Lecture Notes in Computer Science 3967

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

Editorial Board

David Hutchison
Lancaster University, 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, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Dima Grigoriev John Harrison
Edward A. Hirsch (Eds.)

Computer Science – Theory and Applications

First International Computer Science
Symposium in Russia, CSR 2006
St. Petersburg, Russia, June 8-12, 2006
Proceedings

Springer

Volume Editors

Dima Grigoriev
Université de Rennes, IRMAR
Campus de Beaulieu, 35042 Rennes, Cedex, France
E-mail: dimitri.grigoriev@math.univ-rennes1.fr

John Harrison
Intel Corporation
JF1-13, 2111 NE 25th Avenue, Hillsboro, OR 97124, USA
E-mail: johnh@ichips.intel.com

Edward A. Hirsch
Steklov Institute of Mathematics at St. Petersburg
27 Fontanka, St. Petersburg, 191023, Russia
E-mail: hirsch@pdmi.ras.ru

Library of Congress Control Number: 2006925113

CR Subject Classification (1998): F.1.1-2, F.2.1-2, F.4.1, I.2.6, J.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-34166-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34166-6 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 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11753728 06/3142 5 4 3 2 1 0

Preface

The International Symposium on Computer Science in Russia (CSR 2006) was held on June 8–12, 2006 in St. Petersburg, Russia, hosted by the Steklov Institute of Mathematics at St. Petersburg. It was the first event in a planned series of regular international meetings that are united by their location (Russia).

The symposium was composed of two tracks: Theory and Applications/Technology. The opening lecture was given by Stephen A. Cook and ten other invited plenary lectures were given by Boaz Barak, Gerard Berry, Bob Colwell, Byron Cook, Melvin Fitting, Russell Impagliazzo, Michael Kaminski, Michael Kishinevsky, Pascal Koiran, and Omer Reingold. This volume contains the accepted papers of both tracks and also some of the abstracts of the invited speakers. The scope of the proposed topics for the symposium was quite broad and covered basically all areas of computer science and its applications. We received 279 papers in total, the contributors being from 45 countries. The Program Committee of the Theory Track selected 35 papers out of 121 submissions. The Program Committee of the Applications/Technology Track selected 29 papers out of 158 submissions.

Two workshops were co-located with CSR 2006:

- Workshop on Words and Automata (WOWA 2006);
- Tutorial on Automata-Based Programming.

The reviewing process was organized using the EasyChair conference system, thanks to Andrei Voronkov.

We are grateful to our sponsors:

- The U.S. Civilian Research & Development Foundation;
- Russian Foundation for Basic Research.

We also thank the local Organizing Committee: Dmitry Karpov, Arist Kojevnikov, Alexander Kulikov, Yury Lifshits, Sergey Nikolenko, Svetlana Obraztsova, Alexei Pastor, and, in particular, Elena Novikova.

March 2006

Dima Grigoriev
John R. Harrison
Edward A. Hirsch

Organization

Program Committee

Theory Track

Sergei Artemov	*Graduate Center CUNY, USA*
Paul Beame	*University of Washington, USA*
Michael Ben-Or	*The Hebrew University, Israel*
Andrei Bulatov	*Simon Fraser University, Canada*
Peter Bürgisser	*Paderborn, Germany*
Felipe Cucker	*City University of Hong Kong, China*
Evgeny Dantsin	*Roosevelt University, USA*
Volker Diekert	*Stuttgart, Germany*
Dima Grigoriev (Chair)	CNRS, IRMAR, *Rennes, France*
Yuri Gurevich	*Microsoft Research, USA*
Johann A. Makowsky	*Technion – Israel Institute of Technology, Israel*
Yuri Matiyasevich	*Steklov Institute/St.Petersburg, Russia*
Peter Bro Miltersen	*Aarhus, Denmark*
Grigori Mints	*Stanford, USA*
Pavel Pudlák	*Prague, Czech Republic*
Prabhakar Raghavan	*Verity Inc., USA*
Alexander Razborov	*IAS, USA and Steklov Institute/Moscow, Russia*
Michael E. Saks	*Rutgers, USA*
Alexander Shen	*LIF CNRS, France and Moscow, Russia*
Amin Shokrollahi	*EPF Lausanne, Switzerland*
Anatol Slissenko	*Paris-12, France*
Mikhail Volkov	*Ural State University, Russia*

Applications and Technology Track

Boris Babayan	*Intel, Russia*
Robert T. Bauer	*PSU, USA*
Matthias Blume	*Toyota Technological Institute, USA*
Walter Daelemans	*Antwerpen, Belgium*
Vassil Dimitrov	*Calgary, Canada*
Richard Fateman	*Berkeley, USA*
Dina Goldin	*University of Connecticut, USA*
John R. Harrison (Chair)	*Intel, USA*
John Mashey	*Techviser, USA*
Bertrand Meyer	*ETH Zurich, Switzerland and Eiffel Software, USA*
Fedor Novikov	*St. Petersburg State Polytechnical University, Russia*
Michael Parks	*Sun Microsystems, USA*

Andreas Reuter	*European Media Laboratory, Germany*
Mary Sheeran	*Chalmers University of Technology, Sweden*
Elena Troubitsyna	*Åbo Akademi University, Finland*
Miroslav Velev	*Carnegie Mellon University, USA*
Sergey Zhukov	*Transas, Russia*

Conference Chair

Edward A. Hirsch	*Steklov Institute/St. Petersburg, Russia*

Steering Committee for CSR Conferences

Anna Frid	*Sobolev Institute/Novosibirsk, Russia*
Edward A. Hirsch	*Steklov Institute/St. Petersburg, Russia*
Juhani Karhumäki	*Turku, Finland*
Mikhail Volkov	*Ural State University, Russia*

Referees

Emrah Acar
Noga Alon
Jean-Paul Allouche
Eugene Asarin
Maxim Babenko
Laurent Bartholdi
Reuven Bar-Yehuda
Danièle Beauquier
Magnus Björk
Johannes Borgstroem
Ahmed Bouajjani
Mihai Budiu
Eduardo Camponogara
Olivier Carton
Hsun-Hsien Chang
Swarat Chaudhuri
Alessandra Cherubini
David Chung
Joëlle Cohen
Richard Cole
Stephen A. Cook
Matteo Corti
Maxime Crochemore
Stefan Dantchev
Junxiong Deng
Amer Diwan
Niklas Eèn
Robert Elsaesser
Henning Fernau
Eldar Fischer
Morten Fjeld
Lance Fortnow
Ian Foster
Anna Frid
Joaquim Gabarro
Healfdene Goguen
Raphael Hauser
Rogardt Heldal
Ulrich Hertrampf
John Hughes
Piotr Indyk
Alon Itai
David Janin
Michael Kaminski
Graham Kemp
Barbara König
Teresa Krick
Manfred Kufleitner

Oliver Kullmann
Daniel Larsson
Dan Li
Yury Lifshits
Alexei Lisitsa
Anders Logg
Markus Lohrey
Martin Lotz
Sus Lundgren
Sergio Maffeis
David McAllester
Burkhard Monien
S. Muthu Muthukrishnan
Lorenz Minder
Anca Muscholl
Francesco Zappa Nardelli
Bengt Nordström
Dirk Nowotka
Matti Nykänen
Christos Papadimitriou
Holger Petersen
Rossella Petreschi
Franck Pommereau
Chung Keung Poon
Harald Raecke
Deva Ramanan
Dror Rawitz
Jan Reimann
Angelo Restificar
Søren Riis
Philip Ruemmer
Igor Rystsov
Viktor Sabelfeld
Ashish Sabharwal
Arseny Shur
Terence Sim
Jan Smith
Niklas Sörensson
Arne Storjohann
Karsten Tiemann
Michael Tiomkin
Siegbert Tiga
Paul Vitanyi
Nicolai Vorobjov
Vladimir Vovk
Vladimir Vyugin
Chao Wang
Zhenghong Wang
Alexander Wolpert
Hideki Yamasaki
Martin Ziegler
Silvano Dal Zilio Uri Zwick

Sponsors

The U.S. Civilian Research & Development Foundation.
Russian Foundation for Basic Research.

Table of Contents

Invited Papers

Non-black-box Techniques in Cryptography
Boaz Barak 1

Complexity of Polynomial Multiplication over Finite Fields
Michael Kaminski 2

Synchronous Elastic Circuits
Mike Kishinevsky, Jordi Cortadella, Bill Grundmann, Sava Krstić, John O'Leary 3

Theory Track

SZK Proofs for Black-Box Group Problems
V. Arvind, Bireswar Das 6

Canonical Decomposition of a Regular Factorial Language
S.V. Avgustinovich, A.E. Frid 18

Acyclic Bidirected and Skew-Symmetric Graphs: Algorithms and Structure
Maxim A. Babenko 23

Inductive Type Schemas as Functors
Freiric Barral, Sergei Soloviev 35

Unfolding Synthesis of Asynchronous Automata
Nicolas Baudru, Rémi Morin 46

Conjugacy and Equivalence of Weighted Automata and Functional Transducers
Marie-Pierre Béal, Sylvain Lombardy, Jacques Sakarovitch 58

Applications of the Linear Matroid Parity Algorithm to Approximating Steiner Trees
Piotr Berman, Martin Fürer, Alexander Zelikovsky 70

Tuples of Disjoint NP-Sets
Olaf Beyersdorff 80

Constructive Equivalence Relations on Computable Probability Measures
Laurent Bienvenu 92

Planar Dimer Tilings
Olivier Bodini, Thomas Fernique 104

The Complexity of Equality Constraint Languages
Manuel Bodirsky, Jan Kára 114

Window Subsequence Problems for Compressed Texts
Patrick Cégielski, Irène Guessarian, Yury Lifshits, Yuri Matiyasevich 127

Efficient Algorithms in Zero-Characteristic for a New Model of Representation of Algebraic Varieties
Alexander L. Chistov 137

Relativisation Provides Natural Separations for Resolution-Based Proof Systems
Stefan Dantchev 147

Bounded-Degree Forbidden Patterns Problems Are Constraint Satisfaction Problems
Stefan Dantchev, Florent Madelaine 159

Isolation and Reducibility Properties and the Collapse Result
Sergey M. Dudakov 171

Incremental Branching Programs
Anna Gál, Michal Koucký, Pierre McKenzie 178

Logic of Proofs for Bounded Arithmetic
Evan Goris 191

On a Maximal NFA Without Mergible States
Igor Grunsky, Oleksiy Kurganskyy, Igor Potapov 202

Expressiveness of Metric Modalities for Continuous Time
Yoram Hirshfeld, Alexander Rabinovich 211

Extending Dijkstra's Algorithm to Maximize the Shortest Path by Node-Wise Limited Arc Interdiction
Leonid Khachiyan, Vladimir Gurvich, Jihui Zhao 221

Weighted Logics for Traces
Ingmar Meinecke 235

On Nonforgetting Restarting Automata That Are Deterministic and/or Monotone
Hartmut Messerschmidt, Friedrich Otto 247

Unwinding a Non-effective Cut Elimination Proof
Grigori Mints 259

Enumerate and Expand: Improved Algorithms for Connected Vertex Cover and Tree Cover
Daniel Mölle, Stefan Richter, Peter Rossmanith 270

Shannon Entropy vs. Kolmogorov Complexity
An. Muchnik, N. Vereshchagin 281

Language Equations with Symmetric Difference
Alexander Okhotin 292

On Primitive Recursive Realizabilities
Valery Plisko 304

Evidence Reconstruction of Epistemic Modal Logic S5
Natalia Rubtsova 313

Linear Temporal Logic with Until and Before on Integer Numbers, Deciding Algorithms
V. Rybakov 322

On the Frequency of Letters in Morphic Sequences
Kalle Saari 334

Functional Equations in Shostak Theories
Sergey P. Shlepakov 346

All Semi-local Longest Common Subsequences in Subquadratic Time
Alexander Tiskin 352

Non-approximability of the Randomness Deficiency Function
Michael A. Ustinov 364

Multi-agent Explicit Knowledge
Tatiana Yavorskaya (Sidon) 369

Applications and Technology Track

Polarized Subtyping for Sized Types
Andreas Abel 381

Neural-Network Based Physical Fields Modeling Techniques
Konstantin Bournayev 393

Approximate Methods for Constrained Total Variation Minimization
Xiaogang Dong, Ilya Pollak 403

Dynamic Isoline Extraction for Visualization of Streaming Data
Dina Goldin, Huayan Gao 415

Improved Technique of IP Address Fragmentation Strategies for DoS Attack Traceback
Byung-Ryong Kim, Ki-Chang Kim 427

Performance Comparison Between Backpropagation, Neuro-Fuzzy Network, and SVM
Yong-Guk Kim, Min-Soo Jang, Kyoung-Sic Cho, Gwi-Tae Park 438

Evolutionary Multi-objective Optimisation by Diversity Control
Pasan Kulvanit, Theera Piroonratana, Nachol Chaiyaratana, Djitt Laowattana 447

3D Facial Recognition Using Eigenface and Cascade Fuzzy Neural Networks: Normalized Facial Image Approach
Yeung-Hak Lee, Chang-Wook Han 457

A New Scaling Kernel-Based Fuzzy System with Low Computational Complexity
Xiaojun Liu, Jie Yang, Hongbin Shen, Xiangyang Wang 466

Bulk Synchronous Parallel ML: Semantics and Implementation of the Parallel Juxtaposition
F. Loulergue, R. Benheddi, F. Gava, D. Louis-Régis 475

A Shortest Path Algorithm Based on Limited Search Heuristics
Feng Lu, Poh-Chin Lai 487

A New Hybrid Directory Scheme for Shared Memory Multi-processors
Guoteng Pan, Lunguo Xie, Qiang Dou, Erhua He 498

Manipulator Path Planning in 3-Dimensional Space
Dmitry Pavlov 505

Least Likely to Use: A New Page Replacement Strategy for Improving Database Management System Response Time
Rodolfo A. Pazos R., Joaquín Pérez O., José A. Martínez F., Juan J. González B., Mirna P. Ponce F. 514

Nonlinear Visualization of Incomplete Data Sets
Sergiy Popov 524

A Review of Race Detection Mechanisms
Aoun Raza 534

Fuzzy-Q Knowledge Sharing Techniques with Expertness Measures: Comparison and Analysis
Panrasee Ritthipravat, Thavida Maneewarn, Jeremy Wyatt, Djitt Laowattana 544

Explaining Symbolic Trajectory Evaluation by Giving It a Faithful Semantics
Jan-Willem Roorda, Koen Claessen 555

Analytic Modeling of Channel Traffic in n-Cubes
Hamid Sarbazi-Azad, Hamid Mahini, Ahmad Patooghy 567

Capturing an Intruder in the Pyramid
Pooya Shareghi, Navid Imani, Hamid Sarbazi-Azad 580

Speech Enhancement in Short-Wave Channel Based on Empirical Mode Decomposition
Li-Ran Shen, Qing-Bo Yin, Xue-Yao Li, Hui-Qiang Wang 591

Extended Resolution Proofs for Conjoining BDDs
Carsten Sinz, Armin Biere 600

Optimal Difference Systems of Sets with Multipliers
Vladimir D. Tonchev, Hao Wang 612

Authentication Mechanism Using One-Time Password for 802.11 Wireless LAN
Binod Vaidya, SangDuck Lee, Jae-Kyun Han, SeungJo Han 619

Optimizing Personalized Retrieval System Based on Web Ranking
Hao-ming Wang, Ye Guo, Bo-qin Feng 629

Instruction Selection for ARM/Thumb Processors Based on a Multi-objective Ant Algorithm
Shengning Wu, Sikun Li 641

A New Flow Control Algorithm for High Speed Computer Network
Haoran Zhang, Peng Sun 652

Nonlinear Systems Modeling and Control Using Support Vector Machine Technique
Haoran Zhang, Xiaodong Wang 660

Fast Motif Search in Protein Sequence Databases
Elena Zheleva, Abdullah N. Arslan 670

Author Index 683