

# 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>**

## ■ 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 Mančinska, 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 Satharishi* ..... 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