13th Innovations in Theoretical Computer Science Conference

ITCS 2022, January 31–February 3, 2022, Berkeley, CA, USA

Edited by

Mark Braverman

Part 1 of 3

LIPICS

Editor

Mark Braverman
Princeton University, USA
mbraverm@gmail.com

ACM Classification 2012
Mathematics of computing; Theory of computation

ISBN 978-3-95977-217-4

PRINT ISBN: 978-1-7138-4384-9

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at https://www.dagstuhl.de/dagpub/978-3-95977-217-4.

Publication date
January, 2022

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 https://portal.dnb.de.

License
This work is licensed under a Creative Commons Attribution 4.0 International license (CC-BY 4.0): https://creativecommons.org/licenses/by/4.0/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.2022.0

Contents

Preface
Mark Braverman 0:xiii

List of Authors
.... 0:xv–0:xxiv

Papers

Maximizing Revenue in the Presence of Intermediaries
Gagan Aggarwal, Kshipra Bhawalkar, Guru Guruganesh, and Andres Perlroth 1:1–1:22

Algebraic Restriction Codes and Their Applications
Divesh Aggarwal, Nico Döttling, Jesko Dujmovic, Mohammad Hajiabadi, Giulio Malavolta, and Maciej Obremski 2:1–2:15

Improved Merlin-Arthur Protocols for Central Problems in Fine-Grained Complexity
Shyan Akmal, Lijie Chen, Ce Jin, Malvika Raj, and Ryan Williams 3:1–3:25

Pre-Constrained Encryption
Prabhanjan Ananth, Abhishek Jain, Zhengzhong Jin, and Giulio Malavolta 4:1–4:20

Domain Sparsification of Discrete Distributions Using Entropic Independence
Nima Anari, MichalDereziński, Thuy-Duong Vuong, and Elizabeth Yang 5:1–5:23

Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians
Anurag Anshu and Chinmay Nirkhe 6:1–6:22

Near-Optimal Distributed Implementations of Dynamic Algorithms for Symmetry Breaking Problems
Shiri Antaki, Quanquan C. Liu, and Shay Solomon 7:1–7:25

Secret Sharing, Slice Formulas, and Monotone Real Circuits
Benny Applebaum, Amos Beimel, Oded Nir, Naty Peter, and Toniann Pitassi 8:1–8:23

An Asymptotically Optimal Algorithm for Maximum Matching in Dynamic Streams
Sepehr Assadi and Vihan Shah 9:1–9:23

Sublinear Time and Space Algorithms for Correlation Clustering via Sparse-Dense Decompositions
Sepehr Assadi and Chen Wang 10:1–10:20

Multi-Channel Bayesian Persuasion
Yakov Babichenko, Inbal Talgam-Cohen, Haifeng Xu, and Konstantin Zabarnyi ... 11:1–11:2

Randomness Extraction from Somewhat Dependent Sources
Marshall Ball, Oded Goldreich, and Tal Malkin 12:1–12:14

Prefix Discrepancy, Smoothed Analysis, and Combinatorial Vector Balancing
Nikhil Bansal, Haotian Jiang, Raghu Meka, Sahil Singla, and Makrand Sinha 13:1–13:22

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).
Editor: Mark Braverman
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Classical Algorithms and Quantum Limitations for Maximum Cut on High-Girth Graphs
Boaz Barak and Kunal Marwaha 14:1–14:21

Indistinguishability Obfuscation of Null Quantum Circuits and Applications
James Bartusek and Giulio Malavolta 15:1–15:13

An Efficient Semi-Streaming PTAS for Tournament Feedback Arc Set with Few Passes
Anubhav Baweja, Justin Jia, and David P. Woodruff 16:1–16:23

FPT Algorithms for Finding Near-Cliques in c-Closed Graphs
Balaram Behera, Edin Husić, Shweta Jain, Tim Roughgarden, and C. Seshadhri . 17:1–17:24

What Does Dynamic Optimality Mean in External Memory?
Michael A. Bender, Martín Farach-Colton, and William Kuszmaul 18:1–18:23

Improved Hardness of BDD and SVP Under Gap-(S)ETH
Huck Bennett, Chris Peikert, and Yi Tang 19:1–19:12

Mixing of 3-Term Progressions in Quasirandom Groups
Amey Bhangale, Prahladh Harsha, and Sourya Roy 20:1–20:9

Max-3-Lin over Non-Abelian Groups with Universal Factor Graphs
Amey Bhangale and Aleksa Stanković 21:1–21:21

Separating the NP-Hardness of the Grothendieck Problem from the Little-Grothendieck Problem
Vijay Bhattiprolu, Euiwoong Lee, and Madhur Tulsiani 22:1–22:17

Fixed-Parameter Sensitivity Oracles
Davide Bilò, Katrin Casel, Keerti Choudhary, Sarel Cohen, Tobias Friedrich, J.A. Gregor Lagodzinski, Martin Schirneck, and Simon Wietheger 23:1–23:18

Local Access to Random Walks
Amartya Shankha Biswas, Edward Pyne, and Ronitt Rubinfeld 24:1–24:22

Vertex Fault-Tolerant Emulators
Greg Bodwin, Michael Dinitz, and Yasamin Nazari 25:1–25:22

Bounded Indistinguishability for Simple Sources
Andrej Bogdanov, Krishnamoorthy Dinesh, Yuval Filmus, Yuval Ishai, Avi Kaplan, and Akshayaram Srinivasan 26:1–26:18

Locality-Preserving Hashing for Shifts with Connections to Cryptography
Elette Boyle, Itai Dinur, Niv Gilboa, Yuval Ishai, Nathan Keller, and Ohad Klein 27:1–27:24

Lattice-Inspired Broadcast Encryption and Succinct Ciphertext-Policy ABE
Zvika Brakerski and Vinod Vaikuntanathan 28:1–28:20

Local Problems on Trees from the Perspectives of Distributed Algorithms, Finitary Factors, and Descriptive Combinatorics
Sebastian Brandt, Yi-Jun Chang, Jan Grebík, Christoph Grunau, Václav Rozhoň, and Zoltán Vidnyánszky 29:1–29:26

PCPs and Instance Compression from a Cryptographic Lens
Liron Bronfman and Ron D. Rothblum 30:1–30:19

Limits of Quantum Speed-Ups for Computational Geometry and Other Problems: Fine-Grained Complexity via Quantum Walks
Harry Buhrman, Bruno Loff, Subhasree Patro, and Florian Speelman 31:1–31:12

Small Hazard-Free Transducers
Johannes Bund, Christoph Lenzen, and Moti Medina 32:1–32:24

Faster Sparse Matrix Inversion and Rank Computation in Finite Fields
Sílvia Casacuberta and Rasmus Kyng 33:1–33:24

Algorithms and Lower Bounds for Comparator Circuits from Shrinkage
Bruno P. Cavalar and Zhenjian Lu 34:1–34:21

Quantum Distributed Algorithms for Detection of Cliques
Keren Censor-Hillel, Orr Fischer, François Le Gall, Dean Leitersdorf, and Rotem Oshman 35:1–35:25

Distributed Vertex Cover Reconfiguration
Keren Censor-Hillel, Yannic Maus, Shahar Romem-Peled, and Tigran Tonoyan .. 36:1–36:23

Adversarially Robust Coloring for Graph Streams
Amit Chakrabarti, Prantar Ghosh, and Manuel Stoeckl 37:1–37:23

Smaller ACC0 Circuits for Symmetric Functions
Brynmor Chapman and R. Ryan Williams 38:1–38:19

Monotone Complexity of Spanning Tree Polynomial Re-Visited
Arkadev Chattopadhyay, Rajit Datta, Utsab Ghosal, and Partha Mukhopadhyay ... 39:1–39:21

The Space Complexity of Sampling
Eshan Chattopadhyay, Jesse Goodman, and David Zuckerman 40:1–40:23

On the Existence of Competitive Equilibrium with Chores
Bhaskar Ray Chaudhury, Jugal Garg, Peter McGlaughlin, and Ruta Mehta 41:1–41:13

Individual Fairness in Advertising Auctions Through Inverse Proportionality
Shuchi Chawla and Meena Jagadeesan 42:1–42:21

Improved Decoding of Expander Codes
Xue Chen, Kuan Cheng, Xin Li, and Minghui Ouyang 43:1–43:3

Cursed yet Satisfied Agents
Yiling Chen, Alon Eden, and Juntao Wang 44:1–44:1

Average-Case Hardness of NP and PH from Worst-Case Fine-Grained Assumptions
Lijie Chen, Shuichi Hirahara, and Neekon Vafa 45:1–45:16

Symmetric Sparse Boolean Matrix Factorization and Applications
Sitan Chen, Zhao Song, Runzhou Tao, and Ruizhe Zhang 46:1–46:25

Quantum Meets the Minimum Circuit Size Problem
Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang 47:1–47:16

Larger Corner-Free Sets from Combinatorial Degenerations
Matthias Christandl, Omar Fawzi, Hoang Ta, and Jeroen Zuiddam 48:1–48:20

Optimal Deterministic Clock Auctions and Beyond
Giorgos Christodoulou, Vasilis Gkatzelis, and Daniel Schoepflin 49:1–49:23

Nonlinear Repair Schemes of Reed-Solomon Codes.
Roni Con and Itzhak Tamo 50:1–50:1

A Complete Linear Programming Hierarchy for Linear Codes
Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones 51:1–51:22

Lower Bounds for Symmetric Circuits for the Determinant
Anuj Dawar and Gregory Wilsenach 52:1–52:22

Convex Influences
Anindya De, Shivam Nadimpalli, and Rocco A. Servedio 53:1–53:21

The Importance of the Spectral Gap in Estimating Ground-State Energies
Abhinav Deshpande, Alexey V. Gorshkov, and Bill Fefferman 54:1–54:6

Mechanism Design with Moral Bidders
Shahar Dobzinski and Sigal Oren 55:1–55:17

Small-Box Cryptography
Yevgeniy Dodis, Harish Karthikeyan, and Daniel Wichs 56:1–56:25

Interaction-Preserving Compilers for Secure Computation
Nico Döttling, Vipul Goyal, Giulio Malavolta, and Justin Raizes 57:1–57:18

Matroid Secretary Is Equivalent to Contention Resolution
Shaddin Dughmi 58:1–58:23

Uniform Brackets, Containers, and Combinatorial Macbeath Regions
Kunal Dutta, Arijit Ghosh, and Shay Moran 59:1–59:10

Multiscale Entropic Regularization for MTS on General Metric Spaces
Farzam Ebrahimnejad and James R. Lee 60:1–60:21

Counting and Sampling Perfect Matchings in Regular Expanding Non-Bipartite Graphs
Farzam Ebrahimnejad, Ansh Nagda, and Shayan Oveis Gharan 61:1–61:12

Embeddings and Labeling Schemes for A*
Talya Eden, Piotr Indyk, and Haike Xu 62:1–62:19

A Unifying Framework for Characterizing and Computing Width Measures
Eduard Eiben, Robert Ganian, Thekla Hamm, Lars Jaffke, and O-joung Kwon ... 63:1–63:23

Reduction from Non-Unique Games to Boolean Unique Games
Ronen Eldan and Dana Moshkovitz 64:1–64:25

Pseudorandom Self-Reductions for NP-Complete Problems
Reyad Abed Elrazik, Robert Robere, Assaf Schuster, and Gal Yehuda 65:1–65:12

Credible, Strategyproof, Optimal, and Bounded Expected-Round Single-Item Auctions for All Distributions
Meryem Essaidi, Matheus V. X. Ferreira, and S. Matthew Weinberg 66:1–66:19

Small Circuits Imply Efficient Arthur-Merlin Protocols
Michael Ezra and Ron D. Rothblum 67:1–67:16

A Lower Bound on the Space Overhead of Fault-Tolerant Quantum Computation
Omar Fawzi, Alexander Müller-Hermes, and Ala Shayeghi 68:1–68:20

On Semi-Algebraic Proofs and Algorithms
Noah Fleming, Mika Göös, Stefan Grosser, and Robert Robere 69:1–69:25

Extremely Deep Proofs
Noah Fleming, Toniann Pitassi, and Robert Robere 70:1–70:23

On the Download Rate of Homomorphic Secret Sharing
Ingerid Fosli, Yuval Ishai, Victor I. Kolobov, and Mary Wootters 71:1–71:22

A Variant of the VC-Dimension with Applications to Depth-3 Circuits
Peter Frankl, Svyatoslav Gryaznov, and Navid Talebanfard 72:1–72:19

Continuous Tasks and the Asynchronous Computability Theorem
Hugo Rincon Galeana, Sergio Rajsbaum, and Ulrich Schmid 73:1–73:27

Correlation Detection in Trees for Planted Graph Alignment
Luca Ganassali, Laurent Massoulié, and Marc Lelarge 74:1–74:8

On Polynomially Many Queries to NP or QMA Oracles
Sevag Gharibian and Dorian Rudolph 75:1–75:27

Eliminating Intermediate Measurements Using Pseudorandom Generators
Uma Girish and Ran Raz 76:1–76:18

Sample-Based Proofs of Proximity
Guy Goldberg and Guy N. Rothblum 77:1–77:19

Testing Distributions of Huge Objects
Oded Goldreich and Dana Ron 78:1–78:19

Omnipredictors
Parikshit Gopalan, Adam Tauman Kalai, Omer Reingold, Vatsal Sharan, and Udi Wieder 79:1–79:21

Mixing in Non-Quasirandom Groups
W. T. Gowers and Emanuele Viola 80:1–80:9

Time-Traveling Simulators Using Blockchains and Their Applications
Vipul Goyal, Justin Raizes, and Pratik Soni 81:1–81:19

Online Multivalid Learning: Means, Moments, and Prediction Intervals
Varun Gupta, Christopher Jung, Georgy Noarov, Mallesh M. Pai, and Aaron Roth 82:1–82:24

Adaptive Massively Parallel Constant-Round Tree Contraction
MohammadTaghi Hajiaghayi, Marina Knittel, Hamed Saleh, and Hsin-Hao Su ... 83:1–83:23

Errorless Versus Error-Prone Average-Case Complexity
Shuichi Hirahara and Rahul Santhanam 84:1–84:23

Excluding PH Pessiland
Shuichi Hirahara and Rahul Santhanam 85:1–85:25

Nash-Bargaining-Based Models for Matching Markets: One-Sided and Two-Sided; Fisher and Arrow-Debreu
Mojtaba Hosseini and Vijay V. Vazirani 86:1–86:20

Symbolic Determinant Identity Testing and Non-Commutative Ranks of Matrix Lie Algebras
Gábor Ivanyos, Tushant Mittal, and Youming Qiao 87:1–87:21

Explicit Abelian Lifts and Quantum LDPC Codes
Fernando Granha Jeronimo, Tushant Mittal, Ryan O'Donnell, Pedro Paredes, and Madhur Tulsiani 88:1–88:21

Almost-Orthogonal Bases for Inner Product Polynomials
Chris Jones and Aaron Potechin 89:1–89:21

Sublinear-Time Computation in the Presence of Online Erasures
Iden Kalemaj, Sofya Raskhodnikova, and Nithin Varma 90:1–90:25

Noisy Boolean Hidden Matching with Applications
Michael Kapralov, Amulya Musipatla, Jakab Tardos, David P. Woodruff, and Samson Zhou 91:1–91:19

On Fairness and Stability in Two-Sided Matchings
Gili Karni, Guy N. Rothblum, and Gal Yona 92:1–92:17

Optimal Bounds for Dominating Set in Graph Streams
Sanjeev Khanna and Christian Konrad 93:1–93:23

Deterministic Dynamic Matching in Worst-Case Update Time
Peter Kiss 94:1–94:21

More Dominantly Truthful Multi-Task Peer Prediction with a Finite Number of Tasks
Yuqing Kong 95:1–95:20

Dynamic Matching Algorithms Under Vertex Updates
Hung Le, Lazar Milenković, Shay Solomon, and Virginia Vassilevska Williams ... 96:1–96:24

Quantum Meets Fine-Grained Complexity: Sublinear Time Quantum Algorithms for String Problems
François Le Gall and Saeed Seddighin 97:1–97:23

Optimal Sub-Gaussian Mean Estimation in Very High Dimensions
Jasper C. H. Lee and Paul Valiant 98:1–98:21

Double Coverage with Machine-Learned Advice
Alexander Lindermayr, Nicole Megow, and Bertrand Simon 99:1–99:18

Beating Classical Impossibility of Position Verification
Jiahui Liu, Qipeng Liu, and Luowen Qian 100:1–100:11

A Gaussian Fixed Point Random Walk
Yang P. Liu, Ashwin Sah, and Mehtaab Sawhney 101:1–101:10

Correlation-Intractable Hash Functions via Shift-Hiding
Alex Lombardi and Vinod Vaikuntanathan 102:1–102:16

Balanced Allocations with Incomplete Information: The Power of Two Queries
Dimitrios Los and Thomas Sauerwald 103:1–103:23

Lifting with Sunflowers
Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang 104:1–104:24

Interactive Communication in Bilateral Trade
Jieming Mao, Renato Paes Leme, and Kangning Wang 105:1–105:21

Support Recovery in Universal One-Bit Compressed Sensing
Arya Mazumdar and Soumyabrata Pal 106:1–106:20

Keep That Card in Mind: Card Guessing with Limited Memory
Boaz Menuhin and Moni Naor 107:1–107:28

A Spectral Approach to Polytope Diameter
Hariharan Narayanan, Rikhav Shah, and Nikhil Srivastava 108:1–108:22

Geometric Bounds on the Fastest Mixing Markov Chain
Sam Olesker-Taylor and Luca Zanetti 109:1–109:1

Lower Bounds on Stabilizer Rank
Shir Peleg, Ben Lee Volk, and Amir Shpilka 110:1–110:4

Beating the Folklore Algorithm for Dynamic Matching
Mohammad Roghani, Amin Saberi, and David Wajc 111:1–111:23

Interactive Proofs for Synthesizing Quantum States and Unitaries
Gregory Rosenthal and Henry Yuen 112:1–112:4

Budget-Smoothed Analysis for Submodular Maximization
Aviad Rubinstein and Junyao Zhao 113:1–113:23

Uniform Bounds for Scheduling with Job Size Estimates
Ziv Scully, Isaac Grosof, and Michael Mitzenmacher 114:1–114:30

$3 + \epsilon$ Approximation of Tree Edit Distance in Truly Subquadratic Time
Masoud Seddighin and Saeed Seddighin 115:1–115:22

On Hardness Assumptions Needed for "Extreme High-End" PRGs and Fast Derandomization
Ronen Shaltiel and Emanuele Viola 116:1–116:17

Low-Bandwidth Recovery of Linear Functions of Reed-Solomon-Encoded Data
Noah Shutty and Mary Wootters 117:1–117:19

Efficient Reconstruction of Depth Three Arithmetic Circuits with Top Fan-In Two
Gaurav Sinha 118:1–118:33

Polynomial Identity Testing via Evaluation of Rational Functions
Dieter van Melkebeek and Andrew Morgan 119:1–119:24

Probing to Minimize
Weina Wang , Anupam Gupta, and Jalani K. Williams 120:1–120:23