

Contents

Foundation of Algorithms in Mathematics, Engineering and Scientific Computation

Automated Reasoning for Knot Semigroups and π -orbifold Groups of Knots	3
<i>Alexei Lisitsa and Alexei Vernitski</i>	
Balancing Expression Dags for More Efficient Lazy Adaptive Evaluation . . .	19
<i>Martin Wilhelm</i>	
Certification Using Newton-Invariant Subspaces	34
<i>Jonathan D. Hauenstein</i>	
Decomposition of Low Rank Multi-symmetric Tensor	51
<i>Jouhayna Harmouch, Bernard Mourrain, and Houssam Khalil</i>	
Dimension Quasi-polynomials of Inversive Difference Field Extensions with Weighted Translations	67
<i>Alexander Levin</i>	
Efficient Certification of Numeric Solutions to Eigenproblems	81
<i>Joris van der Hoeven and Bernard Mourrain</i>	
Fast Chinese Remaindering in Practice.	95
<i>Joris van der Hoeven</i>	
Homotopies for Connected Components of Algebraic Sets with Application to Computing Critical Sets	107
<i>Daniel J. Bates, Dani A. Brake, Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler</i>	
Implementing Fast Carryless Multiplication	121
<i>Joris van der Hoeven, Robin Larrieu, and Grégoire Lecerf</i>	
Improving Enclosure of Interval Scalar Projection Operation	137
<i>Tomasz Dobrowolski</i>	
Integrating Algebraic and SAT Solvers	147
<i>Jan Horáček, Jan Burchard, Bernd Becker, and Martin Kreuzer</i>	
Isabelle Formalization of Set Theoretic Structures and Set Comprehensions	163
<i>Cezary Kaliszyk and Karol Pąk</i>	

Jordan Canonical Form with Parameters from Frobenius Form with Parameters	179
<i>Robert M. Corless, Marc Moreno Maza, and Steven E. Thornton</i>	
Knowledge-Based Interoperability for Mathematical Software Systems	195
<i>Michael Kohlhase, Luca De Feo, Dennis Müller, Markus Pfeiffer, Florian Rabe, Nicolas M. Thiéry, Victor Vasilyev, and Tom Wiesing</i>	
On Interval Methods with Zero Rewriting and Exact Geometric Computation	211
<i>Stefan Schirra and Martin Wilhelm</i>	
Sparse Rational Function Interpolation with Finitely Many Values for the Coefficients	227
<i>Qiao-Long Huang and Xiao-Shan Gao</i>	
Virtual Theories – A Uniform Interface to Mathematical Knowledge Bases	243
<i>Tom Wiesing, Michael Kohlhase, and Florian Rabe</i>	
On Real Roots Counting for Non-radical Parametric Ideals.	258
<i>Ryoya Fukasaku and Yosuke Sato</i>	
On the Bit-Size of Non-radical Triangular Sets	264
<i>Xavier Dahan</i>	
Rapidly Convergent Integrals and Function Evaluation	270
<i>Heba al Kafri, David J. Jeffrey, and Robert M. Corless</i>	
Stirling Numbers, Lambert W and the Gamma Function	275
<i>David J. Jeffrey and Nick Murdoch</i>	
The Potential and Challenges of CAD with Equational Constraints for SC-Square.	280
<i>James H. Davenport and Matthew England</i>	
Combinatorics and Codes in Computer Science	
New Small 4-Designs with Nonabelian Automorphism Groups	289
<i>Vedran Krčadinac and Mario Osvin Pavčević</i>	
On Classifying Steiner Triple Systems by Their 3-Rank.	295
<i>Dieter Jungnickel, Spyros S. Magliveras, Vladimir D. Tonchev, and Alfred Wassermann</i>	
Right-Justified Characterization for Generating Regular Pattern Avoiding Permutations.	306
<i>Phan Thuan Do, Thi Thu Huong Tran, and Vincent Vajnovszki</i>	

Experimental Study of the Ehrhart Interpolation Polytope.	320
<i>Vissarion Fisikopoulos and Zafeirakis Zafeirakopoulos</i>	
On Testing Isomorphism of Graphs of Bounded Eigenvalue Multiplicity	325
<i>Takunari Miyazaki</i>	
Data Modeling and Analysis	
A Simple Streaming Bit-Parallel Algorithm for Swap Pattern Matching	333
<i>Václav Blažej, Ondřej Suchý, and Tomáš Valla</i>	
Epidemic Intelligence Statistical Modelling for Biosurveillance.	349
<i>Christina Parpoula, Alex Karagrigoriou, and Angeliki Lambrou</i>	
Mining Acute Stroke Patients' Data Using Supervised Machine Learning. . . .	364
<i>Ritu Kundu and Toktam Mahmoodi</i>	
Parallel and Robust Empirical Risk Minimization via the Median Trick	378
<i>Alexander Kogler and Patrick Traxler</i>	
Mathematical Aspects of Information Security and Cryptography	
Leakage-Resilient Riffle Shuffle	395
<i>Paweł Lorek, Michał Kulis, and Filip Zagórski</i>	
Ordinary Pairing-Friendly Genus 2 Hyperelliptic Curves with Absolutely Simple Jacobians.	409
<i>Georgios Fotiadis and Elisavet Konstantinou</i>	
Statistical Testing of PRNG: Generalized Gambler's Ruin Problem	425
<i>Paweł Lorek, Marcin Słowik, and Filip Zagórski</i>	
Subtleties in Security Definitions for Predicate Encryption with Public Index	438
<i>Johannes Blömer and Gennadij Liske</i>	
Code-Based Key Encapsulation from McEliece's Cryptosystem	454
<i>Edoardo Persichetti</i>	
Author Index	461

Mathematical Aspects of Computer and Information
Sciences

7th International Conference, MACIS 2017, Vienna,
Austria, November 15-17, 2017, Proceedings

Blömer, J.; Kotsireas, I.S.; Kutsia, T.; Simos, D.E. (Eds.)

2017, XI, 462 p. 71 illus., Softcover

ISBN: 978-3-319-72452-2