

31st Conference on Computational Complexity

CCC'16, May 29 to June 1, 2016, Tokyo, Japan

Edited by
Ran Raz



Editor

Ran Raz
Department of Computer Science and Applied Math.
Weizmann Institute of Science
Rehovot 76100
Israel
ran.raz@weizmann.ac.il

ACM Classification 1998
F. Theory of Computation

ISBN 978-3-95977-008-8

Published online and open access by

Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at <http://www.dagstuhl.de/dagpub/978-3-95977-008-8>.

Publication date

May, 2016

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available from the Internet at <http://dnb.d-nb.de>.

License

This work is licensed under a Creative Commons Attribution 3.0 Unported license (CC-BY 3.0): <http://creativecommons.org/licenses/by/3.0/legalcode>.



In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work under the following conditions, without impairing or restricting the authors' moral rights:

- Attribution: The work must be attributed to its authors.

The copyright is retained by the corresponding authors.

Digital Object Identifier: 10.4230/10.4230/LIPIcs.CCC.2016.i

ISBN 978-3-95977-008-8

ISSN 1868-8969

<http://www.dagstuhl.de/lipics>

LIPICs – Leibniz International Proceedings in Informatics

LIPICs is a series of high-quality conference proceedings across all fields in informatics. LIPICs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

Editorial Board

- Susanne Albers (TU München)
- Chris Hankin (Imperial College London)
- Deepak Kapur (University of New Mexico)
- Michael Mitzenmacher (Harvard University)
- Madhavan Mukund (Chennai Mathematical Institute)
- Catuscia Palamidessi (INRIA)
- Wolfgang Thomas (*Chair*, RWTH Aachen)
- Pascal Weil (CNRS and University Bordeaux)
- Reinhard Wilhelm (Saarland University)

ISSN 1868-8969

<http://www.dagstuhl.de/lipics>

■ Contents

Preface	
<i>Ran Raz</i>	0:ix–0:ix
Average-Case Lower Bounds and Satisfiability Algorithms for Small Threshold Circuits	
<i>Ruiwen Chen, Rahul Santhanam, and Srikanth Srinivasan</i>	1:1–1:35
Strong ETH Breaks With Merlin and Arthur: Short Non-Interactive Proofs of Batch Evaluation	
<i>Richard Ryan Williams</i>	2:1–2:17
Toward the KRW Composition Conjecture: Cubic Formula Lower Bounds via Communication Complexity	
<i>Irit Dinur and Or Meir</i>	3:1–3:51
Nearly Optimal Separations Between Communication (or Query) Complexity and Partitions	
<i>Andris Ambainis, Martins Kokainis, and Robin Kothari</i>	4:1–4:14
A Composition Theorem for Conical Juntas	
<i>Mika Göös and T. S. Jayram</i>	5:1–5:16
Tight Bounds for Communication-Assisted Agreement Distillation	
<i>Venkatesan Guruswami and Jaikumar Radhakrishnan</i>	6:1–6:17
New Extractors for Interleaved Sources	
<i>Eshan Chattopadhyay and David Zuckerman</i>	7:1–7:28
Non-Malleable Extractors – New Tools and Improved Constructions	
<i>Gil Cohen</i>	8:1–8:29
Pseudorandomness When the Odds are Against You	
<i>Sergei Artemenko, Russell Impagliazzo, Valentine Kabanets, and Ronen Shaltiel</i>	9:1–9:35
Learning Algorithms from Natural Proofs	
<i>Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova</i>	10:1–10:24
Decoding Reed-Muller Codes Over Product Sets	
<i>John Y. Kim and Swastik Kopparty</i>	11:1–11:28
Lower Bounds for Constant Query Affine-Invariant LCCs and LTCs	
<i>Arnab Bhattacharyya and Sivakanth Gopi</i>	12:1–12:17
Degree and Sensitivity: Tails of Two Distributions	
<i>Parikshit Gopalan, Rocco A. Servedio, and Avi Wigderson</i>	13:1–13:23
New Hardness Results for Graph and Hypergraph Colorings	
<i>Joshua Brakensiek and Venkatesan Guruswami</i>	14:1–14:27
Invariance Principle on the Slice	
<i>Yuval Filmus, Guy Kindler, Elchanan Mossel, and Karl Wimmer</i>	15:1–15:10



Harmonicity and Invariance on Slices of the Boolean Cube <i>Yuval Filmus and Elchanan Mossel</i>	16:1–16:13
On the Sum-of-Squares Degree of Symmetric Quadratic Functions <i>Troy Lee, Anupam Prakash, Ronald de Wolf, and Henry Yuen</i>	17:1–17:31
Limits of Minimum Circuit Size Problem as Oracle <i>Shuichi Hirahara and Osamu Watanabe</i>	18:1–18:20
New Non-Uniform Lower Bounds for Uniform Classes <i>Lance Fortnow and Rahul Santhanam</i>	19:1–19:14
New Characterizations in Turnstile Streams with Applications <i>Yuqing Ai, Wei Hu, Yi Li, and David P. Woodruff</i>	20:1–20:22
Evolution and Computation (<i>Invited Talk</i>) <i>Nisheeth K. Vishnoi</i>	21:1–21:1
Tight SoS-Degree Bounds for Approximate Nash Equilibria <i>Aram W. Harrow, Anand V. Natarajan, and Xiaodi Wu</i>	22:1–22:25
Understanding PPA-Completeness <i>Xiaotie Deng, Jack R. Edmonds, Zhe Feng, Zhengyang Liu, Qi Qi, and Zeying Xu</i>	23:1–23:25
Polynomial Bounds for Decoupling, with Applications <i>Ryan O’Donnell and Yu Zhao</i>	24:1–24:18
Polynomials, Quantum Query Complexity, and Grothendieck’s Inequality <i>Scott Aaronson, Andris Ambainis, Jānis Iraids, Martins Kokainis, and Juris Smotrovs</i>	25:1–25:19
Sculpting Quantum Speedups <i>Scott Aaronson and Shalev Ben-David</i>	26:1–26:28
A Linear Time Algorithm for Quantum 2-SAT <i>Niel de Beaudrap and Sevag Gharibian</i>	27:1–27:21
Complexity Classification of Two-Qubit Commuting Hamiltonians <i>Adam Bouland, Laura Mančinská, and Xue Zhang</i>	28:1–28:33
Identity Testing for Constant-Width, and Commutative, Read-Once Oblivious ABPs <i>Rohit Gurjar, Arpita Korwar, and Nitin Saxena</i>	29:1–29:16
Identity Testing and Lower Bounds for Read- k Oblivious Algebraic Branching Programs <i>Matthew Anderson, Michael A. Forbes, Ramprasad Saptharishi, Amir Shpilka, and Ben Lee Volk</i>	30:1–30:25
Reconstruction of Real Depth-3 Circuits with Top Fan-In 2 <i>Gaurav Sinha</i>	31:1–31:53
Proof Complexity Lower Bounds from Algebraic Circuit Complexity <i>Michael A. Forbes, Amir Shpilka, Iddo Zameret, and Avi Wigderson</i>	32:1–32:17

Functional Lower Bounds for Arithmetic Circuits and Connections to Boolean
Circuit Complexity
Michael A. Forbes, Mrinal Kumar, and Ramprasad Saptharishi 33:1–33:19

Arithmetic Circuits with Locally Low Algebraic Rank
Mrinal Kumar and Shubhangi Saraf 34:1–34:27

Sums of Products of Polynomials in Few Variables: Lower Bounds and Polynomial
Identity Testing
Mrinal Kumar and Shubhangi Saraf 35:1–35:29

■ Preface

The papers in this volume were accepted for presentation at the 31st Conference on Computational Complexity (CCC'16), held May 29 to June 1, 2016 in Tokyo, Japan. The conference is organized by the Computational Complexity Foundation (CCF) and the Center for Exploring the Limits of Computation (CELC) in cooperation with the European Association for Theoretical Computer Science (EATCS) and the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT). CCC'16 is sponsored by Microsoft Research.

The call for papers sought original research papers in all areas of computational complexity theory. Of the 91 submissions the program committee selected 34 for presentation at the conference.

The program committee would like to thank everyone involved in the conference, including all those who submitted papers for consideration as well as the reviewers for their scientific contributions; the board of trustees of the Computational Complexity Foundation and especially its president Dieter van Melkebeek for extensive advice and assistance; Jacobo Toran and Jeff Kinne for a variety of assistance; David Zuckerman for sharing his knowledge as 2015 PC chair; the Local Arrangements Committee and especially its chair Osamu Watanabe; Nisheeth Vishnoi for contributing an invited talk; and Marc Herbstritt for coordinating the production of these proceedings.

Ran Raz
Program Committee Chair



■ Awards

The program committee of the 31st Conference on Computational Complexity is happy to present the *Best Paper Award* to Marco Carmosino, Russell Impagliazzo, Valentine Kabanets and Antonina Kolokolova for their paper

“Learning Algorithms from Natural Proofs”.¹

¹ See <http://dx.doi.org/10.4230/LIPIcs.CCC.2016.34>.



■ Conference Organization

Program Committee

Anindya De, Northwestern University
Prahlahd Harsha, Tata Institute of Fundamental Research
Neeraj Kayal, Microsoft Research
Jakob Nordström, KTH Royal Institute of Technology
Toniann Pitassi, University of Toronto
Anup Rao, University of Washington
Ran Raz (chair), Weizmann Institute & IAS
David Steurer, Cornell University
Thomas Vidick, California Institute of Technology
Amir Yehudayoff, Technion
Sergey Yekhanin, Microsoft Research

Local Arrangements Committee

Takashi Horiyama, Saitama University
Akinori Kawachi, Tokushima University
Takeshi Koshihara (co-chair), Saitama University
Kazuhisa Makino, Kyoto University
Ryuhei Mori, Tokyo Institute of Technology
Jun Tarui, University of Electro-Communications
Osamu Watanabe (chair), Tokyo Institute of Technology

Board of Trustees

Eric Allender (Treasurer), Rutgers University
Boaz Barak, Harvard University
Venkatesan Guruswami, Carnegie Mellon University
Jeff Kinne (Secretary), Indiana State University
Dieter van Melkebeek (President), University of Wisconsin-Madison
Madhu Sudan, Harvard University
Jacob Toran, University of Ulm
Osamu Watanabe, Tokyo Institute of Technology



■ External Reviewers

Scott Aaronson	Divesh Aggarwal	Nir Ailon
James Aisenberg	Eric Allender	Per Austrin
Arturs Backurs	Paul Beame	Xiaohui Bei
Aleksandrs Belovs	Arnab Bhattacharyya	Nir Bitansky
Eric Blais	Andrej Bogdanov	Ilario Bonacina
Michael Bremner	Joshua Brody	Clément Canonne
Siu On Chan	Arkadev Chattopadhyay	Eshan Chattopadhyay
Ruiwen Chen	Alessandro Chiesa	Kai-Min Chung
Daniel Dadush	Susanna F. de Rezende	Andrew Drucker
Jan Elffers	Uriel Feige	Yuval Filmus
Michael A. Forbes	Benjamin Fuller	Konstantinos Georgiou
Mika Göös	Joshua Grochow	Ankit Gupta
Rohit Gurjar	Ronald de Haan	Pooya Hatami
Samuel Hopkins	Pavel Hrubes	Sangxia Huang
Rahul Jain	Stacey Jeffery	Valentine Kabanets
Yael Tauman Kalai	Tali Kaufman	Hartmut Klauck
Antonina Kolokolova	Ashutosh Kumar	Mrinal Kumar
Massimo Lauria	Francois Le Gall	James Lee
Troy Lee	Satya Lokam	Shachar Lovett
Dieter Van Melkebeek	Mladen Miksa	Moni Naor
Jelani Nelson	Huy Nguyen	Ryan O'Donnell
Igor Carboni Oliveira	Rafael Pass	Sylvain Perifel
Youming Qiao	Charles Rackoff	Jaikumar Radhakrishnan
Ron Rothblum	Aviad Rubinfeld	Atri Rudra
Chandan Saha	Rishi Saket	Miklos Santha
Rahul Santhanam	Ramprasad Saptharishi	Shubhangi Saraf
Nitin Saxena	Rocco Servedio	C. Seshadhri
Ronen Shaltiel	Asaf Shapira	Alexander Sherstov
Amir Shpilka	Florian Speelman	Srikanth Srinivasan
Noah Stephens-Davidowitz	Xiaoming Sun	Avishay Tal
Li-Yang Tan	Sébastien Tavenas	Madhur Tulsiani
Vinod Vaikuntanathan	Marc Vinyals	Emanuele Viola
Nisheeth Vishnoi	John Watrous	Thomas Watson
Omri Weinstein	Ryan Williams	Virginia Vassilevska Williams
Angela Wu	Grigory Yaroslavtsev	David Zuckerman

