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 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). A companion volume includes 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). 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:

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
VI  Preface

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 consid-
eration, 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 grate-
ful to all members of the Organizing Committee in the School of Computer Sci-
ence and to the Facilities and Technical staff of Reykjavik University. Thanks to
Andrei Voronkov and Shai Halevi for writing the conference-management sys-
tems 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
VIII Organization

Radha Jagadeesan, 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

Michel Abdalla
Andreas Abel
Jiri Adamek
Ben Adida
Foto Afrati
Benjamin Aminof
Torben Amtoft
Vikraman Arvind
Giuseppe Ateniese
Albert Atserias
Jean-Philippe Aumasson
Thomas Baigures
Steffen van Bakel
Vince Barany
Joerg Bauer
Nick Benton
C`ome Berbain
Martin Berger
Lennart Beringer
Nathalie Bertrand
Puneet Bhatia
Henrik Björklund
Bruno Blanchet
Manuel Bodirsky
Mikolaj Bojanczyk
Benedikt Bollig
Michele Boreale
Hoppe Bos
Charles Bouillaguet
Patricia Bouyer
Tomas Brazdil
Thomas Brihaye
Andrei Bulatov
Manuela Burojani
Thomas Bäck
Cristian S. Calude
Olivier Carton
Frank Cassez
Dario Catalano
Balder ten Cate
Rafik Chaabouni
Amine Chaieb
Supratik Chakraborty
Prakash Chandrasekaran
Krishnendu Chatterjee
Jan Chomicki
Evelyne Contejean
Scott Contini
Veronique Cortier
Arnaud Da Costa
Deepak D’Souza
Victor Dalmau
Mads Dam
Pierpaolo Degano
Gioergio Delzanno
Stephane Demri
Yuxin Deng
Alex Dent
Josee Desharnais
Dan Dougherty
Ross Duncan
Ir`ene Durand
Stephen A. Edwards
Jean-Daniel Fujisaki
Javier Esparza
John Fearney
Serge Fehr
Jerome Feret
Anna Lisa Ferrara
Maribel Fernandez
Marc Fischlin
Matthias Fitzi
Riccardo Focardi
Wan Fokkink
Georg Fuchs
Murdoch Gabbay
Fabio Gadducci
Tobias Ganzow
Juan Garay
Stephane Gaubert
Blaise Genest
Silvia Ghilezan
Giuseppe De Giacomo
Hugo Gimbert
Cinzia Di Giusto
Rob van Glabek
Stefania Gnesi
Emmanuel Godard
Rodolfo Gomez
Michaela Goetz
Mikael Goldmann
Daniele Gorla
Nathaniel Gray
Gianluigi Greco
Matthew Green
Alain Griffault
Gary Griffing
Serge Grigorieff
Colas Le Guernic
Stefano Guerrini
Peter Habermehl
Serge Haddad
Esfandiar Haghighi
Matthew Hague
Noomene Ben Henda
Monika Henzinger
Holger Hermanns
Thomas Hildebrandt
Jane Hillston
Peter Hines
Markus Holzer
Andreas Holzer
Haruo Hosoya
Nick Howgrave-Graham
C`at`al`in Hritcu
Juraj Hromkovic
Emeline Hufschmitt
Radu Iosif
Ellen Jochemsz
Jan Johannsen
Lisa Kaati
Joost-Pieter Katoen
Stefan Kiefer
Eike Kiltz
Joachim Klein
Joost Kok
Pavel Krcal
Gunar Kreitz
Manfred Kufleitner
Stefan Kugele
K. Narayan Kumar
# Table of Contents – Part II

## Invited Lectures

Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency ................................................................. 1  
*Ran Canetti*

Newton’s Method for $\omega$-Continuous Semirings ........................ 14  
*Javier Esparza, Stefan Kiefer, and Michael Luttenberger*

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

### Bounds

The Tractability Frontier for NFA Minimization ............................... 27  
*Henrik Björklund and Wim Martens*

Finite Automata, Digraph Connectivity, and Regular Expression Size (Extended Abstract) ......................................................... 39  
*Hermann Gruber and Markus Holzer*

Leftist Grammars Are Non-primitive Recursive .............................. 51  
*Tomasz Jurdziński*

On the Computational Completeness of Equations over Sets of Natural Numbers ................................................................. 63  
*Artur Jeż and Alexander Okhotin*

## Distributed Computation

Placement Inference for a Client-Server Calculus ............................. 75  
*Matthias Neubauer and Peter Thiemann*

Extended pi-Calculi ........................................................................ 87  
*Magnus Johansson, Joachim Parrow, Björn Victor, and Jesper Bengtson*

Completeness and Logical Full Abstraction in Modal Logics for Typed Mobile Processes ......................................................... 99  
*Martin Berger, Kohei Honda, and Nobuko Yoshida*
# Real-Time and Probabilistic Systems

On the Sets of Real Numbers Recognized by Finite Automata in Multiple Bases ................................................... 112
*Bernard Boigelot, Julien Brusten, and Véronique Bruyère*

On Expressiveness and Complexity in Real-Time Model Checking ...... 124
*Patricia Bouyer, Nicolas Markey, Joël Ouaknine, and James Worrell*

STORMED Hybrid Systems ........................................ 136
*Vladimeros Vladimerou, Pavithra Prabhakar, Mahesh Viswanathan, and Geir Dullerud*

Controller Synthesis and Verification for Markov Decision Processes with Qualitative Branching Time Objectives ....................... 148
*Tomáš Brázdil, Vojtěch Forejt, and Antonín Kučera*

# Logic and Complexity

On Datalog vs. LFP .................................................... 160
*Anuj Dawar and Stephan Kreutzer*

Directed $st$-Connectivity Is Not Expressible in Symmetric Datalog ...... 172
*László Egri, Benoît Larose, and Pascal Tesson*

Non-dichotomies in Constraint Satisfaction Complexity ............... 184
*Manuel Bodirsky and Martin Grohe*

Quantified Constraint Satisfaction and the Polynomially Generated Powers Property (Extended Abstract) .............................. 197
*Hubie Chen*

# Words and Trees

When Does Partial Commutative Closure Preserve Regularity? .......... 209
*Antonio Cano Gómez, Giovanna Guaiana, and Jean-Éric Pin*

Weighted Logics for Nested Words and Algebraic Formal Power Series ................................................................. 221
*Christian Mathissen*

Tree Languages Defined in First-Order Logic with One Quantifier Alternation ............................................................... 233
*Mikołaj Bojańczyk and Luc Segoufin*

Duality and Equational Theory of Regular Languages .................. 246
*Mai Gehrke, Serge Grigorieff, and Jean-Éric Pin*
# Table of Contents – Part II

## Nonstandard Models of Computation

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

## Reasoning about Computation

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

## Verification

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

Theory

Weak Pseudorandom Functions in Minicrypt .................................. 423
  Krzysztof Pietrzak and Johan Sjödin

On Black-Box Ring Extraction and Integer Factorization ............. 437
  Kristina Altmann, Tibor Jager, and Andy Rupp

Extractable Perfectly One-Way Functions .................................. 449
  Ran Canetti and Ronny Ramzi Dakdouk

Error-Tolerant Combiners for Oblivious Primitives ...................... 461
  Bartosz Przydatek and Jürg Wullschleger

Secure Computation

Asynchronous Multi-party Computation with Quadratic Communication .................................................. 473
  Martin Hirt, Jesper Buus Nielsen, and Bartosz Przydatek

Improved Garbled Circuit: Free XOR Gates and Applications .......... 486
  Vladimir Kolesnikov and Thomas Schneider

Improving the Round Complexity of VSS in Point-to-Point Networks . . 499
  Jonathan Katz, Chiu-Yuen Koo, and Ranjit Kumaresan

How to Protect Yourself without Perfect Shredding ...................... 511
  Ran Canetti, Dror Eiger, Shafi Goldwasser, and Dah-Yoh Lim

Two-Party Protocols and Zero-Knowledge

Universally Composable Undeniable Signature ............................. 524
  Kaoru Kurosawa and Jun Furukawa

Interactive PCP ........................................................................ 536
  Yael Tauman Kalai and Ran Raz

Constant-Round Concurrent Non-malleable Zero Knowledge in the Bare Public-Key Model ............................... 548
  Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti

Encryption with Special Properties/Quantum Cryptography

Delegating Capabilities in Predicate Encryption Systems ............. 560
  Elaine Shi and Brent Waters
Bounded Ciphertext Policy Attribute Based Encryption .......................... 579  
Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai

Making Classical Honest Verifier Zero Knowledge Protocols Secure  
against Quantum Attacks ........................................................................ 592  
Sean Hallgren, Alexandra Kolla, Pranab Sen, and Shengyu Zhang

Composable Security in the Bounded-Quantum-Storage Model ........ 604  
Stephanie Wehner and Jürg Wullschleger

Various Types of Hashing

On the Strength of the Concatenated Hash Combiner When All the  
Hash Functions Are Weak ........................................................................ 616  
Jonathan J. Hoch and Adi Shamir

History-Independent Cuckoo Hashing .................................................. 631  
Moni Naor, Gil Segev, and Udi Wieder

Building a Collision-Resistant Compression Function from  
Non-compressing Primitives (Extended Abstract) .............................. 643  
Thomas Shrimpton and Martijn Stam

Robust Multi-property Combiners for Hash Functions Revisited .... 655  
Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak

Public-Key Cryptography/Authentication

Homomorphic Encryption with CCA Security ................................... 667  
Manoj Prabhakaran and Mike Rosulek

How to Encrypt with the LPN Problem ............................................. 679  
Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin

Could SFLASH be Repaired? ............................................................... 691  
Jintai Ding, Vivien Dubois, Bo-Yin Yang,  
Owen Chia-Hsin Chen, and Chen-Mou Cheng

Password Mistyping in Two-Factor-Authenticated Key Exchange .... 702  
Vladimir Kolesnikov and Charles Rackoff

Affiliation-Hiding Envelope and Authentication Schemes with Efficient  
Support for Multiple Credentials ..................................................... 715  
Stanisław Jarecki and Xiaomin Liu

Author Index ...................................................................................... 727
# Table of Contents – Part I

## Invited Lectures

Graph Structure and Monadic Second-Order Logic: Language Theoretical Aspects .............................................. 1  
*Bruno Courcelle*

Internet Ad Auctions: Insights and Directions ..................... 14  
*S. Muthukrishnan*

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

### Complexity: Boolean Functions and Circuits

The Complexity of Boolean Formula Minimization ................. 24  
*David Buchfuhrer and Christopher Umans*

Optimal Cryptographic Hardness of Learning Monotone Functions ...... 36  
*Dana Dachman-Soled, Homin K. Lee, Tal Malkin, Rocco A. Servedio, Andrew Wan, and Hoeteck Wee*

On Berge Multiplication for Monotone Boolean Dualization .......... 48  
*Endre Boros, Khaled Elbassioni, and Kazuhisa Makino*

Diagonal Circuit Identity Testing and Lower Bounds ............... 60  
*Nitin Saxena*

## Data Structures

Cell-Probe Proofs and Nondeterministic Cell-Probe Complexity ........ 72  
*Yitong Yin*

Constructing Efficient Dictionaries in Close to Sorting Time .......... 84  
*Milan Ružić*

On List Update with Locality of Reference .......................... 96  
*Susanne Albers and Sonja Lauer*

A New Combinatorial Approach for Sparse Graph Problems .......... 108  
*Guy E. Blelloch, Virginia Vassilevska, and Ryan Williams*
Random Walks and Random Structures

How to Explore a Fast-Changing World .......................... 121  
Chen Avin, Michal Koucký, and Zvi Lotker

Networks Become Navigable as Nodes Move and Forget ............ 133  
Augustin Chaintreau, Pierre Fraigniaud, and Emmanuelle Lebhar

Fast Distributed Computation of Cuts Via Random Circulations ...... 145  
David Pritchard

Finding a Maximum Matching in a Sparse Random Graph in $O(n)$ Expected Time .......................................................... 161  
Prasad Chebolu, Alan Frieze, and Páll Melsted

Design and Analysis of Algorithms

Function Evaluation Via Linear Programming in the Priced Information Model ................................................................. 173  
Ferdinando Cicalese and Eduardo Sany Laber

Improved Approximation Algorithms for Budgeted Allocations ......... 186  
Yossi Azar, Benjamin Birnbaum, Anna R. Karlin, Claire Mathieu, and C. Thach Nguyen

The Travelling Salesman Problem in Bounded Degree Graphs .......... 198  
Andreas Björklund, Thore Husfeldt, Petteri Kaski, and Mikko Koivisto

Treewidth Computation and Extremal Combinatorics ................ 210  
Fedor V. Fomin and Yngve Villanger

Scheduling

Fast Scheduling of Weighted Unit Jobs with Release Times and Deadlines ................................................................. 222  
C. Greg Plaxton

Approximation Algorithms for Scheduling Parallel Jobs: Breaking the Approximation Ratio of 2 ......................................... 234  
Klaus Jansen and Ralf Thöle

A PTAS for Static Priority Real-Time Scheduling with Resource Augmentation ................................................................. 246  
Friedrich Eisenbrand and Thomas Rothvoß

Codes and Coding

Optimal Monotone Encodings ............................................. 258  
Noga Alon and Rani Hod
Polynomial-Time Construction of Linear Network Coding .......................... 271
   Kazuo Iwama, Harumichi Nishimura, Mike Paterson,
   Rudy Raymond, and Shigeru Yamashita

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

**Coloring**

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

The Randomized Coloring Procedure with Symmetry-Breaking ............... 306
   Sriram Pemmaraju and Aravind Srinivasan

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

Approximating List-Coloring on a Fixed Surface ............................... 333
   Ken-ichi Kawarabayashi

**Randomness in Computation**

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

The Smoothed Complexity of Edit Distance ..................................... 357
   Alexandr Andoni and Robert Krauthgamer

Randomized Self-assembly for Approximate Shapes ............................ 370
   Ming-Yang Kao and Robert Schweller

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

**Online and Dynamic Algorithms**

Competitive Weighted Matching in Transversal Matroids ...................... 397
   Nedialko B. Dimitrov and C. Greg Plaxton

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

Faster Algorithms for Incremental Topological Ordering ..................... 421
   Bernhard Haeupler, Telikepalli Kavitha, Rogers Mathew,
   Siddhartha Sen, and Robert E. Tarjan
Dynamic Normal Forms and Dynamic Characteristic Polynomial ........ 434  
*Gudmund Skovbjerg Frandsen and Piotr Sankowski*

**Approximation Algorithms**

Algorithms for $\varepsilon$-Approximations of Terrains ................. 447  
*Jeff M. Phillips*

An Approximation Algorithm for Binary Searching in Trees ............. 459  
*Eduardo Laber and Marco Molinaro*

Algorithms for 2-Route Cut Problems .................................... 472  
*Chandra Chekuri and Sanjeev Khanna*

The Two-Edge Connectivity Survivable Network Problem in Planar Graphs .......................................................... 485  
*Glencora Borradaile and Philip Klein*

**Property Testing**

Efficiently Testing Sparse $GF(2)$ Polynomials ......................... 502  
*Ilias Diakonikolas, Homin K. Lee, Kevin Matulef, Rocco A. Servedio, and Andrew Wan*

Testing Properties of Sets of Points in Metric Spaces ................. 515  
*Krzysztof Onak*

An Expansion Tester for Bounded Degree Graphs ......................... 527  
*Satyen Kale and C. Seshadhri*

Property Testing on $k$-Vertex-Connectivity of Graphs .................. 539  
*Yuichi Yoshida and Hiro Ito*

**Parameterized Algorithms and Complexity**

Almost 2-SAT Is Fixed-Parameter Tractable (Extended Abstract) ....... 551  
*Igor Razgon and Barry O’Sullivan*

On Problems without Polynomial Kernels (Extended Abstract) ........... 563  
*Hans L. Bodlaender, Rodney G. Downey, Michael R. Fellows, and Danny Hermelin*

Faster Algebraic Algorithms for Path and Packing Problems ............ 575  
*Ioannis Koutis*

Understanding the Complexity of Induced Subgraph Isomorphisms ...... 587  
*Yijia Chen, Marc Thurley, and Mark Weyer*
## Graph Algorithms

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

## Computational Complexity

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

## Games and Automata

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approximative Methods for Monotone Systems of Min-Max-Polynomial Equations</td>
<td>698</td>
</tr>
<tr>
<td>Javier Esparza, Thomas Gawlitza, Stefan Kiefer, and Helmut Seidl</td>
<td></td>
</tr>
<tr>
<td>Recursive Stochastic Games with Positive Rewards</td>
<td>711</td>
</tr>
<tr>
<td>Kousha Etessami, Dominik Wojtczak, and Mihalis Yannakakis</td>
<td></td>
</tr>
<tr>
<td>Complementation, Disambiguation, and Determinization of Büchi Automata Unified</td>
<td>724</td>
</tr>
<tr>
<td>Detlef Kähler and Thomas Wilke</td>
<td></td>
</tr>
<tr>
<td>Tree Projections: Hypergraph Games and Minimality</td>
<td>736</td>
</tr>
<tr>
<td>Gianluigi Greco and Francesco Scarcello</td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents – Part I

## Group Testing, Streaming, and Quantum

- **Explicit Non-adaptive Combinatorial Group Testing Schemes** ........................................... 748  
  *Ely Porat and Amir Rothschild*

- **Tight Lower Bounds for Multi-pass Stream Computation Via Pass Elimination** ........................................ 760  
  *Sudipto Guha and Andrew McGregor*

- **Impossibility of a Quantum Speed-Up with a Faulty Oracle** ........................................... 773  
  *Oded Regev and Liron Schiff*

- **Superpolynomial Speedups Based on Almost Any Quantum Circuit** ........................................... 782  
  *Sean Hallgren and Aram W. Harrow*

## Algorithmic Game Theory

- **The Speed of Convergence in Congestion Games under Best-Response Dynamics** ........................................ 796  
  *Angelo Fanelli, Michele Flammini, and Luca Moscardelli*

- **Uniform Budgets and the Envy-Free Pricing Problem** ........................................... 808  
  *Patrick Briest*

- **Bayesian Combinatorial Auctions** ........................................... 820  
  *George Christodoulou, Annamária Kovács, and Michael Schapira*

- **Truthful Unification Framework for Packing Integer Programs with Choices** ........................................... 833  
  *Yossi Azar and Iftah Gamzu*

## Quantum

- **Upper Bounds on the Noise Threshold for Fault-Tolerant Quantum Computing** ........................................ 845  
  *Julia Kempe, Oded Regev, Falk Unger, and Ronald de Wolf*

- **Finding Optimal Flows Efficiently** ........................................... 857  
  *Mehdi Mhalla and Simon Perdrix*

- **Optimal Quantum Adversary Lower Bounds for Ordered Search** ........................................... 869  
  *Andrew M. Childs and Troy Lee*

- **Quantum SAT for a Qutrit-Cinquit Pair Is QMA$_1$-Complete** ........................................... 881  
  *Lior Eldar and Oded Regev*

## Author Index

 ........................................... 893