Dagstuhl-Seminar (98241)

on

Real Computation and Complexity

IBFI Schloß Dagstuhl
June 15 – 19, 1998

Organizers:

Felipe Cucker (Barcelona)

Thomas Lickteig (Limoges)

Marie-Françoise Roy (Rennes)

Michael Shub (Yorktown Heights)

Summary

The field of algorithmic complexity of real computational problems has received much attention in recent years. This topic with geometrical, algebraic, analytic, and numerical aspects encompasses the foundational area of scientific computing and has a wide range of relevant applications. The main object is the computation with polynomials, the better understanding of what makes these computations difficult or easy in order to design faster Computer algebra algorithms. Due to their omnipresence, the case of real polynomials evidently plays a predominant role. Many new algorithms have been designed during the last decade for deciding the existence of solutions of equations and inequalities, or for computing solutions.

The seminar was intended to be broad and open. While clearly focussed on real computational problems, scientists with rather different backgrounds such as computer science, numerical analysis, algebraic geometry, logic, and abstract real algebraic geometry could be brought together to know and discuss main problems from different perspectives. This is important as scientific questions often don't find their answers within their domain of origin. One aim of the seminar was to support the collaboration of people of different origin.

We had 33 participants coming from Belgium, France, Germany, Great Britain, Italy, Poland, Russia, Spain, and the United States. During the meeting 30 lectures have been given that have been continued by informal evening discussions in smaller groups. The talks focussed on new concrete algorithmic results, others introduced to main ongoing work or to the way of looking at things in important neighboring fields. Main topics addressed include

- quantitative bounds in real algebraic geometry related to lower and upper complexity bounds,
- computation schemes (straight line programs) as basic data structure to cope with multivariate polynomial computation,
- translation of theoretical knowledge into fast implementations,
- univariate and multivariate root finding and root isolation,
- BSS discussion of differential equations, other ground fields, and counting problems,
- exact real computation, and
- approximation methods in the bit model.

Both, senior researchers as well as young researchers contributed to seminar. A JOURNAL OF COMPLEXITY (http://www.apnet.com/www/journal/cm.htm) special issue is dedicated to the workshop with selected papers addressing topics covered by this seminar.

The field has two major challenges. The first one, on the theoretical level, is the mathematical understanding of obstructions to the existence of fast polynomial computations, that is to say, lower bounds via an intrinsic *inherent geometric complexity* of a computational task. By knowing what must be avoided knowledge of lower bounds can furnish a guide-line in the design of algorithms. The second one, the design, is just now going in the direction of putting into effective use the theoretical knowledge of algebraic and arithmetic complexity, that is to say, translation into *really real* real algorithms that are fast in practice with new basic organizational designs.

We thank the IBFI scientific board for making available to us the Schloß Dagstuhl conference center. Likewise we express our sincere appreciation of the outstanding organization of Dagstuhl. On behalf of all participants we thank Dagstuhl for making available support by the TMR program of the European Community funding the participation of young European researchers and keynote speakers. Last but not least, we appreciate the friendly and efficient help we received from the Dagstuhl staff, in particular from Annette Beyer and Angelika Müller. They did a very good job.

Abstracts

On the Combinatorial and Topological Complexity of a Single Cell

by Saugata Basu, Courant Institute, New York University

The problem of bounding the *combinatorial complexity* of a single connected component (a single cell) of the complement of a set of n geometric objects in R^k of constant description complexity is an important problem in computational geometry which has attracted much attention over the past decade. It has been conjectured that the conjectured that the combinatorial complexity of a single cell is bounded by a function much closer to $O(n^{k-1})$ rather than $O(n^k)$ which is the bound for the combinatorial complexity of the whole arrangement. Currently, this is known to be true only for $k \leq 3$ and only for some special cases in higher dimensions.

A classic result in real algebraic geometry due to Oleinik and Petrovsky, Thom and Milnor, bounds the *topological complexity* (the sum of the Betti numbers) of basic semi-algebraic sets. However, till now no better bounds were known if we restricted attention to a single connected component of a basic semi-algebraic set.

In this paper, we show how these two problems are related. We prove a new bound of the sum of the Betti numbers of one connected component of a basic semi-algebraic set which is an improvement over the Oleinik-Petrovsky-Thom-Milnor bound. This also implies that the topological complexity of a single cell, measured by the sum of the Betti numbers, is bounded by $O(n^{k-1})$. Finally, we show that under a certain natural geometric assumption on the objects (namely that, whenever they intersect the intersection is robustly transversal on average) it is possible to prove a bound of $O(n^{k-1})$ on the combinatorial complexity of a single cell. We also show that this geometric assumption is satisfied by most arrangements and deduce that the *expected* complexity of a single cell in a *randomly* chosen arrangement is $O(n^{k-1})$.

Two results on polynomial root-finding

by Dario A. Bini, Università di Pisa

Two results on the approximation of polynomial roots are presented.

The first result concerns the reduction of splitting a polynomial of degree n to solving a banded Toeplitz system with band with n. An algorithm is proposed for the latter computation having arithmetic cost $O(n \cdot \log^2 n \cdot \log\log \epsilon^{-1})$, ϵ being the approximation error. The algorithm is based on tools from numerical linear algebra and Toeplitz matrix technology. Correlations with Graeffe's method are pointed out.

The second result concerns the design and analysis of an adaptive algorithm for polynomial root-finding. Informally, adaptive means that the algorithm must adjust the computation to the specific features of the polynomial and of the roots that must be computed, say, sparsity of coefficient and conditioning. Tools for the design of adaptive algorithms are introduced, in particular: the concept of root-neighbourhood and the related results; inclusion theorems; a posteriori error bounds; point-wise backward error analysis; cluster analysis; choice of starting approximations. These tools are used to design an adaptive algorithm based on simultaneous iteration of Börsch-Soupan. From the numerical experiments performed on a wide set of test polynomials it results that the adaptive algorithm is much faster than the available software. In particular, comparisons with the packages Mathematica, Pari, Maple, show a speed-up factor of 2-3 orders of magnitude. Besides approximating all the roots with a given relative error bound, our software allows isolation and counting the roots in a given subset of $\mathcal{C}$.

A fast version of the Schur-Cohn algorithm

by Cyril Brunie, Université de Limoges

We describe a fast algorithm for counting the number of roots of complex polynomials in the open unit disk, classically called the Schur-Cohn problem. For degree d polynomials our bound is of order $d \log^2 d$ in terms of field operations and comparisons, but our approach nicely allows to integrate the bit size as a further complexity parameter as well. For bit size σ integer input polynomials of our running time is of order $d^2\sigma \cdot \log(d\sigma) \cdot \log\log(d\sigma) \cdot \log(d)$ in the multitape Turing machine model, thus improving all previously proposed approaches. (Joint work with Philippe Saux Picart.)

Analytic Machines

by Thomas Chadzelek, Universität des Saarlandes

Analytic machines are basically Blum-Shub-Smale machines executing *infinite convergent* computations. We consider initial value problems for systems of explicit first-order ODEs where the right-hand side is $\mathcal{R}$-computable without division. After making precise the notion of solution in this context, we give sufficient conditions for the uniqueness of solutions and then show them to be $\mathcal{R}$-analytically computable. Finally we reduce a certain stability problem for dynamic systems to the analytic equivalent of the halting problem. This shows that it is undecidable even for exact real arithmetic and infinite computing time whether the solution of a dynamic system described by ODEs as above converges to a fixed point or not. (Joint work with Günter Hotz.)

Polar Varieties, Real Equation Solving and Data Structures

by Marc Giusti, École Polytechnique

We presented an application of a new method for multivariate polynomial equation complex solving to the real case. This algorithm on which we rely yields a procedure for symbolically solving zero-dimensional polynomial systems over the complex numbers. One feature of central importance is the use of a problem-adapted data type represented by the data structures arithmetic network and straight-line programs (arithmetic circuit).

Our main result concerns the problem of finding at least one representative point (given in a suitable encoding) for each connected component of a real compact hypersurface. The input equation is supposed to be given by a straight-line program.

We give an algorithm solving this problem with sequential time complexity which is polynomial in the length of the input straight-line program, the total degree of the input equation, the dimension of the ambient space and a suitably defined real (or complex) degree of the generic polar varieties.

Finally, we showed how to extend this result to compact real complete intersections, beginning with the smoothness of generic polar varieties. (Joint work with B. Bank, J. Heintz and G.H. Mbakop.)

Randomized Complexity Lower Bounds

by Dima Grigoriev, Pennsylvania State University

Obtaining complexity lower bounds for computation trees is one of the most challenging problems in the complexity theory. There are quite known "topological" methods due to Ben-Or, Björner, Lovasz, Yao based on the estimating the Betti numbers. They allow to prove the lower bounds for *deterministic* computation trees, in particular, the bound $n \log n$ for the DISTINCTNESS and SET EQUALITY problems, and the bound n^2 for the KNAPSACK and BOUNDED INTEGER PROGRAMMING problems. The "topological" methods fail for recognising sets with the trivial topological structure, like polyhedra. For obtaining lower bounds for polyhedra we developed differential-geometric methods.

On the other hand all the mentioned methods fail for the *randomized* computation trees. Recently the methods were devised which involve some ideas from algebra, combinatorics, real algebraic geometry, that allowed to prove the lower bounds for *randomized* computation trees, in particular the bound n^2 for the KNAPSACK and BOUNDED INTEGER PROGRAMMING problems and the bound $n \log n$ for the DISTINCTNESS problem. For the SET EQUALITY problem and more generally for the BOUNDED SETS DIFFERENCE problem a *randomized* complexity linear upper bound is known.

Exact Real Arithmetic via Möbius Tranformations

by Reinhold Heckmann, Universität des Saarlandes

This talk presents the Edalat-Potts approach to exact real arithmetic and, in particular, some preliminary complexity results. In this approach the representation of real numbers as well as the calculations with real numbers are done by means of Möbius transformations internally represented by integer matrices. In particular, a real number is represented by a potentially infinite stream of digit matrices, and calculations are reduced to matrix operations. In order to obtain bounds for the complexity of calculations in this approach, two questions must be answered: How many argument digits are needed to compute n result digits, and what is the cost of finding these n digits? The main tool for answering the first question is the contractivity of Möbius transforms. Contractivities can not only be used to verify the convergence of infinite expressions but also to obtain information about the speed of convergence which leads to the desired answers. The second question is simple at first glance since it is easy to see how many integer operations are needed to do the matrix operations that are used in the calculations. However, the integers occurring in the matrices may grow unboundedly during the course of a calculation, so that their bit sizes have to be taken into account. In the last part of the talk, lower and upper bounds for these sizes are presented, and complexity results are derived from these bounds.

Algebraic vs. Approximate Computability over the Reals

by Armin Hemmerling, Ernst-Moritz-Arndt–Universität Greifswald

We consider algebraic and approximate computations of (partial) real functions $f : \mathbb{R}^d \rightarrowtail \mathbb{R}$. Algebraic computability is defined by means of (parameter-free) finite algorithmic procedures. The notion of approximate computability is a straightforward generalisation of the Ko-Friedman approach, based on oracle Turing machines, to functions with not necessarily recursively open domains. The main results of the talk give characterisations of approximate computability by means of the passing sets of finite algorithmic procedures, i.e., characterisations from the algebraic point of view. Some consequences and also modifications of the concepts are discussed. Finally, two variants of arithmetical hierarchies over the reals are defined and used to classify and mutually compare the domains, graphs and ranges of algebraically resp. approximately computable real functions.

Contour Integrals of Rational Functions

by Peter Kirrinnis, Universität Bonn

We present fast algorithms for computing numerical approximations for contour integrals of rational functions. Given the coefficients of two polynomials q

and $p \in \mathbf{C}[\mathbf{z}]$, a curve Γ in the complex plane, and an error bound ϵ, the integral $\int_\Gamma q(z)/p(z)dz$ is computed up to an error of $\epsilon = 2^{-s}$. In the special case that the zeros of p lie in a small disc not intersected by Γ, the integral is computed by summing up the integrals of an initial segment of a suitable Laurent series of q/p. The general case is reduced to the special one by numerical partial fraction decomposition, using an extension of Schönhage‘s splitting circle method. If $\deg q \leq \deg p = n$ and the distance between the zeros of p and the curve Γ is at least $2^{-\gamma}$, then a suitable partial fraction decomposition can be computed with $O(\psi(n^3 \cdot \log n + n^3 \cdot \gamma + s \cdot n \cdot \log n))$ bit operations, where $\psi(N)$ is a time bound for N bit integer multiplication. The required approximation for the integral can be computed with $O(\psi(n^2 \cdot s) + n \cdot \psi(s) \cdot \log s)$ bit operations, if $s \geq n \cdot (\gamma + \log n)$, which is a reasonable assumption. While the condition parameter γ affects the time bound, it need not be known in advance.

Monoreflections in real algebraic geometry

by Manfred Knebusch, Universität Regensburg

Let POR/N denote the category of partially ordered commutative rings (A, P) with 1 such that A is reduced, i.e. does not have nilpotent elements. We are interested in monoreflections $v : POR/N \rightarrow D$ to subcategories D of POR/N, which we always assume to be full and closed under isomorphisms of POR/N. (A reflection v is mono, if every reflection morphism $v_{(A,P)} : (A, P) \rightarrow v(A?P)$ is a monomorphism, i.e. injective in our case.)

In the talk I indicated the construction of two monomorphisms $\rho : POR/N \rightarrow RCR$ and $\sigma : POR/N \rightarrow SAFR$. Here $\sigma(A, P)$ is the ring of "semialgebraic functions" (in an abstract sense) on the real spectrum $X = Spec(A, P)$ of (A, P). A "function" means here an element of $\Pi\rho(\alpha)$ with $\rho(\alpha)$ the real closed field attached to the point $\alpha \in X$, and "semialgebraic" means that the function f is computable from the elements of A in a precise sense. Thus $SAFR$ is the category of semialgebraic function rings. The central theorem is that $SAFR$ is the unique smallest monoreflective subcategory of POR/N. Thus the objects of any monoreflective subcategory of POR/N are suitable rings of semialgebraic functions. RCR is the category of real closed rings, as introduced by N. Schwartz in the 80's. ρ can be characterised as the strongest monoreflector on POR/N, such that every reflection morphism $\rho_{(A,P)}$ induces a homeomorphism on the real spectra. (Joint work with N. Schwartz and J. Madden.)

Are lower bounds easier over the reals?

by Pascal Koiran, LIP, Ecole Normale Supérieure de Lyon

We show that proving lower bounds in algebraic models of computation may not be easier than in the standard Turing machine model. For instance, a superpolynomial lower bound on the size of an algebraic circuit solving the real knapsack problem would imply a separation of P from PSPACE. A more general result relates parallel complexity classes in Boolean and real models of computation. We also propose a few problems in algebraic complexity and topological complexity. (Joint work with Hervé Fournier.)

Symbolic-numeric Sinus polynomial Equations Real Solving

by Aude Maignan, Université de Limoges

This paper deals with the localization of all the real roots of sinus-polynomials.

D. Richardson has already studied this type of analytic function. He showed how to find the number of real roots in a bounded interval.

Here we propose an algorithm which determines whether a sinus-polynomial has a finite number of real roots or not. Moreover in the finite case we construct an explicit interval containing all of them. We also construct a generalized exclusion method to find all the real roots in a bounded interval and we adapt it to the infinite case.

The Equivalence Problem for Commutative Semigroups

by Ernst W. Mayr, Technische Universität München

We present a decision procedure for the equivalence problem for commutative semigroups. It requires at most space $2^{c \cdot n}$, where n is the size of the problem instance, and c is some problem independent constant. Furthermore, we show that the exponential space hardness of the above problem follows from the work of Mayr and Meyer on the complexity of the word problem for commutative semigroups. Thus, the presented algorithms are space optimal. Our results close the gap between the $2^{c' \cdot n \cdot \log n}$ space upper bound, shown by Huynh, and the exponential space lower bound resulting from the corresponding bound for the uniform word problem established by Mayr and Meyer. (Joint work with Ulla Koppenhagen.)

Descriptive Complexity and Counting over the reals

by Klaus Meer, RWTH Aachen

The purpose of this talk is to introduce and analyze counting problems over the real numbers from a logical point of view. Consider a non-deterministic polynomial time verification algorithm M (according to the computational model of Blum, Shub, and Smale). The counting function f_M related to M is given as

$$f_M(x) := \#\{z \in R^{q(n)} | M \text{ on input } (x, z) \text{ accepts}\}$$

(here n denotes the real size of x and q is a polynomial bound on the running time of M). The union of all such functions constitutes the class $\#P_R$ of counting functions over the reals. We study $\#P_R$ from a logical point of view using descriptive complexity theory for real number models as introduced by Grädel and Meer. It is shown that $\#P_R$ splits into five different levels. Each of the latter is determined by the specific structure of quantifiers in FO-formulas over R-structures. The relation between such FO-formulas and $\#P_R$ is given by counting the number of models for the given formula.

Dimension Theory and Isomorphism Theorem for BSS-Recursively Enumerable Sets over Real Closed Fields

by C. Michaux, Université de Mons-Hainaut

The main result of this paper lies in the framework of BSS computability over a real closed field R : it shows roughly that any infinite r.e. set S in R^N, $N \leq \infty$ is isomorphic to $R^{\dim S}$ by a bijection ϕ which is decidable over S. (This is done under the technical assumption that the relation "to be infinitesimal" is BSS-computable over R. We give a complete characterization of real closed fields where this condition holds.) Moreover the map which associates ϕ to S is computable. The underlying notion of dimension (denoted here by $dimS$) is linked with the semi-algebraic dimension in the case where the transcendence degree of R over the rationals is infinite. In the case of finite transcendence degree, every infinite r.e. set is isomorphic to R. The techniques of proofs relate to the "cell decomposition theorem for semi-algebraic sets" and to some glueing process going back to the proof of Borel isomorphism theorem for Polish spaces. (Joint work with C. Troestler.)

A Combinatorial Method to show Computational Hardness of Polynomial Evaluation and Transcendence of Power Series

by José Luis Montaña, Universidad Pública de Navarra

We exhibit a new method for showing lower bounds for the time complexity of polynomial evaluation procedures. Time, denoted by L, is measured in terms of nonscalar arithmetic operations. In contrast with known methods for proving lower complexity bounds, our method is purely combinatorial and does not require powerful tools from algebraic or diophantine geometry.

By means of our method we are able to verify the computational hardness of new natural families of univariate polynomials for which this was impossible up to now. By computational hardness we mean that the complexity function L^2 grows linearly in the degree of the polynomials of the family we are considering.

Our method can also be applied to classical questions of transcendence proofs in number theory and geometry. A list of (old and new) formal power series is given whose transcendence can be shown easily by our method.

Intrinsic height and complexity estimates for the Arithmetic Nullstellensatz

by José Enrique Morais, Universidad Pública de Navarra

In this talk, we present several arithmetic estimates for Hilbert's Nullstellensatz. This includes an algorithm procedure computing a straight-line program representation of the polynomials and constants occurring in a Bézout identity, whose complexity is polynomial in the geometric degree of the system. Moreover, we show for the first time height estimates of intrinsic type for the polynomials and constants appearing, again polynomial in the geometric degree and linear in the height of the system. These results are based on a suitable representation of polynomials (straight-line programs) and duality techniques using the Trace Formula for Gorenstein algebras.
As application of these arithmetic and complexity estimates we show precise bounds for the function $\pi_S(x)$ counting the number of primes yielding an inconsistent modular equation system. We also give a computationally interesting lower bound for the density of small prime numbers of controlled bit length for the reduction to positive characteristic of inconsistent systems.
Finally, we show how the use of the parallel complexity measure of a straight–line program improves on the height bounds for a witness theorem and how the rather technical concept of the height of the systems can be used in order to obtain bounds for the height of an approximate zero of a polynomial equation system. (Joint work with K. Hägele, L.M. Pardo, and M. Sombra.)

Asymptotic Acceleration of Solving Multivariate Polynomial Systems of Equations

by Victor Y. Pan, City University of New York

We propose new Las Vegas randomized algorithms for the solution of a multivariate generic or sparse polynomial system of equations. The algorithms use $O^*((\delta + 4^n)D^2 \log b)$ arithmetic operations to approximate all real roots of the system as well as all roots lying in a fixed n-dimensional box or disc. Here D is an upper bound on the number of all the roots of the system, δ is the number of real roots or the roots lying in the box or disc, $\epsilon = 2^{-b}$ is the required upper bound on the output errors, and $O^*(s)$ stands for $O(s \log^c s)$, c being a constant independent of s. We also yield the bounds $O^*(12^n D^2)$ for the complexity of counting the numbers of all roots in a fixed box (disc) and all real roots and $O^*(12^n D^2 \log b)$ for the complete solution of generic system. For a large class of inputs and typically in practical computations, the factor δ is much smaller than D, $\delta = o(D)$. This improves by order of magnitude the known complexity estimates of order at least $D^3 \log b$ or D^3, which so far are the record ones even for approximating a single root of a system and for each of the cited counting problems, respectively. Our progress relies on proposing several novel techniques. In particular, we exploit the structure of matrices associated to a given polynomial system and relate it to the associated linear operators, dual space of linear forms, and algebraic residues; furthermore, our techniques support the new nontrivial extension of the matrix sign and quadratic inverse power iterations to the case of multivariate polynomial systems, where we emulate the recursive splitting of a univariate polynomial into factors of smaller degree. (Joint work with Bernard Mourrain.)

Complexification and degree of a semi-algebraic set

by Marie-Françoise Roy, IRMAR (CNRS, Université de Rennes I) and FRISCO (ESPRIT LTR)

This is joint work with N. Vorobjov. Using the notion of "irreducible real algebraic set coinciding locally with an algebraic set" and convenient complete intersection approximating varieties, we prove that the "total real degree of a real algebraic set" defined by a polynomial of degree d in k variables is $O(d)^k$, and the degree of a semi-algebraic set defined by s polynomials of degree d in k variables (i.e. the degree of its complexification, the smallest complex algebraic set containing it) is $s^{2k}O(d)^k$. In the basic case the real degree is $O(d)^k$.

Finding at least one point in each connected component of a real algebraic set defined by a single equation

by Mohab Safey, Université de Paris VI

Finding at least one point on each semi-algebraically connected component of a real algebraic set defined by a single equation in $R[X_1, \ldots, X_k]$ (where R is a real closed field) is a fundamental algorithmic problem of Real Algebraic Geometry. We propose a practically efficient algorithm reducing this problem to deciding the existence of a real critical points of the distance function. (Joint work with F. Rouiller and M.F. Roy.)

Evaluation Complexity of Functions Under Analytic Continuation

by Arnold Schönhage, Universität Bonn

Consider machines (like TM's, or RAM's) with some fair cost measure of bit complexity evaluating (up to precision 2^{-n}) holomorphic functions $f_D(z) = \sum_{k\geq 0} a_k(z-a)^k$ defined on some disk D, where $z \in D$ is given by some *oracle* providing binary approximations x, y such that, for any given k, $|(x+iy)-z| <$

2^{-k}. Such f_D is computable in time $\leq t(n)$ if there is a machine M with input of any such $z \in D$, and $n \in \mathbf{N}$, stopping after $\leq t(n)$ steps with output w such that $|w - f(z)| < 2^{-n}$.

Theorem *If f_D admits analytic continuation (along curve C) to some other germ $f_E : E \to \mathbf{C}$ on disk E, then there exists $c > 0$ such that*
f_D computable in time $\leq t(n) \implies f_E$ computable in time $\leq O(n) \cdot t(cn)$.

For polynomial bounds $t(n) = \gamma \cdot n^\alpha$, this implies that f_E is computable in time $\leq O(n^{\alpha+1})$.

Conjecture *In this polynomially bounded case, the sharper conclusion*
f_E computable in time $\leq O(t(n))$ *is true.*

Degree bounds for Hilbert‘s 17th problem

by Joachim Schmid, Universität Dortmund

Hilbert's 17th problem asks whether a positive semidefinite polynomial $f \in R[X_1, \ldots, X_n]$ (i.e., $f(x) \geq 0$ for all $x \in R^n$) is a sum of squares in the field $R(X_1, \ldots, X_n)$ of rational functions.

An affirmative answer to this question was given by Artin. However, his proof does not yield any information how to obtain a representation

$$f = \sum_{i=1}^{r} \left(\frac{g_i}{h_i} \right)^2$$

for certain $g_1, \ldots, g_r, h_1, \ldots, h_r \in R[X_1, \ldots, X_n]$, neither it gives bounds for r and the degrees of $g_1, \ldots, g_r$, $h_1, \ldots, h_r$. In this talk a method was presented how to obtain an explicit bound for these degrees. The main tools were the theory of quadratic forms and valuation theory. Actually a sketch of a proof for the following result was given:

Theorem: Let $f \in R[X_1, \ldots, X_n]$ be positive semidefinite, $\deg f = d$. Then there are $r \in N$ and $g, g_1, \ldots, g_r \in R[X_1, \ldots, X_n]$, $g \neq 0$ such that

$$g^2 f = \sum_{i=1}^{r} g_i^2$$

and

$$\deg g_i \leq 2^{\cdot^{\cdot^{2^{6nd^4}}}}$$

where the number of 2's in the tower is n.

In the case $n \leq 4$ this improves a result by Lombardi and Roy.

More on Newton's Method

by Mike Shub, IBM T.J. Watson Research Center

In joint work with Jean-Pierre Dedieu, we consider Newton's method for overdetermined systems of equations. We prove versions of Smale's alpha and gamma theorems. There is quadratic convergence to a non-degenerate zero and geometric convergence to a critical point of a least squares problem in case there is no zero, for appropriate values of alpha and gamma. An application was made to estimate the complexity of a path following algorithm for locating zeros of overdetermined systems.

Betti Numbers of Sub-Pfaffian Sets

by Nicolai Vorobjov, University of Bath

We prove that there exists a cylindrical cell decomposition of a compact variety $V = \{f = 0\}$, where f is a Pfaffian function in n variables, such that the number of cells is bounded from above by a doubly exponential function in n. This implies a similar upper bound for the sum of Betti numbers of a projection of V. Previously known bounds were non-elementary.

Real Elimination applied in Solid Modeling

by Volker Weispfenning, Universität Passau

We describe a new approach to solid modelling, where solids are respresented as regular closed semialgebraic sets, Common operations on solids then lead to first-order definable sets. The task to compute a semialgebraic description of these sets is then a special case of the real quantifier elimination problem.

We study the operations of rounding and blending and the computation of boundary representations for solids from this viewpoint. Using the REDLOG-package of REDUCE (www.fmi.uni-passau.de/ redlog/) we show that this approach is successful in practice for non-trivial problems. (Joint work with Thomas Sturm.)

On uniform and non uniform algorithms

by Henryk Wozniakowski, Columbia University

We present examples of problems for which:

1. the class of uniform algorithms is empty whereas the nonuniform complexity is small or trivial,
2. the cost of any uniform algorithm is much more expensive than the nonuniform complexity,

3. there exist uniform algorithms whose cost is comparable to the nonuniform complexity.

We also mention some recent results concerning the complexity of linear problems when the basis of output is fixed. (Joint work with E. Novak.)

Contraction, Robustness and Numerical Path-Following Using Secant Maps

by Jean-Claude Yakoubsohn, Université Paul Sabatier

Secant type methods are useful for finding zeros of analytic equations that includes polynomial system. This paper prove new results concerning contraction and robustness theorem for secant maps. It is also showed that numerical path-following using secant maps has the same order of complexity that numerical path-following using Newton's map to approximate a zero. A such algorithm was implemented and some numerical experiments are displayed.