

10th Innovations in Theoretical Computer Science

ITCS 2019, January 10-12, 2019, San Diego, CA, USA

Edited by
Avrim Blum



Editor

Avrim Blum
Toyota Technological Institute at Chicago (TTIC)
Chicago, IL, USA
avrim@ttic.edu

ACM Classification 2012

Theory of computation, Mathematics of computing

ISBN 978-3-95977-095-8

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/978-3-95977-095-8>.

Publication date

January, 2019

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.ITCS.2019.0

ISBN 978-3-95977-095-8

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

- Luca Aceto (*Chair*, Gran Sasso Science Institute and Reykjavik University)
- Susanne Albers (TU München)
- Christel Baier (TU Dresden)
- Javier Esparza (TU München)
- 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>Avrim Blum</i>	0:ix

Regular Papers

Submodular Secretary Problem with Shortlists	
<i>Shipra Agrawal, Mohammad Shadravan, and Cliff Stein</i>	1:1–1:19
Hamiltonian Sparsification and Gap-Simulation	
<i>Dorit Aharonov and Leo Zhou</i>	2:1–2:21
On Solving Linear Systems in Sublinear Time	
<i>Alexandr Andoni, Robert Krauthgamer, and Yosef Pogrow</i>	3:1–3:19
Placing Conditional Disclosure of Secrets in the Communication Complexity Universe	
<i>Benny Applebaum and Prashant Nalini Vasudevan</i>	4:1–4:14
Bitcoin: A Natural Oligopoly	
<i>Nick Arnosti and S. Matthew Weinberg</i>	5:1–5:1
A Simple Sublinear-Time Algorithm for Counting Arbitrary Subgraphs via Edge Sampling	
<i>Sepehr Assadi, Michael Kapralov, and Sanjeev Khanna</i>	6:1–6:20
Tensor Network Complexity of Multilinear Maps	
<i>Per Austrin, Petteri Kaski, and Kaie Kubjas</i>	7:1–7:21
A #SAT Algorithm for Small Constant-Depth Circuits with PTF Gates	
<i>Swapnam Bajpai, Vaibhav Krishan, Deepanshu Kush, Nutan Limaye, and Srikanth Srinivasan</i>	8:1–8:20
Small-Set Expansion in Shortcode Graph and the 2-to-2 Conjecture	
<i>Boaz Barak, Pravesh K. Kothari, and David Steurer</i>	9:1–9:12
Algorithms, Bounds, and Strategies for Entangled XOR Games	
<i>Adam Bene Watts, Aram W. Harrow, Gurtej Kanwar, and Anand Natarajan</i>	10:1–10:18
Testing Local Properties of Arrays	
<i>Omri Ben-Eliezer</i>	11:1–11:20
The Complexity of User Retention	
<i>Eli Ben-Sasson and Eden Saig</i>	12:1–12:30
Torus Polynomials: An Algebraic Approach to ACC Lower Bounds	
<i>Abhishek Bhrushundi, Kaave Hosseini, Shachar Lovett, and Sankeerth Rao</i>	13:1–13:16
Almost Envy-Free Allocations with Connected Bundles	
<i>Vittorio Bilò, Ioannis Caragiannis, Michele Flammini, Ayumi Igarashi, Gianpiero Monaco, Dominik Peters, Cosimo Vinci, and William S. Zwickler</i>	14:1–14:21

10th Innovations in Theoretical Computer Science (ITCS 2019).

Editor: Avrim Blum



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

“Quantum Supremacy” and the Complexity of Random Circuit Sampling <i>Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani</i>	15:1–15:2
Adversarially Robust Property-Preserving Hash Functions <i>Elette Boyle, Rio LaVigne, and Vinod Vaikuntanathan</i>	16:1–16:20
On Closest Pair in Euclidean Metric: Monochromatic is as Hard as Bichromatic <i>Karthik C. S. and Pasin Manurangsi</i>	17:1–17:16
Expander-Based Cryptography Meets Natural Proofs <i>Igor C. Oliveira, Rahul Santhanam, and Roei Tell</i>	18:1–18:14
A Note on the Quantum Query Complexity of Permutation Symmetric Functions <i>André Chailloux</i>	19:1–19:7
Adaptive Boolean Monotonicity Testing in Total Influence Time <i>Deeparnab Chakrabarty and C. Seshadhri</i>	20:1–20:7
On Locality-Sensitive Orderings and Their Applications <i>Timothy M. Chan, Sariel Har-Peled, and Mitchell Jones</i>	21:1–21:17
Pseudorandom Generators from the Second Fourier Level and Applications to AC0 with Parity Gates <i>Eshan Chattopadhyay, Pooya Hatami, Shachar Lovett, and Avishay Tal</i>	22:1–22:15
Classical Algorithms from Quantum and Arthur-Merlin Communication Protocols <i>Lijie Chen and Ruosong Wang</i>	23:1–23:20
Capturing Complementarity in Set Functions by Going Beyond Submodularity/Subadditivity <i>Wei Chen, Shang-Hua Teng, and Hanrui Zhang</i>	24:1–24:20
Probabilistic Checking Against Non-Signaling Strategies from Linearity Testing <i>Alessandro Chiesa, Peter Manohar, and Igor Shinkar</i>	25:1–25:17
On the Algorithmic Power of Spiking Neural Networks <i>Chi-Ning Chou, Kai-Min Chung, and Chi-Jen Lu</i>	26:1–26:20
Last-Iterate Convergence: Zero-Sum Games and Constrained Min-Max Optimization <i>Constantinos Daskalakis and Ioannis Panageas</i>	27:1–27:18
Density Estimation for Shift-Invariant Multidimensional Distributions <i>Anindya De, Philip M. Long, and Rocco A. Servedio</i>	28:1–28:20
From Local to Robust Testing via Agreement Testing <i>Irit Dinur, Prahladh Harsha, Tali Kaufman, and Noga Ron-Zewi</i>	29:1–29:18
Every Set in \mathcal{P} Is Strongly Testable Under a Suitable Encoding <i>Irit Dinur, Oded Goldreich, and Tom Gur</i>	30:1–30:17
Alea Iacta Est: Auctions, Persuasion, Interim Rules, and Dice <i>Shaddin Dughmi, David Kempe, and Ruixin Qiang</i>	31:1–31:20
Spanoids – An Abstraction of Spanning Structures, and a Barrier for LCCs <i>Zeev Dvir, Sivakanth Gopi, Yuzhou Gu, and Avi Wigderson</i>	32:1–32:20

Fairness Under Composition <i>Cynthia Dwork and Christina Ilvento</i>	33:1–33:20
A Log-Sobolev Inequality for the Multislice, with Applications <i>Yuval Filmus, Ryan O’Donnell, and Xinyu Wu</i>	34:1–34:12
Cubic Formula Size Lower Bounds Based on Compositions with Majority <i>Anna Gál, Avishay Tal, and Adrian Trejo Nuñez</i>	35:1–35:13
The Space Complexity of Mirror Games <i>Sumegha Garg and Jon Schneider</i>	36:1–36:14
The Subgraph Testing Model <i>Oded Goldreich and Dana Ron</i>	37:1–37:19
Adventures in Monotone Complexity and TFNP <i>Mika Göös, Pritish Kamath, Robert Robere, and Dmitry Sokolov</i>	38:1–38:19
Algorithmic Polarization for Hidden Markov Models <i>Venkatesan Guruswami, Preetum Nakkiran, and Madhu Sudan</i>	39:1–39:19
On the Communication Complexity of Key-Agreement Protocols <i>Iftach Haitner, Noam Mazon, Rotem Oshman, Omer Reingold, and Amir Yehudayoff</i>	40:1–40:16
The Paulsen Problem Made Simple <i>Linus Hamilton and Ankur Moitra</i>	41:1–41:6
How to Subvert Backdoored Encryption: Security Against Adversaries that Decrypt All Ciphertexts <i>Thibaut Horel, Sunoo Park, Silas Richelson, and Vinod Vaikuntanathan</i>	42:1–42:20
On Integer Programming and Convolution <i>Klaus Jansen and Lars Rohwedder</i>	43:1–43:17
Empowering the Configuration-IP – New PTAS Results for Scheduling with Setups Times <i>Klaus Jansen, Kim-Manuel Klein, Marten Maack, and Malin Rau</i>	44:1–44:19
Being Corrupt Requires Being Clever, But Detecting Corruption Doesn’t <i>Yan Jin, Elchanan Mossel, and Govind Ramnarayan</i>	45:1–45:14
Simulating Random Walks on Graphs in the Streaming Model <i>Ce Jin</i>	46:1–46:15
On the Complexity of Symmetric Polynomials <i>Markus Bläser and Gorav Jindal</i>	47:1–47:14
The Orthogonal Vectors Conjecture for Branching Programs and Formulas <i>Daniel M. Kane and Richard Ryan Williams</i>	48:1–48:15
SOS Lower Bounds with Hard Constraints: Think Global, Act Local <i>Pravesh K. Kothari, Ryan O’Donnell, and Tselil Schramm</i>	49:1–49:21
Semi-Online Bipartite Matching <i>Ravi Kumar, Manish Purohit, Aaron Schild, Zoya Svitkina, and Erik Vee</i>	50:1–50:20

Strategies for Quantum Races <i>Troy Lee, Maharshi Ray, and Miklos Santha</i>	51:1–51:21
Lower Bounds for Tolerant Junta and Unateness Testing via Rejection Sampling of Graphs <i>Amit Levi and Erik Waingarten</i>	52:1–52:20
Secret Sharing with Binary Shares <i>Fuchun Lin, Mahdi Cheraghchi, Venkatesan Guruswami, Reihaneh Safavi-Naini, and Huaxiong Wang</i>	53:1–53:20
On the Communication Complexity of High-Dimensional Permutations <i>Nati Linial, Toniann Pitassi, and Adi Shraibman</i>	54:1–54:20
Fisher Zeros and Correlation Decay in the Ising Model <i>Jingcheng Liu, Alistair Sinclair, and Piyush Srivastava</i>	55:1–55:8
Quadratic Time-Space Lower Bounds for Computing Natural Functions with a Random Oracle <i>Dylan M. McKay and Richard Ryan Williams</i>	56:1–56:20
Random Projection in the Brain and Computation with Assemblies of Neurons <i>Christos H. Papadimitriou and Santosh S. Vempala</i>	57:1–57:19
Local Computation Algorithms for Spanners <i>Merav Parter, Ronitt Rubinfeld, Ali Vakilian, and Anak Yodpinyanee</i>	58:1–58:21
Proofs of Catalytic Space <i>Krzysztof Pietrzak</i>	59:1–59:25
Simple Verifiable Delay Functions <i>Krzysztof Pietrzak</i>	60:1–60:15
Sum of Squares Lower Bounds from Symmetry and a Good Story <i>Aaron Potechin</i>	61:1–61:20
Learning Time Dependent Choice <i>Zachary Chase and Siddharth Prasad</i>	62:1–62:19
Erasures vs. Errors in Local Decoding and Property Testing <i>Sofya Raskhodnikova, Noga Ron-Zewi, and Nithin Varma</i>	63:1–63:21
A New Approach to Multi-Party Peer-to-Peer Communication Complexity <i>Adi Rosén and Florent Urrutia</i>	64:1–64:19
A Schur Complement Cheeger Inequality <i>Aaron Schild</i>	65:1–65:15
Game Efficiency Through Linear Programming Duality <i>Nguyễn Kim Thắng</i>	66:1–66:20

■ Preface

The papers in this volume were presented at the 10th Innovations in Theoretical Computer Science (ITCS 2019) conference. The conference was held at UC San Diego in San Diego, CA, USA, January 10-12, 2019, and co-located with SODA 2019. ITCS seeks to promote research that carries a strong conceptual message, for instance, introducing a new concept or model, opening a new line of inquiry within traditional or cross-interdisciplinary areas, introducing new techniques, or making novel connections between existing areas and ideas. The conference format is single-session and aims to promote the exchange of ideas between different areas of theoretical computer science and with other disciplines. The call for papers welcomed all submissions, whether aligned with current theory of computation research directions or deviating from them. A record 202 submissions were received. Of these, the program committee selected 66 papers. I would like to thank the authors of all submissions, whether accepted or not, for their interest in ITCS.

The program committee consisted of 39 members (plus the chair): Scott Aaronson, UT Austin; Eric Blais, Waterloo; Jeremiah Blocki, Purdue; Simina Branzei, Purdue; Bernard Chazelle, Princeton University; Amit Daniely, Hebrew University; Sanjoy Dasgupta, UC San Diego; Zeev Dvir, Princeton University; Uriel Feige, Weizmann; Michal Feldman, Tel-Aviv University; Rong Ge, Duke; Venkatesan Guruswami, CMU; Moritz Hardt, UC Berkeley; Russell Impagliazzo, UC San Diego; Brendan Juba, Washington University St Louis; Varun Kanade, University of Oxford; Eyal Kushilevitz, Technion; Yingyu Liang, University of Wisconsin - Madison; Shachar Lovett, UC San Diego; Sepideh Mahabadi, TTIC; Yishay Mansour, Tel-Aviv University; Rafael Pass, Cornell University; Sofya Raskhodnikova, Boston University; Dana Ron, Tel-Aviv University; Ron Rothblum, Technion; Aviad Rubinfeld, Stanford University; Aaron Sidford, Stanford University; Yaron Singer, Harvard University; Mohit Singh, Georgia Tech; Adam Smith, Boston University; Jacob Steinhardt, UC Berkeley; Madhur Tulsiani, TTIC; Vinod Vaikuntanathan, MIT; Thomas Vidick, Caltech; Matt Weinberg, Princeton University; Ryan Williams, MIT; Mary Wootters, Stanford University; Mihalis Yannakakis, Columbia University; Shengyu Zhang, CUHK and Tencent. I wish to express my heartfelt thanks to them for agreeing to join the committee as well as for investing a great deal of time and effort to evaluate the submissions. I am also grateful to the many subreviewers who assisted with the reviewing process. The local organizer was Shachar Lovett from UC San Diego. I would like to thank him very much for his service. I'm also grateful to Umesh Vazirani, chair of the ITCS Steering Committee, and to Thomas Vidick, who helped with the website among other things. Finally, I would like to thank all the presenters and the audience at ITCS for making ITCS a wonderful experience.

Avrim Blum
ITCS 2019 Program Chair
Toyota Technological Institute at Chicago (TTIC)
Chicago, IL USA



ITCS 2019 Conference Organization

Program Chair: Avrim Blum (TTIC)

Local Organization: Shachar Lovett (UC San Diego)

Steering Committee Chair: Umesh Vazirani (UC Berkeley)

Steering Committee Sanjeev Arora, Princeton
Manuel Blum, Carnegie Mellon
Bernard Chazelle, Princeton
Irit Dinur, Weizmann
Oded Goldreich, Weizmann
Shafi Goldwasser, MIT and Weizmann
Richard Karp, Berkeley
Robert Kleinberg, Cornell University
Ueli Maurer, ETH
Silvio Micali, MIT
Christos Papadimitriou, Berkeley
Michael Rabin, Harvard
Omer Reingold, Stanford
Tim Roughgarden, Stanford
Madhu Sudan, Harvard
Leslie Valiant, Harvard
Umesh Vazirani, Berkeley
Thomas Vidick, Caltech
Avi Wigderson, IAS
Andy Yao, Tsinghua

Program Committee: Scott Aaronson, UT Austin
Eric Blais, Waterloo
Jeremiah Blocki, Purdue
Avrim Blum, TTIC
Simina Branzei, Purdue
Bernard Chazelle, Princeton University
Amit Daniely, Hebrew University
Sanjoy Dasgupta, UC San Diego
Zeev Dvir, Princeton University
Uriel Feige, Weizmann
Michal Feldman, Tel-Aviv University
Rong Ge, Duke
Venkatesan Guruswami, CMU
Moritz Hardt, UC Berkeley
Russell Impagliazzo, UC San Diego
Brendan Juba, Washington University St Louis
Varun Kanade, University of Oxford
Eyal Kushilevitz, Technion

Program Committee Yingyu Liang, University of Wisconsin - Madison
(continued): Shachar Lovett, UC San Diego
 Sepideh Mahabadi, TTIC
 Yishay Mansour, Tel-Aviv University
 Rafael Pass, Cornell University
 Sofya Raskhodnikova, Boston University
 Dana Ron, Tel-Aviv University
 Ron Rothblum, Technion
 Aviad Rubinstein, Stanford University
 Aaron Sidford, Stanford University
 Yaron Singer, Harvard University
 Mohit Singh, Georgia Tech
 Adam Smith, Boston University
 Jacob Steinhardt, UC Berkeley
 Madhur Tulsiani, TTIC
 Vinod Vaikuntanathan, MIT
 Thomas Vidick, Caltech
 Matt Weinberg, Princeton University
 Ryan Williams, MIT
 Mary Wootters, Stanford University
 Mihalis Yannakakis, Columbia University
 Shengyu Zhang, CUHK and Tencent

Additional	Maryam Aliakbarpour	Jonathan Allcock	Josh Alman
Reviewers:	Sepehr Assadi	Miriam Backens	Arturs Backurs
	Eric Balkanski	Marshall Ball	Paul Beame
	Xiaohui Bei	Alexander Belov	Hedyeh Beyhaghi
	Arnab Bhattacharyya	Alexander Block	Andrej Bogdanov
	Joshua Brody	Niv Buchbinder	Yang Cai
	Clement Canonne	T-H. Hubert Chan	Eshan Chattopadhyay
	Lijie Chen	Yu Cheng	Bram Cohen
	Ran Cohen	Vincent Cohen-Addad	Yuval Dagan
	Sarah Dean	Holger Dell	Travis Dick
	Dean Doron	Andy Drucker	Talya Eden
	Faith Ellen	Meryem Essaidi	Tomer Ezra
	Arman Fazeli	Bill Fefferman	Zhe Feng
	Yuval Filmus	Aris Filos-Ratsikas	Ophir Friedler
	Hu Fu	Jugal Garg	Michal Garlik
	Kira Goldner	Mika Goos	Fernando Jeronimo
	Fred Green	Elena Grigorescu	Joshua Grochow
	Siyao Guo	Avinatan Hassidim	Matt Hastings
	Pooya Hatami	Niao He	John Hitchcock
	Jan Hladky	Samuel Hopkins	Kaave Hosseini

Additional Reviewers (continued):

Justin Hsu	Rahul Jain	Dimitris Kalimeris
Daniel Kane	Thomas Kesselheim	Hartmut Klauck
Shimon Kogan	Ilan Komargodski	Tomer Koren
Elias Koutsoupias	Robert Krauthgamer	Janardhan Kulkarni
Akash Kumar	Matt Kusner	Lap Chi Lau
Vedat Levi Alev	Jian Li	Ben Liao
Lydia Liu	Zhenming Liu	Pinyan Lu
Mohammad Mahmoody	Hemanta Maji	Frederik Mallmann-Trenn
Jieming Mao	Andrew McGregor	John Miller
Dor Minzer	Slobodan Mitrovic	Divyarthi Mohan
Ryuhei Mori	Cameron Musco	Hoi Nguyen
Aleksandar Nikolov	Katarzyna Paluch	Denis Pankratov
Eric Price	Christos-Alexandros Psomas	Sharon Qian
Miklos Z. Racz	Manish Raghavan	Govind Ramnarayan
Dror Rawitz	Alireza Rezaei	Andrea Rocchetto
Liam Roditty	Will Rosenbaum	Nir Rosenfeld
Adi Rosen	Guy Rothblum	Tim Roughgarden
Shubhangi Saraf	Tselil Schramm	Ariel Schwartzman
Kineret Segal	Siddhartha Sen	C. Seshadhri
Amirbehshad Shahrashbi	Asaf Shapira	Max Simchowitz
Sahil Singla	Christian Sohler	David Soloveichik
Yonatan Sompolinsky	Vasilis Syrgkanis	Avishay Tal
Inbal Talgam-Cohen	Nirvan Tyagi	Falk Unger
Ali Vakilian	Shai Vardi	Nithin Varma
Virginia Vassilevska Williams	Suresh Venkatasubramanian	Matheus Venturynne
Erik Waingarten	Omri Weinstein	John Wright
Ning Xie	Lin Yang	Junjie Ye
Amir Yehudayoff	Anak Yodpinyanee	Eylon Yogev
Henry Yuen	Chihao Zhang	Hongyang Zhang
Jiapeng Zhang	Samson Zhou	Vassilis Zikas
Tijana Zrnic		