

*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*

Luca Aceto Ivan Damgård  
Leslie Ann Goldberg  
Magnús M. Halldórsson  
Anna Ingólfssdóttir Igor Walukiewicz (Eds.)

# Automata, Languages and Programming

35th International Colloquium, ICALP 2008  
Reykjavik, Iceland, July 7-11, 2008  
Proceedings, Part I

## Volume Editors

Luca Aceto  
Magnús M. Halldórsson  
Anna Ingólfssdóttir  
Reykjavik University, School of Computer Science  
Kringlan 1, 103 Reykjavík, Iceland  
E-mail: {luca, mmh, annai}@ru.is

Ivan Damgård  
University of Aarhus, Department of Computer Science, IT-Parken  
Åbogade 34, 8200 Århus N, Denmark  
E-mail: ivan@daimi.au.dk

Leslie Ann Goldberg  
University of Liverpool, Department of Computer Science  
Ashton Building, Liverpool L69 3BX, UK  
E-mail: l.a.goldberg@liverpool.ac.uk

Igor Walukiewicz  
Université de Bordeaux-1, LaBRI  
351, Cours de la Libération, 33405 Talence cedex, France  
E-mail: igw@labri.fr

Library of Congress Control Number: 2008930136

CR Subject Classification (1998): F, D, C.2-3, G.1-2, I.3, E.1-2

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

ISSN 0302-9743  
ISBN-10 3-540-70574-0 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-70574-1 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: 12322985 06/3180 5 4 3 2 1 0

# Preface

ICALP 2008, the 35th edition of the International Colloquium on Automata, Languages and Programming, was held in Reykjavik, Iceland, July 7–11, 2008. ICALP is a series of annual conferences of the European Association for Theoretical Computer Science (EATCS) which first took place in 1972. This year, the ICALP program consisted of the established Track A (focusing on algorithms, automata, complexity and games) and Track B (focusing on logic, semantics and theory of programming), and of the recently introduced Track C (focusing on security and cryptography foundations).

In response to the call for papers, the Program Committees received 477 submissions, the highest ever: 269 for Track A, 122 for Track B and 86 for Track C. Out of these, 126 papers were selected for inclusion in the scientific program: 70 papers for Track A, 32 for Track B and 24 for Track C. The selection was made by the Program Committees based on originality, quality, and relevance to theoretical computer science. The quality of the manuscripts was very high indeed, and many deserving papers could not be selected.

ICALP 2008 consisted of five invited lectures and the contributed papers. This volume of the proceedings contains all contributed papers presented at the conference in Track A, together with the papers by the invited speakers S. Muthukrishnan (Google, USA) and Bruno Courcelle (Labri, Université Bordeaux, France). A companion volume contains all contributed papers presented in Track B and Track C together with the papers by the invited speakers Ran Canetti (IBM T.J. Watson Research Center and MIT, USA) and Javier Esparza (Technische Universität München, Germany). The program had an additional invited lecture by Peter Winkler (Dartmouth, USA), which does not appear in the proceedings.

The following workshops were held as satellite events of ICALP 2008:

ALGOSENSORS 2008 – 4th International Workshop on Algorithmic Aspects of Wireless Sensor Networks

CL&C 2008 – Second International Workshop on Classical Logic and Computation

FOCLASA 2008 – 7th International Workshop on the Foundations of Coordination Languages and Software Architectures

FIMN 2008 – Foundations of Information Management in Networks

FBTC 2008 – From Biology To Concurrency and Back

ICE 2008 – Interaction and Concurrency Experience

MatchUP 2008 – Matching Under Preferences - Algorithms and Complexity

MSFP 2008 – Second Workshop on Mathematically Structured Functional Programming

PAuL 2008 – Third International Workshop on Probabilistic Automata and Logics

QPL/DCM 2008 – 5th Workshop on Quantum Physics and Logic and 4th Workshop on Development of Computational Models

SOS 2008 – 5th Workshop on Structural Operational Semantics

IMAGINE 2008 – Second International Workshop on Mobility, Algorithms and Graph Theory in Dynamic Networks

DYNAMO 2008 – Second Training School on Algorithmic Aspects of Dynamic Networks

We wish to thank all authors who submitted extended abstracts for consideration, the Program Committees for their scholarly effort, and all referees who assisted the Program Committees in the evaluation process.

Thanks to the sponsors (CCP Games, Icelandair, IFIP TC1, Teymi) for their support, and to Reykjavik University for hosting ICALP 2008. We are also grateful to all members of the Organizing Committee in the School of Computer Science and to the Facilities and Technical staff of Reykjavik University. Thanks to Andrei Voronkov and Shai Halevi for writing the conference-management systems EasyChair and Web-Submission-and-Review software, which were used in handling the submissions and the electronic PC meeting as well as in assisting in the assembly of the proceedings.

May 2008

Luca Aceto  
Ivan Damgård  
Leslie Ann Goldberg  
Magnús M. Halldórsson  
Anna Ingólfssdóttir  
Igor Walukiewicz

# Organization

## Program Committee

### Track A

Michael Bender, State University of New York at Stony Brook, USA  
Magnus Bordewich, Durham University, UK  
Lenore Cowen, Tufts University, USA  
Pierluigi Crescenzi, Università di Firenze, Italy  
Artur Czumaj, University of Warwick, UK  
Edith Elkind, University of Southampton, UK  
David Eppstein, University of California at Irvine, USA  
Leslie Ann Goldberg, University of Liverpool, UK (Chair)  
Martin Grohe, Humboldt-Universität zu Berlin, Germany  
Giuseppe F. Italiano, Università di Roma “Tor Vergata”, Italy  
Christos Kaklamanis, University of Patras, Greece  
Peter Bro Miltersen, University of Aarhus, Denmark  
Michael Mitzenmacher, Harvard University, USA  
Ian Munro, University of Waterloo, Canada  
Ryan O’Donnell, Carnegie Mellon University, USA  
Dana Ron, Tel-Aviv University, Israel  
Tim Roughgarden, Stanford University, USA  
Christian Scheideler, Technische Universität München, Germany  
Christian Sohler, University of Paderborn, Germany  
Luca Trevisan, University of California at Berkeley, USA  
Berthold Voecking, RWTH Aachen University, Germany  
Gerhard Woeginger, Eindhoven University of Technology, The Netherlands

### Track B

Parosh Abdulla, Uppsala University, Sweden  
Luca de Alfaro, University of California, Santa Cruz, USA  
Christel Baier, Technische Universität Dresden, Germany  
Giuseppe Castagna, Université Paris 7, France  
Rocco de Nicola, Università di Firenze, Italy  
Javier Esparza, Technische Universität München, Germany  
Marcelo Fiore, University of Cambridge, UK  
Erich Grädel, RWTH Aachen, Germany  
Jason Hickey, California Institute of Technology, USA  
Martin Hofmann, Ludwig-Maximilians-Universität München, Germany  
Hendrik Jan Hoogeboom, Leiden University, The Netherlands

Radha Jagadeesen, DePaul University, USA  
Madhavan Mukund, Chennai Mathematical Institute, India  
Luke Ong, Oxford University, UK  
Dave Schmidt, Kansas State University, USA  
Philippe Schnoebelen, ENS Cachan, France  
Igor Walukiewicz, Labri, Université Bordeaux, France (Chair)  
Mihalis Yannakakis, Columbia University, USA  
Wieslaw Zielonka, Université Paris 7, France

## Track C

Christian Cachin, IBM Research Zürich, Switzerland  
Jan Camenisch, IBM Research Zürich, Switzerland  
Ivan Damgård, University of Aarhus, Denmark (Chair)  
Stefan Dziembowski, Università di Roma “La Sapienza”, Italy  
Dennis Hofheinz, CWI Amsterdam, The Netherlands  
Susan Hohenberger, Johns Hopkins University, USA  
Yuval Ishai, Technion Haifa, Israel  
Lars Knudsen, DTU Copenhagen, Denmark  
Arjen Lenstra, EPFL Lausanne, Switzerland  
Anna Lysyanskaya, Brown University, USA  
Rafael Pass, Cornell University, USA  
David Pointcheval, ENS Paris, France  
Dominique Unruh, Saarland University, Germany  
Serge Vaudenay, EPFL Lausanne, Switzerland  
Bogdan Warinschi, Bristol University, UK  
Douglas Wikström, KTH Stockholm, Sweden  
Stefan Wolf, ETH Zürich, Switzerland

## Organizing Committee

Luca Aceto, Reykjavik University (Conference Chair)  
Bjarni V. Halldórsson, Reykjavik University (Workshop Co-chair)  
Magnús M. Halldórsson, Reykjavik University (Conference Chair)  
Anna Ingólfssdóttir, Reykjavik University (Conference Chair)  
MohammadReza Mousavi, Eindhoven University of Technology (Workshop Co-chair)

## Sponsoring Institutions

CCP Games  
Icelandair  
IFIP TC1  
Reykjavik University  
Teymi

## Referees

Dimitris Achlioptas	Ioannis Caragiannis	Piotr Faliszewski
Isolde Adler	Marco Cesati	Angelo Fanelli
Pavan Aduri	Chandra Chekuri	Martin Farach-Colton
Panos Aliferis	Eric Chen	Arash Farzan
Andris Ambainis	Ning Chen	Henning Fernau
Christoph Ambühl	Jianer Chen	Jiri Fiala
Aris Anagnostopoulos	Qi Cheng	Jeremy Fineman
Spyros Angelopoulos	Giorgos Christodoulou	Irene Finocchi
Chrisil Arackaparambil	Andrea Clementi	Eldar Fischer
James Aspnes	Amin Coja-Oghlan	Felix Fischer
Albert Atserias	Vincent Conitzer	Simon Fischer
Peter Auer	Colin Cooper	Michele Flammini
Vincenzo Auletta	Graham Cormode	Abraham Flaxman
Giorgio Ausiello	Bruno Courcelle	Lisa Fleischer
Chen Avin	Andy Curtis	Fedor Fomin
Yossi Azar	Victor Dalmau	Lance Fortnow
Nikhil Bansal	Constantinos Daskalakis	Dimitris Fotakis
Sanjoy Baruah	Giuseppe Di Battista	Pierre Fraigniaud
Tuğkan Batu	Gabriele Di Stefano	Paolo Giulio Franciosa
Niel de Beaudrap	Florian Diedrich	Gudmund Frandsen
Luca Becchetti	Martin Dietzfelbinger	Anna Frid
Paul Bell	Irit Dinur	Tom Friedetzky
Michael Bender	Shahar Dobzinski	Alan Frieze
Petra Berenbrink	Michael Dom	Martin Fürer
Anna Bernasconi	Frederic Dorn	Peter Gacs
Nadja Betzler	Reza Dorri-Giv	Travis Gagie
Olaf Beyersdorff	Shaddin Dughmi	Anna Gal
Vittorio Bilo	Dominic Dumrauf	Clemente Galdi
Eric Blais	Stephane Durocher	Nicola Galesi
Avrim Blum	Christoph Durr	Luisa Gargano
Johannes Blömer	Martin Dyer	Bill Gasarch
Hans Bodlaender	Kord Eickmeyer	Serge Gaspers
Andrej Bogdanov	Friedrich Eisenbrand	Dmitry Gavinsky
Mikolaj Bojanczyk	Robert Elsaesser	Joachim Gehweiler
Paul Bonsma	Matthias Englert	Blaise Genest
Endre Boros	Amir Epstein	Loukas Georgiadis
Mark Braverman	Leah Epstein	Stefanie Gerke
Tomas Brazdil	Funda Ergun	Seth Gilbert
Patrick Briest	Jeff Erickson	Christian Glasser
Andre Brinkmann	Thomas Erlebach	Wayne Goddard
Harry Buhrman	Kousha Etessami	Paul Goldberg
David Bunde	Guy Even	Oded Goldreich
Jonathan Buss	Eyal Even-Dar	Daniel Gottesman
Tiziana Calamoneri	Alex Fabrikant	Vipul Goyal



Fabrizio Grandoni	Panagiotis	Daniel Kuntze
Catherine Greenhill	Kanellopoulos	Orna Kupferman
Alexander Grigoriev	Viggo Kann	Dietrich Kuske
Roberto Grossi	Haim Kaplan	Shay Kutten
Jens Groth	Sanjiv Kapoor	Johannes Köbler
Magdalena Grüber	George Karakostas	Oded Lachish
Jiong Guo	Howard Karloff	Christiane Lammersen
Anupam Gupta	Marek Karpinski	Michael Langberg
Venkatesan Guruswami	Telikepalli Kavitha	Alexander Langer
Vladimir Gurvich	Steven Kelk	John Langford
Falk Hüffner	Hans Kellerer	Luigi Laura
Esther Haenggi	Julia Kempe	Ranko Lazic
Torben Hagerup	David Kempe	Homin Lee
MohammadTaghi	Iordanis Kerenidis	Hing Leung
Hajiaghayi	Sanjeev Khanna	David Levin
Angele Hamel	Valerie King	Asaf Levin
Kristoffer Arnsfelt	Carl Kingsford	Ming Li
Hansen	Ralf Klasing	Andrzej Lingas
Ramesh Hariharan	Hartmut Klauck	Maciej Liskiewicz
Nick Harvey	Robert Kleinberg	Christof Loeding
Soha Hassoun	Lasse Kliemann	Markus Lohrey
Elad Hazan	Bettina Klinz	Michele Loreti
Lisa Hellerstein	Adam Klivans	Vadim Lozin
Benjamin Hescott	Joachim Kneis	Eyal Lubetzky
Jan van den Heuvel	Ker-i Ko	Fabrizio Luccio
Thomas Holenstein	Petr Kolman	Yoad Lustig
Peter Hoyer	Spyros Kontogiannis	Christof Löding
Chien-Chung Huang	Tsvi Kopelowitz	Bin Ma
Yumei Huo	Swastik Kopparty	Michael Mahoney
Thore Husfeldt	Nitish Korula	Elitza Maneva
Martin Höfer	Michal Koucky	David F. Manlove
Samuel Jeong	Elias Koutsoupias	Giovanni Manzini
Nicole Immorlica	Lukasz Kowalik	Alberto
Sandy Irani	Darek Kowalski	Marchetti-Spaccamela
Kazuo Iwama	Dariusz Kowalski	Russell Martin
Riko Jacob	Robi Krauthgamer	Dániel Marx
Markus Jalsenius	Stephan Kreutzer	Monaldo Mastrolilli
Maurice Jansen	Danny Krizanc	Jiri Matousek
Klaus Jansen	Andrei Krokhin	Marios Mavronicolas
Peter Jeavons	Sven Krumke	Andrew McGregor
Mark Jerrum	Piotr Krysta	Klaus Meer
Albert Jiang	Daniela Kuehn	Jan Mehler
Lisa Kaati	Ravi Kumar	Aranyak Mehta
Valentine Kabanets	Amit Kumar	Dieter van Melkebeek
Christos Kaklamanis	Michal Kunc	Raghu Meka

Ulrich Meyer	Igor Potapov	Amir Shpilka
Adam Meyerson	Daniel Preda	Adi Shraibman
Zoltan Miklos	Geppino Pucci	Anastasios Sidiropoulos
Miriam Di Ianni	Rosario Pugliese	Riccardo Silvestri
Vahab Mirrokni	Jaikumar	Matthew Skala
Bojan Mohar	Radhakrishnan	Alexander Skopalik
Michael Molloy	Tomasz Radzik	Miroslava Sotakova
Morteza Monemizadeh	Rajmohan Rajaraman	Holger Spakowski
Burkhard Monien	Jörg Rambau	Robert Spalek
Angelo Monti	Anup Rao	Bettina Speckmann
Michele Mosca	Robert Raussendorf	Aravind Srinivasan
Luca Moscardelli	R. Ravi	Rob van Stee
Georg Moser	Oded Regev	Ken Steiglitz
Hannes Moser	David Richerby	Martin Strauss
Elchanan Mossel	Liam Roditty	Mukund Sundararajan
Shay Mozes	Gianluca Rossi	Maxim Sviridenko
S. Muthukrishnan	Wojciech Rytter	Troels Bjerre Sørensen
Veli Mäkinen	Harald Räcke	Prasad Tetali
Stefanie Naewe	Heiko Röglin	Dimitrios Thilikos
Daniel Nagaj	Mohammad Salavatipour	Wolfgang Thomas
Ashwin Nayak	Alejandro Salinger	Marc Thurley
Jaroslav Nesetril	Piotr Sankowski	Alex Tiskin
Vincent Nesme	Rahul Santhanam	Isaac K. K. To
Ilan Newman	Thomas Sauerwald	Ben Toner
Pat Nicholson	Petr Savicky	Hanjo Täubig
Carlo Nocentini	Nitin Saxena	Walter Unger
Lars Olbrich	Christian Schaffner	Ugo Vaccaro
Svetlana Olonetsky	Rob Schapire	Salil Vadhan
Krzysztof Onak	Arthur Schmidt	Matt Valeriote
Friedrich Otto	Henning Schnoor	Gregory Valiant
Rasmus Pagh	Nicole Schweikardt	Virginia Vassilevska
Linda Pagli	Robert Schweller	Carmine Ventre
Alessandro Panconesi	Thomas Schwentick	Adrian Vetta
Rina Panigrahy	Jacob Scott	Thomas Vidick
Evi Papaioannou	Danny Segev	Eric Vigoda
Mihai Patrascu	Rocco Servedio	Emanuele Viola
Chris Peikert	C. Seshadhri	Ivan Visconti
David Peleg	Jiri Sgall	Nisheeth Vishnoi
Rudi Pendavingh	Hadas Shachnai	Paola Vocca
Paolo Penna	Ronen Shaltiel	Heribert Vollmer
Carlos Perez-Delgado	Ron Shamir	Jan Vondrak
Giuseppe Persiano	Asaf Shapira	Sergei Vorobyov
Andrea Pietracaprina	Sasha Sherstov	Johannes Waldmann
Alexei Piunovskiy	Yaoyun Shi	Xin Wang
Wojciech Plandowski	Nahum Shimkin	John Watrous

Renato Werneck  
Matthias Westermann  
Mark Weyer  
Peter Widmayer  
Thomas Wilke  
Ryan Williams  
David Williamson

Anthony Wirth  
Pawel Wocjan  
Philipp Woelfel  
Ronald de Wolf  
Prudence W.H. Wong  
Qiqi Yan  
Shi Yaoyun

Shengyu Zhang  
Hairong Zhao  
Martin Ziegler  
Marius Zimand  
David Zuckerman  
Uri Zwick

# Table of Contents – Part I

## Invited Lectures

Graph Structure and Monadic Second-Order Logic: Language Theoretical Aspects . . . . .	1
<i>Bruno Courcelle</i>	
Internet Ad Auctions: Insights and Directions . . . . .	14
<i>S. Muthukrishnan</i>	

## Track A: Algorithms, Automata, Complexity, and Games

### Complexity: Boolean Functions and Circuits

The Complexity of Boolean Formula Minimization . . . . .	24
<i>David Buchfuhrer and Christopher Umans</i>	
Optimal Cryptographic Hardness of Learning Monotone Functions . . . . .	36
<i>Dana Dachman-Soled, Homin K. Lee, Tal Malkin, Rocco A. Servedio, Andrew Wan, and Hoeteck Wee</i>	
On Berge Multiplication for Monotone Boolean Dualization . . . . .	48
<i>Endre Boros, Khaled Elbassioni, and Kazuhisa Makino</i>	
Diagonal Circuit Identity Testing and Lower Bounds . . . . .	60
<i>Nitin Saxena</i>	

### Data Structures

Cell-Probe Proofs and Nondeterministic Cell-Probe Complexity . . . . .	72
<i>Yitong Yin</i>	
Constructing Efficient Dictionaries in Close to Sorting Time . . . . .	84
<i>Milan Ružić</i>	
On List Update with Locality of Reference . . . . .	96
<i>Susanne Albers and Sonja Lauer</i>	
A New Combinatorial Approach for Sparse Graph Problems . . . . .	108
<i>Guy E. Blelloch, Virginia Vassilevska, and Ryan Williams</i>	

## Random Walks and Random Structures

How to Explore a Fast-Changing World . . . . .	121
<i>Chen Avin, Michal Koucký, and Zvi Lotker</i>	
Networks Become Navigable as Nodes Move and Forget . . . . .	133
<i>Augustin Chaintreau, Pierre Fraigniaud, and Emmanuelle Lebhar</i>	
Fast Distributed Computation of Cuts Via Random Circulations . . . . .	145
<i>David Pritchard</i>	
Finding a Maximum Matching in a Sparse Random Graph in $O(n)$ Expected Time . . . . .	161
<i>Prasad Chebolu, Alan Frieze, and Páll Melsted</i>	

## Design and Analysis of Algorithms

Function Evaluation Via Linear Programming in the Priced Information Model . . . . .	173
<i>Ferdinando Cicalese and Eduardo Sany Laber</i>	
Improved Approximation Algorithms for Budgeted Allocations . . . . .	186
<i>Yossi Azar, Benjamin Birnbaum, Anna R. Karlin, Claire Mathieu, and C. Thach Nguyen</i>	
The Travelling Salesman Problem in Bounded Degree Graphs . . . . .	198
<i>Andreas Björklund, Thore Husfeldt, Petteri Kaski, and Mikko Koivisto</i>	
Treewidth Computation and Extremal Combinatorics . . . . .	210
<i>Fedor V. Fomin and Yngve Villanger</i>	

## Scheduling

Fast Scheduling of Weighted Unit Jobs with Release Times and Deadlines . . . . .	222
<i>C. Greg Plaxton</i>	
Approximation Algorithms for Scheduling Parallel Jobs: Breaking the Approximation Ratio of 2 . . . . .	234
<i>Klaus Jansen and Ralf Thöle</i>	
A PTAS for Static Priority Real-Time Scheduling with Resource Augmentation . . . . .	246
<i>Friedrich Eisenbrand and Thomas Rothvoß</i>	

## Codes and Coding

Optimal Monotone Encodings . . . . .	258
<i>Noga Alon and Rani Hod</i>	

Polynomial-Time Construction of Linear Network Coding . . . . .	271
<i>Kazuo Iwama, Harumichi Nishimura, Mike Paterson, Rudy Raymond, and Shigeru Yamashita</i>	

Complexity of Decoding Positive-Rate Reed-Solomon Codes . . . . .	283
<i>Qi Cheng and Daqing Wan</i>	

## Coloring

Computational Complexity of the Distance Constrained Labeling Problem for Trees . . . . .	294
<i>Jiří Fiala, Petr A. Golovach, and Jan Kratochvíl</i>	

The Randomized Coloring Procedure with Symmetry-Breaking . . . . .	306
<i>Sriram Pemmaraju and Aravind Srinivasan</i>	

The Local Nature of List Colorings for Graphs of High Girth . . . . .	320
<i>Flavio Chierichetti and Andrea Vattani</i>	

Approximating List-Coloring on a Fixed Surface . . . . .	333
<i>Ken-ichi Kawarabayashi</i>	

## Randomness in Computation

Asymptotically Optimal Hitting Sets Against Polynomials . . . . .	345
<i>Markus Bläser, Moritz Hardt, and David Steurer</i>	

The Smoothed Complexity of Edit Distance . . . . .	357
<i>Alexandr Andoni and Robert Krauthgamer</i>	

Randomized Self-assembly for Approximate Shapes . . . . .	370
<i>Ming-Yang Kao and Robert Schweller</i>	

Succinct Data Structures for Retrieval and Approximate Membership (Extended Abstract) . . . . .	385
<i>Martin Dietzfelbinger and Rasmus Pagh</i>	

## Online and Dynamic Algorithms

Competitive Weighted Matching in Transversal Matroids . . . . .	397
<i>Nedialko B. Dimitrov and C. Greg Plaxton</i>	

Scheduling for Speed Bounded Processors . . . . .	409
<i>Nikhil Bansal, Ho-Leung Chan, Tak-Wah Lam, and Lap-Kei Lee</i>	

Faster Algorithms for Incremental Topological Ordering . . . . .	421
<i>Bernhard Haeupler, Telikepalli Kavitha, Rogers Mathew, Siddhartha Sen, and Robert E. Tarjan</i>	

Dynamic Normal Forms and Dynamic Characteristic Polynomial . . . . .	434
<i>Gudmund Skovbjerg Frandsen and Piotr Sankowski</i>	

## Approximation Algorithms

Algorithms for $\varepsilon$ -Approximations of Terrains . . . . .	447
<i>Jeff M. Phillips</i>	
An Approximation Algorithm for Binary Searching in Trees . . . . .	459
<i>Eduardo Laber and Marco Molinaro</i>	
Algorithms for 2-Route Cut Problems . . . . .	472
<i>Chandra Chekuri and Sanjeev Khanna</i>	
The Two-Edge Connectivity Survivable Network Problem in Planar Graphs . . . . .	485
<i>Glencora Borradaile and Philip Klein</i>	

## Property Testing

Efficiently Testing Sparse $GF(2)$ Polynomials . . . . .	502
<i>Ilias Diakonikolas, Homin K. Lee, Kevin Matulef, Rocco A. Servedio, and Andrew Wan</i>	
Testing Properties of Sets of Points in Metric Spaces . . . . .	515
<i>Krzysztof Onak</i>	
An Expansion Tester for Bounded Degree Graphs . . . . .	527
<i>Satyen Kale and C. Seshadhri</i>	
Property Testing on $k$ -Vertex-Connectivity of Graphs . . . . .	539
<i>Yuichi Yoshida and Hiro Ito</i>	

## Parameterized Algorithms and Complexity

Almost 2-SAT Is Fixed-Parameter Tractable (Extended Abstract) . . . . .	551
<i>Igor Razgon and Barry O’Sullivan</i>	
On Problems without Polynomial Kernels (Extended Abstract) . . . . .	563
<i>Hans L. Bodlaender, Rodney G. Downey, Michael R. Fellows, and Danny Hermelin</i>	
Faster Algebraic Algorithms for Path and Packing Problems . . . . .	575
<i>Ioannis Koutis</i>	
Understanding the Complexity of Induced Subgraph Isomorphisms . . . . .	587
<i>Yijia Chen, Marc Thurley, and Mark Weyer</i>	

## Graph Algorithms

Spanners in Sparse Graphs . . . . .	597
<i>Feodor F. Dragan, Fedor V. Fomin, and Petr A. Golovach</i>	
Distance Oracles for Unweighted Graphs: Breaking the Quadratic Barrier with Constant Additive Error . . . . .	609
<i>Surender Baswana, Akshay Gaur, Sandeep Sen, and Jayant Upadhyay</i>	
All-Pairs Shortest Paths with a Sublinear Additive Error . . . . .	622
<i>Liam Roditty and Asaf Shapira</i>	
Simpler Linear-Time Modular Decomposition Via Recursive Factorizing Permutations . . . . .	634
<i>Marc Tedder, Derek Corneil, Michel Habib, and Christophe Paul</i>	

## Computational Complexity

The Complexity of the Counting Constraint Satisfaction Problem . . . . .	646
<i>Andrei A. Bulatov</i>	
On the Hardness of Losing Weight . . . . .	662
<i>Andrei Krokhin and Dániel Marx</i>	
Product Theorems Via Semidefinite Programming . . . . .	674
<i>Troy Lee and Rajat Mittal</i>	
Sound 3-Query PCPPs Are Long . . . . .	686
<i>Eli Ben-Sasson, Prahladh Harsha, Oded Lachish, and Arie Matsliah</i>	

## Games and Automata

Approximative Methods for Monotone Systems of Min-Max-Polynomial Equations . . . . .	698
<i>Javier Esparza, Thomas Gawlitza, Stefan Kiefer, and Helmut Seidl</i>	
Recursive Stochastic Games with Positive Rewards . . . . .	711
<i>Kousha Etessami, Dominik Wojtczak, and Mihalis Yannakakis</i>	
Complementation, Disambiguation, and Determinization of Büchi Automata Unified . . . . .	724
<i>Detlef Köhler and Thomas Wilke</i>	
Tree Projections: Hypergraph Games and Minimality . . . . .	736
<i>Gianluigi Greco and Francesco Scarcello</i>	



## Group Testing, Streaming, and Quantum

Explicit Non-adaptive Combinatorial Group Testing Schemes . . . . .	748
<i>Ely Porat and Amir Rothschild</i>	
Tight Lower Bounds for Multi-pass Stream Computation Via Pass Elimination . . . . .	760
<i>Sudipto Guha and Andrew McGregor</i>	
Impossibility of a Quantum Speed-Up with a Faulty Oracle . . . . .	773
<i>Oded Regev and Liron Schiff</i>	
Superpolynomial Speedups Based on Almost Any Quantum Circuit . . . .	782
<i>Sean Hallgren and Aram W. Harrow</i>	

## Algorithmic Game Theory

The Speed of Convergence in Congestion Games under Best-Response Dynamics . . . . .	796
<i>Angelo Fanelli, Michele Flammini, and Luca Moscardelli</i>	
Uniform Budgets and the Envy-Free Pricing Problem . . . . .	808
<i>Patrick Briest</i>	
Bayesian Combinatorial Auctions . . . . .	820
<i>George Christodoulou, Annamária Kovács, and Michael Schapira</i>	
Truthful Unification Framework for Packing Integer Programs with Choices . . . . .	833
<i>Yossi Azar and Iftah Gamzu</i>	

## Quantum

Upper Bounds on the Noise Threshold for Fault-Tolerant Quantum Computing . . . . .	845
<i>Julia Kempe, Oded Regev, Falk Unger, and Ronald de Wolf</i>	
Finding Optimal Flows Efficiently . . . . .	857
<i>Mehdi Mhalla and Simon Perdrix</i>	
Optimal Quantum Adversary Lower Bounds for Ordered Search . . . . .	869
<i>Andrew M. Childs and Troy Lee</i>	
Quantum SAT for a Qutrit-Cinquit Pair Is QMA <sub>1</sub> -Complete . . . . .	881
<i>Lior Eldar and Oded Regev</i>	

<b>Author Index</b> . . . . .	893
-------------------------------	-----

# Table of Contents – Part II

## Invited Lectures

Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency . . . . .	1
<i>Ran Canetti</i>	
Newton’s Method for $\omega$ -Continuous Semirings . . . . .	14
<i>Javier Esparza, Stefan Kiefer, and Michael Luttenberger</i>	

## Track B: Logic, Semantics, and Theory of Programming

### Bounds

The Tractability Frontier for NFA Minimization . . . . .	27
<i>Henrik Björklund and Wim Martens</i>	
Finite Automata, Digraph Connectivity, and Regular Expression Size (Extended Abstract) . . . . .	39
<i>Hermann Gruber and Markus Holzer</i>	
Leftist Grammars Are Non-primitive Recursive . . . . .	51
<i>Tomasz Jurdziński</i>	
On the Computational Completeness of Equations over Sets of Natural Numbers . . . . .	63
<i>Artur Jež and Alexander Okhotin</i>	

### Distributed Computation

Placement Inference for a Client-Server Calculus . . . . .	75
<i>Matthias Neubauer and Peter Thiemann</i>	
Extended pi-Calculi . . . . .	87
<i>Magnus Johansson, Joachim Parrow, Björn Victor, and Jesper Bengtson</i>	
Completeness and Logical Full Abstraction in Modal Logics for Typed Mobile Processes . . . . .	99
<i>Martin Berger, Kohei Honda, and Nobuko Yoshida</i>	

## Real-Time and Probabilistic Systems

On the Sets of Real Numbers Recognized by Finite Automata in Multiple Bases . . . . .	112
<i>Bernard Boigelot, Julien Brusten, and Véronique Bruyère</i>	
On Expressiveness and Complexity in Real-Time Model Checking . . . . .	124
<i>Patricia Bouyer, Nicolas Markey, Joël Ouaknine, and James Worrell</i>	
STORMED Hybrid Systems . . . . .	136
<i>Vladimeros Vladimerou, Pavithra Prabhakar, Mahesh Viswanathan, and Geir Dullerud</i>	
Controller Synthesis and Verification for Markov Decision Processes with Qualitative Branching Time Objectives . . . . .	148
<i>Tomáš Brázdil, Vojtěch Forejt, and Antonín Kučera</i>	

## Logic and Complexity

On Datalog vs. LFP . . . . .	160
<i>Anuj Dawar and Stephan Kreutzer</i>	
Directed <i>st</i> -Connectivity Is Not Expressible in Symmetric Datalog . . . . .	172
<i>László Egri, Benoît Larose, and Pascal Tesson</i>	
Non-dichotomies in Constraint Satisfaction Complexity . . . . .	184
<i>Manuel Bodirsky and Martin Grohe</i>	
Quantified Constraint Satisfaction and the Polynomially Generated Powers Property (Extended Abstract) . . . . .	197
<i>Hubie Chen</i>	

## Words and Trees

When Does Partial Commutative Closure Preserve Regularity? . . . . .	209
<i>Antonio Cano Gómez, Giovanna Guaiana, and Jean-Éric Pin</i>	
Weighted Logics for Nested Words and Algebraic Formal Power Series . . . . .	221
<i>Christian Mathissen</i>	
Tree Languages Defined in First-Order Logic with One Quantifier Alternation . . . . .	233
<i>Mikołaj Bojańczyk and Luc Segoufin</i>	
Duality and Equational Theory of Regular Languages . . . . .	246
<i>Mai Gehrke, Serge Grigorieff, and Jean-Éric Pin</i>	

## Nonstandard Models of Computation

Reversible Flowchart Languages and the Structured Reversible Program Theorem .....	258
<i>Tetsuo Yokoyama, Holger Bock Axelsen, and Robert Glück</i>	
Attribute Grammars and Categorical Semantics .....	271
<i>Shin-ya Katsumata</i>	
A Domain Theoretic Model of Qubit Channels.....	283
<i>Keye Martin</i>	
Interacting Quantum Observables .....	298
<i>Bob Coecke and Ross Duncan</i>	

## Reasoning about Computation

Perpetuality for Full and Safe Composition (in a Constructive Setting) .....	311
<i>Delia Kesner</i>	
A System F with Call-by-Name Exceptions.....	323
<i>Sylvain Lebesne</i>	
Linear Logical Algorithms.....	336
<i>Robert J. Simmons and Frank Pfenning</i>	
A Simple Model of Separation Logic for Higher-Order Store .....	348
<i>Lars Birkedal, Bernhard Reus, Jan Schwinghammer, and Hongseok Yang</i>	

## Verification

Open Implication .....	361
<i>Karin Greimel, Roderick Bloem, Barbara Jobstmann, and Moshe Vardi</i>	
ATL* Satisfiability Is 2EXPTIME-Complete .....	373
<i>Sven Schewe</i>	
Visibly Pushdown Transducers.....	386
<i>Jean-François Raskin and Frédéric Servais</i>	
The Non-deterministic Mostowski Hierarchy and Distance-Parity Automata .....	398
<i>Thomas Colcombet and Christof Löding</i>	
Analyzing Context-Free Grammars Using an Incremental SAT Solver ...	410
<i>Roland Axelsson, Keijo Heljanko, and Martin Lange</i>	

**Track C: Security and Cryptography Foundations****Theory**

Weak Pseudorandom Functions in Minicrypt . . . . .	423
<i>Krzysztof Pietrzak and Johan Sjödin</i>	
On Black-Box Ring Extraction and Integer Factorization . . . . .	437
<i>Kristina Altmann, Tibor Jager, and Andy Rupp</i>	
Extractable Perfectly One-Way Functions . . . . .	449
<i>Ran Canetti and Ronny Ramzi Dakdouk</i>	
Error-Tolerant Combiners for Oblivious Primitives . . . . .	461
<i>Bartosz Przydatek and Jürg Wullschleger</i>	

**Secure Computation**

Asynchronous Multi-party Computation with Quadratic Communication . . . . .	473
<i>Martin Hirt, Jesper Buus Nielsen, and Bartosz Przydatek</i>	
Improved Garbled Circuit: Free XOR Gates and Applications . . . . .	486
<i>Vladimir Kolesnikov and Thomas Schneider</i>	
Improving the Round Complexity of VSS in Point-to-Point Networks . . .	499
<i>Jonathan Katz, Chiu-Yuen Koo, and Ranjit Kumaresan</i>	
How to Protect Yourself without Perfect Shredding . . . . .	511
<i>Ran Canetti, Dror Eiger, Shafi Goldwasser, and Dah-Yoh Lim</i>	

**Two-Party Protocols and Zero-Knowledge**

Universally Composable Undeniable Signature . . . . .	524
<i>Kaoru Kurosawa and Jun Furukawa</i>	
Interactive PCP . . . . .	536
<i>Yael Tauman Kalai and Ran Raz</i>	
Constant-Round Concurrent Non-malleable Zero Knowledge in the Bare Public-Key Model . . . . .	548
<i>Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti</i>	

**Encryption with Special Properties/Quantum  
Cryptography**

Delegating Capabilities in Predicate Encryption Systems . . . . .	560
<i>Elaine Shi and Brent Waters</i>	

Bounded Ciphertext Policy Attribute Based Encryption . . . . .	579
<i>Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai</i>	
Making Classical Honest Verifier Zero Knowledge Protocols Secure against Quantum Attacks . . . . .	592
<i>Sean Hallgren, Alexandra Kolla, Pranab Sen, and Shengyu Zhang</i>	
Composable Security in the Bounded-Quantum-Storage Model . . . . .	604
<i>Stephanie Wehner and Jürg Wullschleger</i>	

## Various Types of Hashing

On the Strength of the Concatenated Hash Combiner When All the Hash Functions Are Weak . . . . .	616
<i>Jonathan J. Hoch and Adi Shamir</i>	
History-Independent Cuckoo Hashing . . . . .	631
<i>Moni Naor, Gil Segev, and Udi Wieder</i>	
Building a Collision-Resistant Compression Function from Non-compressing Primitives (Extended Abstract) . . . . .	643
<i>Thomas Shrimpton and Martijn Stam</i>	
Robust Multi-property Combiners for Hash Functions Revisited . . . . .	655
<i>Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak</i>	

## Public-Key Cryptography/Authentication

Homomorphic Encryption with CCA Security . . . . .	667
<i>Manoj Prabhakaran and Mike Rosulek</i>	
How to Encrypt with the LPN Problem . . . . .	679
<i>Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin</i>	
Could SFLASH be Repaired? . . . . .	691
<i>Jintai Ding, Vivien Dubois, Bo-Yin Yang, Owen Chia-Hsin Chen, and Chen-Mou Cheng</i>	
Password Mistyping in Two-Factor-Authenticated Key Exchange . . . . .	702
<i>Vladimir Kolesnikov and Charles Rackoff</i>	
Affiliation-Hiding Envelope and Authentication Schemes with Efficient Support for Multiple Credentials . . . . .	715
<i>Stanisław Jarecki and Xiaomin Liu</i>	
<b>Author Index</b> . . . . .	727