

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board Members

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, Zurich, 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, Chennai, 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


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


Miroslav Ćirić · Manfred Droste ·
Jean-Éric Pin (Eds.)

Algebraic Informatics

8th International Conference, CAI 2019
Niš, Serbia, June 30 – July 4, 2019
Proceedings

Editors

Miroslav Ćirić 
University of Niš
Niš, Serbia

Manfred Droste 
University of Leipzig
Leipzig, Germany

Jean-Éric Pin
Université Paris Denis Diderot and CNRS
Paris, France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-21362-6 ISBN 978-3-030-21363-3 (eBook)
<https://doi.org/10.1007/978-3-030-21363-3>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2019

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, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

These proceedings contain the papers presented at the 8th International Conference on Algebraic Informatics (CAI 2019) held from June 30 to July 4, 2019, in Niš, Serbia, and organized under the auspices of the University of Niš and its Faculty of Science.

CAI is the biennial conference serving the community interested in the intersection of theoretical computer science, algebra, and related areas. As with the previous seven CAIs, the goal of CAI 2019 was to enhance the understanding of syntactic and semantic problems by algebraic models, as well as to propagate the application of modern techniques from computer science in algebraic computation.

This volume contains the abstracts of three invited lectures and 20 contributed papers that were presented at the conference. The invited lectures were given by Paul Gastin, Bane Vasić, and Franz Winkler. In total, 20 contributed papers were carefully selected from 35 submissions. The peer review process was single blind and each submission was reviewed by at least three, and on average 3.1, Program Committee members and additional reviewers. The papers report original unpublished research and cover a broad range of topics from automata theory and logic, cryptography and coding theory, computer algebra, design theory, natural and quantum computation, and related areas.

We are grateful to a great number of colleagues for making CAI 2019 a successful event. We would like to thank the members of the Steering Committee, the colleagues in the Program Committee and the additional reviewers for careful evaluation of the submissions, and all the authors for submitting high-quality papers. We would also thank Jelena Ignjatović, chair of the Organizing Committee, Ivan Stanković, who created and maintained the conference website, and all other members of the Organizing Committee, for a successful organization of the conference.

The reviewing process was organized using the EasyChair conference system created by Andrei Voronkov. We would like to acknowledge that this system helped greatly to improve the efficiency of the committee work.

Special thanks are due to Alfred Hofmann and Anna Kramer from Springer LNCS, who helped us to publish the proceedings of CAI 2019 in the LNCS series.

The sponsors of CAI 2019 are also gratefully acknowledged.

April 2019

Miroslav Ćirić
Manfred Droste
Jean-Éric Pin

Organization

CAI 2019 was organized by the Faculty of Sciences and Mathematics, University of Niš, Serbia.

Steering Committee

Symeon Bozapalidis	Aristotle University of Thessaloniki, Greece
Olivier Carton	Université Paris-Diderot, Paris, France
Manfred Droste	University of Leipzig, Germany
Zoltan Esik (Deceased)	University of Szeged, Hungary
Werner Kuich	Technical University of Vienna, Austria
Dimitrios Poulakis	Aristotle University of Thessaloniki, Greece
Arto Salomaa	University of Turku, Finland

Program Committee Chairs

Miroslav Ćirić	University of Niš, Serbia
Manfred Droste	University of Leipzig, Germany
Jean-Éric Pin	Université Paris-Diderot, CNRS, Paris, France

Program Committee

Claude Carlet	Université Paris 8, France
Charles Colbourn	Arizona State University, Tempe, USA
Zoltán Fülöp	University of Szeged, Hungary
Dora Giammarresi	Università di Roma Tor Vergata, Italy
Mika Hirvensalo	University of Turku, Finland
Lila Kari	University of Waterloo, Canada
Nataša Jonoska	University of South Florida, Tampa, USA
Dino Mandrioli	Politecnico di Milano, Italy
Miodrag Mihaljević	Mathematical Institute of the SASA, Belgrade, Serbia
Benjamin Monmege	Aix-Marseille Université, France
Lucia Moura	University of Ottawa, Canada
Dimitrios Poulakis	Aristotle University of Thessaloniki, Greece
Svetlana Puzynina	Saint Petersburg State University, Russia
George Rahonis	Aristotle University of Thessaloniki, Greece
Robert Rolland	Aix-Marseille Université, France
Kai Salomaa	Queen's University, Kingston, Canada
Rafael Sendra	University of Alcalá, Alcalá de Henares, Madrid, Spain
Dimitris Simos	SBA Research, Vienna, Austria
Branimir Todorović	University of Niš, Serbia

Bianca Truthe
Heiko Vogler
Mikhail Volkov

Justus Liebig University, Giessen, Germany
Technical University of Dresden, Germany
Ural Federal University, Ekaterinburg, Russia

Additional Reviewers

Johanna Björklund	Ludwig Kappel	Matteo Pradella
Eunice Chan	Nikos Karampetakis	Matthieu Rambaud
Siniša Crvenković	János Karsai	Ioannis Refanidis
Igor Dolinka	Hwee Kim	Ivan Szabolcs
Sven Dziadek	Christos Konaxis	Éric Schost
Margherita Maria Ferrari	Maria Madonia	David Sevilla
Kilian Gebhardt	Pavlos Marantidis	Jean-Marc Talbot
Gustav Grabolle	Pierrick Meaux	Pavlos Tzermias
Kishan Gupta	Irini-Eleftheria Mens	Sam van Gool
Tero Harju	Johann Mitteramskogler	Tamás Vinkó
Luisa Herrmann	Timothy Ng	Michael Wagner
Iiro Honkala	Paulina Paraponiari	Johannes Waldmann
Velimir Ilić	Erik Paul	Alfred Wassermann
Bryan Jurish	Martin Pavlovski	Markus Whiteland

Organizing Committee

Jelena Ignjatović (Chair)	Jelena Milovanović
Milan Bašić	Aleksandar Stamenković
Velimir Ilić	Stefan Stanimirović
Zorana Jančić	Ivan Stanković
Dejan Mančev	Lazar Stojković
Jelena Matejić	Aleksandar Trokicić
Ivana Micić	

Sponsoring Institutions

University of Niš
University of Niš – Faculty of Science
Ministry of Education, Science and Technological Development, Republic of Serbia

Abstracts of Invited Talks

Neural Network Decoding of Quantum LDPC Codes

Bane Vasić, Xin Xiao, and Nithin Raveendran

Department of Electrical and Computer Engineering,
Department of Mathematics, University of Arizona, Tucson
vasic@ece.arizona.edu
<http://www2.engr.arizona.edu/~vasic>

Quantum error correction (QEC) codes [1] are vital in protecting fragile qubits from decoherence. QEC codes are indispensable for practical realizations of fault tolerant quantum computing. Designing good QEC codes, and more importantly low-complexity high-performance decoders for those codes that can be constructed using lossy and noisy devices, is arguably the most important theoretical challenge in quantum computing, key-distribution and communications.

Quantum low-density parity check (QLDPC) codes [4] based on the stabilizer formalism [3] has led to a myriad of QLDPC codes whose constructions and decoding algorithms rely on classical LDPC codes and the theory of syndrome measurement based decoding of quantum stabilizer codes. QLDPC codes are a promising candidate for both quantum computing and quantum optical communications as they admit potentially simple local decoding algorithms, and the history of success in classical LDPC codes in admitting low-complexity decoding and near-capacity performance.

Traditional iterative message-passing algorithms for decoding of LDPC codes are based on *belief propagation* (BP) [5], and operate on a *Tanner graph* [6] of the code's parity check matrix. The BP, as an algorithm to compute marginals of functions on a graphical model, has its roots in the broad class of Bayesian inference problems [2]. While inference using BP is exact only on loop-free graphs (trees), and provides close approximations to exact marginals on loopy graphs with large girth, due to the topology of Tanner graphs of finite-length LDPC codes and additional constraints imposed by quantum version, the application of traditional BP for QEC codes in general, and for QLDPC codes in particular has some fundamental limitations.

Despite the promise of QLDPC codes for quantum information processing, they have several important current limitations. In this talk we will discuss these limitations and present a method to design practical low-complexity high-performance codes and decoders. Our approach is based on using neural networks (NN). The neural network performs the syndrome matching algorithm over a depolarizing channel with noiseless error syndrome measurements. We train our NN to minimize the bit error rate, which is an accurate metric to measure the performance of iterative decoders. In addition it uses straight through estimator (STE) technique to tackle the zero-gradient problem of the

objective function and outperforms conventional min-sum algorithm up to an order of magnitude of logical error rate.

Keywords: Quantum error correction · Quantum low-density parity check codes · Iterative decoding · Neural networks · Neural network decoding

References

1. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. *Phys. Rev. A* **54**, 1098–1105 (1996)
2. Frey, B.J.: *Graphical Models for Machine Learning and Digital Communication*. MIT Press, Cambridge (1998)
3. Gottesman, D.: Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A* **54**(3), 1862–1868 (1996)
4. MacKay, D., Mitchison, G., McFadden, P.: Sparse-graph codes for quantum error correction. *IEEE Trans. Inf. Theory* **50**(10), 2315–2330 (2004)
5. Pearl, J.: *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers Inc., San Francisco (1988)
6. Tanner, R.M.: A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory* **27**(5), 533–547 (1981)

Algebraic Differential Equations – Parametrization and Symbolic Solution

Franz Winkler

RISC, Johannes Kepler University Linz
franz.winkler@risc.jku.at

An algebraic differential equation (ADE) is a polynomial relation between a function, some of its partial derivatives, and the variables in which the function is defined. Regarding all these quantities as unrelated variables, the polynomial relation leads to an algebraic relation defining a hypersurface on which the solution is to be found. A solution in a certain class of functions, such as rational or algebraic functions, determines a parametrization of the hypersurface in this class. So in the algebro-geometric method we first decide whether a given ADE can be parametrized with functions from a given class; and in the second step we try to transform a parametrization into one respecting also the differential conditions.

This approach is called the algebro-geometric method for solving ADEs. It is relatively well understood for rational and algebraic solutions of single algebraic ordinary differential equations (AODEs). First steps are taken in a generalization to other types of solutions such as power series solution. Partial differential equations and systems of equations are the topic of current research.

References

1. Eremenko, A.: Rational solutions of first-order differential equations. *Annales Academiae Scientiarum Fennicae* **23**(1), 181–190 (1990)
2. Feng, R., Gao, X.S.: Rational general solutions of algebraic ordinary differential equations. In: Gutierrez, J. (ed.) *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation (ISSAC 2004)*, pp. 155–162. ACM Press, New York (2004)
3. Feng, R., Gao, X.S.: A polynomial time algorithm for finding rational general solutions of first order autonomous ODEs. *J. Symb. Comput.* **41**(7), 739–762 (2006)
4. Fuchs, L.: Über Differentialgleichungen, deren Integrale feste Verzweigungspunkte besitzen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* **11**(3), 251–273 (1884)
5. Grasegger, G., Lastra, A., Sendra, J.R., Winkler, F.: Rational general solutions of systems of first-order algebraic partial differential equations. *J. Comput. Appl. Math.* **331**, 88–103 (2018)
6. Grasegger, G., Vo, N.T.: An algebraic-geometric method for computing Zolotarev polynomials. In: Burr, M. (ed.) *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC 2017)*, pp. 173–180. ACM Press, New York (2017)
7. Kamke, E.: *Differentialgleichungen: Lösungsmethoden und Lösungen I*. B.G. Teubner, Stuttgart (1983)

8. Ngô, L.X.C., Sendra, J.R., Winkler, F.: Classification of algebraic ODEs with respect to rational solvability. *Contemp. Math.* **572**, 193–210 (2012)
9. Ngô, L.X.C., Sendra, J.R., Winkler, F.: Birational transformations preserving rational solutions of algebraic ordinary differential equations. *J. Comput. Appl. Math.* **286**, 114–127 (2015)
10. Ngô, L.X.C., Winkler, F.: Rational general solutions of first order non-autonomous parametrizable ODEs. *J. Symb. Comput.* **45**(12), 1426–1441 (2010)
11. Ngô, L.X.C., Winkler, F.: Rational general solutions of planar rational systems of autonomous ODEs. *J. Symb. Comput.* **46**(10), 1173–1186 (2011)
12. Sendra, J.R., Winkler, F., Pérez-D az, S.: *Rational Algebraic Curves – A Computer Algebra Approach*. Springer-Verlag, Heidelberg (2008)
13. Vo, N.T., Grasegger, G., Winkler, F.: Deciding the existence of rational general solutions for first-order algebraic ODEs. *J. Symb. Comput.* **87**, 127–139 (2018)
14. Winkler, F.: *Polynomial Algorithms in Computer Algebra*. Springer-Verlag, Wien (1996)

Contents

Invited Paper

Modular Descriptions of Regular Functions	3
<i>Paul Gastin</i>	

Contributed Papers

Enhancing an Attack to DSA Schemes	13
<i>Marios Adamoudis, Konstantinos A. Draziotis, and Dimitrios Poulakis</i>	
Constraint Satisfaction Through GBP-Guided Deliberate Bit Flipping	26
<i>Mohsen Bahrami and Bane Vasić</i>	
On the Diffusion Property of the Improved Generalized Feistel with Different Permutations for Each Round	38
<i>Tsonka Baicheva and Svetlana Topalova</i>	
Fast Computing the Algebraic Degree of Boolean Functions.	50
<i>Valentin Bakoev</i>	
On the Scalar Complexity of Chudnovsky ² Multiplication Algorithm in Finite Fields	64
<i>Stéphane Ballet, Alexis Bonnetcaze, and Thanh-Hung Dang</i>	
Maximal Diameter on a Class of Circulant Graphs	76
<i>Milan Bašić, Aleksandar Ilić, and Aleksandar Stamenković</i>	
Parallelisms of $PG(3, 4)$ Invariant Under Cyclic Groups of Order 4.	88
<i>Anton Betten, Svetlana Topalova, and Stela Zhelezova</i>	
Bounds on Covering Codes in RT Spaces Using Ordered Covering Arrays	100
<i>André Guerino Castoldi, Emerson Luiz do Monte Carmelo, Lucia Moura, Daniel Panario, and Brett Stevens</i>	
Detecting Arrays for Main Effects.	112
<i>Charles J. Colbourn and Violet R. Syrotiuk</i>	
Regular Languages as Local Functions with Small Alphabets	124
<i>Stefano Crespi Reghizzi and Pierluigi San Pietro</i>	

Rational Weighted Tree Languages with Storage and the Kleene-Goldstine Theorem	138
<i>Zoltán Fülöp and Heiko Vogler</i>	
Commutative Regular Languages – Properties and State Complexity	151
<i>Stefan Hoffmann</i>	
Algebraic Systems Motivated by DNA Origami	164
<i>James Garrett, Nataša Jonoska, Hwee Kim, and Masahico Saito</i>	
Algebraic Models for Arbitrary Strength Covering Arrays over v -ary Alphabets	177
<i>Ludwig Kampel, Dimitris E. Simos, Bernhard Garn, Ilias S. Kotsireas, and Evgeny Zhereshchin</i>	
The Precise Complexity of Finding Rainbow Even Matchings	190
<i>Martin Loebl</i>	
New Cryptocodes for Burst Channels	202
<i>Daniela Mechkaroska, Aleksandra Popovska-Mitrovikj, and Verica Bakeva</i>	
Zeroing Neural Network Based on the Equation $AXA = A$	213
<i>Marko D. Petković and Predrag S. Stanimirović</i>	
An Application of Computer Algebra and Dynamical Systems	225
<i>Predrag S. Stanimirović, Yimin Wei, Dejan Kolundžija, Juan Rafael Sendra, and Juana Sendra</i>	
Intersecting Two Quadrics with GeoGebra	237
<i>Alexandre Trocado, Laureano Gonzalez-Vega, and José Manuel Dos Santos</i>	
Randomized Nyström Features for Fast Regression: An Error Analysis	249
<i>Aleksandar Trokicić and Branimir Todorović</i>	
Author Index	259