

8th Innovations in Theoretical Computer Science Conference

ITCS 2017, January 9–11, 2017 - Berkeley, CA, USA

Edited by

Christos H. Papadimitriou



Editors

Christos H. Papadimitriou
Columbia University, New York City
christos@columbia.edu

ACM Classification 1998

F. Theory of Computation, G. Mathematics of Computing

ISBN 978-3-95977-029-3

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/978-3-95977-029-3>.

Publication date

November, 2017

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.2017.0

ISBN 978-3-95977-029-3

ISSN 1868-8969

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

■ Contents

Preface	
<i>Christos H. Papadimitriou</i>	0:ix

Papers

Separators in Region Intersection Graphs	
<i>James R. Lee</i>	1:1–1:8
Gradient Descent Only Converges to Minimizers: Non-Isolated Critical Points and Invariant Regions	
<i>Ioannis Panageas and Georgios Piliouras</i>	2:1–2:12
Linear Coupling: An Ultimate Unification of Gradient and Mirror Descent	
<i>Zeyuan Allen-Zhu and Lorenzo Orecchia</i>	3:1–3:22
High Dimensional Random Walks and Colorful Expansion	
<i>Tali Kaufman and David Mass</i>	4:1–4:27
Real Stability Testing	
<i>Prasad Raghavendra, Nick Ryder, and Nikhil Srivastava</i>	5:1–5:15
Very Simple and Efficient Byzantine Agreement	
<i>Silvio Micali</i>	6:1–6:1
Low-Complexity Cryptographic Hash Functions	
<i>Benny Applebaum, Naama Haramaty-Krasne, Yuval Ishai, Eyal Kushilevitz, and Vinod Vaikuntanathan</i>	7:1–7:31
Hierarchical Functional Encryption	
<i>Zvika Brakerski, Nishanth Chandran, Vipul Goyal, Aayush Jain, Amit Sahai, and Gil Segev</i>	8:1–8:27
Inferential Privacy Guarantees for Differentially Private Mechanisms	
<i>Arpita Ghosh and Robert Kleinberg</i>	9:1–9:3
Towards Human Computable Passwords	
<i>Jeremiah Blocki, Manuel Blum, Anupam Datta, and Santosh Vempala</i>	10:1–10:47
Towards Hardness of Approximation for Polynomial Time Problems	
<i>Amir Abboud and Arturs Backurs</i>	11:1–11:26
Parameterized Property Testing of Functions	
<i>Ramesh Krishnan S. Pallavoor, Sofya Raskhodnikova, and Nithin Varma</i>	12:1–12:17
The Complexity of Problems in P Given Correlated Instances	
<i>Shafi Goldwasser and Dhiraj Holden</i>	13:1–13:19
Multi-Clique-Width	
<i>Martin Fürer</i>	14:1–14:13

8th Innovations in Theoretical Computer Science Conference (ITCS 2017).

Editor: Christos H. Papadimitrou



Leibniz International Proceedings in Informatics

LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Computational Tradeoffs in Biological Neural Networks: Self-Stabilizing Winner-Take-All Networks <i>Nancy Lynch, Cameron Musco, and Merav Parter</i>	15:1–15:44
Mutation, Sexual Reproduction and Survival in Dynamic Environments <i>Ruta Mehta, Ioannis Panageas, Georgios Piliouras, Prasad Tetali, and Vijay V. Vazirani</i>	16:1–16:29
Self-Sustaining Iterated Learning <i>Bernard Chazelle and Chu Wang</i>	17:1–17:17
Coding in Undirected Graphs Is Either Very Helpful or Not Helpful at All <i>Mark Braverman, Sumegha Garg, and Ariel Schwartzman</i>	18:1–18:18
Compression in a Distributed Setting <i>Badih Ghazi, Elad Haramaty, Pritish Kamath, and Madhu Sudan</i>	19:1–19:22
Outlaw Distributions and Locally Decodable Codes <i>Jop Briët, Zeev Dvir, and Sivakanth Gopi</i>	20:1–20:19
Constant-Rate Interactive Coding Is Impossible, Even In Constant-Degree Networks <i>Ran Gelles and Yael T. Kalai</i>	21:1–21:13
Parallel Repetition via Fortification: Analytic View and the Quantum Case <i>Mohammad Bavarian, Thomas Vidick, and Henry Yuen</i>	22:1–22:33
The Classification of Reversible Bit Operations <i>Scott Aaronson, Daniel Grier, and Luke Schaeffer</i>	23:1–23:34
Nondeterministic Quantum Communication Complexity: the Cyclic Equality Game and Iterated Matrix Multiplication <i>Harry Buhrman, Matthias Christandl, and Jeroen Zuiddam</i>	24:1–24:18
Quantum Codes from High-Dimensional Manifolds <i>Matthew B. Hastings</i>	25:1–25:26
Conditional Hardness for Sensitivity Problems <i>Monika Henzinger, Andrea Lincoln, Stefan Neumann, and Virginia Vassilevska Williams</i>	26:1–26:31
An Improved Homomorphism Preservation Theorem From Lower Bounds in Circuit Complexity <i>Benjamin Rossman</i>	27:1–27:17
Low-Sensitivity Functions from Unambiguous Certificates <i>Shalev Ben-David, Pooya Hatami, and Avishay Tal</i>	28:1–28:23
Testing k -Monotonicity <i>Clément L. Canonne, Elena Grigorescu, Siyao Guo, Akash Kumar, and Karl Wimmer</i>	29:1–29:21
What Circuit Classes Can Be Learned with Non-Trivial Savings? <i>Rocco A. Servedio and Li-Yang Tan</i>	30:1–30:21
Expander Construction in VNC ¹ <i>Sam Buss, Valentine Kabanets, Antonina Kolokolova, and Michal Koucký</i>	31:1–31:26

Finding Clearing Payments in Financial Networks with Credit Default Swaps is PPAD-complete <i>Steffen Schauldenzucker, Sven Seuken, and Stefano Battiston</i>	32:1–32:20
Testing Submodularity and Other Properties of Valuation Functions <i>Eric Blais and Abhinav Bommireddi</i>	33:1–33:17
Algorithmic Aspects of Private Bayesian Persuasion <i>Yakov Babichenko and Siddharth Barman</i>	34:1–34:16
Condorcet-Consistent and Approximately Strategyproof Tournament Rules <i>Jon Schneider, Ariel Schwartzman, and S. Matthew Weinberg</i>	35:1–35:20
Nash Social Welfare, Matrix Permanent, and Stable Polynomials <i>Nima Anari, Shayan Oveis Gharan, Amin Saberi, and Mohit Singh</i>	36:1–36:12
Multiplayer Parallel Repetition for Expanding Games <i>Irit Dinur, Prahladh Harsha, Rakesh Venkat, and Henry Yuen</i>	37:1–37:16
Cumulative Space in Black-White Pebbling and Resolution <i>Joël Alwen, Susanna F. de Rezende, Jakob Nordström, and Marc Vinyals</i>	38:1–38:21
A Hierarchy Theorem for Interactive Proofs of Proximity <i>Tom Gur and Ron D. Rothblum</i>	39:1–39:43
Cube vs. Cube Low Degree Test <i>Amey Bhangale, Irit Dinur, and Inbal Livni Navon</i>	40:1–40:31
On the Power of Learning from k -Wise Queries <i>Vitaly Feldman and Badri Ghazi</i>	41:1–41:32
Detecting Communities Is Hard (And Counting Them Is Even Harder) <i>Aviad Rubinfeld</i>	42:1–42:13
Inherent Trade-Offs in the Fair Determination of Risk Scores <i>Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan</i>	43:1–43:23
Non-Backtracking Spectrum of Degree-Corrected Stochastic Block Models <i>Lennart Gulikers, Marc Lelarge, and Laurent Massoulié</i>	44:1–44:27
Conditional Sparse Linear Regression <i>Brendan Juba</i>	45:1–45:14
Rigorous Rg Algorithms and Area Laws for Low Energy Eigenstates In 1D <i>Itai Arad, Zeph Landau, Umesh Vazirani, and Thomas Vidick</i>	46:1–46:14
The Flow of Information in Interactive Quantum Protocols: the Cost of Forgetting <i>Mathieu Laurière and Dave Touchette</i>	47:1–47:1
Overlapping Qubits <i>Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick</i>	48:1–48:21
Quantum Recommendation System <i>Iordanis Kerenidis and Anupam Prakash</i>	49:1–49:21
Random Walks in Polytopes and Negative Dependence <i>Yuval Peres, Mohit Singh, and Nisheeth K. Vishnoi</i>	50:1–50:10

Simultaneously Load Balancing for Every p -norm, With Reassignments <i>Aaron Bernstein, Tsvi Kopelowitz, Seth Pettie, Ely Porat, and Clifford Stein</i>	51:1–51:14
Approximating Approximate Distance Oracles <i>Michael Dinitz and Zeyu Zhang</i>	52:1–52:14
Fast Cross-Polytope Locality-Sensitive Hashing <i>Christopher Kennedy and Rachel Ward</i>	53:1–53:16
The Distortion of Locality Sensitive Hashing <i>Flavio Chierichetti, Ravi Kumar, Alessandro Panconesi, and Erisa Terolli</i>	54:1–54:18
Constructive Non-Commutative Rank Computation Is in Deterministic Polynomial Time <i>Gábor Ivanyos, Youming Qiao, and K Venkata Subrahmanyam</i>	55:1–55:19
The Duality Gap for Two-Team Zero-Sum Games <i>Leonard J. Schulman and Umesh V. Vazirani</i>	56:1–56:8
Well-Supported vs. Approximate Nash Equilibria: Query Complexity of Large Games <i>Xi Chen, Yu Cheng, and Bo Tang</i>	57:1–57:9
Metatheorems for Dynamic Weighted Matching <i>Daniel Stubbs and Virginia Vassilevska Williams</i>	58:1–58:14
SOS Is Not Obviously Automatizable, Even Approximately <i>Ryan O’Donnell</i>	59:1–59:10
The Journey from NP to TFNP Hardness <i>Pavel Hubáček, Moni Naor, and Eylon Yogev</i>	60:1–60:21