short description and aims of the seminar

Recently, a number of problems have been solved by so-called computer-assisted proofs, among them the celebrated one of the Kepler conjecture, the proof of existence of chaos, the verification of the existence of the Lorenz attractor, and more. All those problems have two things in common: first, the computer is used to assist the proof by solving certain subproblems, and second these subproblems are of numerical nature.

There are also many famous results of nontrivial proofs which can be performed automatically by symbolic means. For example, Risch's algorithm for integration in finite terms, solution of polynomial systems by Gröbner bases, quantifier elimination and more. Any of those solves a nontrivial mathematical problem which could be quite hard to solve by pencil and paper.

Those algorithms are frequently executed in exact arithmetic over the field of rationals or an algebraic extension field using well known methods from computer algebra, while the problems mentioned in the first paragraph are continuous in nature. They can be solved by so-called verification or self-validating methods.

⋆ Unfortunately, one of the organizers (S.M. Rump) was not able to attend the workshop on grounds of ill health, so C. Jansson kindly helped with preparing this report.

Dagstuhl Seminar Proceedings 05391
Algebraic and Numerical Algorithms and Computer-assisted Proofs
http://drops.dagstuhl.de/opus/volltexte/2006/454

Basically, self-validating methods verify the validity of assertions of certain theorems, where the latter are formulated in such a way that validation is possible by means of numerical computations. The main point is that this validation is absolutely rigorous including all possible procedural or rounding errors, and usually solely IEEE 754 double precision floating point arithmetic is used. On the one hand, the use of finite precision arithmetic implies very fast calculations, but on the other hand it limits the scope of applicability.

In contrast, most algorithms in computer algebra are 'never failing', that is they are proved to provide a solution for any input, and the maximum computing time for this is estimated a priori. To speed up practical implementations, also hybrid methods combining computer algebra with numerical verification methods are used.

Self-validating and computer algebra methods share the aim to solve certain mathematical problems with complete rigor and with the aid of computers. This seems a very natural task. Other areas such as computer geometry and graphics, real number theory and more have similar aims. Therefore it was very fruitful to create a link of information between experts in those different fields. The common basis or goal is the computer-assisted solution of mathematical problems with certainty.

The choice of organizers also reflects different fields of interest and expertise. The stimulating atmosphere in Dagstuhl was definitely a very fruitful environment for this enterprise.

2 Symbolic Computation and Real Number Theory

Talks from the symbolic computation community ranged from purely symbolic algorithm talks to talks in which the interaction of symbolics and numerics were demonstrated in concrete examples.

As an introduction to the symbolics talks, Freek Wiedijk gave an overview on existing systems of the "proof assistant" type. In this paradigm, algorithmic reasoners are used for checking the correctness of mathematical proofs provided by humans. This paradigm is different from the "algorithmic proof generation" paradigm in which, for certain classes of formulae or areas of mathematics, proofs or disproofs of mathematical statements are generated automatically. In the talk of Bruno Buchberger, he showed how induction provers following this second paradigm can be used to synthesize algorithms from specifications by his "lazy thinking" method: For a given specification, various algorithm schemes (formulae that describe algorithms in terms of subalgorithms) are tried out. For a given scheme, an automated proof of the correctness of a scheme relative to the specification is attempted. The proof will normally fail because nothing is known on the subalgorithms. From the partial proof object, specifications for the subalgorithms are then generated automatically.

Markus Rosenkranz presented a new, purely symbolic, method for the solution of linear boundary value problems in a purely operator theoretic setting

that translates the problem into the problem of solving a system of equations in a non-commutative polynomial domain using the Gröbner bases technique.

Kazuhiro Yokoyama presented ways how to compute the greatest common divisor for univariate polynomials whose exponents are indeterminates. The method can deliver answers for certain classes and, as an output, yields a classification of the values of the indeterminate exponents and the respective form of the gcd. He showed applications for computing Galois groups and the splitting field of polynomials and gave an outlook for the more general problem of computing Gröbner bases of sets of multivariate polynomials with indeterminate exponents.

Sylvie Boldo demonstrated a successful application of two of the most powerful proof assistants to the verification of basic algorithms for floating point operations. She gave some comments on the range of application of this technology for the verification of elementary numerical operations and also made suggestions for necessary improvements of the proof assistants.

Stefan Ratschan discussed a problem from the first-order theory of real numbers and a problem occurring in the verification of hybrid dynamical systems. The common aspect of the two problems is that, in principle, they are undecidable but can be made decidable for a specific subclass of inputs that excludes degenerate cases. The decision algorithms are based on validated floating-point arithmetic.

Hirokazu Anai introduced a variant of the purely symbolic cylindric algebraic decomposition (cad) method, in which some of the (costly) algebraic number computations are replaced by floating point operations with validation of the results. He showed how this version of the cad method can be used for solving certain semidefinite programming problems that occur in industrial applications.

In a comprehensive survey, Prashant Batra presented many of the various fundamental approaches (inconstructive, symbolic, numeric) taken in history for proving the fundamental theory of algebra on the total number of roots of a complex univariate polynomial and discussed their constructive content. He then focused on Smale's approach to determine the total cost of algorithms considering root-finding by Newton's method and showed how the approach can be improved to provide an algorithm of polynomial cost that may be implemented using validated inclusions. Also Kurt Mehlhorn considered the root isolation problem. The specific setting assumes that the coefficients of the input polynomial are given in bitstream mode, i.e. additional bits can be requested (at no cost) if necessary for achieving the desired accuracy. The approach taken is a randomized variant of Descartes' algorithm, which results in good time complexity.

Stefan Schirra started from an interesting application problem that asks about how to direct a straight line (e.g. a surgery instrument) into a cloud of points (e.g. critical points in the brain) maximizing the minimal distance to the points. He showed how an optimal $O(nlogn)$ algorithm by Follert et al. can be turned into a practical variant that avoids non-rational computations and uses the exact geometric computation paradigm by Yap et al. for a guaranteed result.

3 Computer-assisted Proofs and Self-validating Methods

A substantial number of talks was devoted to computer-assisted proofs for boundary value problems with partial (and ordinary) differential equations, using numerical verification methods. Here, one usually starts with a numerical approximation, and then uses functional analytical tools (e.g. fixed point theorems or variational characterizations) to prove the existence of a solution which is "close to" the approximation with respect to some suitable function space norm.

Yoshitaka Watanabe and Mitsuhiro T. Nakao proposed such an approach for the heat convection problem (on a rectangular domain); Watanabe treated the two-dimensional case and is thus able to make use of the stream function, while Nakao attacks the three-dimensional case by divergence-free basis functions.

Kenta Kobayashi proved global uniqueness for the extreme Stokes wave using monotone/antitone iteration techniques and verified numerical integration. Nobito Yamamoto gave a more abstract result on existence and local uniqueness for differential and integral equations by deriving conditions which can be checked by computer assistance and guarantee the applicability of Banach's Fixed Point Theorem.

A different mathematical approach was proposed by Christian Wieners to treat nonlinear variational inequalities constituting a simplified model of perfect plasticity: Using both the primal and the dual problem enables him to obtain an enclosure for the dual solution directly from the variational characterizations.

Kaori Nagatou aims at enclosures and – in particular – exclosures for eigenvalues of selfadjoint eigenvalue problems. Her computer-assisted approach is new in the sense that it does not use variational characterizations and is therefore applicable also in gaps of the essential spectrum.

Henning Behnke considered parameter-dependent clamped plate problems; by computer assistance he proves rigorously that the eigenvalue curves do not cross (as a first rough inspection might suggest), but veer. For the clamped plate boundary value problem, Borbála Fazekas proposed a computer-assisted enclosure method, which uses approximations possessing only first (weak) derivatives, even if the problem is of fourth order.

In a tutorial lecture, Arnold Neumaier presented his view on the interactions between mathematics, computer science, approximating numerical methods, rigorous numerics, and algebraic and symbolic approaches, in particular under the aspect of computer-assisted proofs.

A number of talks dealt with floating point arithmetic as a basis of a computer assisted proof. Takeshi Ogita presented fast and accurate algorithms for computing sum and dot product of vectors of floating point numbers, which is a joint work with Siegfried M. Rump and Shin'ichi Oishi. Oishi presented a scalable and meta-algorithm for giving verified numerical solutions for linear systems with large condition numbers and/or with large dimensions using the ORO algorithm by Ogita, Rump and Oishi.

Philippe Langlois presented, as an application of ORO algorithm, accurate and validated polynomial evaluation methods. Olga Holtz has discussed, for a given multivariate real (or complex) polynomial p and a domain D, a procedure

which decides whether an algorithm exists to evaluate $p(x)$ accurately for all x in D using rounded real (or complex) arithmetic.

Further applications of verifying numerical computations were presented, for example, by Andreas Frommer, who gave a report to improve over previous attempts to computationally verify the existence of spherical t–designs. These are quadrature rules for the sphere with equal weights and $(t+1)^2$ nodes having a degree of exactness of t. Luiz Henrique de Figueiredo presented a guaranteed algorithm for computing images of quadratic Julia sets, which is in sharp contrast to the usual, purely heuristical pictures. Furthermore, Jean-Marie Chesneaux has discussed a new statistical test applied to a classical interval problem.

Moreover, applications to engineering modeling were presented. Wolfram Luther discussed strategies to enhance modern modeling and simulation software using numerical verification tools. Balazs Banhelyi presented computer assisted proofs of conjectured properties for certain delayed differential equations with chaotic behavior.

Eric Walter presented interval analysis based tools for designing parametric controllers to achieve robust performance. Stef Graillat discussed about interval polynomials and their stability radius.

Several talks were presented in the area of numerical optimization with result verification, reaching from special classes (linear or convex programming problems) to nonconvex combinatorial and global optimization.

Götz Alefeld presented a computational enclosure method for the solution of a class of nonlinear complementarity problems. This method is based on interval arithmetic and delivers a proof for the uniqueness of the solution. Tibor Csendes investigated chaotic regions of dynamical systems. The problem of finding chaotic regions of certain systems can be described as a global optimization model. Theoretical results proving correctness and convergence properties were discussed.

Christian Jansson presented a method for solving rigorously combinatorial optimization problems. Occasionally, due to solving relaxations of these combinatorial problems within a branch-and-bound framework, rounding errors may produce erroneous results, although the algorithm should compute the exact solution in a finite number of steps. This may occur especially if the relaxations are ill-conditioned or ill-posed, and if Slater's constraint qualifications fail.

A software package was presented by Christian Keil for computing rigorous optimal value bounds for linear programming problems. He discussed his numerical experience with the Netlib lp library, a collection of problems with numerous applications and showed that many real world problems exhibit numerical difficulties due to ill-conditioning. His package can handle point and interval problems.

Arnold Neumaier introduced new necessary and sufficient conditions for global optimality of polynomial global optimization problems. These conditions are based on the Positivstellensatz. He applied these conditions within a branch-and-bound framework for rigorously solving algebraic equations and inequalities over the reals. Some examples together with a Matlab implementation were demonstrated.