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

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 $(n!)_{n\in\mathbb{N}}$ <u>cannot</u> 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.*

Abstracts

Polar Varieties, Real Elimination & Application to the Wavelet Design: Part II The Algorithm and philosophy of an application

by Bernd Bank, Humboldt Universität zu Berlin

In the first part of the talk I describe the following result:
If the real variety $S_{\mathbb{R}} := S \cap \mathbb{R}^n$ is non–empty and smooth and if S is given by a regular sequence $f_1, \ldots, f_p$ in $\mathbb{Q}[X_1, \ldots, X_n]$ such that, for any $1 \le h \le p$, the ideal generated by $f_1, \ldots, f_h$ is radical, then there is an **arithmetic network** that finds a (real algebraic) representative point of each connected component of $S_{\mathbb{R}}$ in (polynomial) sequential time $\binom{n}{p} L^2 (nd\Delta)^{O(1)}$ (counting arithmetic operations in $\mathbb{Q}$ at unit cost). Here d is an upper bound for the degrees of the polynomials $f_1, \ldots, f_p$; L denotes the (sequential time) *arithmetic circuit complexity* of them and, $\delta \le d^n p^{n-p}$ is the (suitably defined) *degree of the real interpretation* of the polynomial equation system $f_1, \ldots, f_p$.
This talk is also devoted to the application of the algorithm combined with the software package Kronecker [Lecerf, 01], designed for the solution of polynomial equations over the complex numbers, in order to find the coefficients of suitable one–dimensional wavelet transforms (**MRA**) for the construction of optimal image compression filters (see also [LeWa, 01].
Joint work with M. Giusti, J. Heintz, L. Lehmann, L.M. Pardo.

References

- [Lecerf, 01] G. Lecerf. “Une alternative aux méthodes de reécriture pour la résolution des systémes algébriques”. Thése, École Polytechnique, 2001.
- [LeWa, 01] L. Lehmann, A. Waisbein. “Wavelets and semi–algebraic sets”. *Annales JAIIO*, **30** (2001) 139–155.

Fast multiple polynomial evaluation and interpolation

M. Bläser, ETH Zürich.

Exploiting a trick we learned from Arnold Schönhage, we devise an algorithm for evaluating a univariate polynomial of degree $< d$ at d points that uses $6d \log d + O(d)$ nonscalar operations. This algorithm is then used to show that univariate polynomial interpolation can be performed with $8d \log d + O(d)$ nonscalar operations. During the Dagstuhl Seminar it came to our attention that Baston, Lecerf, and Schost (ISSAC 2003) obtained bounds that are better than ours.

On $o-$minimal hybrid systems
T. Brihaye, Université de Mons–Hainaut.
This paper is driven by a general motto: bisimulate a hybrid system by a finite symbolic dynamical system. In the case of o-minimal hybrid systems, the continuous and discrete components can be decoupled, and hence, the problem reduces in building a finite symbolic dynamical system for the continuous dynamics of each location. We show that this can be done for a quite general class of hybrid systems defined on o-minimal structures. In particular, we recover the main result of a paper by Lafferriere G., Pappas G.J. and Sastry S. on o-minimal hybrid systems. We also study decidability questions in the general framework of the BSS model.

Joint work with C. Michaux, C. Rivière, C. Troestler

On the average complexity of algorithms over the rationals
D. Castro, Universidad de Alcalá.
In our talk we consider the following two questions:
1.- *Is there any relationship between continuous average complexity analysis and discrete ones?*
2.- Can be continuous average complexity analysis transferred to discrete ones?
We give positive answers for both questions and we state transfer principles which allow us to derive average complexity estimates in a discrete setting from similar estimates in the continuous case. Usually it is simpler to do things in a continuous setting and the moral of our talk is that, under certain assumptions, these continuous estimates reflect the practical average complexity.
We apply the transfer principles developed to the case of two different approaches to solve linear programming problems: simplex and barrier methods, obtaining that both of them are efficient for rational entries on the average. We do so, considering Borgwardt and Huhn's estimates that were done in a continuous setting.
Joint work with J.E. Morais, L.M. Pardo.

On the Curvature of the Central Path of Linear Programming Theory

by JEAN–PIERRE DEDIEU, Université Paul Savatier, Toulouse, and GREGORIO MALAJOVICH, UFRJ, Rio de Janeiro.

We prove a linear bound on the average total curvature of the central path of linear programming theory in terms on the number of independent variables of the primal problem, and independent on the number of constraints.
Joint work with M. SHUB.

A Structure of Finite Signature with P=NP

by CHRISTINE GASSNER, Universität Greifswald.

We use a uniform model of computation over structures of finite signatures. The permitted computing operations are given by the functions of the considered structure. The test conditions are defined by means of the relations of such a structure. This is a generalization of the Blum-Shub-Smale model. The considered structure is a structure of trees which are used for structuring data for the efficient inserts and searches of data in the computer science. It can be expanded by a relation such that P=NP is valid respecting the uniform computation model over this.

Resultant computation for polynomials in Bernstein form

by LUCA GEMIGNANI, Università di Pisa

We devise a fast fraction-free algorithm for the computation of the triangular factorisation of Bernstein-Bezoutian matrices with entries over an integral domain. Our approach uses the Bareiss fraction-free variant of Gaussian elimination, suitably modified to take into account the structural properties of Bernstein-Bezoutian matrices. The algorithm can be used for solving problems in algebraic geometry that arise in computer aided geometric design and computer graphics. In particular, an example of the application to this algorithm to the numerical computation of the intersection points of two planar rational Bézier curves is presented.

Polar Varieties, Real Elimination & Application to the Wavelet Design: Part I Polar Varieties

by MARC GIUSTI, École Polytechnique/C.N.R.S.

Let W be a closed algebraic subvariety of the $n-$dimensional projective space over the complex or real numbers and suppose that W is non–empty and equi–dimensional. In this talk (based on [BGHP, 03]) the classic notion of polar variety of W associated with a given linear subvariety of the ambient space of W is

generalized. As particular instances of this new notion of generalized polar variety we re-obtain the classic ones and tow new types of polar varieties, called *dual* and (in case that W is affine) *conic*. In the case that the variety W is affine and smooth and has a complete intersection ideal of definition, we are able, for a generic parameter choice, to describe locally the generalized polar varieties of W by explicit equations.
We show constructively that for a generic parameter choice, the generalized polar varieties of W are either empty or equi–dimensional and smooth in any regular point of W.
Joint work with M. Giusti, J. Heintz, L. Lehmann, L.M. Pardo.
References

- [BGHP, 03] B. Bank, M. Giusti, J. Heintz, L.M. Pardo. "Generalized Polar Varieties: Geometry and algorithms". Manuscript, Humboldt Universität (2003).

Weak Bézout inequality for $\mathcal{D}-$modules

by Dima Grigoriev, Université de Rennes I

Let $\{w_{i,j}\}_{1\leq i\leq n,1\leq j\leq s} \subset L_m = F(X_1,\ldots,X_m)[\frac{\partial}{\partial X_1},\ldots,\frac{\partial}{\partial X_m}]$ be linear partial operators of orders with respect to $\frac{\partial}{\partial X_1},\ldots,\frac{\partial}{\partial X_m}$ at most d. We prove an upper bound

$$n(4m^2dmin\{n,s\})^{4^{m-t-1}(2(m-t))}$$

on the leading coefficient of the Hilbert–Kolchin polynomial of the left L_m-module $\langle\{w_{1,j},\ldots,w_{n,j}\}_{1\leq j\leq s}\rangle \subset L_m^n$ having the differential type t (also being equal to the degree of the Hilbert–Kolchin polynomial). The main technical tool is the complexity bound on solving linear equations over *algebras of fractions* of the form

$$L_m(F[X_1,\ldots,X_m,\frac{\partial}{\partial X_1},\ldots,\frac{\partial}{\partial X_k}])^{-1}.$$

Approximate factorization of multivariate polynomials via differential equations

by Erich Kaltofen, North Carolina State University

The input to our algorithm is a polynomial $f(x,y)$, whose complex rational coefficients are considered imprecise with an unknown error that causes f to be irreducible over the complex numbers $\mathbb{C}$. We seek to perturb the coefficients by a small quantity such that the resulting polynomial factors over $\mathbb{C}$. Ideally, one would like to minimize the perturbation in some selected distance measure, but

no efficient algorithm for that is known. We give a numerical multivariate greatest common divisor algorithm and use it on a numerical variant of algorithms by W. M. Ruppert and S. Gao.
Our numerical factorizer makes repeated use of singular value decompositions. We demonstrate on a significant body of experimental data that our algorithm is practical and can find factorizable polynomials within a distance that is about the same in relative magnitude as the input error, that even when the relative error in the input is substantial (10^{-5}).
Joint work with SHUHONG GAO, JOHN P. MAY, ZHENGFENG YANG AND LIHONG ZHI

Valiant's model and the cost of computing integers

by PASCAL KOIRAN, E.N.S. Lyon

Let $\tau(k)$ be the minimum number of arithmetic operations required to build the integer $k \in \mathbb{N}$ from the constants 1 and 2. A sequence x_k is said to be "easy to compute" if there exists a polynomial p such that $\tau(x_k) \leq p(\log k)$ for all $k \geq 1$. It is natural to conjecture that sequences such as $\lfloor 2^n \ln 2 \rfloor$ or $n!$ are not easy to compute. In this talk we show that a proof of this conjecture for the first sequence would imply a superpolynomial lower bound for the arithmetic circuit size of the permanent polynomial. For the second sequence, a proof would imply a superpolynomial lower bound for the permanent or P $\neq$ PSPACE.

Logical Approach to Computability over Continuous Data Tpyes

by MARGARITA KOROVINA, McMaster University

It is well-known that the classical theory of computation, which works with discrete structures,is not suitable for formalisation of computations that operate on real-valued data. Most computational problems in physics and engineering are of this type, e.g. problems relevant to foundation of dynamical and hybrid systems. Since computational processes are discrete in their nature and objects we consider are continuous, formalisation of computability of such objects is already a challenging research problem.
In this talk we will report about logical approach to computability on the reals based on the notion of definability. In this approach continuous objects and computational processes involving these objects can be defined using finite formulas in a suitable structure.
We will discuss beneficial features of this approach, recent results and future work.

A bound for the number of components of a $4-$nomial in the positive orthant

by TERESA KRICK, University of Buenos Aires

This talk presents a recent result by Daniel Perrucci, Universidad de Buenos Aires [Perrucci, 03] that follows (and slightly improves) statements and techniques developed by T.Y. Li, M. Rojas and X. Wang [LRW, 03]. The result is the following: the intersection between the zero set of a $4-$nomial in n variables and the positive orthant in $\mathbb{R}^n$ has at most 3 connected components, and the bound is sharp (the previous bound was 10).
There is also a general bound for $m-$nomials (that slightly improves the previous one by Li, Rojas and Wang) and an improved bound for a large subclass of $5-$nomials in 3 variables.
These results can be considered as a search for a generalization of Descartes' Rule of Signs for *one* multivariate polynomial, in the opposite direction of Khovanskii's result on the number of non–degenerate solutions of a system of n sparse polynomials in n variables.

References

- [LRW, 03]] T.Y. Li, M. Rojas, X. Wang. " Counting real connected components of trinomial curve intersections and $m-$nomial hypersurfaces". *Discrete and Computational Geometry* **30** (2003) 379–414.

- [Perrucci, 03] D. Perrucci. " Some bounds for the number of components of real zero sets of sparse polynomials". Preprint Universidad de Buenos Aires (2003).

On Existence and Approximation of Clusters of Zeros: Case of Embedding Dimension One

by GRGOIRE LECERF, Université de Versailles, and JEAN–CLAUDE YAKOUBSOHN, Université Paul Sabatier, Toulouse.

In the beginning of the eighties, S. Smale developed a quantitative analysis of Newton's method for multivariate analytic maps. In particular, his alpha-theory gives an effective criterion that ensures safe convergence to a simple isolated zero, i.e. where the map has co–rank zero. This criterion requires only information concerning the map at the initial point of the iteration. Generalizing this theory to multiple zeros is still a challenging problem. In this talk we deal with situations where the analytic map has co–rank one at the multiple zero, which has embedding dimension one. More generally, we define clusters of embedding dimension one. We provide a criterion for detecting such clusters of zeros and a fast algorithm for approximating them, with quadratic convergence. In the case of a cluster with positive diameter this algorithm stops at a distance of the cluster

which is about its diameter.
Joint work with Marc Giusti, Bruno Salvy.

Polar Varieties, Real Elimination & Application to the Wavelet Design: Part III Preparation, implementation & results; Kronecker versus Gröbner basis software

by Lutz Lehmann, Humboldt Universität zu Berlin

Wavelet bases and related generating systems of $L^2(\mathbb{R})$ recently became of high interest in approximation theory and signal/image processing. The main tool for constructing such objects is the multi–resolution analysis (MRA) and its scaling function. This scaling function satisfies a refinement equation which connects functional analysis and algebra.
The conditions originating in both field are conflicting, so the solution of the resulting system of algebraic equations is crucial. Cases with low complexity were solved manually, other cases lead to solution varieties of positive dimension, which are difficult to solve even when using conventional computer algebra software (CAS).
We present a short approach to the analytic theory [CM, 96] that allows to deduce semi–algebraic conditions [BW, 99] on the existence of the desired scaling function. Then we explain how the theory of polar varieties [BGHP, 03] and the method of stepwise elimination as implemented in the Kronecker package [Lecerf, 01] was applied to the problem of constructing symmetric orthogonal and continuous scaling. We obtained competitive results and computational complexity.
References

- [BGHP, 03] B. Bank, M. Giusti, J. Heintz, L.M. Pardo. “Generalized Polar Varieties: Geometry and algorithms”. Manuscript, Humboldt Universität (2003).

- [BW, 99] E. Belogay, Y. Wang. “Construction of compactly supported symmetric scaling functions”. *Applied and Computational Harmonic Analysis* **7** (1999) 137–150.

- [CM, 96] C. Cabrelli, U. Molter. “ Generalized Self–Similarity applied to Matrix Refinement Equations”. *Z. Angew. Math. Mech.* **76** (1996) 493–494.

- [Lecerf, 01] G. Lecerf. “Une alternative aux méthodes de reécriture pour la résolution des systémes algébriques”. Thése, École Polytehnique, 2001.

- [LeWa, 01] L. Lehmann, A. Waisbein. “Wavelets and semi–algebraic sets”. *Annales JAIIO*, **30** (2001) 139–155.

Splitting formulas for graph polynomials and their algorithmic use

by Johann Makowsky, Technion - Haifa

We give an overview and unify various techniques of computing graph polynomials efficiently on input which satisfy various structural properties. The abstract, and only theoretically efficient, version of the technique is based on a generalization of the Feferman–Vaught theorem for Monadic Second Order Logic. Practically efficient versions include the Tutte polynomial and colored Tutte polynomials, the generating function for SAT and others.

Non–Universal Algorithms to Solve Systems of Polynomial Equations

by Jorge San Martín, Universidad Rey Juan Carlos, Móstoles

In this talk, I introduce the notion of Non–Universal Algorithm applied to the problem of solving systems of multivariate polynomial equations. Roughly speaking, such algorithms do not compute full information on the solution variety, but only a piece of it.

I exhibit two different approaches: a symbolic procedure and a numerical one. In the first case, a symbolic algorithm is presented to solve a very general family of polynomial systems, the so called *Generalised Pham Systems*. In the second case, we study the complexity of the Numerical Linear Homotopy Deformation Algorithm within the context of the Approximate Zero Theory under the classical Turing Machine Model.

Joint work with C. Beltán and Luis M. Pardo.

Numeric vs. symbolic homotopy algorithms in polynomial equation solving: a case study

by Guillermo Matera, Universidad de Buenos Aires

We consider a family of polynomial equation systems which arises in the analysis of the stationary solutions of a standard discretization of certain semi–linear second order parabolic partial differential equations. We prove that this family of systems is well–conditioned from the numeric point of view, and ill–conditioned from the symbolic point of view. We exhibit a polynomial–time numeric algorithm solving any member of this family, which significantly contrasts the exponential behaviour of all known symbolic algorithms solving a generic instance of this family of systems.

Joint work with M. De Leo and E. Dratman.

Evolutionary Algorithms for NP-hard problems

by Jose Luis Montaña, Universidad de Cantabria

In 1977, Makanin stated that the solvability problem for word equation systems is decidable. Makanin's algorithm is very complicated and the solvability problem for word equations remains NP-hard even if one looks for short solutions. We show that testing solvability of word equation systems is a NP-complete problem if we look for solutions of length bounded by some given constant greater than or equal to two over some single letter alphabet. We propose a local search genetic algorithm for this problem and give some experimental results which indicate that our approach to this problem becomes a promising strategy.

Solving Integral Equations Using Random Bits

by Erich Novak, Universität Jena

Integral equations with Lipschitz kernels and right-hand sides are intractable for deterministic methods, the complexity increases exponentially in the dimension d. This is true even if we only want to compute a single function value of the solution. For this latter problem we study coin tossing algorithms (or restricted Monte Carlo methods), where only random bits are allowed. We construct a restricted Monte Carlo method with error ϵ that uses roughly ϵ^{-2} function values and only $d \log^2 \epsilon$ random bits. The number of arithmetic operations is of the order $\epsilon^{-2} + d \log^2 \epsilon$.
Hence, the cost of our algorithm increases only mildly with the dimension d, we obtain the upper bound $C \cdot (\epsilon^{-2} + d \log^2 \epsilon)$ for the complexity.
In particular, the problem is tractable for coin tossing algorithms.

A new method for cell decomposition of restricted sub–analytic sets and some complexity results

by Savvas Pericleous, Université de Rennes I

We present a method which decomposes the closed unit cube $I^n \subset \mathbb{R}$ into a disjoint union of cylindrical cells, compatible with a given semianalytic subset $S \subset I^n$, in such a way that if S is described by members of any family of restricted analytic functions closed under addition, multiplication and taking partial derivatives, then each cell of the decomposition is a subanalytic set described by functions from the same family. In the important particular case when the analytic functions involved in the definition of S come from a certain broad finitely defined class (namely, the class of Pfaffian functions) we are able to actually construct an algorithm for producing such a cylindrical cell decomposition, provided we are given an oracle for deciding emptiness of semi-Pfaffian sets. This implies the possibility of effective elimination of one sort of quantifiers from a first-order

formula involving restricted Pfaffian functions. The complexity of the algorithm as well as the bounds on parameters of the output are doubly exponential in $O(n^2)$ and are the best up-to-date.
Joint work with N. Vorobjov.

Two situations with unit–cost: ordered abelian semi–groups and some commutative rings

by Mihai Prunescu, Universität Freiburg

The talk presents two situations where unit–cost complexity results are closely related with results from the classical computability.
In the first part we study an important Theorem by Pascal Koiran and Hervé Fournier from an axiomatic point of view. It is proved that the algebraic Knapsack problem belongs to P over some ordered abelian semi–group if and only if $P = NP$ classically. In this case there would exist a unit–cost machine solving the algebraic Knapsack over all abelian semi–groups in some uniform polynomial time.
In the second part we apply the Theorem of Matijasevich in order to construct a ring with $P \neq NBP \neq NP$ and such that its polynomial hierarchy does not collapse at any level.

Real Roots of parametric Systems of polynomial equalities and inequalities

by Fabrice Rouillier, Université Paris VI

We propose a new method for studying simple sets like $\mathcal{S} = \{x \in \mathbb{R}^n\ ,\ p_1(x) = 0, \dots, p_s(x) = 0, f_1(x) > 0, \dots f_s(x) > 0\}$ or $\mathcal{C} = \{x \in \mathbb{C}^n\ ,\ p_1(x) = 0, \dots, p_s(x) = 0, f_1(x) \neq 0, \dots f_s(x) \neq 0\}$ where p_i, f_j are polynomials that belong to
$\mathbb{Q}[U_1, \dots U_d, X_{d+1}, \dots X_n]$. We suppose that $U_1, \dots, U_d$ are parameters and we denote by Π_U the projection from C^n to the parameter's space.

A "good" parameter u is a point of a sub-manifold of $\Pi_U(\mathcal{C})$ such that there exists a compact neighborhood $\mathcal{U}$ of u such that $(\Pi_U^{-1}(\mathcal{U}), \Pi_U)$ is a n analytic covering of $\mathcal{U}$. We show that the set of "bad" parameters is a Zariski c losed subset and we name it the discriminant variety of $\mathcal{C}$ w.r.t. Π_U. We show how to compute it efficiently, using existing computational tools, and how to use it to solve parametric systems of equations and inequations in the real case.

Generalized virtual roots

by Marie–Françoise Roy, Université de Rennes I

We define a generalization of virtual roots introduced recently by Gonzalez-

Vega, Lombardi, Mahé to a situation which can take care simultaneously of polynomials and monomials, and prove that the sign variations in the list of (generalized) derivatives count the number of (generalized) virtual roots. Even for the ordinary notion of virtual roots, this result is new. The result implies a generalization of the classical Budan-Fourier's theorem to this context.
Joint work with Tomas Lajous and Henri Lombardi.

Fast Algorithms for Computing exp, ln, sin, cos at Medium Precision

by Arnold Schönhage, Universität Bonn

Low precision methods for the elementary functions are well established in modern computer hardware, high precision methods are based on the AGM, see Borwein & Borwein, "Pi and the AGM". Here we present a new idea for medium precision of 50-2500 bits, say. Standard domain reductions like $x' = x - n.ln2$ for exp, $x' = x.2^n \in [1, 2)$ for ln, $x' = x - n.\pi/2$ for $cos + i.sin$ plus Taylor approximations are combined with further reductions by diophantine combinations of incommensurable logarithms, like $z = x' - (k.ln3 - m.ln2)$ for exp, or $z = x' - (\pm k.arctan(1/2) - m.\pi/4)$ for cos, sin, with small $|z|$ and subsequent multiplication by 3^k, or by $(2 \pm i)^k.e^{iz}/5^{(k/2)}$, respectively. Variations of this idea are discussed.

Shifted number systems for safe semi–numeric computation

by Arne Storjohann, University of Waterloo

Exact linear algebra computations on integer matrices, like linear system solving, can be speeded by using approximate arithmetic. For example, the leading coefficient of the $p-$adic expansion of the product of two integer may be recovered from the first few leading coefficients of the operands. Unfortunately, the phenomenon of integer carries may lead to errors. The shifted number system gives a method for detecting error-producing carries, together with a method, based on a single random shift choice, for bounding the probability of such egregious carries.

Numerical Decomposition of the Intersection of Algebraic Varieties

by Jan Verschelde, University of Illinois, Chicago

In a recent joint work with Andrew J. Sommese (University of Notre Dame) and Charles W. Wampler (General Motors Research and Development) we have developed numerical homotopy methods to decompose positive dimensional solution sets of polynomial systems into irreducible components. The problem addressed in this talk is the intersection of two irreducible solution components of two possibly identical polynomial systems, a problem which could not be solved by any previous numerical homotopy. To develop new homotopies to solve this problem, we generalize our algorithms for a numerical irreducible decomposition to polynomial systems restricted to an algebraic set. Considering the diagonal system of equations u - v = 0 restricted to the product of the two components we wish to intersect leads to the "diagonal homotopy", providing a numerical representation of the intersection. Computational experiments illustrate the efficiency of this new diagonal homotopy.

Betti numbers of definable sets

by Nicolai Vorobjov, University of Bath

The talk presents the new upper bounds on Betti numbers of definable sets, including semi–algebraic and sub–Pfaffian sets, described by quantifier-free formulae and formulae with quantifiers. The main technical tool is a spectral sequence converging to the homologies of the image of a definable set.

Towards a Higher Level Programming Language for Analysis

by Klaus Weihrauch, FernUniversität Hagen

This is a talk on the foundation of real number computation and complexity. Some models for defining computability in Analysis can be refined naturally to a definition of a programming language with syntax and semantics. Still none of these programming languages seems to be satisfactory. Either they work only on a small subset of the real numbers, they are unrealistic or they are of very low level like Turing machines. In the talk ingredients will be presented for a realistic higher level programming language on the real numbers and higher types, where a type is an equivalence class of multi–representations.

Modular methods for factoring differential operators

by Jacques–Arthur Weil, Université de Limoges

In this lecture, I present a work of Thomas Cluzeau and Mark van Hoeij on factorization of differential operators.

Let $\mathcal{D} := C(x)[\partial]$ (where $\partial = \frac{d}{dx}$, and C is an extension of the field Q of rational numbers) denote the ring of differential operators. This is a non-commutative ring, with multiplication $\partial.x = x\partial + 1$ which corresponds to the composition of differential operators. Factoring is of course useful for solving linear differential equations, and is a building block for finding various types of algebraic properties of solutions. However, the non-commutativity yields some difficulties, such as the

non-unicity of factorization (e.g for any constant c, we have $\partial^2 = (\partial + \frac{1}{c+x})(\partial - \frac{1}{c+x})$).
The authors' aim is to develop a modular algorithm for finding first order factors. Traditionally, such an algorithm would compute factors modulo a prime p, lift those to p-adic factors, and use some bound like Mignotte's bound to reconstruct factors from this. In our case, this is not possible, essentially because there is no Mignotte bound for differential operators, and no good Hensel lifting for p-adic factorization.
The authors' wonderful variant is to compute infomation at singularities (i.e factorization over $C((x))$) and then use modular information to recombine them. Technically speaking, first order factors yield roots of the caracteristic polynomial of the p-curvature; relevant local data can hence be extracted from roots of the caracteristic polynomial of the p-curvature. Using this observation, the authors solve a combinatorial problem (how to "glue" local data at various points) and a field problem (what is the smallest field necessary to perform the computation). I hope to convince the audience that the result is a brilliant algorithm.

Minimal decomposition of model based invariants

by Michael Werman, University of Jerusalem

Methods for computing model based invariants for object recognition tasks are presented. The algorithms are based on elimination theory and the computation of the singular value decomposition. The methods produce minimal length (dimension) description that are useful for indexing into node data bases.

Complexity Questions arising from N-Body Simulations

by Martin Ziegler, Universität Paderborn

The innermost loop of many algorithms simulating the dynamics of a system of N particles under mutual forces consists in calculating the N quantities

$$F_k = \sum_{\ell=1,\ell\neq k} f(x_k - x_\ell), \quad k = 1, \ldots, N \tag{1}$$

from given vectors $x_1, \ldots, X_N$ where f denotes some fixed function. The naive algorithm for (1) takes quadratic time but some functions f allow for softly linear computation within $O(N \cdot \text{polylog} N)$ whereas for others the complexity is still unknown. We present relations among these classes and some new functions f admitting softly linear running time.

Program

Dagstuhl Seminar “Real Computation and Complexity”

Program Monday, February 2, 2004

8:50h– 9:00h	Opening	
9:00h– 9:30h	A. Schönhage, Bonn:	Fast Algorithms for Computing $\exp, \ln, \sin, \cos$ at Medium Precision
9:30h – 10:00h	J.P. Dedieu, Toulouse:	Newton Flow and Interior Point Methods in Linear Programming
10:00h – 10:30h	G. Malajovich, Rio:	On the Curvature of the Central Path of Linear Programming Theory
10:30h – 11:00h	Coffee break	
11:00h – 11:30h	G. Lecerf, Versailles:	On Existence and Approximation of Clusters of Zeros: Case of Embedding Dimension One
11:30h – 12:00h	J.C. Yakoubsohn, Toulouse:	On Existence and Approximation of Clusters of Zeros: Case of univariate analytic functions
12:00h – 14:30h	Lunch break	
14:30h – 15:00h	K. Weihrauch, Hagen:	Towards a higher level programming language for Analysis
15:00h – 15:30h	M. Ziegler, Paderborn:	Complexity Questions arising from Many–Body Simulations
15:30h – 16:00h	E. Novak, Jena:	Solving Integral Equations using Random Bits
16:00h – 16:30h	Coffee break	
16:30h – 17:00h	M. Prunescu, Freiburg:	Two situations with unit-cost: Ordered abelian semi-groups and some commutative rings
17:00h – 17:30h	C. Gassner, Greifswald:	A Structure of Finite Signature with $P = NP$

Dagstuhl Seminar “Real Computation and Complexity”

Program Tuesday, February 3, 2004

9:00h – 9:30h	J. Makowsky, Haifa:	Computing graph polynomials
9:30h – 10:00h	E. Kaltofen, North Carolina:	Approximate Factorization
10:00h – 10:30h	D. Grigoriev, Rennes:	Weak Bézout inequality for $\mathcal{D}$-modules
10:30h – 11:00h	Coffee break	
11:00h – 11:30h	L. Gemignani, Pisa:	Resultant computation for polynomials in Bernstein form
11:30h – 12:00h	T. Krick, Buenos Aires:	A bound for the number of components of a 4-nomial in the positive orthant
12:00h – 14:30h	Lunch break	
14:30h – 15:00h	J. Verschelde, Chicago:	Numerical Decomposition of the Intersection of Algebraic Varieties
15:00h – 15:30h	T. Brihaye, Mons:	o-minimal hybrid systems
15:30h - 16:30h	Coffee break	
16:30h – 17:00h	M. Korovina, Mc Master:	Logical Approach to Computability over Continuous Data Tpyes

Dagstuhl Seminar “Real Computation and Complexity”

Program Wednesday, February 4, 2004

9:00h – 9:30h	M.F. Roy, Rennes:	Generalized virtual roots and Budan-Fourier
9:30h – 10:00h	N. Vorobjov, Bath:	Betti numbers of definable sets
10:00h – 10:30h	Coffee break	
10:30h – 11:00h	A. Storjohann, Waterloo:	Shifted Number Systems for safe seminumeric Computation
11:00h – 11:30h	G. Matera, Buenos Aires:	Numeric vs. symbolic homotopy algorithms in polynomial equation solving: a case study
12:05h :	Group photo:	gather at the stairs outside

EXCURSION:

a) for the hike, we meet outside at 13:45h

b) for Trier: There are problems with getting a bus. The office will inform us Wednesday morning whether it works out.

Dagstuhl Seminar “Real Computation and Complexity”

Program Thursday, February 5, 2004

9:00h – 10:30h		Polar Varieties, real Elimination and Application to Wavelet Design
9:00h – 9:30h	M. Giusti, Palaiseau:	Part I: Generalized polar varieties and their description by equations
9:30h – 10:00h	B. Bank, Berlin:	Part II: The algorithm and philosophy of an application
10:00h – 10:30h	L. Lehmann, Berlin:	Part III: Preparation, implementation and results: KRONECKER-software vs. Gröbner-software
10:30h – 11:00h	Coffee break	
11:00h – 11:30h	J. San Martin, Cantabria:	Non–Universal Procedures to Solve Sytems of Polynomial Equations
11:30h – 12:00h	M. Werman, Jerusalem:	Minimal decomposition of model based invariants
12:00h – 14:30h	Lunch break	
14:30h – 15:00h	M. Bläser, Zürich:	Fast multiple polynomial evaluation and interpolation
15:00h – 15:30h	J.L Montaña, Cantabria:	Evolutionary algorithms for solving NP-hard problems
15:30h – 16:00h	J.A. Weil, Limoges:	Modular methods for factoring differential operators
16:00h –	Coffee break	

Dagstuhl Seminar “Real Computation and Complexity”

Program Friday, February 6, 2004

9:00h – 9:30h	F. Rouillier, Paris:	Real Roots of parametric systems of polynomial equalities and inequalities
9:30h – 10:00h	S. Pericleous, Rennes:	A new method for cell decomposition of restricted subanalytic sets and some complexity results
10:00h – 10:30h	Coffee break	
10:30h – 11:00h	D. Castro, Alcalá:	On the average complexity of algorithms over the rationals
11:00h – 11:30h	P. Koiran, Lyon:	Valiant’s model and the cost of computing integers
11:30h	End of seminar	