

# 33rd Computational Complexity Conference

CCC 2018, June 22–24, 2018, San Diego, California, USA

Edited by

Rocco A. Servedio



*Editor*

Rocco A. Servedio  
Department of Computer Science  
Columbia University  
500 West 120 Street  
New York, New York 10027  
USA  
rocco@cs.columbia.edu

*ACM Classification 2012*

Theory of computation

**ISBN 978-3-95977-069-9**

*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/978-3-95977-069-9>.

*Publication date*

June, 2018

*Bibliographic information published by the Deutsche Nationalbibliothek*

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in 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/LIPIcs.CCC.2018.0

ISBN 978-3-95977-069-9

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*

- Luca Aceto (*Chair*, Gran Sasso Science Institute and Reykjavik University)
- Susanne Albers (TU München)
- Chris Hankin (Imperial College London)
- Deepak Kapur (University of New Mexico)
- Michael Mitzenmacher (Harvard University)
- Madhavan Mukund (Chennai Mathematical Institute)
- Anca Muscholl (University Bordeaux)
- Catuscia Palamidessi (INRIA)
- Raimund Seidel (Saarland University and Schloss Dagstuhl – Leibniz-Zentrum für Informatik)
- Thomas Schwentick (TU Dortmund)
- Reinhard Wilhelm (Saarland University)

**ISSN 1868-8969**

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



## ■ Contents

Preface	
<i>Rocco A. Servedio</i> .....	0:vii

### Papers

Pseudorandom Generators from Polarizing Random Walks	
<i>Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett</i> .....	1:1–1:21
A PRG for Boolean PTF of Degree 2 with Seed Length Subpolynomial in $\epsilon$ and Logarithmic in $n$	
<i>Daniel Kane and Sankeerth Rao</i> .....	2:1–2:24
A New Approach for Constructing Low-Error, Two-Source Extractors	
<i>Avraham Ben-Aroya, Eshan Chattopadhyay, Dean Doron, Xin Li, and Amnon Ta-Shma</i> .....	3:1–3:19
Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs	
<i>Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing</i> .....	4:1–4:16
NP-hardness of Minimum Circuit Size Problem for OR-AND-MOD Circuits	
<i>Shuichi Hirahara, Igor C. Oliveira, and Rahul Santhanam</i> .....	5:1–5:31
Limits on Representing Boolean Functions by Linear Combinations of Simple Functions: Thresholds, ReLUs, and Low-Degree Polynomials	
<i>Richard Ryan Williams</i> .....	6:1–6:24
The Power of Natural Properties as Oracles	
<i>Russell Impagliazzo, Valentine Kabanets, and Ilya Volkovich</i> .....	7:1–7:20
Linear Sketching over $\mathbb{F}_2$	
<i>Sampath Kannan, Elchanan Mossel, Swagato Sanyal, and Grigory Yaroslavtsev</i> ..	8:1–8:37
Communication Complexity with Small Advantage	
<i>Thomas Watson</i> .....	9:1–9:17
Algebraic Dependencies and PSPACE Algorithms in Approximative Complexity	
<i>Zeyu Guo, Nitin Saxena, and Amit Sinhababu</i> .....	10:1–10:21
Unbalancing Sets and an Almost Quadratic Lower Bound for Syntactically Multilinear Arithmetic Circuits	
<i>Noga Alon, Mrinal Kumar, and Ben Lee Volk</i> .....	11:1–11:16
Hardness Amplification for Non-Commutative Arithmetic Circuits	
<i>Marco L. Carmosino, Russell Impagliazzo, Shachar Lovett, and Ivan Mihajlin</i> ....	12:1–12:16
Hardness vs Randomness for Bounded Depth Arithmetic Circuits	
<i>Chi-Ning Chou, Mrinal Kumar, and Noam Solomon</i> .....	13:1–13:17
On The Hardness of Approximate and Exact (Bichromatic) Maximum Inner Product	
<i>Lijie Chen</i> .....	14:1–14:45

33rd Computational Complexity Conference (CCC 2018).

Editor: Rocco A. Servedio



Leibniz International Proceedings in Informatics  
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Hardness of Function Composition for Semantic Read once Branching Programs <i>Jeff Edmonds, Venkatesh Medabalimi, and Toniann Pitassi</i> .....	15:1–15:22
Reordering Rule Makes OBDD Proof Systems Stronger <i>Sam Buss, Dmitry Itsykson, Alexander Knop, and Dmitry Sokolov</i> .....	16:1–16:24
Testing Linearity against Non-Signaling Strategies <i>Alessandro Chiesa, Peter Manohar, and Igor Shinkar</i> .....	17:1–17:37
Earthmover Resilience and Testing in Ordered Structures <i>Omri Ben-Eliezer and Eldar Fischer</i> .....	18:1–18:35
New Hardness Results for the Permanent Using Linear Optics <i>Daniel Grier and Luke Schaeffer</i> .....	19:1–19:29
Two-Player Entangled Games are NP-Hard <i>Anand Natarajan and Thomas Vidick</i> .....	20:1–20:18
Complexity Classification of Conjugated Clifford Circuits <i>Adam Bouland, Joseph F. Fitzsimons, and Dax Enshan Koh</i> .....	21:1–21:25
Efficient Batch Verification for UP <i>Omer Reingold, Guy N. Rothblum, and Ron D. Rothblum</i> .....	22:1–22:23
A Tight Lower Bound for Entropy Flattening <i>Yi-Hsiu Chen, Mika Göös, Salil P. Vadhan, and Jiapeng Zhang</i> .....	23:1–23:28
Worst-Case to Average Case Reductions for the Distance to a Code <i>Eli Ben-Sasson, Swastik Kopparty, and Shubhangi Saraf</i> .....	24:1–24:23
On the Complexity of the Cayley Semigroup Membership Problem <i>Lukas Fleischer</i> .....	25:1–25:12
Small Normalized Boolean Circuits for Semi-disjoint Bilinear Forms Require Logarithmic Conjunction-depth <i>Andrzej Lingas</i> .....	26:1–26:10
Lower Bounds on Non-Adaptive Data Structures Maintaining Sets of Numbers, from Sunflowers <i>Sivaramakrishnan Natarajan Ramamoorthy and Anup Rao</i> .....	27:1–27:16
Dimension Reduction for Polynomials over Gaussian Space and Applications <i>Badih Ghazi, Pritish Kamath, and Prasad Raghavendra</i> .....	28:1–28:37

## ■ Preface

The papers in this volume were accepted for presentation at the 33rd Computational Complexity Conference (CCC 2018), held June 22–24, 2018 in San Diego, California. The conference is organized by the Computational Complexity Foundation in cooperation with the European Association for Theoretical Computer Science (EATCS) and the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT). CCC 2018 is sponsored by Microsoft Research.

The call for papers sought original research papers in all areas of computational complexity theory. Of the 74 submissions the program committee selected 28 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 (listed separately) 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; Ryan O’Donnell and David Zuckerman for sharing their knowledge as prior PC chairs for CCC; Andrei Krokhin for contributing two one-hour tutorials on the topic of “Constraints, Consistency and Complexity”; and Michael Wagner for coordinating the production of these proceedings.

Rocco A. Servedio

Program Committee Chair, on behalf of the Program Committee







## ■ Awards

The program committee of the 33rd Computational Complexity Conference is very pleased to present the **Best Student Paper Award** to Lukas Fleischer for his paper

*The Complexity of the Cayley Semigroup Membership Problem.*

Funding for the best student paper award is provided by the European Association for Theoretical Computer Science (EATCS).





## ■ Conference Organization

### Program Committee

Eric Allender, Rutgers University  
Paul Beame, University of Washington  
Eric Blais, University of Waterloo  
Mark Braverman, Princeton University  
Michael A. Forbes, University of Illinois Urbana-Champaign  
Shafi Goldwasser, Massachusetts Institute of Technology and Weizmann Institute  
Rocco A. Servedio (Chair), Columbia University  
Srikanth Srinivasan, Indian Institute of Technology Bombay  
Thomas Thierauf, Aalen University  
Madhur Tulsiani, Toyota Technological Institute at Chicago  
Henry Yuen, University of California, Berkeley and University of Toronto

### Local Arrangements Committee

Sam Buss, University of California, San Diego  
Shachar Lovett (chair), University of California, San Diego

### Board of Trustees

Boaz Barak, Harvard University  
Sevag Gharibian, University of Paderborn and Virginia Commonwealth University  
Shachar Lovett, University of California, San Diego  
Dieter van Melkebeek (President), University of Wisconsin-Madison  
Ryan O'Donnell, Carnegie Mellon University  
Rahul Santhanam, Oxford University  
Rocco A. Servedio, Columbia University





## ■ External Reviewers

Amir Abboud	Divesh Aggarwal	Robert Andrews
Nikhil Balaji	Jess Banks	David Barrington
Niel de Beaudrap	Alexander Belov	Shalev Ben-David
Amev Bhangale	Arnab Bhattacharyya	Pranav Bisht
Andrej Bogdanov	Adam Bouland	Karl Bringmann
Joshua Brody	Jonah Brown-Cohen	Amit Chakrabarti
Richard Chang	Arkadev Chattopadhyay	Eshan Chattopadhyay
Gil Cohen	Samir Datta	Anindya De
Jian Ding	Dean Doron	Andrew Drucker
Lior Eldar	Shai Evra	Omar Fawzi
Bill Fefferman	Stephen Fenner	Eldar Fischer
Venkata Gandikota	Sumegha Garg	Dmitry Gavinsky
Sumanta Ghosh	Michael Goodrich	Elena Grigorescu
Ofer Grossman	Tom Gur	Iftach Haitner
Dhiraj Holden	Justin Holmgren	Pavel Hrubes
Pavel Hubacek	Christian Ikenmeyer	Fernando Jeronimo
Zhengfeng Ji	Stasys Jukna	Valentine Kabanets
Yael Tauman Kalai	Neeraj Kayal	Swastik Kopparty
Robin Kothari	Alexander Kulikov	Akash Kumar
Alex Lubotzky	Guillaume Malod	Pasin Manurangsi
Jieming Mao	Pierre Mckenzie	Or Meir
Stefan Mengel	Dor Minzer	Ashley Montanaro
Anand Natarajan	Joe Neeman	Huy Nguyen
Chinmay Nirkhe	Jerri Nummenpalo	Igor Carboni Oliveira
Eran Omri	Ori Parzanchevski	Ramamohan Paturi
Aduri Pavan	Supartha Podder	Aaron Potechin
Manoj Prabhakaran	Youming Qiao	Jaikumar Radhakrishnan
Nicolas Resch	Robert Robere	Cristobal Rojas
Ron Rothblum	Aviad Rubinstein	Michael Saks
Rahul Santhanam	Nitin Saxena	Luke Schaeffer
Dominik Scheder	Jon Schneider	Uwe Schöning
Matthias Schroder	Igor Sergeev	Ronen Shaltiel
Suhail Sherif	Igor Shinkar	Amir Shpilka
Amit Sinhababu	Nick Spooner	Noah Stephens-Davidowitz
Avishay Tal	Li-Yang Tan	Justin Thaler
Robin Thomas	Jacobo Toran	Prashant Vasudevan
Thomas Vidick	Marc Vinyals	Ben Lee Volk
Erik Waingarten	Thomas Watson	Omri Weinstein
Ryan Williams	Karl Wimmer	John Wright
Grigory Yaroslavtsev	Amir Yehudayoff	Yuichi Yoshida
Shengyu Zhang	Standa Zivny	

33rd Computational Complexity Conference (CCC 2018).  
Editor: Rocco A. Servedio



Leibniz International Proceedings in Informatics  
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

