Lecture Notes in Computer Science 9582

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Springer

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

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: Chengi 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 Iliopoulous	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

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 Autonoma 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 Böhm[1(✉)], Wolfram Decker[1], Simon Keicher[2] and Yue Ren[1]

[1] University of Kaiserslautern, 67663 Kaiserslautern, Germany
{boehm, decker, ren}@mathematik.uni-kl.de
[2] Universidad de Concepción, Casilla 160-C, Concepción, Chile
simonkeicher@googlemail.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 the probing model (i.e.: every noisy leakage function can be simulated be 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)

Partly supported by the WELCOME/2010-4/2 grant founded within the framework of the EU Innovative Economy (National Cohesion Strategy) Operational Programme.

Solving Structured Polynomial Systems with Gröbner Bases

Jean-Charles Faugère

Inria, Equipe POLSYS, Centre Paris Rocquencourt, F-75005, Paris, France
Sorbonne Universits, 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 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

Data and Knowledge Exploration

Algorithm Engineering in Geometric Computing

Real Complexity: Theory and Practice

Global Optimization

General Session