Lecture Notes in Computer Science 5010

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

Alfred Kobsa
University of California, Irvine, CA, 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

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

Edward A. Hirsch Alexander A. Razborov
Alexei Semenov Anatol Slissenko (Eds.)

Computer Science – Theory and Applications

Third International Computer Science Symposium in Russia, CSR 2008
Moscow, Russia, June 7-12, 2008
Proceedings

Springer

Volume Editors

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

Alexander A. Razborov
Institute for Advanced Study, School of Mathematics
Einstein Drive, Princeton, NJ 08540, USA
E-mail: razborov@ias.edu

Alexei Semenov
Moscow Institute of Open Education
6 Aviatsionny per., 125167 Moscow, Russia
E-mail: alsemenov@umail.ru

Anatol Slissenko
University Paris 12, Dept. of Informatics
61 Av. du Gén. de Gaulle, 94010, Créteil, France
E-mail: slissenko@univ-paris12.fr

Library of Congress Control Number: 2008926412

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 3-540-79708-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-79708-1 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: 12265961 06/3180 5 4 3 2 1 0

Preface

The Third International Computer Science Symposium in Russia (CSR-2008) was held during June 7–12, 2008 in Moscow, Russia, hosted by Dorodnicyn Computing Centre of Russian Academy of Sciences, Institute for System Programming of Russian Academy of Sciences, Moscow State University, Moscow Institute of Open Education, and Institute of New Technologies. It was the third event in the series of regular international meetings following CSR-2006 in St. Petersburg and CSR-2007 in Ekaterinburg.

The symposium was composed of two tracks: Theory and Applications/Technology. The opening lecture was given by Avi Wigderson and eight other invited plenary lectures were given by Eric Allender, Zurab Khasidashvili, Leonid Levin, Pavel Pudlák, Florin Spanachi, Limsoon Wong, Yuri Zhuravlev and Konstantin Rudakov, and Uri Zwick.

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 103 papers in total. The Program Committee of the Theory Track selected 27 papers out of 62 submissions. The Program Committee of the Applications/Technology Track selected 6 papers out of 41 submissions.

Yandex provided Best Paper Awards; the recepients of these awards were selected by the Program Committee:

- Marius Zimand, "Two Sources Are Better Than One for Increasing the Kolmogorov Complexity of Infinite Sequences" — Best Paper Award for the Theory Track
- Laura Kovács, "Invariant Generation for P-solvable Loops with Assignments" — Best Paper Award for the Application/Technology Track
- Vladimir Podolskii, "A Uniform Lower Bound on Weights of Perceptrons" — Best Student Paper Award

The symposium featured two special sessions, "Andrei Muchnik. In Memoriam" and "Teaching Computer Science," and one pre-conference workshop ACC 2008 (Russian-Indian Workshop on Algebra, Combinatorics and Complexity) organized by Meena Mahajan and Mikhail Volkov.

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

We are grateful to our sponsors:

- Russian Foundation for Basic Research
- NIX Computer Company (hardware and software selling, system integration)
- Institute of New Technologies (INT, Russian leader of ICT in school education)

– Yandex (the largest Russian Internet portal providing key Web services)
– Microsoft Russia

We also thank a group of young Moscow computer scientists, headed by Yuri Pritykin, who significantly helped with local organizational issues.

March 2008

Edward A. Hirsch
Alexander Razborov
Alexei Semenov
Anatol Slissenko

Organization

Program Committee

Theory Track

Sergei Artemov	CUNY Graduate Center, USA
Matthias Baaz	University of Technology, Vienna, Austria
Boaz Barak	Princeton University, USA
Lev Beklemishev	Steklov Institute/Moscow, Russia
Harry Buhrman	CWI / University of Amsterdam, Netherlands
Andrei Bulatov	Simon Fraser University, Canada
Evgeny Dantsin	Roosevelt University, USA
Volker Diekert	University of Stuttgart, Germany
Anna Frid	Sobolev Institute/Novosibirsk, Russia
Andreas Goerdt	TU Chemnitz, Germany
Andrew V. Goldberg	Microsoft Research — SVC, USA
Dima Grigoriev	University of Rennes, France
Yuri Gurevich	Microsoft Research, USA
Edward A. Hirsch	Steklov Institute/St.Petersburg, Russia
Nicole Immorlica	CWI, Netherlands
Pascal Koiran	ENS Lyon, France
Michal Koucký	Institute of Mathematics, Prague, Czech Republic
Yury Makarychev	Microsoft Research, USA
Yuri Matiyasevich	Steklov Institute/St.Petersburg, Russia
Alexander Razborov (Chair)	IAS, USA and Steklov Institute/Moscow, Russia
Victor Selivanov	Novosibirsk Pedagogical University, Russia
Alexander Shen	LIF CNRS, France and IPPI, Russia
Helmut Veith	TU Darmstadt, Germany
Nikolay Vereshchagin	Moscow State University, Russia
Sergey Yekhanin	IAS, USA

Application and Technology Track

Robert T. Bauer	IBM, USA
Egon Börger	University of Pisa, Italy
Stephane Bressan	National University of Singapore, Singapore
Gabriel Ciobanu	Cuza University, Iasi, Romania
Edward A. Hirsch	Steklov Institute/St.Petersburg, Russia
Michael Kishinevsky	Intel, USA

Gregory Kucherov	CNRS / LIFL / INRIA, France
Alexandre Petrenko	CRIM, Canada
Andreas Reuter	European Media Laboratory, Germany
Anatol Slissenko (Chair)	University of Paris-12, France
Elena Troubitsyna	Åbo Akademi University, Finland
Andrei Voronkov	University of Manchester, UK
Sergey Zhukov	Transas, Russia

Conference Chair

Alexei Semenov	Moscow Institute of Open Education, Russia

Steering Committee for CSR Conferences

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

External Reviewers

Omran Ahmadi	Alexandre Guitton	Hak-Keung Lam
Krzysztof R. Apt	Vesa Halava	Klaus-Jörn Lange
Sergey Avgustinovich	Hesham Hallal	Jürn Laun
Maxim A. Babenko	Kristoffer Arnsfelt Hansen	Martin Leucker
Marie-Pierre Beal	Johan Håstad	Nutan Limaye
Emmanuel Beffara	Reiko Heckel	Thomas Lukasiewicz
Anne Benoit	Tom Hirschowitz	Konstantin Makarychev
Dario Andrea Bini	Thomas Hofmeister	Larisa Maksimova
Eduardo Bonelli	Dmitry Itsykson	Qaisar Ahmad Malik
Sergiy Boroday	Cornel Izbasa	Maurice Margenstern
Octav Brudaru	Sham Kakade	Frédéric Mazoit
Olivier Carton	Panagiotis Kalnis	Klaus Meer
Nadia Creignou	Juhani Karhumäki	Ilya Mezhirov
Michel Dayde	Jarkko Kari	Ilya Mironov
Fredrik Degerlund	Dmitry Karpov	Petr Mitrichev
Walter Didimo	Manuel Kauers	Michael Moortgat
Alexandre Dikovsky	Alexander Khodyrev	Daniil Musatov
Gillian Dobbie	Boris Konev	Nanjangud Narendra
Arnaud Dury	Oleg Kudinov	Sergey Nikolenko
Lance Fortnow	Alexander Kulikov	Dirk Nowotka
Frederic Gava	Dietrich Kuske	Michael Nuesken
Alexander Gotmanov	Linas Laibinis	Alexander Okhotin

Dmitry Pasechnik
Alexei Pastor
Holger Petersen
Martha Plaska
Alexander Pljasunov
Vladimir Podolskii
Ilia Ponomarenko
Alexey Pospelov
Ulrike Prange
Steven Prestwich
Yuri Pritykin
Svetlana Puzynina
Michael Raskin
Gaetan Richard
Lorenzo Robbiano
Andrei Romashchenko
Andrei Rumyantsev
Sattanathan Subramanian
Azadeh Saffarian
Martin Sauerhoff
Hans Juergen Schneider
Stefan Schwoon
Phil Scott
Natasha Sharygina
Amir Shpilka
Vladimir Shpilrain
Arseny M. Shur
Henny Sipma
Evgeny Skvortsov
Ludwig Staiger
Lev Stankevich
Rainer Steinwandt
Kazushige Terui
Pascal Tesson
Alexander Tiskin
Elpida Tzafestas
Vinodchandrad Variyam
Oleg Verbitsky
Konstantin Verchinine
Rakesh Vohra
Mikhail Volkov
Nicolai Vorobjov
Fabian Wagner
Derry Tanti Wijaya
Alexander Wolpert
Tatiana Yavorskaya

Table of Contents

Opening Lecture

Randomness – A Computational Complexity Perspective 1
Avi Wigderson

Invited Papers

Cracks in the Defenses: Scouting Out Approaches on Circuit Lower Bounds 3
Eric Allender

On Formal Equivalence Verification of Hardware 11
Zurab Khasidashvili

Twelve Problems in Proof Complexity 13
Pavel Pudlák

Manifestation and Exploitation of Invariants in Bioinformatics 28
Limsoon Wong

Simple Stochastic Games, Mean Payoff Games, Parity Games 29
Uri Zwick

Theory Track

Topological Semantics of Justification Logic 30
Sergei Artemov and Elena Nogina

A Logspace Algorithm for Partial 2-Tree Canonization 40
Vikraman Arvind, Bireswar Das, and Johannes Köbler

A Triple Correspondence in Canonical Calculi: Strong Cut-Elimination, Coherence, and Non-deterministic Semantics 52
Arnon Avron and Anna Zamansky

Computing Longest Common Substrings Via Suffix Arrays 64
Maxim A. Babenko and Tatiana A. Starikovskaya

Logic and Rational Languages of Words Indexed by Linear Orderings . . . 76
Nicolas Bedon, Alexis Bès, Olivier Carton, and Chloé Rispal

Complexity of the Bollobás-Riordan Polynomial: Exceptional Points and Uniform Reductions 86
Markus Bläser, Holger Dell, and Johann A. Makowsky

A Complete Characterization of Nash-Solvability of Bimatrix Games in Terms of the Exclusion of Certain 2×2 Subgames 99
Endre Boros, Khaled Elbassioni, Vladimir Gurvich, Kazuhisa Makino, and Vladimir Oudalov

Synchronization of Grammars 110
Didier Caucal and Stéphane Hassen

Lower Bounds for Depth-2 and Depth-3 Boolean Circuits with Arbitrary Gates 122
Dmitriy Yu. Cherukhin

A Semantic Proof of Polytime Soundness of Light Affine Logic 134
Ugo Dal Lago and Martin Hofmann

On Subword Complexity of Morphic Sequences 146
Rostislav Deviatov

Comparing Universal Covers in Polynomial Time 158
Jiří Fiala and Daniël Paulusma

S4LP and Local Realizability 168
Melvin Fitting

On the Expressive Power of Permanents and Perfect Matchings of Matrices of Bounded Pathwidth/Cliquewidth (Extended Abstract) 180
Uffe Flarup and Laurent Lyaudet

The Most General Conservation Law for a Cellular Automaton 194
Enrico Formenti, Jarkko Kari, and Siamak Taati

Lower Bounds on Frequency Estimation of Data Streams (Extended Abstract) 204
Sumit Ganguly

From Invariants to Canonization in Parallel 216
Johannes Köbler and Oleg Verbitsky

Self-referentiality of Justified Knowledge 228
Roman Kuznets

On the Complexity of Membership and Counting in Height-Deterministic Pushdown Automata 240
Nutan Limaye, Meena Mahajan, and Antoine Meyer

Public Key Encryption and Encryption Emulation Attacks 252
Denis Osin and Vladimir Shpilrain

A Uniform Lower Bound on Weights of Perceptrons 261
Vladimir V. Podolskii

Lambek Grammars with One Division Are Decidable in Polynomial Time 273
Yury Savateev

Cryptanalysis of Stickel's Key Exchange Scheme 283
Vladimir Shpilrain

Combinatorial Complexity of Regular Languages 289
Arseny M. Shur

On Sequences with Non-learnable Subsequences 302
Vladimir V. V'yugin

Algorithms for Multiterminal Cuts 314
Mingyu Xiao

Two Sources Are Better Than One for Increasing the Kolmogorov Complexity of Infinite Sequences 326
Marius Zimand

Applications and Technology Track

Multilayer Neuro-fuzzy Network for Short Term Electric Load Forecasting 339
Yevgeniy Bodyanskiy, Sergiy Popov, and Taras Rybalchenko

Invariant Generation for P-Solvable Loops with Assignments 349
Laura Kovács

Using Coloured Petri Nets to Model and Verify Telecommunications Systems 360
Valery Nepomniaschy, Dmitry Beloglazov, Tatiana Churina, and Mikhail Mashukov

Additive Preconditioning for Matrix Computations 372
Victor Y. Pan, Dmitriy Ivolgin, Brian Murphy, Rhys Eric Rosholt, Yuqing Tang, and Xiaodong Yan

Network as a Computer: Ranking Paths to Find Flows 384
Dusko Pavlovic

A Unified Categorical Approach for Attributed Graph Rewriting 398
Maxime Rebout, Louis Féraud, and Sergei Soloviev

Author Index 411