Dagstuhl-Seminar (Nr. 04061)

on

Real Computation and Complexity

IBFI Schloss Dagstuhl
February 1–6, 2004

Organizers:

Thomas Lickteig (Limoges)

Klaus Meer (Odense)

Luis M. Pardo (Santander)

Summary

The seminar "Real Computation and Complexity" was intended as a meeting place of several tendencies in the complexity analysis of algorithms in real computation. One main idea therefore was to bring together scientists with rather different backgrounds such as numerical analysis, symbolic computing, real and complex algebraic geometry, logic, differential algebra and computational complexity. This broadness guaranteed to get a thorough overview of current results, methods and trends in the area. It allowed as well to discuss main problems related to all aspects of real computation and complexity from different perspectives.

The seminar was attended by 43 participants from 14 different countries (Argentina, Belgium, Brazil, Canada, Denmark, Germany, England, France, Israel, Italy, Russia, Spain, Switzerland, USA). About 18 of the participants were at

Dagstuhl Seminar Proceedings 04061
Real Computation and Complexity
http://drops.dagstuhl.de/opus/volltexte/2006/499

the age of 35 or younger. During the five days 34 talks were presented, each of which lasted 25 minutes plus 5 minutes for discussion. This left plenty of time for informal discussions and work outside the time slots scheduled for talks.

In the following we outline the main contributions as presented in the talks as well as some future directions that turned out to be important in additional discussions (either directly after a talk or during the week). The main topics addressed were

- complexity upper bounds for linear optimization problems;
- models of computation with real numbers and structural transfer results between them;
- complexity issues and algorithmics in symbolic and numeric multivariate polynomial equation solving and elimination theory;
- quantitative aspects in real equation solving;
- algorithmic aspects and quantitative estimates in differential equation solving;
- fast evaluation of polynomial and analytic functions.

A first group of talks was dealing with the development of **new techniques** to analyze the **complexity of the Linear Programming** problem in **algebraic models** and its translation to the bit model. Note that one of the major open problems in LP theory is the question whether there exist strongly polynomial algorithms or not, i.e. whether LP $\in P_{\mathbb{R}}$ over the reals. Dedieu and Malajovich presented a very interesting approach that studies the curvature of the central paths defined on each of the faces of a feasible polyhedron. In a first step, a concise analysis of interior point methods under the perspective of dynamical systems is done. To each face of the feasible region a Newton vector field is associated that has as its unique singular point the analytic center of the corresponding central path on that particular face. Next, the idea is that long-step interior point methods are the more efficient the closer the central path is to a straight line (i.e. the smaller its curvature is). Under reasonable probability distributions it can then be shown that the total curvature of the central path (both primal, dual and primal-dual) is of order $O(n), n$ number of variables of the problem instance. This is done by reducing the question to zero-counting for special polynomial systems.
One of the most interesting questions for future work is in how far the above idea can be formalized, i.e. whether a complete complexity analysis of LP can be given in terms of the total curvature. This would parallel some of the most important recent developments in LP relating the complexity to condition numbers

(work by Ye et. al). Another approach was taken by Castro et al. Here, a general **transfer principle** for average case analysis between the Blum-Shub-Smale model (with rational constants) and the Turing model was presented. As one main result there were given precise conditions under which a discrete probability analysis approximates a continuous one. The approach was exemplified with an application to LP; combining it with results by Borgwardt and Borgwardt-Huhn a strongly polynomial average case complexity of interior point methods can be established.

A yet different promising way for a future analysis of LP with respect to strongly polynomiality is given by the framework of Monadic Second Order Logic, see below.

Structural complexity and the **impact of logic** for designing efficient algorithms were crucial aspects of another group of presentations. Makowsky presented new results on the efficient evaluation of certain families of graph polynomials on graphs of bounded tree-width. In general, many of these problems are NP-hard. The main new technical tool is a splitting lemma for such polynomials that allows their evaluation according to a decomposition of the given input structure. Expressibility of the properties to compute in Monadic Second Order Logic MSOL together with a generalization of the classical Feferman-Vaught theorem are the crucial logical framework that makes the approach working. Its generalization to other than finite structures allows the methods to work as well for certain algebraic problems.
One future idea (based on previous work by Makowsky and Meer) is to find subclasses of the LP (and other) optimization problem that can be solved in strongly polynomial time using the MSOL framework. This would result in a completely different approach than those mentioned before.
The importance of complexity results in different computational models together with implications of such results to classical complexity theory was treated in the presentations of Koiran, Gassner and Prunescu. Prunescu showed the equivalence of the classical P versus NP question with the problem whether there exists an ordered abelian semi-group in which the Knapsack problem is efficiently solvable. An extremely interesting talk was given by Koiran. Here, he related fundamental complexity questions in three models of computation, namely the Turing model, the BSS model over $\mathbb{C}$ and Valiant's model. Starting point is the question of computing sequences of integers from the constants $-1, 0, 1$ with $+, \bullet$ as operations. Particularly interesting such sequences are multiples $(b_n \cdot n!)_{n\in\mathbb{N}}$ of the sequence $(n!)_{n\in\mathbb{N}}$. It was known before (Shub and Smale) that the non-existence of fast (to be precised) algorithms for at least one such sequence implies P $\neq$ NP over the complex numbers. Koiran now combines that question with a constant-free version of Valiant's model. As main result he shows that if $(n!)_{n\in\mathbb{N}}$ cannot be computed efficiently, then either P $\neq$ PSPACE or the permanent is not in Valiant's class VP_0 (the index 0 standing for the constant free version). Note

that both options are major unproven conjectures in the corresponding computational models. The result thus stresses the importance of considering the complexity of computing $(n!)_{n\in\mathbb{N}}$ for all the before mentioned models.
Since the efficient computation of $(n!)_{n\in\mathbb{N}}$ is closely related to efficient factoring algorithms over the integers a very important future direction of this work is to check in how far quantum computers could be used to speed up the computations of such sequences. This might as well give new insight into the question in how far Quantum Computers are more powerful than classical ones.

Some more talks proved the variety of important questions arising from computational questions in **different models related to the real numbers**.
Montaña presented work on evolutionary algorithms and outlined an application of such algorithms to semi-algebraic problems. Weihrauch developed foundations of a higher type programming language for computations over $\mathbb{R}$ based on recursive analysis. Korovina studied logical characterizations of computability over continuous data types using hereditarily finite sets with $\mathbb{R}$ as base structure.
Novak analyzed randomized approximation algorithms (in terms of numerical analysis) for problems in IBC (where the BSS model together with an oracle is used as underlying computational model). He focused on restricted randomization where only random bits are used and gave precise complexity bounds for a number of problems (f.e. approximation of means, approximation of integrals, integral equations etc.).
The reachability problem of certain states in hybrid (dynamical) systems was studied by Brihaye and Michaux. They established an interesting relation to the concept of o-minimality of the underlying topological space: If the latter property is given the system admits bisimulation. This result gives a Myhill-Nerode like theorem for certain dynamical systems used as computational model.
The concept of o-minimality also provides a link back to semi-algebraic and analytic functions. Cell-decompositions for zero sets of (Boolean combinations of) such functions are based on o-minimality and are crucially underlying many algorithmic questions (like quantifier elimination, computing road-maps, robot-motion-planning). Ziegler gave improved complexity bounds on a class of functions simulating, for example, the dynamics of an N particle system.

Complexity Estimates in Polynomial Equation Solving both in a symbolic (exact) and a numeric (approximate) setting was a third major topic. A polynomial system solver is an algorithm that takes as input a system of multivariate polynomial equations. It then outputs information that can be used to answer elimination questions concerning the solution variety. For instance, deciding consistency of a system of polynomial (in-)equations would become a simple task provided that an accurate polynomial system solver prepares the data. Usual polynomial system solvers reduce the consistency problem to the evaluation of the determinant of a huge matrix (the resultant of the system). The two most important approaches for that problem are **numerical analysis**

solving procedures on the one side and **symbolic computing and computational algebraic geometry** on the other. The complexity of polynomial system solvers is a central topic in computational mathematics; it is a longstanding open problem to decide whether this task can be performed in sub–exponential time. Important progress on several related questions was achieved. For instance, the talks by G. Lecerf and J. C. Yakoubsohn presented some complexity estimates of deflection techniques to approximate singular zeros of systems of multivariate polynomial equations. As in the non-singular case, where a Newton operator is used, both talks presented several estimates that may lead to some $\alpha-$theory in the singular case. The latter become upper bound estimates for the complexity of approximating singular zeros of multivariate polynomial equations. In his talk J. San Martín discussed upper complexity bounds from both the numeric and symbolic approach to solving. He introduced the paradigm of **non-universal solvers**. From the work by [Castro et al., 2003] universal system solvers require exponential running time to solve systems of multivariate polynomial equations. Then, the only way out to have sub-exponential algorithms is the search for non-universal polynomial system solvers. Hence, San Martín presented a non-universal symbolic polynomial system solver well-suited for generalized Pham systems. In addition, he proved global Newton deformation non–universal solvers behave as universal ones: their output contains universal information in infinitely many cases. Hence, the worst case time complexity is also exponential. Upper bounds on the average complexity of homotopic deformation techniques dealing with systems of polynomial equations with rational coefficients were also exhibited. The talk by J. Verschelde presented another approach to this open problem. Verschelde discussed the main drawback in numerical analysis solvers: How the information provided by a numerical solver can be used to eliminate a single block of quantifiers (decision of consistency). His technique, based on a combinatorial strategy, replaces the computation of the determinant of huge matrices by the **combination of approximations of the irreducible components** of the solution variety. Verschelde could show that the experimental behavior of his algorithms is close to efficiency. Finally, the talk by G. Matera discussed an example (originating in a particular parabolic differential equation) where the concurrence of numerical analysis and symbolic computation polynomial system solvers yields as consequence the better performance of numerical solvers.

Real polynomial equation solving (i.e. the computation of information about real solutions) was another important theme. In a series of lectures M. Giusti, B. Bank and L. Lehmann considered the notion of a **polar variety** of a complete intersection real algebraic variety as starting point. Its relation to the design of efficient algorithms computing real solutions of multivariate polynomial equations was described. Applications of these intrinsic algorithmic techniques to the problem of Image Processing (Wavelets) were given. This included as well the development of an efficient software package.

Semi-numerical and **virtual real polynomial equation solving** were also discussed in the works by L. Gemignani and M.F. Roy. Starting point of Roy was the gap between upper bounds of the number of real solutions given by the Budan–Fourier Theorem and the exact number of real solutions. The notion of virtual root of a polynomial was generalized to the multivariate case, showing the connections of that notion with the Budan–Fourier multivariate theorem (counting the number of real solutions with virtual multiplicities by counting sign changes). In Gemignani's talk a semi–numerical treatment of the Bézoutian matrix of polynomials given in Bernstein bases was reported. Pericleous (in joint work with Vorobjov) presented a new cell-decomposition algorithm for restricted sub-analytic sets together with improved upper bounds on the number of cells in such a decomposition. One main future question is in how far that approach also gives new results for the semi-algebraic framework.

Several other talks were concerned with the exhibition of **upper bound estimates of the topology of semi–algebraic and definable subsets of a real affine space**. Such estimates are important both for upper and lower complexity bounds in real algorithmics. N. Vorobjov reported on upper bounds estimates for the sum of Betti numbers of definable sets, including semi–algebraic and sub–Pfaffian sets, given by first order formulae (with or without quantifiers). The main ingredient was the spectral sequence introduced in a joint work with A. Gabrielov and T. Zell. In the talk of T. Krick, new upper bound estimates of the number of connected components of semi–algebraic sets in terms of the number of monomials of the defining polynomials were given (based on improvements of estimates by Li, Rojas and Wand obtained by Perucci). Finally, Werman reported about work relating quantifier elimination to applications arising from Computer Vision problems.

Several talks were concerned with complexity aspects in **Differential Equation Solving**. D.Yu. Grigor'ev presented a Bézout type upper estimate for the number of solutions of a linear partial differential equation. The main technical ingredient is a new treatment of the quasi-inverse matrices over Weyl algebras. J.A. Weil presented some ongoing research in cooperation with T. Cluzeau concerning the use of factorization and mod p differential equation solving techniques.

The **complexity of fundamental base algorithms** was analyzed by E. Kaltofen, A. Storjohann, M. Bläser and A. Schönhage. Kaltofen reported on recent joint work with J. May on the complexity of multivariate polynomial approximate factorization. This is a new example of an algorithm were the interplay of numeric and symbolic techniques through a linear partial differential equation (Ruppert's Theorem) yields meaningful progress. Storjohann's contribution was motivated by fast and exact linear algebra computations on integer matrices (f.e. for linear system solving). His main outcome was to observe how exact linear algebra can be speeded up by using approximate arithmetic. For example, the

leading coefficient of the p-adic expansion of the product of two integers may be recovered from the first few leading coefficients of the operands. The phenomenon of integer-carries may lead to errors; fortunately, most of these drawbacks can be avoided using the shifted number system. M. Bläser and A. Schönhage's talks were mainly concerned with sharpened bounds on base algorithms. Bläser proposed refined algorithms for multi–point polynomial evaluation and polynomial interpolation procedures yielding improved upper bounds. In A. Schönhage's talk new evaluation algorithms of transcendental functions as exp, log and trigonometric functions with given precision arithmetics (medium precision semi–numeric algorithms) were analyzed.

The atmosphere of the meeting was characterized by open minded culture of discussion. The feedback among the participants was very positive. Many of them pointed out both the chance to meet colleagues working on the same subject, but also learning about new approaches to problems they have been working on following different points of view. This was seen as a big plus of the meeting.

Needless to say that the excellent facilities in Dagstuhl did their own to make the seminar a success. We want to close this report by thanking very much both the local team and Annette Beyer and Angelika Mueller from Saarbrücken for their extraordinary work.

The Dagstuhl-Seminar was devoted to honor renowned scientist, complexity theory pioneer and celebrity Arnold Schönhage on the occasion of his 70th birthday in December 2004. There will be a ***Festschrift for Arnold Schönhage*** *special volume of* ***Journal of Complexity*** *issue of this Dagstuhl meeting.*