Lecture Notes in Computer Science 5125

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

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

Automata, Languages and Programming

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

Springer

Volume Editors

Luca Aceto
Magnús M. Halldórsson
Anna Ingólfsdóttir
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

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

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

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

Track A: Algorithms, Automata, Complexity, and Games

Complexity: Boolean Functions and Circuits

Data Structures

Random Walks and Random Structures

Design and Analysis of Algorithms

Scheduling

Codes and Coding

Coloring

Randomness in Computation

Online and Dynamic Algorithms

Approximation Algorithms

Property Testing

Parameterized Algorithms and Complexity

Graph Algorithms

Computational Complexity

Games and Automata

Group Testing, Streaming, and Quantum

Algorithmic Game Theory

Quantum

Table of Contents – Part II

Invited Lectures

Track B: Logic, Semantics, and Theory of Programming

Bounds

Distributed Computation

Real-Time and Probabilistic Systems

Logic and Complexity

Words and Trees

Nonstandard Models of Computation

Reasoning about Computation

Verification

Track C: Security and Cryptography Foundations

Theory

Secure Computation

Two-Party Protocols and Zero-Knowledge

Encryption with Special Properties/Quantum Cryptography

Various Types of Hashing

Public-Key Cryptography/Authentication