16th Innovations in Theoretical Computer Science Conference

ITCS 2025, January 7–10, 2025, Columbia University, New York, NY, USA

Edited by

Raghu Meka

Part 1 of 3

LIPICS

Editors

Raghu Meka
University of California, Los Angeles, CA, USA
raghum@cs.ucla.edu

ACM Classification 2012
Mathematics of computing; Theory of computation

ISBN 978-3-95977-361-4
PRINT ISBN: 979-8-3313-1495-8

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/978-3-95977-361-4.

Publication date
February, 2025

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.2025.0

ISBN 978-3-95977-361-4 **ISSN 1868-8969** **https://www.dagstuhl.de/lipics**

Contents

Preface
Raghu Meka 0:xi

List of Authors
0:xiii

Papers

Simple Is COOL: Graded Dispersal and Its Applications for Byzantine Fault Tolerance
Ittai Abraham, Gilad Asharov, and Anirudh Chandramouli 1:1–1:20

Improved Lower Bounds for 3-Query Matching Vector Codes
Divesh Aggarwal, Pranjal Dutta, Zeyong Li, Maciej Obremski, and Sidhant Saraogi 2:1–2:19

Sparsity Lower Bounds for Probabilistic Polynomials
Josh Alman, Arkadev Chattopadhyay, and Ryan Williams 3:1–3:25

A Bicriterion Concentration Inequality and Prophet Inequalities for k-Fold Matroid Unions
Noga Alon, Nick Gravin, Tristan Pollner, Aviad Rubinstein, Hongao Wang, S. Matthew Weinberg, and Qianfan Zhang 4:1–4:22

Edge-Minimum Walk of Modular Length in Polynomial Time
Antoine Amarilli, Benoît Groz, and Nicole Wein 5:1–5:23

Doubly Sub-Linear Interactive Proofs of Proximity
Noga Amir, Oded Goldreich, and Guy N. Rothblum 6:1–6:25

Simultaneous Haar Indistinguishability with Applications to Unclonable Cryptography
Prabhanjan Ananth, Fatih Kaleoglu, and Henry Yuen 7:1–7:23

Single-Round Proofs of Quantumness from Knowledge Assumptions
Petia Arabadjieva, Alexandru Gheorghiu, Victor Gitton, and Tony Metger 8:1–8:16

The Local Hamiltonian Problem for Quasi-Quantum States: A Toy Model for the Quantum PCP Conjecture
Itai Arad and Miklos Santha 9:1–9:1

Algorithmic Collusion Without Threats
Eshwar Ram Arunachaleswaran, Natalie Collina, Sampath Kannan, Aaron Roth, and Juba Ziani 10:1–10:21

Rank Lower Bounds on Non-Local Quantum Computation
Vahid R. Asadi, Eric Culf, and Alex May 11:1–11:18

Stable Matching with Interviews
Itai Ashlagi, Jiale Chen, Mohammad Roghani, and Amin Saberi 12:1–12:19

16th Innovations in Theoretical Computer Science Conference (ITCS 2025).
Editor: Raghu Meka
LIPICS Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Low Sensitivity Hopsets
Vikrant Ashvinkumar, Aaron Bernstein, Chengyuan Deng, Jie Gao, and Nicole Wein 13:1–13:23

The More the Merrier! On Total Coding and Lattice Problems and the Complexity of Finding Multicollisions
Huck Bennett, Surendra Ghentiyala, and Noah Stephens-Davidowitz 14:1–14:22

Exponential-Time Approximation (Schemes) for Vertex-Ordering Problems
Matthias Bentert, Fedor V. Fomin, Tanmay Inamdar, and Saket Saurabh 15:1–15:18

On Fault Tolerant Single-Shot Logical State Preparation and Robust Long-Range Entanglement
Thiago Bergamaschi and Yunchao Liu 16:1–16:9

Random Restrictions of Bounded Low Degree Polynomials Are Juntas
Sreejata Kishor Bhattacharya 17:1–17:21

Finite Matrix Multiplication Algorithms from Infinite Groups
Jonah Blasiak, Henry Cohn, Joshua A. Grochow, Kevin Pratt, and Chris Umans 18:1–18:23

Differential Privacy and Sublinear Time Are Incompatible Sometimes
Jeremiah Blocki, Hendrik Fichtenberger, Elena Grigorescu, and Tamalika Mukherjee 19:1–19:18

Estimating Euclidean Distance to Linearity
Andrej Bogdanov and Lorenzo Taschin 20:1–20:18

Adjacency Labeling Schemes for Small Classes
Édouard Bonnet, Julien Duron, John Sylvester, and Viktor Zamaraev 21:1–21:22

Round-Vs-Resilience Tradeoffs for Binary Feedback Channels
Mark Braverman, Klim Efremenko, Gillat Kol, Raghuvansh R. Saxena, and Zhijun Zhang 22:1–22:23

Accumulation Without Homomorphism
Benedikt Bünz, Pratyush Mishra, Wilson Nguyen, and William Wang 23:1–23:25

Sampling List Packings
Evan Camrud, Ewan Davies, Alex Karduna, and Holden Lee 24:1–24:15

Locally Private Histograms in All Privacy Regimes
Clément L. Canonne and Abigail Gentle 25:1–25:24

Settling the Complexity of Testing Grainedness of Distributions, and Application to Uniformity Testing in the Huge Object Model
Clément L. Canonne, Sayantan Sen, and Joy Qiping Yang 26:1–26:19

The Randomness Complexity of Differential Privacy
Clément L. Canonne, Francis E. Su, and Salil P. Vadhan 27:1–27:21

Coresets for 1-Center in ℓ_1 Metrics
Amir Carmel, Chengzhi Guo, Shaofeng H.-C. Jiang, and Robert Krauthgamer 28:1–28:20

Extracting Dual Solutions via Primal Optimizers
Yair Carmon, Arun Jambulapati, Liam O'Carroll, and Aaron Sidford 29:1–29:24

Provability of the Circuit Size Hierarchy and Its Consequences
Marco Carmosino, Valentine Kabanets, Antonina Kolokolova, Igor C. Oliveira, and Dimitrios Tsintsilidas 30:1–30:22

Quantum Advantage and Lower Bounds in Parallel Query Complexity
Joseph Carolan, Amin Shiraz Gilani, and Mahathi Vempati 31:1–31:14

Succinct Fermion Data Structures
Joseph Carolan and Luke Schaeffer 32:1–32:21

Bosonic Quantum Computational Complexity
Ulysse Chabaud, Michael Joseph, Saeed Mehraban, and Arsalan Motamedi 33:1–33:19

Directed Hypercube Routing, a Generalized Lehman-Ron Theorem, and Monotonicity Testing
Deeparnab Chakrabarty and C. Seshadhri 34:1–34:15

Unraveling Universally Closest Refinements via Symmetric Density Decomposition and Fisher Market Equilibrium
T-H. Hubert Chan and Quan Xue 35:1–35:23

Entry-Specific Matrix Estimation Under Arbitrary Sampling Patterns Through the Lens of Network Flows
Yudong Chen, Xumei Xi, and Christina Lee Yu 36:1–36:2

A Lower Bound on the Trace Norm of Boolean Matrices and Its Applications
Tsun-Ming Cheung, Hamed Hatami, Kaave Hosseini, Aleksandar Nikolov, Toniann Pitassi, and Morgan Shirley 37:1–37:15

Backdoor Defense, Learnability and Obfuscation
Paul Christiano, Jacob Hilton, Victor Lecomte, and Mark Xu 38:1–38:21

Data Reconstruction: When You See It and When You Don't
Edith Cohen, Haim Kaplan, Yishay Mansour, Shay Moran, Kobbi Nissim, Uri Stemmer, and Eliad Tsfadia 39:1–39:23

Derandomized Squaring: An Analytical Insight into Its True Behavior
Gil Cohen, Itay Cohen, Gal Maor, and Yuval Peled 40:1–40:24

Query Complexity of Stochastic Minimum Vertex Cover
Mahsa Derakhshan, Mohammad Saneian, and Zhiyang Xun 41:1–41:12

Nearest Neighbor Complexity and Boolean Circuits
Mason DiCicco, Vladimir Podolskii, and Daniel Reichman 42:1–42:23

Space Complexity of Minimum Cut Problems in Single-Pass Streams
Matthew Ding, Alexandro Garces, Jason Li, Honghao Lin, Jelani Nelson, Vihan Shah, and David P. Woodruff 43:1–43:23

Learning-Augmented Streaming Algorithms for Approximating MAX-CUT
Yinhao Dong, Pan Peng, and Ali Vakilian 44:1–44:24

Distributed and Parallel Low-Diameter Decompositions for Arbitrary and Restricted Graphs
Jinfeng Dou, Thorsten Götte, Henning Hillebrandt, Christian Scheideler, and Julian Werthmann 45:1–45:26

Data-Driven Solution Portfolios
Marina Drygala, Silvio Lattanzi, Andreas Maggiori, Miltiadis Stouras, Ola Svensson, and Sergei Vassilvitskii 46:1–46:15

Concentration of Submodular Functions and Read-k Families Under Negative Dependence
Sharmila Duppala, George Z. Li, Juan Luque, Aravind Srinivasan, and Renata Valieva 47:1–47:16

Robust Restaking Networks
Naveen Durvasula and Tim Roughgarden 48:1–48:21

Confusion Matrix Design for Downstream Decision-Making
Yiding Feng and Wei Tang 49:1–49:1

Fully Characterizing Lossy Catalytic Computation
Marten Folkertsma, Ian Mertz, Florian Speelman, and Quinten Tupker 50:1–50:13

Parameterized Geometric Graph Modification with Disk Scaling
Fedor V. Fomin, Petr A. Golovach, Tanmay Inamdar, Saket Saurabh, and Meirav Zehavi 51:1–51:17

Combinatorial Pen Testing (Or Consumer Surplus of Deferred-Acceptance Auctions)
Aadityan Ganesh and Jason Hartline 52:1–52:22

Differential Privacy on Trust Graphs
Badih Ghazi, Ravi Kumar, Pasin Manurangsi, and Serena Wang 53:1–53:23

Partial Minimum Branching Program Size Problem Is ETH-Hard
Ludmila Glinskih and Artur Riazanov 54:1–54:22

Completeness Theorems for k-SUM and Geometric Friends: Deciding Fragments of Linear Integer Arithmetic
Geri Gokaj and Marvin Künnemann 55:1–55:25

Incompressible Functional Encryption
Rishab Goyal, Venkata Koppula, Mahesh Sreekumar Rajasree, and Aman Verma 56:1–56:22

Deterministic Approximation for the Volume of the Truncated Fractional Matching Polytope
Heng Guo and Vishvajeet N 57:1–57:14

The Computational Complexity of Factored Graphs
Shreya Gupta, Boyang Huang, Russell Impagliazzo, Stanley Woo, and Christopher Ye 58:1–58:19

Error Correction for Message Streams
Meghal Gupta and Rachel Yun Zhang 59:1–59:18

List Decoding Bounds for Binary Codes with Noiseless Feedback
Meghal Gupta and Rachel Yun Zhang 60:1–60:20

Hardness of Sampling for the Anti-Ferromagnetic Ising Model on Random Graphs
Neng Huang, Will Perkins, and Aaron Potechin 61:1–61:23

A High Dimensional Cramer's Rule Connecting Homogeneous Multilinear Equations to Hyperdeterminants
Antoine Joux and Anand Kumar Narayanan 62:1–62:16

Complexity Classification of Product State Problems for Local Hamiltonians
John Kallaugher, Ojas Parekh, Kevin Thompson, Yipu Wang, and Justin Yirka 63:1–63:32

A Universal Sequence of Tensors for the Asymptotic Rank Conjecture
Petteri Kaski and Mateusz Michałek 64:1–64:24

Online Versus Offline Adversaries in Property Testing
Esty Kelman, Ephraim Linder, and Sofya Raskhodnikova 65:1–65:18

Graph Reconstruction via MIS Queries
Christian Konrad, Conor O'Sullivan, and Victor Traistaru 66:1–66:19

Error-Correcting Graph Codes
Swastik Kopparty, Aditya Potukuchi, and Harry Sha 67:1–67:20

New Pseudorandom Generators and Correlation Bounds Using Extractors
Vinayak M. Kumar 68:1–68:23

Approximate Unitary k-Designs from Shallow, Low-Communication Circuits
Nicholas LaRacuente and Felix Leditzky 69:1–69:2

Facility Location on High-Dimensional Euclidean Spaces
Euiwoong Lee and Kijun Shin 70:1–70:21

Toward the Impossibility of Perfect Complete Quantum PKE from OWFs
Longcheng Li, Qian Li, Xingjian Li, and Qipeng Liu 71:1–71:16

Information Design with Unknown Prior
Tao Lin and Ce Li 72:1–72:1

On White-Box Learning and Public-Key Encryption
Yanyi Liu, Noam Mazor, and Rafael Pass 73:1–73:22

Sublinear Metric Steiner Tree via Improved Bounds for Set Cover
Sepideh Mahabadi, Mohammad Roghani, Jakub Tarnawski, and Ali Vakilian 74:1–74:24

Gadgetless Lifting Beats Round Elimination: Improved Lower Bounds for Pointer Chasing
Xinyu Mao, Guangxu Yang, and Jiapeng Zhang 75:1–75:14

A Quantum Unique Games Conjecture
Hamoon Mousavi and Taro Spirig 76:1–76:16

Sketching, Moment Estimation, and the Lévy-Khintchine Representation Theorem
Seth Pettie and Dingyu Wang 77:1–77:23

Randomized Lifting to Semi-Structured Communication Complexity via Linear Diversity
Vladimir Podolskii and Alexander Shekhovtsov 78:1–78:21

Catalytic Communication
Edward Pyne, Nathan S. Sheffield, and William Wang 79:1–79:24

Diversity in Evolutionary Dynamics
Yuval Rabani, Leonard J. Schulman, and Alistair Sinclair 80:1–80:3

Online Balanced Allocation of Dynamic Components
Rajmohan Rajaraman and Omer Wasim 81:1–81:23

Tight Bounds on List-Decodable and List-Recoverable Zero-Rate Codes
Nicolas Resch, Chen Yuan, and Yihan Zhang 82:1–82:21

Fine-Grained Equivalence for Problems Related to Integer Linear Programming
Lars Rohwedder and Karol Węgrzycki 83:1–83:18

Quantum Communication Complexity of Classical Auctions
Aviad Rubinstein and Zixin Zhou 84:1–84:27

Quantum 2-SAT on Low Dimensional Systems Is QMA$_1$-Complete: Direct Embeddings and Black-Box Simulation
Dorian Rudolph, Sevag Gharibian, and Daniel Nagaj 85:1–85:24

Eulerian Orientations and Hadamard Codes: A Novel Connection via Counting
Shuai Shao and Zhuxiao Tang 86:1–86:13

When to Give up on a Parallel Implementation
Nathan S. Sheffield and Alek Westover 87:1–87:18

Detecting and Correcting Computationally Bounded Errors: A Simple Construction Under Minimal Assumptions
Jad Silbak and Daniel Wichs 88:1–88:23

Optimal Communication Complexity of Chained Index
Janani Sundaresan 89:1–89:18

Polynomial Size, Short-Circuit Resilient Circuits for NC
Yael Tauman Kalai and Raghuvansh R. Saxena 90:1–90:18

Simple Norm Bounds for Polynomial Random Matrices via Decoupling
Madhur Tulsiani and June Wu 91:1–91:22

Listing 6-Cycles in Sparse Graphs
Virginia Vassilevska Williams and Alek Westover 92:1–92:21

Polynomials, Divided Differences, and Codes
S. Venkitesh 93:1–93:25

New Direct Sum Tests
Alek Westover, Edward Yu, and Kai Zhe Zheng 94:1–94:26

Toward Separating QMA from QCMA with a Classical Oracle
Mark Zhandry 95:1–95:19

Formulations and Constructions of Remote State Preparation with Verifiability, with Applications
Jiayu Zhang 96:1–96:19