Joachim von zur Gathen, Marek Karpinski
Dexter Kozen (editors):

Algebraic Complexity and Parallelism

Dagstuhl-Seminar-Report; 41
20.-24.7.92 (9230)

ISSN 0940-1121

Tel.: +49-6871 - 2458
Fax: +49-6871 - 5942

Das Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Bezugsadresse: Geschäftsstelle Schloß Dagstuhl
Informatik, Bau 36
Universität des Saarlandes
W - 6600 Saarbrücken
Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: office@dag.uni-sb.de

INTERNATIONALES BEGEGNUNGS- UND
FORSCHUNGSZENTRUM FÜR INFORMATIK

Schloß Dagstuhl

Seminar Report 9230

Algebraic Complexity and Parallelism

July 20 –24, 1992

This report contains the abstracts of the talks given at the Dagstuhl Workshop on "Algebraic Complexity and Parallelism", July 20–24, 1992.

Reported by Kai Werther

Participants

Peter Bürgisser, Bonn
Alexander L. Chistov, St. Petersburg
Sergei Evdokimov, St. Petersburg
Joachim von zur Gathen, Toronto
Erich Kaltofen, Troy
Marek Karpinski, Bonn
Dexter Kozen, Ithaca
Thomas Lickteig, Bonn
Ewa Malesinska, Bonn
Ernst W. Mayr, Frankfurt
Klaus Meer, Aachen
J. L. Montaña, Santander
Luis Miguel Pardo Vasallo, Santander
Igor Shparlinski, Moskau
Kai Werther, Bonn
Thorsten Werther, Bonn

Contents

Abstracts

Decision Complexity of Generic Complete Intersections

by PETER BÜRGISSER

We study the complexity of algebraic decision trees that decide membership in an algebraic subset $X \subseteq R^m$ where R is a real (or algebraically) closed field. We prove a general lower bound on the verification complexity (c.f. Bürgisser, Lickteig and Shub [1]) of the vanishing ideal of an irreducible algebraic subset $X \subseteq R^m$ in terms of the degree of transcendency of its minimal field of definition. As an application we determine exactly the number of additions, subtractions and comparisons that are needed to test membership in a generic complete intersection $X = Z(f_1, \ldots, f_r) \subseteq R^{m+1}$ of homogeneous polynomials f_i; for the number of multiplications, divisions and comparisons needed we obtain an asymptotically optimal lower bound for $\min_i \deg f_i \to \infty$. This generalizes the main results in [1]. A further application is given to the zero testing of rational functions that are given by a partial or continued fraction expansion.

Efficient Parallel Algorithms for Computational Problems in the Theory of Algebraic Curves

by ALEXANDER L. CHISTOV

It is proved that the classical algorithm for computing the Newton-Puiseux expansion of roots of a polynomial using the Newton polygons method has a polynomial complexity in the model of computation when sizes of coefficients and constant fields are taken into account. As a consequence we get polynomial-time algorithms and efficient parallel algorithms for factoring polynomials over field of zero characteristic of formal power series in one variable. Further, there are constructed polynomial-time and efficient parallel algorithms for computing uniformizing elements of local rings of points of algebraic curves, indices of ramification and inertia, the geometrical genus of a curve, the normalization of an algebraic curve. Note that in these parallel algorithms extensions of constant fields are given by primitive elemetns with separable polynomials annihilating them instead of minimal polynomials.

Factoring Polynomials over Finite Fields in Subexponential Time under GRH

by SERGEI EVDOKIMOV

Assuming the Generalized Riemann Hypothesis the following theorem is proved.
Theorem (GRH) There exists a deterministic algorithm decomposing a polynomial $f \in k[x]$ of degree n over a finite field k of cardinality q into irreducible factors over k within time

$$(n^{\log n} \cdot \log q)^{O(1)}.$$

Factoring Polynomials over Finite Fields

by JOACHIM VON ZUR GATHEN (joint work with VICTOR SHOUP)

The factorization of polynomials is a fundamental problem in computer algebra. This talk considers polynomials in one variable over a finite field. The important (probabilistic) algorithm of Cantor and Zassenhaus (1981) can (probably) factor a polynomial of degree n in $\mathsf{F}_q[x]$ with an essentially cubic number $O(n^2 \log q)$ of operations in F_q. I will present an algorithm that uses an essentially (i.e., disregarding factors of $\log n$) quadratic number $O(n^2 + n \log q)$ of operations.

Processor-Efficient Parallel Solution of Systems of Linear Equations

by ERICH KALTOFEN (joint work with V. PAN and B.D. SAUNDERS)

An efficient parallel algorithm for solving a linear system of n equations in n variables must run in time $(\log n)^{O(1)}$ and utilize only $n^\omega (\log n)^{O(1)}$ processors, where $O(n^\omega)$ is the time needed to multiply $n \times n$ matrices. Here a time step is an arithmetic operation in the coefficient field or a test of an element for being 0. We present a randomized algorithm that finds a particular solution, if it exists, and a basis for the null-space for any coefficient field in $O((\log n)^4)$ time with $n^\omega (\log n)$ processors. The solution generalizes our earlier work allowing fields of small positive characteristic and by determining the rank of a matrix without binary search. Our main idea applies recursive triangulation to the algorithm of Le Verrier (1840)/ Csanky (1976) as well as generalizes the Mulmeley (1986) rank algorithm to Toeplitz matrices.

Computational Complexity of Some Algebraic Counting Problems

by MAREK KARPINSKI

We study the computational complexity of some generic algebraic counting problems, both for the exact and the approximate counting models. We characterize these problems in terms of known upper and (relative) lower bounds, and apply these results for the various constant depth circuits counting problems. These problems include:

- Counting the number of solutions of determinantal equations over arbitrary finite fields GF[q];
- Counting the number of zeros (and nonzeros) of arbitrary sparse multivariate polynomials over GF[q] and the number of points on the projective varieties;
- Counting the number of satisfying assignments of the "small" boolean and arithmetic constant depth circuits.

For the above problems we design the (ϵ, δ)-approximation algorithms which work in polynomial time for arbitrary fixed finite fields GF[q]. We discuss also the problem of approximating the number of points on the arbitrary curve $C \in \mathrm{GF}[q][x, y]$ in the time sublinear in q.
Finally the problem of removing randomness (deterministic simulation) from some of the randomized (ϵ, δ)-approximation algorithms has been discussed.

An Algebraic Approach to Types and Term Rewriting

by DEXTER KOZEN

Various concepts in type theory and term rewriting are best described in algebraic and/or automata-theoretic terms. This approach isolates the combinatorial essence of these concepts and in at least two cases has provided efficient polynomial time algorithms for important practical problems for which previously known algorithms were exponential. We describe this approach and give three applications:
(1) An $O(n^2)$ algorithm for type inclusion in the presence of recursive types. This type system was investigated by Amadio and Cardelli and forms the basis of the AMBER and QUEST programming languages. The solution of the inclusion problem is essential for automatic type checking. Previous algorithms were exponential. (Joint work with Palsberg and Schwartzbach.)
(2) An $O(n^3)$ algorithm for type inference for a related system of Thatte, who introduced the system in 1988 and proved semidecidability. Decidability of the system remained open until 1992, when O'Keefe and Wand gave an exponential algorithm for finite types only, but left open the question of recursive types. Our $O(n^3)$ algorithm works equally well for finite or recursive types. (Joint work with Palsberg and Schwartzbach.)
(3) Every ground term rewriting system has a unique canonical equivalent system. This theorem is best viewed as a generalization of the Myhill-Nerode theorem for finitely presented algebras.

On Randomized Algebraic Decision Complexity

by THOMAS LICKTEIG (joint work with PETER BÜRGISSER and MAREK KARPINSKI)

The impact of randomization to algebraic decision complexity is studied. Examples are given where randomization may reduce the decision complexity. A lower bound is also given showing that in certain cases randomization cannot help (much).

On the Algorithmic Complexity of Hilbert's Nullstellensatz

by ERNST W. MAYR

We study the algorithmic complexity of the membership problem for ideals generated by finitely many multivariate polynomials with rational coefficients. From earlier results on finitely presented commutative semigroups, an exponential space lower bound follows. A matching upper bound can be obtained using G. Hermann's double exponential degree bound for solutions and space efficient techniques for computing the rank of matrices. Using exponential degree bounds obtained by Brownawell and others for the case whether the constant polynomial 1 is contained in the ideal, we obtain a PSPACE upper bound for this problem and the radical membership problem. Again, these upper bounds can be matched from below.

Lower Bounds for Arithmetic Networks

by J. L. MONTAÑA (joint work with L. M. PARDO)

We show lower bounds for depth of arithmetic networks over algebraically closed field, real closed fields and the field of the rationals. The parameters used are either the degree or the number of connected components. These lower bounds allow us to show the inefficiency of arithmetic networks to parallelize several natural problems. For instance, we show a $\sqrt{n}$ lower bound for parallel time of the Knapsack problem over the reals and also that the computation of the "greatest integer in" is not well parallelizable by arithmetic networks. Over the rationals, we obtain an $\sqrt{n}$ lower bound for the parallel time of the ϵ-approximation Knapsack problem. A simply exponential lower bound for the parallel time of quantifier elimination is also shown. Finally, separations among classes P_K and NC_K are available for fields K in the above cases.

On the Distribution and Finding Primitive Roots in Finite Fields

by IGOR SHPARLINSKI

The talk is devoted to some recent results an open questions related to the distribution of primitive roots in a finite field. In particular, we consider distribution (and existence) questions in some small subset of the field that either have a "natural" description or have been specially constructed to contain at least one primitive root (after G. I. Perelmuter, V. Shoup and the author). We also mention some results on primitive normal bases (after J. von zur Gathen, M. Giesbrecht, H. .W. Lenstra, R. J. Schoof, S. A. Stepanov, and the author).

VC Dimension and Uniform Learnability of Sparse Polynomials

by THORSTEN WERTHER (joint work with MAREK KARPINSKI)

We derive linear upper $(4t-1)$ and lower $(3t)$ bounds on the VC dimension of the class of t-sparse polynomials over the real numbers, and apply these results to prove uniform learnability of sparse polynomials and rational functions. As an application we give the solution to the open problem of Vapnik [Vapnik '82] on computational approximation of the regression in a class of polynomials used in the theory of empirical data dependencies.

Open Problem Session

Speakers: Joachim von zur Gathen
Kai Werther
Marek Karpinski
Dexter Kozen
Ernst Mayr
Igor Shparlinski

E-Mail Addresses

Peter Bürgisser:	buerg@cs.uni-bonn.de
Alexander L. Chistov:	sliss@iias.spb.su
Sergei Evdokimov:	sliss@iias.spb.su
Joachim von zur Gathen:	gathen@theory.toronto.edu
Erich Kaltofen:	kaltofen@cs.rpi.edu
Marek Karpinski:	marek@cs.uni-bonn.de
Dexter Kozen:	kozen@cs.cornell.edu
Thomas Lickteig:	lickteig@cs.uni-bonn.de
Ewa Malesinska:	ewa@cs.uni-bonn.de
Ernst W. Mayr:	mayr@informatik.uni-bonn.de
Klaus Meer:	LN11OME@DACTH11.BITNET
J. L. Montaña:	pardo@ccucvx.unican.es
Luis Miguel Pardo Vasallo:	pardo@ccucvx.unican.es
Igor Shparlinski:	shpar@plb.icsti.su
Kai Werther:	kai@cs.uni-bonn.de
Thorsten Werther:	thorsten@cs.uni-bonn.de

Addresses

Peter Bürgisser
Universität Bonn
Institut für Informatik
Römerstr. 164
W-5300 Bonn 1
Germany
Tel.: +49-228-550-209

Erich Kaltofen
Rensselaer Polytechnic Institute
Dept. of Computer Science
Troy NY 12180-3590
USA
Tel.: +1-518-276-6907

Alexander L. Chistov
Institute for Informatics Acad. Sci.
14th line 39
St. Petersburg 199178
Russia

Marek Karpinski
Universität Bonn
Institut für Informatik
Römerstr. 164
W-5300 Bonn 1
Germany
Tel.: +49-228-550-224

Sergei Evdokimov
Institute for Informatics Acad. Sci.
14th line 39
St. Petersburg 199178
Russia

Dexter Kozen
Cornell University
Dept. of Computer Science
4130 Upson Hall
Ithaca NY 14853-7510
USA
Tel.: +1-607-255-9209

Joachim von zur Gathen
University of Toronto
Dept. of Computer Science
10 King's College of Road
Toronto Ontario M5S 1A4
Canada
Tel.: 416-978-6024

Thomas Lickteig
Universität Bonn
Institut für Informatik
Römerstr. 164
W-5300 Bonn 1
Germany
Tel.: +49-228-550-209

Ewa Malesinska
Universität Bonn
Institut für Informatik
Römerstr. 164
W-5300 Bonn 1
Germany

Luis Miguel Pardo Vasallo
Universidad de Cantabria
Dept. of Mathematics
Facultad de Ciencias
Av. Los Castros
39071 Santender
Spain
Tel.: +34-42-20-15-25

Ernst W. Mayr
Universität Frankfurt
Fachbereich Informatik (20)
Theoretische Informatik
Robert-Mayer-Str. 11–15
W-6000 Frankfurt 11
Germany
Tel.:+49-69-798-8326

Igor Shparlinski
International Centre for Scientific
and Technical Information
Mosfilmovskaya 2-V-41
Moskow 119285
Russia
Tel.: 932-28-37

Klaus Meer
RWTH Aachen
Fachbereich Mathematik
Templergraben 55
W-5100 Aachen
Germany
Tel.: +49-241-804-540

Kai Werther
Universität Bonn
Institut für Informatik
Römerstr. 164
W-5300 Bonn 1
Germany
Tel.: +49-228-550-319

J. L. Montaña
Universidad de Cantabria
Dept. of Mathematics
Facultad de Ciencias
Av. Los Castros
39071 Santender
Spain
Tel.: +34-42-20-15-24

Thorsten Werther
Universität Bonn
Institut für Informatik
Römerstr. 164
W-5300 Bonn 1
Germany
Tel.: +49-228-550-232

Zuletzt erschienene und geplante Titel:

G. Farin, H. Hagen, H. Noltemeier (editors):
Geometric Modelling, Dagstuhl-Seminar-Report; 17, 1.-5.7.1991 (9127)

A. Karshmer, J. Nehmer (editors):
Operating Systems of the 90s and Beyond, Dagstuhl-Seminar-Report; 18, 8.-12.7.1991 (9128)

H. Hagen, H. Müller, G.M. Nielson (editors):
Scientific Visualization, Dagstuhl-Seminar-Report; 19, 26.8.-30.8.91 (9135)

T. Lengauer, R. Möhring, B. Preas (editors):
Theory and Practice of Physical Design of VLSI Systems, Dagstuhl-Seminar-Report; 20, 2.9.-6.9.91 (9136)

F. Bancilhon, P. Lockemann, D. Tsichritzis (editors):
Directions of Future Database Research, Dagstuhl-Seminar-Report; 21, 9.9.-12.9.91 (9137)

H. Alt , B. Chazelle, E. Welzl (editors):
Computational Geometry, Dagstuhl-Seminar-Report; 22, 07.10.-11.10.91 (9141)

F.J. Brandenburg , J. Berstel, D. Wotschke (editors):
Trends and Applications in Formal Language Theory, Dagstuhl-Seminar-Report; 23, 14.10.-18.10.91 (9142)

H. Comon , H. Ganzinger, C. Kirchner, H. Kirchner, J.-L. Lassez , G. Smolka (editors):
Theorem Proving and Logic Programming with Constraints, Dagstuhl-Seminar-Report; 24, 21.10.-25.10.91 (9143)

H. Noltemeier, T. Ottmann, D. Wood (editors):
Data Structures, Dagstuhl-Seminar-Report; 25, 4.11.-8.11.91 (9145)

A. Dress, M. Karpinski, M. Singer(editors):
Efficient Interpolation Algorithms, Dagstuhl-Seminar-Report; 26, 2.-6.12.91 (9149)

B. Buchberger, J. Davenport, F. Schwarz (editors):
Algorithms of Computeralgebra, Dagstuhl-Seminar-Report; 27, 16.-20.12.91 (9151)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13..-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.02.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Modelling with Programmed Machines, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13.-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.2.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Information-technological Models, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

N. Habermann, W.F. Tichy (editors):
Future Directions in Software Engineering, Dagstuhl-Seminar-Report; 32; 17.2.-21.2.92 (9208)

R. Cole, E.W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms; Dagstuhl-Seminar-Report; 33; 2.3.-6.3.92 (9210)

P. Klint, T. Reps, G. Snelting (editors):
Programming Environments; Dagstuhl-Seminar-Report; 34; 9.3.-13.3.92 (9211)

H.-D. Ehrich, J.A. Goguen, A. Sernadas (editors):
Foundations of Information Systems Specification and Design; Dagstuhl-Seminar-Report; 35; 16.3.-19.3.9 (9212)

W. Damm, Ch. Hankin, J. Hughes (editors):
Functional Languages:
Compiler Technology and Parallelism; Dagstuhl-Seminar-Report; 36; 23.3.-27.3.92 (9213)

Th. Beth, W. Diffie, G.J. Simmons (editors):
System Security; Dagstuhl-Seminar-Report; 37; 30.3.-3.4.92 (9214)

C.A. Ellis, M. Jarke (editors):
Distributed Cooperation in Integrated Information Systems; Dagstuhl-Seminar-Report; 38; 5.4.-9.4.92 (9215)

J. Buchmann, H. Niederreiter, A.M. Odlyzko, H.G. Zimmer (editors):
Algorithms and Number Theory, Dagstuhl-Seminar-Report; 39; 22.06.-26.06.92 (9226)

E. Börger, Y. Gurevich, H. Kleine-Büning, M.M. Richter (editors):
Computer Science Logic, Dagstuhl-Seminar-Report; 40; 13.07.-17.07.92 (9229)

J. von zur Gathen, M. Karpinski, D. Kozen (editors):
Algebraic Complexity and Parallelism, Dagstuhl-Seminar-Report; 41; 20.07.-24.07.92 (9230)

F. Baader, J. Siekmann, W. Snyder (editors):
6th International Workshop on Unification, Dagstuhl-Seminar-Report; 42; 29.07.-31.07.92 (9231)

J.W. Davenport, F. Krückeberg, R.E. Moore, S. Rump (editors):
Symbolic, algebraic and validated numerical Computation, Dagstuhl-Seminar-Report; 43; 03.08.-07.08.92 (9232)

R. Cohen, W. Wahlster (editors):
3rd International Workshop on User Modeling, Dagstuhl-Seminar-Report; 44; 10.-14.8.92 (9233)

R. Reischuk, D. Uhlig (editors):
Complexity and Realization of Boolean Functions, Dagstuhl-Seminar-Report; 45; 24.08.-28.08.92 (9235)

Th. Lengauer, D. Schomburg, M.S. Waterman (editors):
Molecular Bioinformatics, Dagstuhl-Seminar-Report; 46; 07.09.-11.09.92 (9237)

V.R. Basili, H.D. Rombach, R.W. Selby (editors):
Experimental Software Engineering Issues, Dagstuhl-Seminar-Report; 47; 14.-18.09.92 (9238)

Y. Dittrich, H. Hastedt, P. Schefe (editors):
Computer Science and Philosophy, Dagstuhl-Seminar-Report; 48; 21.09.-25.09.92 (9239)

R.P. Daley, U. Furbach, K.P. Jantke (editors):
Analogical and Inductive Inference 1992 , Dagstuhl-Seminar-Report; 49; 05.10.-09.10.92 (9241)

E. Novak, St. Smale, J.F. Traub (editors):
Algorithms and Complexity of Continuous Problems, Dagstuhl-Seminar-Report; 50; 12.10.-16.10.92 (9242)

J. Encarnação, J. Foley (editors):
Multimedia - System Architectures and Applications, Dagstuhl-Seminar-Report; 51; 02.11.-06.11.92 (9245)

F.J. Rammig, J. Staunstrup, G. Zimmermann (editors):
Self-Timed Design, Dagstuhl-Seminar-Report; 52; 30.11.-04.12.92 (9249)