Dagstuhl-Seminar (9545)

on

Real Computation and Complexity

IBFI Schloß Dagstuhl
November 6 − 10, 1995

Organizers:

Felipe Cucker (Barcelona)

Thomas Lickteig (Bonn)

Michael Shub (Yorktown Heights)

Preamble

The field of algorithmic complexity of real computational problems has seen strong developments 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.

This new specific conference intends to join the various directions, to strengthen their unity, and to promote exchange of new ideas. It will take place on a regular and periodic basis, most likely every second year.

Beside participants from the former East and West of Germany participants came from Argentina, Belgium, Brazil, France, Italy, The Netherlands, Poland, Spain, Switzerland, and the United States. Scientists from both, Mathematics and Computer Science, contributed to the success of the seminar. We thank them all for their contribution.

Felipe Cucker, Thomas Lickteig, Mike Shub

Acknowledgments

Abstracts

On the Complexity of Real Equation Solving
by BERND BANK, Humboldt–Universität zu Berlin

The first part of the speech deals with the particular case of integer points in a semi-algebraic set described by quasi-convex polynomial inequalities in the n–dimensional real space. The simply exponential bounds are "optimal" with respect to the dense codification of the polynomials.

Without changing the data structure there is no hope to improve the complexity. In a second part it is discussed, what can be expected if the method recently developed by **GIUSTI/ HEINTZ/ MORAIS/ MORGENSTERN/ PARDO** is transferred to the real case. This method finds the isolated points in a zero–dimensional affine variety. Its main features are the use of straight line programs as data structure and the polynomial sequential time measured in both, the length of the input description and an appropriate affine "geometric" degree of the equation system.

The main result with respect to the real case is the following: the transferred method finds a representative point with algebraic coordinates of each connected component of a given smooth and compact real hypersurface. A suitably defined "real degree" of some polar variety corresponding to the input equation describing the hypersurface in question replaces the affine geometric degree of the equation system.

On Bounding the Betti Numbers of Semi-Algebraic Sets
by SAUGATA BASU, Courant Institute, New York University

In this talk we give a new bound on the sum of the Betti numbers of semi-algebraic sets. This extends a well-known bound due to Oleinik and Petrovsky, Thom and Milnor. In separate papers they proved that the sum of the Betti numbers of a semi-algebraic set $S \subset R^k$, defined by $P_1 \geq 0, \ldots, P_s \geq 0, deg(P_i) \leq d, 1 \leq i \leq s$, is bounded by $(O(sd))^k$. Given a semi-algebraic set $S \subset R^k$ defined

as the intersection of a real variety, $Q = 0, deg(Q) \leq d$, whose real dimension is k', with a set defined by a quantifier-free Boolean formula with atoms of the form, $P_i = 0, P_i > 0, P_i < 0, deg(P_i) \leq d, 1 \leq i \leq s$, we prove that the sum of the Betti numbers of S is bounded by $s^{k'}(O(d))^k$. In the special case, when S is defined by $Q = 0, P_1 > 0, \ldots, P_s > 0$, we get a slightly tighter bound of $\binom{s}{k'}(O(d))^k$. This result generalises the Oleinik-Petrovsky-Thom-Milnor bound in two directions. Firstly, our bound applies to arbitrary semi-algebraic sets, not just for basic semi-algebraic sets. Secondly, the combinatorial part (the part depending on s) in our bound, depends on the dimension of the variety rather than that of the ambient space. It also generalizes a result of Basu-Pollack-Roy where a similar bound is proven for the number of connected components.

On Lower Bounds for the Complexity of Polynomials with Algebraic Coefficients
by WALTER BAUR, Universität Konstanz

We present a very simple method to prove lower bounds for the non-scalar complexity of polynomials having algebraic coefficients. Examples: Let p_i be the i-th prime number. Then $\sum_{i=1}^{n} \sqrt{p_i} T^i$ and $\prod_{i=1}^{n}(T - \sqrt{p_i})$ both have complexity $\geq$ const. $\sqrt{n/\log n}$ (Heintz-Sieveking, Heintz-Morgenstern resp.).

Deciding and Describing Positivity of Real Polynomials
by EBERHARD BECKER, Universität Dortmund

Let $f, g_1, \ldots, g_r \in \mathcal{R}[X_1, \ldots, X_n]$. The following two problems are discussed:

1) decide whether $f \geq 0$ (resp. $f > 0$) on $\mathcal{R}^n$,

2) if $f \geq 0$ (resp. $f > 0$) on $\bar{S} = S(g_1, \ldots, g_r) = \{x \in \mathcal{R}^n | \text{ all } g_i \geq 0\}$, describe f in terms of $g_1, \ldots, g_r$.

Ad 1) The basic idea is to associate to f a zero-dimensional system S_g such that f takes on a negative value iff S_g has a real root. Two examples of such a system are presented. In each case the system describes the set of critical points of a suitable function.

Ad 2) Let T be the quadratic semiring in $\mathcal{R}[X_1, \ldots, X_n]$ generated by $g_1, \ldots, g_r$. According to Stengle ($\approx$ 1976) f can be written as a rational function t_1/t_2 where $t_i \in T$. We discuss results of Polya, Habicht and Schmüdgen (1991, Math. Annalen) about possible denominators t_2. It is outlined that the Kadison-Dubois representation theorem (e.g. Becker-Schwartz, Arch. Math. 1983) provides a uniform way to prove all these results and some others. In addition, from the information about the possible t_2 one can deduce a test to check positivity.

Hybrid and Dynamical Systems Complexity
by OLIVIER BOURNEZ, LIP, École Normale Supérieure de Lyon

We explore the simulation and computational complexity of dynamical systems. We introduce a new discrete model of computation: the analog automaton model. We characterize its computational power as precisely $P/poly$ in polynomial time, and every discrete language in exponential time. So we show that this model is strictly more powerful than Turing machines.

In a first part, we characterize the computational power of discrete dynamical systems with an injective piecewise linear transition function $f : \mathcal{R}^d \to \mathcal{R}^d$ as precisely the computational power of analog automata in polynomial time and in exponential time for $d > 1$.

In a second part, we define some notions of simulation of a discrete dynamical system by a continuous dynamical system. We prove that with some reasonable hypotheses, it is not possible to simulate Turing machines or analog two stack automata with continuous dynamical system over R^d, for $d \leq 2$. We show that, it is actually possible to simulate analog automata with continuous dynamical systems in dimension 3, using mirror systems, piecewise constant derivative systems, Lipschitz differential equations over a bounded space or linear hybrid systems. Thus, we get that these systems do have super-Turing capabilities. We characterize the computational power of linear hybrid systems and piecewise constant derivative systems as precisely the computational power of analog automata in polynomial and in exponential time. (Joint work with M. Cosnard.)

Two Iterative Methods for Numerical Polynomial Solving
by JEAN-PAUL CARDINAL, Universidad de Cantabria

We present in this talk two iterative methods for numerical solving of univariate complex polynomials. Both are based on basic rational operations in the quotient algebra of the polynomial. The cost of one iteration in these two methods is quasi-linear in the degree thanks to Fast Fourier Transform and Toeplitz like techniques. The number of iterations needed for the method to converge is intimately related to the geometry of the roots and turns out to be quite small and regular in practice. The first method finds roots one by one while the second one recursively splits the polynomial into factors of smaller degrees. Tests and examples are shown to illustrate these methods.

Nonlinear Complexity Lower Bounds for Randomized Algebraic Decision Trees
by DIMA GRIGORIEV, Pennsylvania State University

Lower Bounds on the depth of randomized algebraic trees are obtained for the

languages being either the unions of hypersurfaces or polyhedra. As applications we get $\Omega(n^2)$ lower complexity bound for knapsack problem and $\Omega(n \log n)$ for element distinctness problem. (Joint work with M. Karpinski, F. Meyer auf der Heide, and R. Smolenski.)

Estimating Stratfications in Parametric Optimization
by HARALD GÜNZEL, RWTH Aachen

Using the example of multi-objective optimization the possible use of stratifications in optimization theory (and practise) is illustrated. Then, the existence of a stratification of the so-called Karush-Kuhn-Tucker set is shown. Finally, with the help of a combinatorial code, the finiteness of the latter stratification is estimated. The fact that this estimation does not solve the stratification problem entirely has to do with Mnëv's universality theorem.

The Elimination Theory of Dr. Jekyll and Mr. Heintz
by JOOS HEINTZ, Universidad de Buenos Aires & Universidad de Cantabria

Behind the cultivated personality of Dr. Jekyll (Oxford University) the dirty face of Mr. Heintz is showing up. This announces bad news: terrific polynomials are threatening the patient and continuous work of POSSO programmers all over Europe, mothers hide their children, children are crying ....

The community is waiting for the hero arriving from the galaxy of the sparse cosmos who will put again things in order, reestablishing the law of software (as AXIOM, MAPLE, MATHEMATICA), hunting down Mr. Heintz and sending him back to place he is coming from: the **Sing-Sing**ular locus.

Analytic Machines
by GÜNTER HOTZ, Universität des Saarlandes, Saarbrücken

The extension of the R-machines of BSS for $R = \mathcal{Q}$ by a special register δ enables these machines to read real input tapes with a precision δ as rational numbers. $\mathcal{Q}$-analytic computations restart the $\mathcal{Q}$-machines with a higher precision when they reach the halting state. Infinite computations of this type are accepted iff the output tape produces a convergent sequence. Functions which can be computed by this device are called $\mathcal{Q}$-analytic. Extensions of the $\mathcal{R}$-machines M by operations $e_1, \ldots, e_n$ are called $M(e_1, \ldots, e_n)$ machines. The following results are proved in Hotz, Schieffer, and Vierke, *Analytic Machines*, El. Coll. Comp. Compl., ECCC TR95-025 (WWW: http://www.eccc.uni-trier.de./eccc).

Each program p for an $\mathcal{R}$-machine can be transformed into a program $\bar{p}$ for a $\mathcal{Q}$-analytic machine such that both machines compute the same function.

If $e_1, \ldots, e_n$ are strong $\mathcal{Q}$-analytic (computable in the sense of Grzegorczyk), then each $M(e_1, \ldots, e_n)$ computable function is $\mathcal{Q}$-analytic. There are examples of functions which are $\mathcal{Q}$-analytic but not $M(e_1, \ldots, e_n)$ computable for e_i strong $\mathcal{Q}$-analytic and bijective. This has been proved by applying that the Hausdorff dimension of sets can not be enlarged by such computations.

The *halting problem* of $\mathcal{Q}$-analytic machines is the convergence problem of these infinite computations. By standard methods it can be shown that the halting problem of $\mathcal{Q}$-analytic machines can not be decided by $\mathcal{Q}$-analytic functions. This throws new light on the stability problem of dynamic systems.

VC-Dimension of Pfaffian Networks and the Applications
by MAREK KARPINSKI, Universität Bonn

We introduce a new method for proving explicit upper bounds on the VC-dimension of the Pfaffian networks, and more generally, Boolean combinations of general Pfaffian formulas (the case where the o-minimality is not yet even established!). In 1993 the finiteness of VC-dimension for sigmoidal networks has been established for the first time using a deep result in model theory. The explicit bounds on the VC-dimension remained an open problem. In this work we answer to this open problem. We given a quadratic bound in the number of parameters of Pfaffian networks, and formulas, solving also the problem of their sampling complexity. We present also a number of applications of our method. (Joint work with A. MacIntyre, Oxford.)

Partial Fraction Decomposition in $\mathcal{C}(z)$ and Simultaneous Newton Iteration for Factorization in $\mathcal{C}[z]$
by PETER KIRRINNIS, Universität Bonn

This talk presents fast numerical algorithms for factoring univariate complex polynomials and for computing partial fraction decompositions (PFDs) of rational functions in $\mathcal{C}(z)$. Numerically stable and computationally feasible versions of PFD are specified both for rational functions with all singularities in the unit disk and for rational functions with arbitrarily distributed singularities.

Two major algorithms for computing PFDs are presented. The first one is a Newton type algorithm for simultaneously improving the accuracy of all factors in an approximate factorization of a polynomial resp. all partial fractions of an approximate PFD of a rational function. This method includes fast numerical algorithms for the following subproblems: the multiplication of a sequence of polynomials, the addition of a sequence of rational functions, and the computation of modular representations. Algorithmically useful starting value conditions for the Newton algorithm are provided.

The other algorithm is an extension of Schönhage's *splitting circle method*

for factoring polynomials in $\mathcal{C}[z]$ to an algorithm for numerical PFD. Using this method for computing starting values for the above Newton iteration yields favourable time bounds (measured in bit operations) for PFD, polynomial factoring, and root calculation. In particular, the time bounds for computing high accuracy PFDs and high accuracy factorizations are linear in the output size (and hence optimal) up to logarithmic factors.

Approximating the Volume of Definable Sets
by Pascal Koiran, LIP, École Normale Supérieure de Lyon

The first part of this paper deals with finite-precision arithmetic. We give an upper bound on the precision that should be used in a Monte-Carlo integration method. Such bounds have been known only for convex sets; our bound applies to almost any "reasonable" set.

In the second part of the paper, we show how to construct in polynomial time first-order formulas that approximately define the volume of definable sets. This result is based on a VC dimension hypothesis, and is inspired from the well-known complexity-theoretic result "BPP $\subseteq \Sigma_2$".

Finally, we show how these results can be applied to sets defined by systems of inequalities involving polynomial or exponential functions. In particular, section 5 contains an application to a problem of structural complexity in the Blum-Shub-Smale model of computation over the reals.

Solving Polynomial Systems
by Tien-Yien Li, Michigan State University

Numerically solving isolated zeros of polynomial systems in affine space has become increasingly important in applications. Many engineering models, such as power flow problem with PQ-specified buses, the most general six degree of freedom manipulators, and various eigenvalue problems, can be formulated as polynomial systems.

Elimination theory is the classical approach to solving systems of polynomial equations, but its reliance on symbolic manipulation makes it seem unsuitable for all but small problems. Moreover, the method reduces the problem to the ill-conditioned problem of numerically solving a high-degree polynomial equation in one variable.

In this talk, a new approach, developed in the last decade, by using the homotopy continuation method will be surveyed. The method involves first solving a trivial system, and then deforming these solutions along smooth paths to the solutions of the target system. The method has been successfully implemented in solving many polynomial systems, and the amount of computation required to find all solutions can be made roughly proportional to the number of solutions.

Semi-Algebraic Complexity – Additive Complexity of Diagonalization of Quadratic Forms
by THOMAS LICKTEIG, Universität Bonn

We study matrix calculation such as diagonalization of quadratic forms under the aspect of additive complexity and relate these complexites to the complexity of matrix multiplication. For the upper bound we give an uniform BSS algorithm, the asymptotic exponent $\omega_{BSS}(\text{DIAG})$ of which coincides with the non-uniform asymptotic exponent ω of matrix multiplication.

Since matrix multiplication allows an asymptotic uniformization we can use non-uniform methods for the lower bound reduction. While in [Bürgisser-Karpinski-Lickteig 91] for multiplicative complexity the customary "thick path existence" argument was sufficient, here for additive complexity we need the more delicate finess of the real spectrum (cf. [Bochnak-Coste-Roy 87], [Becker 86], [Knebusch-Scheiderer 89]) to obtain a complexity relativization. Our discussions substantiate once more the signification and future rôle of this concept in the mathematical evolution of the field of real algebraic algorithmic complexity.

A further technical tool concerning additive complexity is the structural transport metamorphosis from [Lickteig 90] which constitutes another use of exponentiation and logarithm as it appears in the work on additive complexity by [Grigoriev 82] and [Risler 85] through the use of [Khovanski 80]. (Joint work with K. Meer.)

On the Cost of Splitting Polynomials
by GREGORIO MALAJOVICH, Instituto de Matematica da UFRJ, Rio de Janeiro

The complexity of solving a degree d polynomial equation up to b bits of precision was bounded by Pan to $O(d^{1+\epsilon})$ arithmetic operations os $O(((b+d)d^2)^{1+\epsilon})$ Boolean operations. The algorithm involved requires a very high precision $((((b+d)d)^{1+\epsilon})$ bits). Our objective is to develop fast algorithms using a moderate precision (at least, in most cases). The problem of splitting polynomials seems to be one important bottleneck.

Given a polynomial f with d_1 zeros inside the disk $D(R^{-1}) = \{\zeta : |\zeta| < R^{-1}\}$ and d_2 zeros outside the the disk $D(R)$, we want to find factors g and h, $f = gh$, such that g has all its d_1 zeros inside $D(R^{-1})$, and h has all its d_2 zeros outside $D(R)$.

The factorization of f may be reduced to solving the system $\varphi_f(g, h) = f - gh = 0$ of $d+1$ polynomials in $d+1$ unknowns (it is understood that g is monic).

In vector notation, the system can be written as:

$$\varphi_f(g, h) = \begin{pmatrix} g_0 h_0 & - & f_0 \\ g_1 h_0 + g_0 h_1 & - & f_1 \\ \vdots & & \\ h_{d-1} + g_{d-1} h_d & - & f_{d-1} \\ h_d & - & f_d \end{pmatrix}$$

The system $\varphi_f(g, h)$ may be solved by Newton iteration. We construct a Newton operator and a starting point with the following property: If $\frac{\sum_{i \neq d_1} |f_i|^2}{|f_{d_1}|}$ is small enough, then the iteration will converge quadratically.

The above property is related to the separation annulus, and is implied by large enough R (still depending on d). It remains to investigate some issues related to the numerical stability of the algorithm. (Joint work with J. P. Zubelli.)

On the Structure of $\mathcal{NP}_{\mathbb{C}}$
by Klaus Meer, RWTH Aachen

We deal with complexity classes $\mathcal{P}_{\mathbb{C}}$ and $\mathcal{NP}_{\mathbb{C}}$ as they were defined over the complex numbers by Blum, Shub, and Smale. Under the assumption $\mathcal{P}_{\mathbb{C}} \neq \mathcal{NP}_{\mathbb{C}}$ the existence of non-complete problems in $\mathcal{NP}_{\mathbb{C}}$, not belonging to $\mathcal{P}_{\mathbb{C}}$, is established. (Joint work with G. Malajovich.)

Real Number Oracle Machines and Topological Complexity of Zero Finding
by Erich Novak, Universität Erlangen

The talk is based on ongoing discussion with Steve Smale and Henryk Woźnia-kowski.

The results concerning the topological ϵ-complexity of zero finding depend on
a) the class F of functions;
b) the class of arithmetic operations;
c) the error criterion (root error or residual error).
1) If we allow only operations that are Lipschitz, i.e., no division, then bisection is optimal even for the class F of linear functions $f(x) = ax + b$, where $f(0) < 0$ and $f(1) > 0$.
2) If we allow the sign function or division together with log and exp, then no branching is necessary for the class of increasing functions.

Both results are for the root criterion, but we also discuss examples for the residual error where branching is (or is not) necessary.

Polynomial and Matrix Computations
by VICTOR PAN, Lehman College, City University of New York

One of the major topics of our recent book [B-P] was the study of computations with Toeplitz and other dense structured matrices considered as a link between computations with polynomials and with general matrices. This study has lead us to improving computations in both of the latter areas and to narrowing the gap historically arisen between them. In the talk we recall some examples of correlations between Toeplitz matrices and general matrices and between Toeplitz matrices and polynomials, which enabled us to improve parallel algorithms for some fundamental computations in all 3 areas. For some major computations with $n \times n$ Toeplitz and Toeplitz-like matrices A (rank, inverse, linear system solving), we have obtained the parallel complexity bounds

a) of $O(\log^2 n)$ time and $O(n^2/\log n)$ arithmetic processors over any field of characteristic zero or greater than n (recalled from [B-P]),

b) of $O(\log^3 n)$ and $O(n^2/\log^2 n)$, respectively, over any field [P1], and

c) of $O((\log n)\log(n\log\|A\|))$ and $O(n\log n)$, respectively, over the integers [B-P], [P2].

The two latter results, of b) and c), over any field and integers, are randomized, and our computations over the integers (part c)) only involve $O(n\log\|A\|)$-bit precision.

[B-P] D. Bini, V. Y. Pan, *Polynomial and Matrix Computations*, vol. 1, Birkhäuser, Boston, 1994.
[P1] V. Y. Pan, Parallel Computations of Polynomial GCD and Related Computations, *Proc. Seventh Ann. ACM-SIAM Symp. on Discrete Algorithms*, January 1996.
[P2] V. Y. Pan, Effective Parallel Computations with Toeplitz and Toeplitz-like Matrices Filled with Integers, preprint.

Lower Bounds for Diophantine Approximation
by LUIS MIGUEL PARDO, Universidad de Cantabria & École Polytechnique, Palaiseau

In this talk we introduce some intrinsic upper complexity bounds concerning elimination problems. We show that the Turing machine complexity for solving (within the context of algebraic geometry) is polynomial in terms of the degree of the input polynomials, the number of variables, the syntactical length of the input, the (affine) degree and the (affine) height of the intermediate varieties. The same intrinsic bounds hold true for the decision problem in the Nullstellensatz. These upper complexity bounds imply the existence of algorithms that

profit from the good conditions of the input system, being of current complexity $d^{O(n)}$ for bad conditioned ones. Moreover, these upper complexity bounds yield meaningful lower bounds for the numerical analysis approach to solving systems of multivariate polynomial equations. This is obtained using intrinsic Liouvillian estimates. The consequences say that floating point encoding and binary encoding of rational and Gaussian numbers, are not well suited for numerical solving. In particular, the time becomes exponential or the approximation is far away from the true solution. Hence, the Liovillian estimates yield lower bounds for the length of any "approximate zero" (in the sense of Shub-Smale) in terms of the condition number γ of the system. (Joint work with M. Giusti, K. Hägele, J. Heintz, J. L. Montaña, J. E. Morais.)

An Enumerative Theorem in Real Algebraic Geometry with an Application to Discrete Geometry
by RICHARD POLLACK, Courant Institute, New York University

First we discuss the following enumerative theorem of real algebraic geometry which represents joint work with S. Basu and M.-F. Roy.

Let R be a real closed field and $\mathcal{V}$ a variety of real dimension k' which is the zero set of a polynomial $Q \in R[X_1, \ldots, X_k]$ of degree at most d. Given a family of s polynomials $\mathcal{P} = \{P_1, \ldots, P_s\} \subset R[X_1, \ldots, X_k]$ where each polynomial in $\mathcal{P}$ has degree at most d, we prove that the number of cells defined by $\mathcal{P}$ over $\mathcal{V}$ is $\binom{s}{k'}(O(d))^k$. Note that the combinatorial part of the bound depends on the dimension of the variety rather than on the dimension of the ambient space.

This bound, in the case where the variety $\mathcal{V}$ is the Grassmannian $G_{k,d}$, of k dimensional subspaces of $\mathcal{R}^d$, plays an essential role to obtain the following bound in geometric transversal theory which was obtained jointly with J. E. Goodman and R. Wenger.

A suitably separated family of n compact convex sets in $\mathcal{R}^d$ can be met by k-flat transversals in at most

$$O(k)^{d^2}\left(\binom{2^{k+1}-2}{k}\binom{n}{k+1}\right)^{k(d-k)}$$

or, for fixed k and d, $O(n^{k(k+1)(d-k)})$ different order types. This is the first non-trivial bound for $1 < k < d-1$, and generalizes (asymptotically) the best known bounds for line transversals in $\mathcal{R}^d$, $d > 2$.

Average Case Complexity of Counting Problems
by MICHEL DE ROUGEMONT, Université Paris-Sud

We study Valiant's Graph Reliability problem for the average case complexity.

Let a Gaussian-distance distribution μ be defined such that if $D_n = \{1, \ldots, n\}$ is the set of nodes, the probablility that an edge (i, j) exists is $e^{-(j-i)^2}$.

We show that the Graph Reliability problem (a $\#P$-hard problem) is Average-P for the Gaussian-distance distribution μ. (Joint work with D. Bourago.)

Small Inequalities and Positivstellensatz
by MARIE-FRANÇOISE ROY, IRMAR, Université de Rennes I

We define two notions of equivalence between basic semi-algebraic sets:

- quadratic equivalence, when their ring of quadratic functions are isomorphic,

- logical equivalence, when their defining set of small inequalities can simultaneously be extended, using a set of small deduction rules, to a common set of small inequalities,

and prove that these two notions coincide. Equivalent basic semi-algebraic sets have same dimension and same number of connected components. (Joint work with H. Lombardi and N. Mnëv.)

Aspects of Complexity of Algebraic Geometry over Non-Algebraically Closed Fields
by TOMAS SANDER, Universität Dortmund

A class $\mathcal{K}$ of fields K of characteristic 0 is introduced for which bounds of usually double exponential nature can be proved for properties of the K-rational points V_K of a K-variety V. Model theoretic properties of this class are investigated. This class contains e.g. $\mathcal{C}$, $\mathcal{R}$, $\mathcal{Q}_p$, PAC-fields, and Henselian fields. If for fields in $\mathcal{K}$ systems of algebraic equations can be solved effectively it is possible to compute algebraic-geometric data of V_K effectively.

Soft Branching versus if-then-else
by ARNOLD SCHÖNHAGE, Universität Bonn

Starting from the observation that strict branching by comparison of real numbers is unrealistic (impossible for oracle inputs, extremely difficult for inputs defined by programs) or possibly of very high complexity even for discrete application data, we present the notion of *soft branching* as a (possibly nondeterministic) selection from several alternatives with some overlap:

do branch B_1 with assertion A_1 or do B_2 with A_2,

where A_1 and A_2 are predicate formulae not necessarily excluding each other. Three examples illustrate this concept, among them the intersection of two annuli (soft circles, so to say) and the use of *quasi-gcd*s, cf. J. of Complexity **1**, 118–137 (1985).

Complexity – Algebraic Perspective
by STEVE SMALE, City University of Hong Kong

Hilbert's Nullstellensatz was considered as a decision problem, first over the complex numbers, then over a general field. Via a model of machines (joint with L. Blum and M. Shub), the intractibilty of the Hilbert decision problem is equivalent to the conjecture P is not NP, over that field. This subject was developed.

Kolmogorov Complexity and Real Computation
by PAUL VITANY, CWI - Mathematisch Centrum, Universiteit van Amsterdam

The Kolmogorov complexity of a finite binary string is the length of the shortest effective binary program which computes it – that is, the length of the shortest binary description. This definition is objective and absolute, in the sense of being recursively invariant. In the appropriate way it can be extended to infinite binary sequences, and in that sense to arbitrary reals. Hence it makes sense to talk about recursive reals, r. e. reals, pararecursive reals, random reals, and so on. With respect to real computations, where the description of the real constants involved should be expressed in effective terms, or relative to non-effective descriptions, the known theory of effective descriptions with or without computational resources in terms of e. g. time and space, that is Kolmogorov complexity theory, can (and presumably should) be profitably applied. For details on the theory see the textbook M. LI AND P. VITANY, *An Introduction to Kolmogorov Complexity and its Applications*, Springer-Verlag, New York, 1993.

Applying Quantifier Elimination to Problems in Simulation and Optimization
by VOLKER WEISPFENNING, Universität Passau

I present a new elimination method that eliminates linear (and quadratic) variables from a Boolean combination of polynomial equations and inequalities with parameters. In contrast to the (doubly exponential) classical Fourier-Motzkin method, the method is singly exponential in the worst case; moreover it works in polynomial space for parameter-free problems. The method has been implemented in REDUCE and tested successfully in benchmark LP-problems and

industrial simulation of complex networks with more than 50 variables.

On Information and Arithmetic Complexities
by HENRYK WOŹNIAKOWSKI, Columbia University & Uniwersytet Warszawski

The talk is based on the paper *There exists a linear problem with infinite combinatory complexity* by G. W. WASILKOWSKI and the author. We present a linear problem whose information complexity is finite but whose arithmetic (combinatory) complexity is infinite. This holds in a real number model (BSS) with oracles given by arbitrary linear functionals.

Reported by THOMAS LICKTEIG