

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

LNCS 3967

Computer Science – Theory and Applications

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



Springer

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

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

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

Applications and Technology Track

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

Andreas Reuter
Mary Sheeran
Elena Troubitsyna
Miroslav Velev
Sergey Zhukov

European Media Laboratory, Germany
Chalmers University of Technology, Sweden
Åbo Akademi University, Finland
Carnegie Mellon University, USA
Transas, Russia

Conference Chair

Edward A. Hirsch

Steklov Institute/St. Petersburg, Russia

Steering Committee for CSR Conferences

Anna Frid
Edward A. Hirsch
Juhani Karhumäki
Mikhail Volkov

Sobolev Institute/Novosibirsk, Russia
Steklov Institute/St. Petersburg, Russia
Turku, Finland
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 Maffei
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 Ræcke
Deva Ramanan

Dror Rawitz
Jan Reimann
Angelo Restifcar
Søren Riis
Philip Ruegger
Igor Rystsov
Viktor Sabelfeld
Ashish Sabharwal
Arseny Shur
Terence Sim
Jan Smith
Niklas Sörensson
Arne Storjohann
Karsten Tiemann
Michael Tiomkin
Siegbert Tigg
Paul Vitányi
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.

Lecture Notes in Computer Science

For information about Vols. 1–3882

please contact your bookseller or Springer

- Vol. 3987: M. Hazas, J. Krumm, T. Strang (Eds.), *Location- and Context-Awareness*. X, 289 pages. 2006.
- Vol. 3984: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part V. XXV, 1045 pages. 2006.
- Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part IV. XXVI, 1191 pages. 2006.
- Vol. 3982: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part III. XXV, 1243 pages. 2006.
- Vol. 3981: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part II. XXVI, 1255 pages. 2006.
- Vol. 3980: M. Gavrilova, O. Gervasi, V. Kumar, C.J. K. Tan, D. Taniar, A. Laganà, Y. Mun, H. Choo (Eds.), *Computational Science and Its Applications - ICCSA 2006*, Part I. LXXV, 1199 pages. 2006.
- Vol. 3979: T.S. Huang, N. Sebe, M.S. Lew, V. Pavlović, T. Kölsch, A. Galata, B. Kisačanin (Eds.), *Computer Vision in Human-Computer Interaction*. XII, 121 pages. 2006.
- Vol. 3978: B. Hnich, M. Carlsson, F. Fages, F. Rossi (Eds.), *Recent Advances in Constraints*. VIII, 179 pages. 2006. (Sublibrary LNAI).
- Vol. 3970: T. Braun, G. Carle, S. Fahmy, Y. Kocheryavy (Eds.), *Wired/Wireless Internet Communications*. XIV, 350 pages. 2006.
- Vol. 3968: K.P. Fishkin, B. Schiele, P. Nixon, A. Quigley (Eds.), *Pervasive Computing*. XV, 402 pages. 2006.
- Vol. 3967: D. Grigoriev, J. Harrison, E.A. Hirsch (Eds.), *Computer Science – Theory and Applications*. XVI, 684 pages. 2006.
- Vol. 3964: M. Ü. Uyar, A.Y. Duale, M.A. Fecko (Eds.), *Testing of Communicating Systems*. XI, 373 pages. 2006.
- Vol. 3960: R. Vieira, P. Quaresma, M.d.G.V. Nunes, N.J. Mamede, C. Oliveira, M.C. Dias (Eds.), *Computational Processing of the Portuguese Language*. XII, 274 pages. 2006. (Sublibrary LNAI).
- Vol. 3959: J.-Y. Cai, S. B. Cooper, A. Li (Eds.), *Theory and Applications of Models of Computation*. XV, 794 pages. 2006.
- Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T. Malkin (Eds.), *Public Key Cryptography - PKC 2006*. XIV, 543 pages. 2006.
- Vol. 3956: G. Barthe, B. Gregoire, M. Huisman, J.-L. Lanet (Eds.), *Construction and Analysis of Safe, Secure, and Interoperable Smart Devices*. IX, 175 pages. 2006.
- Vol. 3955: G. Antoniou, G. Potamias, C. Spyropoulos, D. Plexousakis (Eds.), *Advances in Artificial Intelligence*. XVII, 611 pages. 2006. (Sublibrary LNAI).
- Vol. 3954: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision – ECCV 2006*, Part IV. XVII, 613 pages. 2006.
- Vol. 3953: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision – ECCV 2006*, Part III. XVII, 649 pages. 2006.
- Vol. 3952: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision – ECCV 2006*, Part II. XVII, 661 pages. 2006.
- Vol. 3951: A. Leonardis, H. Bischof, A. Pinz (Eds.), *Computer Vision – ECCV 2006*, Part I. XXXV, 639 pages. 2006.
- Vol. 3950: J.P. Müller, F. Zambonelli (Eds.), *Agent-Oriented Software Engineering VI*. XVI, 249 pages. 2006.
- Vol. 3947: Y.-C. Chung, J.E. Moreira (Eds.), *Advances in Grid and Pervasive Computing*. XXI, 667 pages. 2006.
- Vol. 3946: T.R. Roth-Berghofer, S. Schulz, D.B. Leake (Eds.), *Modeling and Retrieval of Context*. XI, 149 pages. 2006. (Sublibrary LNAI).
- Vol. 3945: M. Hagiya, P. Wadler (Eds.), *Functional and Logic Programming*. X, 295 pages. 2006.
- Vol. 3944: J. Quiñero-Candela, I. Dagan, B. Magnini, F. d'Alché-Buc (Eds.), *Machine Learning Challenges*. XIII, 462 pages. 2006. (Sublibrary LNAI).
- Vol. 3943: N. Gueffi, A. Savidis (Eds.), *Rapid Integration of Software Engineering Techniques*. X, 289 pages. 2006.
- Vol. 3942: Z. Pan, R. Aylett, H. Diener, X. Jin, S. Göbel, L. Li (Eds.), *Technologies for E-Learning and Digital Entertainment*. XXV, 1396 pages. 2006.
- Vol. 3939: C. Priami, L. Cardelli, S. Emmott (Eds.), *Transactions on Computational Systems Biology IV*. VII, 141 pages. 2006. (Sublibrary LNBI).
- Vol. 3936: M. Lalmas, A. MacFarlane, S. Rüger, A. Tombros, T. Tsirikka, A. Yavinsky (Eds.), *Advances in Information Retrieval*. XIX, 584 pages. 2006.
- Vol. 3935: D. Won, S. Kim (Eds.), *Information Security and Cryptology - ICISC 2005*. XIV, 458 pages. 2006.
- Vol. 3934: J.A. Clark, R.F. Paige, F.A. C. Polack, P.J. Brooke (Eds.), *Security in Pervasive Computing*. X, 243 pages. 2006.
- Vol. 3933: F. Bonchi, J.-F. Boulicaut (Eds.), *Knowledge Discovery in Inductive Databases*. VIII, 251 pages. 2006.
- Vol. 3931: B. Apolloni, M. Marinaro, G. Nicosia, R. Tagliaferri (Eds.), *Neural Nets*. XIII, 370 pages. 2006.
- Vol. 3930: D.S. Yeung, Z.-Q. Liu, X.-Z. Wang, H. Yan (Eds.), *Advances in Machine Learning and Cybernetics*. XXI, 1110 pages. 2006. (Sublibrary LNAI).

- Vol. 3929: W. MacCaull, M. Winter, I. Düntsch (Eds.), *Relational Methods in Computer Science*. VIII, 263 pages. 2006.
- Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), *Smart Card Research and Advanced Applications*. XI, 359 pages. 2006.
- Vol. 3927: J. Hespanha, A. Tiwari (Eds.), *Hybrid Systems: Computation and Control*. XII, 584 pages. 2006.
- Vol. 3925: A. Valmari (Ed.), *Model Checking Software*. X, 307 pages. 2006.
- Vol. 3924: P. Sestoft (Ed.), *Programming Languages and Systems*. XII, 343 pages. 2006.
- Vol. 3923: A. Mycroft, A. Zeller (Eds.), *Compiler Construction*. XIII, 277 pages. 2006.
- Vol. 3922: L. Baresi, R. Heckel (Eds.), *Fundamental Approaches to Software Engineering*. XIII, 427 pages. 2006.
- Vol. 3921: L. Aceto, A. Ingólfssdóttir (Eds.), *Foundations of Software Science and Computation Structures*. XV, 447 pages. 2006.
- Vol. 3920: H. Hermanns, J. Palsberg (Eds.), *Tools and Algorithms for the Construction and Analysis of Systems*. XIV, 506 pages. 2006.
- Vol. 3918: W.K. Ng, M. Kitsuregawa, J. Li, K. Chang (Eds.), *Advances in Knowledge Discovery and Data Mining*. XXIV, 879 pages. 2006. (Sublibrary LNAI).
- Vol. 3917: H. Chen, F.Y. Wang, C.C. Yang, D. Zeng, M. Chau, K. Chang (Eds.), *Intelligence and Security Informatics*. XII, 186 pages. 2006.
- Vol. 3916: J. Li, Q. Yang, A.-H. Tan (Eds.), *Data Mining for Biomedical Applications*. VIII, 155 pages. 2006. (Sublibrary LNBI).
- Vol. 3915: R. Nayak, M.J. Zaki (Eds.), *Knowledge Discovery from XML Documents*. VIII, 105 pages. 2006.
- Vol. 3914: A. Garcia, R. Choren, C. Lucena, P. Giorgini, T. Holvoet, A. Romanovsky (Eds.), *Software Engineering for Multi-Agent Systems IV*. XIV, 255 pages. 2006.
- Vol. 3910: S.A. Brueckner, G.D.M. Serugendo, D. Hales, F. Zambonelli (Eds.), *Engineering Self-Organising Systems*. XII, 245 pages. 2006. (Sublibrary LNAI).
- Vol. 3909: A. Apostolico, C. Guerra, S. Istrail, P. Pevzner, M. Waterman (Eds.), *Research in Computational Molecular Biology*. XVII, 612 pages. 2006. (Sublibrary LNBI).
- Vol. 3908: A. Bui, M. Bui, T. Böhme, H. Unger (Eds.), *Innovative Internet Community Systems*. VIII, 207 pages. 2006.
- Vol. 3907: F. Rothlauf, J. Branke, S. Cagnoni, E. Costa, C. Cotta, R. Drechsler, E. Lutton, P. Machado, J.H. Moore, J. Romero, G.D. Smith, G. Squillero, H. Takagi (Eds.), *Applications of Evolutionary Computing*. XXIV, 813 pages. 2006.
- Vol. 3906: J. Gottlieb, G.R. Raidl (Eds.), *Evolutionary Computation in Combinatorial Optimization*. XI, 293 pages. 2006.
- Vol. 3905: P. Collet, M. Tomassini, M. Ebner, S. Gustafson, A. Ekárt (Eds.), *Genetic Programming*. XI, 361 pages. 2006.
- Vol. 3904: M. Baldoni, U. Endriss, A. Omicini, P. Torroni (Eds.), *Declarative Agent Languages and Technologies III*. XII, 245 pages. 2006. (Sublibrary LNAI).
- Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), *Information Security Practice and Experience*. XIV, 392 pages. 2006.
- Vol. 3902: R. Kronland-Martinet, T. Voinier, S. Ystad (Eds.), *Computer Music Modeling and Retrieval*. XI, 275 pages. 2006.
- Vol. 3901: P.M. Hill (Ed.), *Logic Based Program Synthesis and Transformation*. X, 179 pages. 2006.
- Vol. 3900: F. Toni, P. Torroni (Eds.), *Computational Logic in Multi-Agent Systems*. XVII, 427 pages. 2006. (Sublibrary LNAI).
- Vol. 3899: S. Frintrop, VOCUS: A Visual Attention System for Object Detection and Goal-Directed Search. XIV, 216 pages. 2006. (Sublibrary LNAI).
- Vol. 3898: K. Tuyls, P.J. 't Hoen, K. Verbeeck, S. Sen (Eds.), *Learning and Adaption in Multi-Agent Systems*. X, 217 pages. 2006. (Sublibrary LNAI).
- Vol. 3897: B. Preneel, S. Tavares (Eds.), *Selected Areas in Cryptography*. XI, 371 pages. 2006.
- Vol. 3896: Y. Ioannidis, M.H. Scholl, J.W. Schmidt, F. Matthes, M. Hatzopoulos, K. Boehm, A. Kemper, T. Grust, C. Boehm (Eds.), *Advances in Database Technology - EDBT 2006*. XIV, 1208 pages. 2006.
- Vol. 3895: O. Goldreich, A.L. Rosenberg, A.L. Selman (Eds.), *Theoretical Computer Science*. XII, 399 pages. 2006.
- Vol. 3894: W. Grass, B. Sick, K. Waldschmidt (Eds.), *Architecture of Computing Systems - ARCS 2006*. XII, 496 pages. 2006.
- Vol. 3893: L. Atzori, D.D. Giusto, R. Leonardi, F. Pereira (Eds.), *Visual Content Processing and Representation*. IX, 224 pages. 2006.
- Vol. 3892: A. Carbone, N.A. Pierce (Eds.), *DNA Computing*. XI, 440 pages. 2006.
- Vol. 3891: J.S. Sichman, L. Antunes (Eds.), *Multi-Agent-Based Simulation VI*. X, 191 pages. 2006. (Sublibrary LNAI).
- Vol. 3890: S.G. Thompson, R. Ghanee-Hercock (Eds.), *Defence Applications of Multi-Agent Systems*. XII, 141 pages. 2006. (Sublibrary LNAI).
- Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), *Independent Component Analysis and Blind Signal Separation*. XXI, 980 pages. 2006.
- Vol. 3888: D. Draheim, G. Weber (Eds.), *Trends in Enterprise Application Architecture*. IX, 145 pages. 2006.
- Vol. 3887: J.R. Correa, A. Hevia, M. Kiwi (Eds.), *LATIN 2006: Theoretical Informatics*. XVI, 814 pages. 2006.
- Vol. 3886: E.G. Bremer, J. Hakenberg, E.-H.(S.) Han, D. Berrar, W. Dubitzky (Eds.), *Knowledge Discovery in Life Science Literature*. XIV, 147 pages. 2006. (Sublibrary LNBI).
- Vol. 3885: V. Torra, Y. Narukawa, A. Valls, J. Domingo-Ferrer (Eds.), *Modeling Decisions for Artificial Intelligence*. XII, 374 pages. 2006. (Sublibrary LNAI).
- Vol. 3884: B. Durand, W. Thomas (Eds.), *STACS 2006*. XIV, 714 pages. 2006.
- Vol. 3883: M. Cesana, L. Fratta (Eds.), *Wireless Systems and Network Architectures in Next Generation Internet*. IX, 281 pages. 2006.

Table of Contents

Invited Papers

Non-black-box Techniques in Cryptography <i>Boaz Barak</i>	1
Complexity of Polynomial Multiplication over Finite Fields <i>Michael Kaminski</i>	2
Synchronous Elastic Circuits <i>Mike Kishinevsky, Jordi Cortadella, Bill Grundmann, Sava Krstić, John O'Leary</i>	3

Theory Track

SZK Proofs for Black-Box Group Problems <i>V. Arvind, Bireswar Das</i>	6
Canonical Decomposition of a Regular Factorial Language <i>S.V. Avgustinovich, A.E. Frid</i>	18
Acyclic Bidirected and Skew-Symmetric Graphs: Algorithms and Structure <i>Maxim A. Babenko</i>	23
Inductive Type Schemas as Functors <i>Freiric Barral, Sergei Soloviev</i>	35
Unfolding Synthesis of Asynchronous Automata <i>Nicolas Baudru, Rémi Morin</i>	46
Conjugacy and Equivalence of Weighted Automata and Functional Transducers <i>Marie-Pierre Béal, Sylvain Lombardy, Jacques Sakarovitch</i>	58
Applications of the Linear Matroid Parity Algorithm to Approximating Steiner Trees <i>Piotr Berman, Martin Fürer, Alexander Zelikovsky</i>	70
Tuples of Disjoint NP-Sets <i>Olaf Beyersdorff</i>	80

Constructive Equivalence Relations on Computable Probability Measures	
<i>Laurent Bienvenu</i>	92
Planar Dimer Tilings	
<i>Olivier Bodini, Thomas Fernique</i>	104
The Complexity of Equality Constraint Languages	
<i>Manuel Bodirsky, Jan Kára</i>	114
Window Subsequence Problems for Compressed Texts	
<i>Patrick Cégielski, Irène Guessarian, Yury Lifshits, Yuri Matiyasevich</i>	127
Efficient Algorithms in Zero-Characteristic for a New Model of Representation of Algebraic Varieties	
<i>Alexander L. Chistov</i>	137
Relativisation Provides Natural Separations for Resolution-Based Proof Systems	
<i>Stefan Dantchev</i>	147
Bounded-Degree Forbidden Patterns Problems Are Constraint Satisfaction Problems	
<i>Stefan Dantchev, Florent Madelaine</i>	159
Isolation and Reducibility Properties and the Collapse Result	
<i>Sergey M. Dudakov</i>	171
Incremental Branching Programs	
<i>Anna Gál, Michal Koucký, Pierre McKenzie</i>	178
Logic of Proofs for Bounded Arithmetic	
<i>Evan Goris</i>	191
On a Maximal NFA Without Mergible States	
<i>Igor Grunsky, Oleksiy Kurganskyy, Igor Potapov</i>	202
Expressiveness of Metric Modalities for Continuous Time	
<i>Yoram Hirshfeld, Alexander Rabinovich</i>	211
Extending Dijkstra's Algorithm to Maximize the Shortest Path by Node-Wise Limited Arc Interdiction	
<i>Leonid Khachiyan, Vladimir Gurvich, Jihui Zhao</i>	221

Weighted Logics for Traces <i>Ingmar Meinecke</i>	235
On Nonforgetting Restarting Automata That Are Deterministic and/or Monotone <i>Hartmut Messerschmidt, Friedrich Otto</i>	247
Unwinding a Non-effective Cut Elimination Proof <i>Grigori Mints</i>	259
Enumerate and Expand: Improved Algorithms for Connected Vertex Cover and Tree Cover <i>Daniel Mölle, Stefan Richter, Peter Rossmanith</i>	270
Shannon Entropy vs. Kolmogorov Complexity <i>An. Muchnik, N. Vereshchagin</i>	281
Language Equations with Symmetric Difference <i>Alexander Okhotin</i>	292
On Primitive Recursive Realizabilities <i>Valery Plisko</i>	304
Evidence Reconstruction of Epistemic Modal Logic S5 <i>Natalia Rubtsova</i>	313
Linear Temporal Logic with Until and Before on Integer Numbers, Deciding Algorithms <i>V. Rybakov</i>	322
On the Frequency of Letters in Morphic Sequences <i>Kalle Saari</i>	334
Functional Equations in Shostak Theories <i>Sergey P. Shlepakov</i>	346
All Semi-local Longest Common Subsequences in Subquadratic Time <i>Alexander Tiskin</i>	352
Non-approximability of the Randomness Deficiency Function <i>Michael A. Ustinov</i>	364
Multi-agent Explicit Knowledge <i>Tatiana Yavorskaya (Sidon)</i>	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 <i>Rodolfo A. Pazos R., Joaquín Pérez O., José A. Martínez F., Juan J. González B., Mirna P. Ponce F.</i>	514
Nonlinear Visualization of Incomplete Data Sets <i>Sergiy Popov</i>	524
A Review of Race Detection Mechanisms <i>Aoun Raza</i>	534
Fuzzy-Q Knowledge Sharing Techniques with Expertness Measures: Comparison and Analysis <i>Panrasee Ritthipravat, Thavida Maneewarn, Jeremy Wyatt, Djitt Laowattana</i>	544
Explaining Symbolic Trajectory Evaluation by Giving It a Faithful Semantics <i>Jan-Willem Roorda, Koen Claessen</i>	555
Analytic Modeling of Channel Traffic in n -Cubes <i>Hamid Sarbazi-Azad, Hamid Mahini, Ahmad Patooghy</i>	567
Capturing an Intruder in the Pyramid <i>Pooya Shareghi, Navid Imani, Hamid Sarbazi-Azad</i>	580
Speech Enhancement in Short-Wave Channel Based on Empirical Mode Decomposition <i>Li-Ran Shen, Qing-Bo Yin, Xue-Yao Li, Hui-Qiang Wang</i>	591
Extended Resolution Proofs for Conjoining BDDs <i>Carsten Sinz, Armin Biere</i>	600
Optimal Difference Systems of Sets with Multipliers <i>Vladimir D. Tonchev, Hao Wang</i>	612
Authentication Mechanism Using One-Time Password for 802.11 Wireless LAN <i>Binod Vaidya, SangDuck Lee, Jae-Kyun Han, SeungJo Han</i>	619
Optimizing Personalized Retrieval System Based on Web Ranking <i>Hao-ming Wang, Ye Guo, Bo-qin Feng</i>	629
Instruction Selection for ARM/Thumb Processors Based on a Multi-objective Ant Algorithm <i>Shengning Wu, Sikun Li</i>	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

Non-black-box Techniques in Cryptography

Boaz Barak

Princeton University

Abstract. In cryptography we typically prove the security of a scheme by reducing the task of breaking the scheme to some hard computational problem. This reduction usually done in a *black-box* fashion. By this we mean that there is an algorithm that can solve the hard problem given any black-box for breaking the scheme.

This lecture concerns exceptions to this rule: that is, schemes that are proven secure using a non-black-box reduction, that actually uses the code of a scheme-breaking attacker to construct a problem-solving algorithm. It turns out that such reductions can be used to obtain schemes with better properties that were known before. In fact, in some cases these non-black-box reductions can be obtain goals that were proven to be impossible to achieve when restricting to black-box reductions. In particular, we will present constructions of zero-knowledge protocols that are proven secure under various compositions [1, 2, 3].

We'll also discuss some of the limitations and open questions regarding non-black-box security proofs.

References

1. Barak, B.: How to go beyond the black-box simulation barrier. In: Proc. 42nd FOCS, IEEE (2001) 106–115
2. Pass, R.: Bounded-concurrent secure multi-party computation with a dishonest majority. In: Proc. 36th STOC, ACM (2004) 232–241
3. Barak, B., Sahai, A.: How to play almost any mental game over the net - concurrent composition using super-polynomial simulation. In: Proc. 46th FOCS, IEEE (2005)