

Lecture Notes in Artificial Intelligence 5081

Edited by R. Goebel, J. Siekmann, and W. Wahlster

Subseries of Lecture Notes in Computer Science

Deepak Kapur (Ed.)

Computer Mathematics

8th Asian Symposium, ASCM 2007
Singapore, December 15-17, 2007
Revised and Invited Papers

Series Editors

Randy Goebel, University of Alberta, Edmonton, Canada

Jörg Siekmann, University of Saarland, Saarbrücken, Germany

Wolfgang Wahlster, DFKI and University of Saarland, Saarbrücken, Germany

Volume Editor

Deepak Kapur

University of New Mexico, Department of Computer Science

Albuquerque, NM 87131-0001, USA

E-mail: kapur@cs.unm.edu

Library of Congress Control Number: 2008935385

CR Subject Classification (1998): I.2.2, I.1-2, F.4.1, G.2, I.6

LNCS Sublibrary: SL 7 – Artificial Intelligence

ISSN 0302-9743

ISBN-10 3-540-87826-2 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-87826-1 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12524266 06/3180 5 4 3 2 1 0

Preface

This volume contains the proceedings of the Eighth Asian Symposium on Computer Mathematics (ASCM 2007), which was held at the Grand Plaza Park Hotel City Hall, Singapore, December 15–17, 2007. Previous ASCM meetings were held in Beijing, China (1995), Kobe, Japan (1996), Lanzhou, China (1998), Chiang Mai, Thailand (2000), Matsuyama, Japan (2001), Beijing, China (2003), and Seoul, Korea (2005).

Amongst 65 submissions by authors from 20 mostly Asian countries, the Program Committee selected 23 regular papers and 13 posters for presentation at the symposium. The presentations and papers went through another round of reviewing after the symposium, and 22 regular papers and five short papers on posters were selected for the proceedings. The international Program Committee of ASCM 2007 had strong Asian participation, and the reviewing process was aided by numerous reviewers from around the world. I am very grateful to the Program Committee members and the reviewers for their work in evaluating the submissions before and after the conference.

In addition to contributed papers, ASCM 2007 had three invited talks—by Rida Farouki on computational geometry, by Xiaoyun Wang on cryptology, and by Georges Gonthier on a computer proof of the celebrated Four Color Theorem. I would like to thank the speakers for their excellent talks. A paper by Prof. Farouki and his coauthors is included in the proceedings. Prof. Wang’s research activities and publications can be found at her home page http://www.infosec.sdu.edu.cn/2person_wangxiaoyun2.htm. Details about Dr. Gonthier’s computerized proof of the four color theorem can be found by visiting his home page <http://research.microsoft.com/~gonthier>.

It is my hope that ASCM continues to provide a forum for participants, especially from Asia, to present original research, to learn about new developments, and to exchange ideas and views on doing mathematics with computers.

ASCM 2007 was organized by the School of Computing of the National University of Singapore, and supported by the Lee Foundation, Kim Seng Holdings, and the Institute of Systems Science, Beijing, China. I thank Eng-Wee Chionh, who served as the General Chair, and the staff of the School of Computing of the National University of Singapore. Finally, I am grateful to Stephan Falke for his help in preparing this volume.

June 2008

Deepak Kapur

Conference Organization

Program Chair

Deepak Kapur University of New Mexico, USA

Program Committee

Manindra Agarwal	IIT Kanpur, India
Leonid Bokut	Sobolev Institute, Russia
Shang-Ching Chou	Wichita State University, USA
Falai Chen	University of Science and Technology of China, China
Guoting Chen	University of Lille I, France
Eng-Wee Chionh	National University of Singapore, Singapore
Andreas Dolzmann	University of Passau, Germany
Ding-Zhu Du	University of Texas at Dallas, USA
Xiao-Shan Gao	Chinese Academy of Sciences, China
Shuhong Gao	Clemson University, USA
Keith Geddes	University of Waterloo, Canada
Vladimir Gerdt	Joint Institute for Nuclear Research, Russia
Hoon Hong	North Carolina State University, USA
Jieh Hsiang	National Taiwan University, Taiwan
Tetsuo Ida	University of Tsukuba, Japan
Seok-Jin Kang	Seoul National University, Korea
Yonggu Kim	Chonnam National University, Korea
Wen-shin Lee	University of Antwerp, Belgium
Ziming Li	Chinese Academy of Sciences, China
Mirosław Majewski	NYIT Abu Dhabi, United Arab Emirates
Matu-Tarow Noda	Ehime Campus Information Services, Japan
Tobias Nipkow	Technical University of Munich, Germany
Hoang Xuan Phu	Academy of Science and Technology, Vietnam
Raja Natarajan	Tata Institute of Fundamental Research, India
Meera Sitharam	University of Florida, USA
Lim Yohanes Stefanus	University of Indonesia, Indonesia
Nobuki Takayama	Kobe University, Japan
Toby Walsh	National ICT, Australia
Dongming Wang	Beihang University, China and CNRS, France
Chaoping Xing	National University of Singapore, Singapore
Lu Yang	East China Normal University, China
Kazuhiro Yokoyama	Rikkyo University, Japan
Jianmin Zheng	Nanyang Technological University, Singapore

Conference Chairs

Eng-Wee Chionh	National University of Singapore, Singapore
Huaxiong Wang	Nanyang Technological University, Singapore

Publicity Chair

Dingkang Wang	Chinese Academy of Sciences, China
---------------	------------------------------------

Local Organizing Committee

Secretariat	Stefanie Ng, Judy Ng
Web, CMT	Zaini Bin Mohammad
Finance	Lay Khim Chng, Noraiszah Hamzah, Rachel Goh
CD, Abstracts	Alexia Leong
Web Registration	Philip Lim
Audio-visual	Bernard Tay, Mohamad Nazri Bin Sulaiman, Chin Ming Chow

External Reviewers

John Abbott	Pavel Pech
Alkiviadis Akritas	John Perry
Amir Amiraslani	Gerhard Pfister
Hirokazu Anai	Krishna Sankaranarayana
Saugata Basu	Eric Schost
Anna Bigatti	Wolfgang Schreiner
Peter Borwein	Naresh Sharma
François Boulier	G. Sivakumar
Jacek Chrzaszcz	K. V. Subrahmanyam
Xavier Dahan	Laurent Théry
Jiansong Deng	Vlad Timofte
Rida Farouki	Michel Toulouse
Mitsushi Fujimoto	Ping-Sing Tsai
Laureano González Vega	Regina Tyshkevich
Benjamin Gregoire	Luca Vigano
Markus Hitz	Dingkang Wang
Fangjian Huang	Wenping Wang
Dorothy Kucar	Xingmao Wang
Alexander Boris Levin	Joab Winkler
Yongbin Li	Min Wu
Bao Liu	Yuzhen Xie
Igor Markov	Pingkun Yan
Marc Moreno Maza	Noson Yanofsky
A. S. Vasudeva Murthy	Alberto Zanoni
Masayuki Noro	Zhengbing Zeng
Wei Pan	

Table of Contents

Algorithms and Implementations

Computing the Minkowski Value of the Exponential Function over a Complex Disk	1
<i>Hyeong In Choi, Rida T. Farouki, Chang Yong Han, and Hwan Pyo Moon</i>	
Unconstrained Parametric Minimization of a Polynomial: Approximate and Exact.....	22
<i>S. Liang and D.J. Jeffrey</i>	
The Nearest Real Polynomial with a Real Multiple Zero in a Given Real Interval	32
<i>Hiroshi Sekigawa</i>	
Practical and Theoretical Issues for the Computation of Generalized Critical Values of a Polynomial Mapping	42
<i>Mohab Safey El Din</i>	
Which Symmetric Homogeneous Polynomials Can Be Proved Positive Semi-definite by Difference Substitution Method?	57
<i>Liangyu Chen and Zhenbing Zeng</i>	
Basis-Independent Polynomial Division Algorithm Applied to Division in Lagrange and Bernstein Basis	72
<i>Manfred Minimair</i>	
Computing the Greatest Common Divisor of Polynomials Using the Comrade Matrix	87
<i>Nor'aini Aris and Shamsatun Nahar Ahmad</i>	
Efficient Algorithms for Computing Noether Normalization	97
<i>Amir Hashemi</i>	
Stability of GPBiCG_AR Method Based on Minimization of Associate Residual	108
<i>Moe Thuthu and Seiji Fujino</i>	
Evaluation of a Java Computer Algebra System.....	121
<i>Heinz Kredel</i>	
A New Property of Hamming Graphs and Mesh of d -ary Trees.....	139
<i>Alain Bretto, Cerasela Jaulin, Luc Gillibert, and Bernard Laget</i>	

Numerical Methods and Applications

An Interpolation Method That Minimizes an Energy Integral of Fractional Order	151
<i>H. Gunawan, F. Pranolo, and E. Rusyaman</i>	
Solving Biomechanical Model Using Third-Order Runge-Kutta Methods	163
<i>R.R. Ahmad, A.S. Rambely, and L.H. Lim</i>	
An Efficient Fourth Order Implicit Runge-Kutta Algorithm for Second Order Systems	169
<i>Basem S. Attili</i>	
Laplace Equation Inside a Cylinder: Computational Analysis and Asymptotic Behavior of the Solution	179
<i>Suvra Sarkar and Sougata Patra</i>	
A Method and Its Implementation for Constructing Bäcklund Transformations to Nonlinear Evolution Equations	188
<i>Zhibin Li, Yinping Liu, and Haifeng Qian</i>	
On the Invariant Properties of Hyperbolic Bivariate Third-Order Linear Partial Differential Operators	199
<i>Ekaterina Shemyakova and Franz Winkler</i>	
Symbolic Solution to Magnetohydrodynamic Hiemenz Flow in Porous Media	213
<i>Seripah Awang Kechil and Ishak Hashim</i>	
Local Similarity Solutions for Laminar Boundary Layer Flow along a Moving Cylinder in a Parallel Stream	224
<i>Anuar Ishak, Roslinda Nazar, and Ioan Pop</i>	

Elimination: Triangular Forms, Resultants, Equation Solving

An Algorithm for Transforming Regular Chain into Normal Chain	236
<i>Banghe Li and Dingkang Wang</i>	
A Modified Van der Waerden Algorithm to Decompose Algebraic Varieties and Zero-Dimensional Radical Ideals	246
<i>Jia Li and Xiao-Shan Gao</i>	
Regular Decompositions	263
<i>Guillaume Moroz</i>	
Floating-Point Gröbner Basis Computation with Ill-conditionedness Estimation	278
<i>Tateaki Sasaki and Fujio Kako</i>	

The Maximality of the Dixon Matrix on Corner-Cut Monomial Supports	293
<i>Eng-Wee Chionh</i>	

Properties of Ascending Chains for Partial Difference Polynomial Systems	307
<i>Gui-Lin Zhang and Xiao-Shan Gao</i>	

Cryptology

Some Mathematical Problems in Cryptanalysis	322
<i>Xiaoyun Wang</i>	
A Reduction Attack on Algebraic Surface Public-Key Cryptosystems ...	323
<i>Maki Iwami</i>	

Computational Logic

The Four Colour Theorem: Engineering of a Formal Proof.....	333
<i>Georges Gonthier</i>	
On the Computation of Elimination Ideals of Boolean Polynomial Rings.....	334
<i>Yosuke Sato, Akira Nagai, and Shutaro Inoue</i>	
Computer Search for Large Sets of Idempotent Quasigroups	349
<i>Feifei Ma and Jian Zhang</i>	

Author Index	359
---------------------------	-----