

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7407>

Ilias S. Kotsireas · Siegfried M. Rump
Chee K. Yap (Eds.)

Mathematical Aspects of Computer and Information Sciences

6th International Conference, MACIS 2015
Berlin, Germany, November 11–13, 2015
Revised Selected Papers

Editors

Ilias S. Kotsireas
Wilfrid Laurier University
Waterloo, ON
Canada

Chee K. Yap
New York University
New York, NY
USA

Siegfried M. Rump
Hamburg University of Technology
Hamburg
Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-32858-4 ISBN 978-3-319-32859-1 (eBook)
DOI 10.1007/978-3-319-32859-1

Library of Congress Control Number: 2016935965

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

Mathematical Aspects of Computer and Information Sciences (MACIS) is a series of biennial conferences focusing on research in mathematical and computational aspects of computing and information science. It is broadly concerned with algorithms, their complexity, and their embedding in larger logical systems. At the algorithmic level, there is a rich interplay along the numerical/algebraic/geometric/topological axes. At the logical level, there are issues of data organization, interpretation, and associated tools. These issues often arise in scientific and engineering computation where we need experimental and case studies to validate or enrich the theory. MACIS is interested in outstanding and emerging problems in all these areas. Previous MACIS conferences have been held in Beijing (2006, 2011), Paris (2007), Fukuoka (2009), and Nanning (2013). MACIS 2015 was held at the Zuse Institute Berlin (ZIB) located in the capital of Germany, in the vicinity of the Freie Universität Berlin. Named after Konrad Zuse, the inventor of the first programmable computer, ZIB is an interdisciplinary research institute for applied mathematics and data-intensive high-performance computing. Its research areas in modeling, simulation, and optimization in partnership with academia and industry are exemplary of the goals of MACIS.

We are grateful to the session organizers (and their referees) for their critical role in putting together the successful technical program. We also wish to extend our gratitude to all MACIS 2015 conference participants—all of them contributed in making the conference a success. The conference would not have been possible without the hard work of the local organizers from ZIB, Winfried Neun, and Benedikt Bodendorf, and the generous support of our sponsors, namely, Maplesoft and Zuse Institute Berlin (ZIB).

This volume contains 55 refereed papers, i.e., seven invited papers and 48 submitted papers, all of which were presented at MACIS. The papers are organized in sections corresponding to 12 special sessions featured in the MACIS 2015 conference. The topics of the MACIS 2015 sessions cover a wide array of research areas as follows:

- SS1: Vikram Sharma: Curves and Surfaces
- SS2: Jon Hauenstein: Applied Algebraic Geometry
- SS3: Johannes Blömer: Implementations of Cryptography
- SS4: Takeshi Ogita: Verified Numerical Computation
- SS5: Johannes Blömer and Jan Camenisch: Cryptography and Privacy
- SS6: Chengji Mou and Eric Schost: Polynomial System Solving
- SS7: Maxime Crochemore and Costas Iliopoulos: Managing Massive Data
- SS8: Viktor Levandovskyy, Alexey Ovchinnikov, Michael Wibmer: Computational Theory of Differential and Difference Equations
- SS9: Xiaoyu Chen and Jie Luo: Data and Knowledge Exploration
- SS10: Rudolf Fleischer and Stefan Schirra: Algorithm Engineering in Geometric Computing

SS11: Akitoshi Kawamura and Martin Ziegler: Real Complexity: Theory and Practice

SS12: Jordan Ninin: Global Optimization

We wish to thank all the session organizers for their hard work in putting together these sessions.

February 2016

Ilias S. Kotsireas
Siegfried M. Rump
Chee K. Yap

Organization

General Chair

Ilias S. Kotsireas

Wilfrid Laurier University, Canada

Local Organization

Winfried Neun

Zuse Institute Berlin, Germany

Benedikt Bodendorf

Zuse Institute Berlin, Germany

Program Chairs

Siegfried Rump

Hamburg University of Technology, Germany

Chee Yap

Courant Institute, NYU, USA

Program Committee

Johannes Blömer

University of Paderborn, Germany

Jan Camenisch

IBM Zurich, Switzerland

Xiaoyu Chen

Beihang University, Beijing, China

Maxime Crochemore

Kings College London, UK

Rudolf Fleischer

German University of Technology in Oman

Mark Giesbrecht

University of Waterloo, Canada

Jonathan Hauenstein

Notre Dame University, USA

Costas Iliopoulos

Kings College London, UK

Akitoshi Kawamura

University of Tokyo, Japan

R. Baker Kearfott

University of Louisiana, Lafayette, USA

Viktor Levandovskyy

RWTH Aachen University, Germany

Jie Luo

Beihang University, Beijing, China

Chenqi Mou

Beihang University, China

Jordan Ninin

ENSTA Bretagne, France

Takeshi Ogita

Tokyo Woman's Christian University, Japan

Alexey Ovchinnikov

CUNY Graduate Center, USA

Mohab Safey El-Din

University of Pierre and Marie Curie, Paris, France

Michael Sagraloff

Max Planck Institute, Saarbrücken, Germany

Stefan Schirra

Otto von Guericke University Magdeburg, Germany

Éric Schost

Western University, London, Ontario, Canada

Vikram Sharma

Institute of Math Sciences, Chennai, India

VIII Organization

Thomas Sturm	Max Planck Institute, Saarbrücken, Germany
Michael Wibmer	RWTH Aachen, Germany; University of Pennsylvania, USA
Martin Ziegler	Technical University Darmstadt, Germany

MACIS Steering Committee

Thomas Sturm (Chair)	Universitat Autònoma de Barcelona, Spain
Ilias Kotsireas	Wilfrid Laurier University, Canada
Stefan Ratschan	Institute of Computer Science, Academy of Sciences of the Czech Republic
Dongming Wang	CNRS, Paris, France
Jinzhao Wu	Guangxi University for Nationalities, China
Zhiming Zheng	Peking University, China

Abstracts of Invited Papers

Current Challenges in Developing Open Source Computer Algebra Systems

Janko Böhm¹(✉), Wolfram Decker¹, Simon Keicher² and Yue Ren¹

¹ University of Kaiserslautern, 67663 Kaiserslautern, Germany
{boehm,decker,ren}@mathematik.uni-kl.de

² Universidad de Concepción, Casilla 160-C, Concepción, Chile
simonkeicher@gmail.com

Abstract. This note is based on the plenary talk given by the second author at MACIS 2015, the Sixth International Conference on Mathematical Aspects of Computer and Information Sciences. Motivated by some of the work done within the Priority Programme SPP 1489 of the German Research Council DFG, we discuss a number of current challenges in the development of Open Source computer algebra systems. The main focus is on algebraic geometry and the system SINGULAR.

The first author acknowledges support from the DFG projects DE 410/8-1 and -2, DE 410/9-1 and -2, and from the OpenDreamKit Horizon 2020 European Research Infrastructures project (#676541). The third author was supported partially by the DFG project HA 3094/8-1 and by proyecto FONDECYT postdoctorado no 3160016.

Modeling Side-Channel Leakage

Stefan Dziembowski

University of Warsaw

Abstract. Physical side-channel attacks that exploit leakage emitted from devices (see, e.g., [8]) are an important threat to cryptographic implementations. A recent trend in cryptography [9, 10] is to construct cryptographic algorithms that are secure in a given leakage model. Over the past 15 years several such models have been proposed in the literature, starting with the probing model of [9], where the computation is modeled as a Boolean circuit, and the adversary can learn a limited number of them. Other models studied in the theory community include the *bounded-leakage paradigm* [1, 5], the *only computation leaks model* [10], the *independent leakage model* [7], the *auxiliary input model* [3], and many others.

Some of these models have been received with skepticism by the practitioners, who often argued that it is much more realistic to model leakage as a noisy function of the secret data. The first model for noisy leakage was proposed in [2], and fully formalized in [11]. Recently in [4] it has been shown that in fact the noisy leakage model of [11] can be reduced to the probing model (i.e.: every noisy leakage function can be simulated by a probing function), which, in particular, greatly simplifies several proofs in the noisy leakage model, and can be viewed as establishing a bridge between theory and practice in this area.

In this talk we give an overview of the leakage models used in the literature. We then present the reduction from [4], and talk about some follow-up work [6].

References

1. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (2009)
2. Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P.: Towards sound approaches to counteract power-analysis attacks. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 398–412. Springer, Heidelberg (1999)
3. Dodis, Y., Goldwasser, S., Kalai, Y.T., Peikert, C., Vaikuntanathan, V.: Public-key encryption schemes with auxiliary inputs. In: Micciancio, D., (ed.) TCC 2010. LNCS, vol. 5978, pp. 361–381. Springer, Heidelberg (2010)
4. Duc, A., Dziembowski, S., Faust, S.: Unifying leakage models: from probing attacks to noisy leakage. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 423–440. Springer, Heidelberg (2014)

Solving Structured Polynomial Systems with Gröbner Bases

Jean-Charles Faugère

Inria, Equipe POLSYS, Centre Paris Rocquencourt, F-75005, Paris, France
Sorbonne Universités, UPMC Univ Paris 06, Equipe POLSYS,
LIP6, F-75005, Paris, France
CNRS, UMR 7606, LIP6, F-75005, Paris, France

Abstract. In most cases, the number of solutions of a polynomial system is exponential, and in finite fields, solving polynomial systems is NP-hard. However, problems coming from applications usually have additional structures. Consequently, a fundamental issue is to design a new generation of algorithms exploiting the special structures that appear ubiquitously in the applications.

At first glance, multi-homogeneity, weighted homogeneity overdeterminedness, sparseness and symmetries seem to be unrelated structures. Indeed, until recently we have obtained specific results for each type of structure: we obtain dedicated algorithm and sharp complexity results too handle a particular structure. For instance, we handle bilinear systems by reducing the problem to determinantal ideals; we also propose ad-hoc techniques to handle symmetries.

All these results have been obtained separately by studying each structure one by one. Recently we found a new unified way to analyze these problems based on monomial sparsity. To this end, we introduce a new notion of sparse Gröbner bases, an analog of classical Gröbner bases for semigroup algebras. We propose sparse variants of the F4/F5 and FGLM algorithms to compute them and we obtain new and sharp estimates on the complexity of solving them (for zero-dimensional systems where all polynomials share the same Newton polytope). As a by product, we can generalize to the multihomogeneous case the already useful bounds obtained in the bilinear case. We can now handle in a uniform way several type of structured systems (at least when the type of structure is the same for every polynomial). From a practical point of view, all these results lead to a striking improvement in the execution time.

We also investigate the non convex case when only a small subset of monomials appear in the equations: the fewnomial case. We can relate the complexity of solving the corresponding algebraic system with some combinatorial property of a graph associated with the support of the polynomials. We show that, in some cases, the systems can be solved in polynomial time.

Joint work with Jules Svartz and Pierre-Jean Spaenlehauer.

Exploiting Structure in Floating-Point Arithmetic

Claude-Pierre Jeannerod

Inria

Laboratoire LIP (CNRS, ENSL, Inria, UCBL), Université de Lyon

Abstract. The analysis of algorithms in IEEE floating-point arithmetic is most often carried out via repeated applications of the so-called standard model, which bounds the relative error of each basic operation by a common epsilon depending only on the format. While this approach has been eminently useful for establishing many accuracy and stability results, it fails to capture most of the low-level features that make floating-point arithmetic so highly structured. In this paper, we survey some of those properties and how to exploit them in rounding error analysis. In particular, we review some recent improvements of several classical, Wilkinson-style error bounds from linear algebra and complex arithmetic that all rely on such structure properties.

Keywords: Floating-point arithmetic · IEEE standard 754-2008 · Rounding error analysis · High relative accuracy

Symbolic Geometric Reasoning with Advanced Invariant Algebras

Hongbo Li^(✉)

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
hli@mmrc.iss.ac.cn

Abstract. In symbolic geometric reasoning, the output of an algebraic method is expected to be geometrically interpretable, and the size of the middle steps is expected to be sufficiently small for computational efficiency. Invariant algebras often perform well in meeting the two expectations for relatively simple geometric problems. For example in classical geometry, symbolic manipulations based on basic invariants such as squared distances, areas and volumes often have great performance in generating readable proofs. For more complicated geometric problems, the basic invariants are still insufficient and may not generate geometrically meaningful results.

An advanced invariant is a monomial in an “advanced algebra”, and can be expanded into a polynomial of basic invariants that are also included in the algebra. In projective incidence geometry, Grassmann-Cayley algebra and Cayley bracket algebra are an advanced algebra in which the basic invariants are determinants of homogeneous coordinates of points, and the advanced invariants are Cayley brackets. In Euclidean conformal geometry, Conformal Geometric Algebra and null bracket algebra are an advanced algebra where the basic invariants are squared distances between points and signed volumes of simplexes, and the advanced invariants are Clifford brackets.

This paper introduces the above advanced invariant algebras together with their applications in automated geometric theorem proving. These algebras are capable of generating extremely short and readable proofs. For projective incidence theorems, the proofs generated are usually two-termed in that the conclusion expression maintains two-termed during symbolic manipulations. For Euclidean geometry, the proofs generated are mostly one-termed or two-termed.

Keywords: Grassmann-Cayley algebra · Cayley bracket algebra · Conformal Geometric Algebra · Null bracket algebra · Automated geometric theorem proving

Decidability from a Numerical Point of View

Stefan Ratschan

Institute of Computer Science
Czech Academy of Sciences

Abstract. An important application of computation is the automatic analysis of mathematical models of real-world systems, for example by simulation or formal verification. Here, the systems to be automatically analyzed can be physical systems (e.g., the wing of an airplane) or computational systems (e.g., computer software). In the past, research in this direction has happened largely independently for those two types of systems: Algorithms for automatically analyzing models of physical systems have been developed mainly by engineers and numerical mathematicians, resulting in notions such as “well-posed problem”, and “condition number”, and algorithms for automatically analyzing models of computational systems have been developed mainly by computer scientists based on logic, and notions such as “decision procedure”, “decidability”, and “computational complexity”.

Nowadays, the boundary between physical and computational systems is vanishing, since computation is more and more intertwined with our everyday physical world (cf. the notion of cyber-physical system). This makes it necessary for the boundary between the two research strands mentioned above to be overcome as well. In the talk, we discussed some examples of results obtained by the speaker that point into this direction, especially results, where inspiration from numerical analysis helps to solve problems that are considered undecidable by computer scientists [1–3].

References

1. Franek, P., Ratschan, S., Zgliczynski, P.: Quasi-decidability of a fragment of the first-order theory of real numbers. *J. Autom. Reason.* (2015). <http://dx.doi.org/10.1007/s10817-015-9351-3>
2. Ratschan, S.: Continuous first-order constraint satisfaction. In: Calmet, J., Benhamou, B., Caprotti, O., Henocque, L., Sorge, V. (eds.) *Artificial Intelligence, Automated Reasoning, and Symbolic Computation. LNCS*, vol. 2385, pp. 181–195. Springer, Berlin (2002)
3. Ratschan, S.: Safety verification of non-linear hybrid systems is quasi-decidable. *Formal Methods Syst. Des.* **44**(1), 71–90 (2014)

The research published in this paper was supported by GAČR grant 15-14484S and with institutional support RVO:67985807.

ORCID: 0000-0003-1710-1513

Congruence Testing of Point Sets in Three and Four Dimensions Results and Techniques

Günter Rote^(✉)

Institut für Informatik, Freie Universität Berlin
rote@inf.fu-berlin.de

Abstract. I will survey algorithms for testing whether two point sets are congruent, that is, equal up to an Euclidean isometry. I will introduce the important techniques for congruence testing, namely dimension reduction and pruning, or more generally, condensation. I will illustrate these techniques on the three-dimensional version of the problem, and indicate how they lead for the first time to an algorithm for four dimensions with near-linear running time (joint work with Heuna Kim). On the way, we will encounter some beautiful and symmetric mathematical structures, like the regular polytopes, and Hopf-fibrations of the three-dimensional sphere in four dimensions.

Contents

Invited Papers

Current Challenges in Developing Open Source Computer Algebra Systems . . .	3
<i>Janko Böhm, Wolfram Decker, Simon Keicher, and Yue Ren</i>	
Exploiting Structure in Floating-Point Arithmetic	25
<i>Claude-Pierre Jeannerod</i>	
Symbolic Geometric Reasoning with Advanced Invariant Algebras	35
<i>Hongbo Li</i>	
Congruence Testing of Point Sets in Three and Four Dimensions: Results and Techniques.	50
<i>Günter Rote</i>	

Curves and Surfaces

Mesh Reduction to Exterior Surface Parts via Random Convex-Edge Affine Features.	63
<i>Andreas Beyrer, Yu Liu, Hubert Mara, and Susanne Krömker</i>	
Numeric and Certified Isolation of the Singularities of the Projection of a Smooth Space Curve.	78
<i>Rémi Imbach, Guillaume Moroz, and Marc Pouget</i>	
Linear k -Monotonicity Preserving Algorithms and Their Approximation Properties.	93
<i>S.P. Sidorov</i>	

Applied Algebraic Geometry

Workspace Multiplicity and Fault Tolerance of Cooperating Robots	109
<i>Daniel A. Brake, Daniel J. Bates, Vakhtang Putkaradze, and Anthony A. Maciejewski</i>	
Numerical Local Irreducible Decomposition	124
<i>Daniel A. Brake, Jonathan D. Hauenstein, and Andrew J. Sommese</i>	
Computing the Chow Variety of Quadratic Space Curves.	130
<i>Peter Bürgisser, Kathlén Kohn, Pierre Lairez, and Bernd Sturmfels</i>	

Numerically Testing Generically Reduced Projective Schemes
for the Arithmetic Gorenstein Property. 137
Noah S. Daleo and Jonathan D. Hauenstein

Some Results Concerning the Explicit Isomorphism Problem
over Number Fields. 143
Péter Kutas

Cryptography

Implementing Cryptographic Pairings on Accumulator Based Smart
Card Architectures. 151
Peter Günther and Volker Krummel

Short Group Signatures with Distributed Traceability. 166
Johannes Blömer, Jakob Juhnke, and Nils Löken

On the Optimality of Differential Fault Analyses on CLEFIA. 181
Ágnes Kiss, Juliane Krämer, and Anke Stüber

Verified Numerical Computation

H^3 and H^4 Regularities of the Poisson Equation on Polygonal Domains 199
Takehiko Kinoshita, Yoshitaka Watanabe, and Mitsuhiro T. Nakao

Explicit Error Bound for Modified Numerical Iterated Integration by Means
of Sinc Methods 202
Tomoaki Okayama

Verified Computations for Solutions to Semilinear Parabolic Equations
Using the Evolution Operator. 218
*Akitoshi Takayasu, Makoto Mizuguchi, Takayuki Kubo,
and Shin'ichi Oishi*

Verified Error Bounds for the Real Gamma Function Using Double
Exponential Formula over Semi-infinite Interval 224
Naoya Yamanaka, Tomoaki Okayama, and Shin'ichi Oishi

Polynomial System Solving

Improving a CGS-QE Algorithm. 231
Ryoya Fukasaku, Hidenao Iwane, and Yosuke Sato

Efficient Subformula Orders for Real Quantifier Elimination
of Non-prenex Formulas 236
*Munehiro Kobayashi, Hidenao Iwane, Takuya Matsuzaki,
and Hirokazu Anai*

Solving Extended Ideal Membership Problems in Rings of Convergent Power Series via Gröbner Bases 252
Katsusuke Nabeshima and Shinichi Tajima

Advanced Algebraic Attack on Trivium 268
Frank-M. Quedenfeld and Christopher Wolf

Managing Massive Data

Compressing Big Data: When the Rate of Convergence to the Entropy Matters 285
Salvatore Aronica, Alessio Langiu, Francesca Marzi, Salvatore Mazzola, Filippo Mignosi, and Giulio Nazzicone

Trends in Temporal Reasoning: Constraints, Graphs and Posets 290
Jacqueline W. Daykin, Mirka Miller, and Joe Ryan

Reconstructing a Sparse Solution from a Compressed Support Vector Machine. 305
Joachim Giesen, Sören Laue, and Jens K. Mueller

Subquadratic-Time Algorithms for Abelian Stringology Problems 320
Tomasz Kociumaka, Jakub Radoszewski, and Bartłomiej Wiśniewski

Using Statistical Search to Discover Semantic Relations of Political Lexica – Evidences from Bulgarian-Slovak EUROPARL 7 Corpus 335
Velislava Stoykova

Computational Theory of Differential and Difference Equations

Simple Differential Field Extensions and Effective Bounds. 343
James Freitag and Wei Li

A New Bound for the Existence of Differential Field Extensions 358
Richard Gustavson and Omar León Sánchez

Dimension Polynomials of Intermediate Fields of Inversive Difference Field Extensions 362
Alexander Levin

A “Polynomial Shifting” Trick in Differential Algebra. 377
Gleb Pogudin

Data and Knowledge Exploration

Searching for Geometric Theorems Using Features Retrieved from Diagrams	383
<i>Wenya An, Xiaoyu Chen, and Dongming Wang</i>	
New Method for Instance Feature Selection Using Redundant Features for Biological Data	398
<i>Waad Bouaguel, Emna Mouelhi, and Ghazi Bel Mufti</i>	
Faceted Search for Mathematics	406
<i>Radu Hambasan and Michael Kohlhase</i>	
Evaluation of a Predictive Algorithm for Converting Linear Strings to Mathematical Formulae for an Input Method	421
<i>Shizuka Shirai and Tetsuo Fukui</i>	

Algorithm Engineering in Geometric Computing

Linear Programs and Convex Hulls Over Fields of Puiseux Fractions	429
<i>Michael Joswig, Georg Loho, Benjamin Lorenz, and Benjamin Schröter</i>	
Another Classroom Example of Robustness Problems in Planar Convex Hull Computation	446
<i>Marc Mörig</i>	
Precision-Driven Computation in the Evaluation of Expression-Dags with Common Subexpressions: Problems and Solutions	451
<i>Marc Mörig and Stefan Schirra</i>	

Real Complexity: Theory and Practice

Rigorous Numerical Computation of Polynomial Differential Equations Over Unbounded Domains	469
<i>Olivier Bournez, Daniel S. Graça, and Amaury Pouly</i>	
Using Taylor Models in Exact Real Arithmetic	474
<i>Franz Brauße, Margarita Korovina, and Norbert Müller</i>	
On the Computational Complexity of Positive Linear Functionals on $C[0; 1]$. . .	489
<i>Hugo Férée and Martin Ziegler</i>	
Average-Case Bit-Complexity Theory of Real Functions	505
<i>Matthias Schröder, Florian Steinberg, and Martin Ziegler</i>	
Certifying Trajectories of Dynamical Systems	520
<i>Joris van der Hoeven</i>	

Global Optimization

A New Matrix Splitting Based Relaxation for the Quadratic Assignment Problem 535
Marko Lange

Global Optimization of H_∞ Problems: Application to Robust Control Synthesis Under Structural Constraints. 550
Dominique Monnet, Jordan Ninin, and Benoit Clement

Global Optimization Based on Contractor Programming: An Overview of the *IBEX* Library. 555
Jordan Ninin

The Bernstein Branch-and-Prune Algorithm for Constrained Global Optimization of Multivariate Polynomial MINLPs. 560
Bhagyesh V. Patil

General Session

Maximum Likelihood Estimates for Gaussian Mixtures Are Transcendental . . . 579
Carlos Améndola, Mathias Drton, and Bernd Sturmfels

On the Quality of Some Root-Bounds 591
Prashant Batra

Relative Hilbert-Post Completeness for Exceptions 596
Jean-Guillaume Dumas, Dominique Duval, Burak Ekici, Damien Pous, and Jean-Claude Reynaud

Optimal Coverage in Automotive Configuration 611
Rouven Walter, Thore Kübart, and Wolfgang Kuchlin

Author Index 627