

# 14th Innovations in Theoretical Computer Science Conference

ITCS 2023, January 10–13, 2023, MIT, Cambridge,  
Massachusetts, USA

Edited by

Yael Tauman Kalai

Part 1 of 3



*Editors*

**Yael Tauman Kalai**

Microsoft Research New England, Cambridge, USA  
yaelism@gmail.com

*ACM Classification 2012*

Mathematics of computing; Theory of computation

**ISBN 978-3-95977-263-1**

PRINT ISBN: 978-1-7138-7066-1

*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/978-3-95977-263-1>.

*Publication date*

January, 2023

*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.2023.0

ISBN 978-3-95977-263-1

ISSN 1868-8969

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

## ■ Contents

Preface	
<i>Yael Tauman Kalai</i> .....	0:xi
List of Authors	
.....	0:xiii
<b>Papers</b>	
Worst-Case to Expander-Case Reductions	
<i>Amir Abboud and Nathan Wallheimer</i> .....	1:1–1:23
Matroid Partition Property and the Secretary Problem	
<i>Dorna Abdolazimi, Anna R. Karlin, Nathan Klein, and Shayan Oveis Gharan</i> ....	2:1–2:9
Kolmogorov Complexity Characterizes Statistical Zero Knowledge	
<i>Eric Allender, Shuichi Hirahara, and Harsha Tirumala</i> .....	3:1–3:19
Communication Complexity of Inner Product in Symmetric Normed Spaces	
<i>Alexandr Andoni, Jarosław Błasiok, and Arnold Filtser</i> .....	4:1–4:22
Concentration Bounds for Quantum States and Limitations on the QAOA from Polynomial Approximations	
<i>Anurag Anshu and Tony Metger</i> .....	5:1–5:8
On Identity Testing and Noncommutative Rank Computation over the Free Skew Field	
<i>V. Arvind, Abhranil Chatterjee, Utsab Ghosal, Partha Mukhopadhyay, and C. Ramya</i> .....	6:1–6:23
All-Norm Load Balancing in Graph Streams via the Multiplicative Weights Update Method	
<i>Sepehr Assadi, Aaron Bernstein, and Zachary Langley</i> .....	7:1–7:24
A Framework for Adversarial Streaming via Differential Privacy and Difference Estimators	
<i>Idan Attias, Edith Cohen, Moshe Shechner, and Uri Stemmer</i> .....	8:1–8:19
Making Auctions Robust to Aftermarkets	
<i>Moshe Babaioff, Nicole Immorlica, Yingkai Li, and Brendan Lucier</i> .....	9:1–9:23
Efficiently Testable Circuits	
<i>Mirza Ahad Baig, Suvradip Chakraborty, Stefan Dziembowski, Małgorzata Gałazka, Tomasz Lizurej, and Krzysztof Pietrzak</i> .....	10:1–10:23
Strategyproof Scheduling with Predictions	
<i>Eric Balkanski, Vasilis Gkatzelis, and Xizhi Tan</i> .....	11:1–11:22
Graph Searching with Predictions	
<i>Siddhartha Banerjee, Vincent Cohen-Addad, Anupam Gupta, and Zhouzi Li</i> .....	12:1–12:24
On Computing Homological Hitting Sets	
<i>Ulrich Bauer, Abhishek Rathod, and Meirav Zehavi</i> .....	13:1–13:21

14th Innovations in Theoretical Computer Science Conference (ITCS 2023).

Editor: Yael Tauman Kalai



Leibniz International Proceedings in Informatics

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

On Disperser/Lifting Properties of the Index and Inner-Product Functions <i>Paul Beame and Sajin Koroth</i> .....	14:1–14:17
Is This Correct? Let’s Check! <i>Omri Ben-Eliezer, Dan Mikulincer, Elchanan Mossel, and Madhu Sudan</i> .....	15:1–15:11
Online Learning and Bandits with Queried Hints <i>Aditya Bhaskara, Sreenivas Gollapudi, Sungjin Im, Kostas Kollias, and Kamesh Munagala</i> .....	16:1–16:24
Bootstrapping Homomorphic Encryption via Functional Encryption <i>Nir Bitansky and Tomer Solomon</i> .....	17:1–17:23
Certification with an NP Oracle <i>Guy Blanc, Caleb Koch, Jane Lange, Carmen Strassle, and Li-Yang Tan</i> .....	18:1–18:22
Matrix Multiplication via Matrix Groups <i>Jonah Blasiak, Henry Cohn, Joshua A. Grochow, Kevin Pratt, and Chris Umans</i> .....	19:1–19:16
Epic Fail: Emulators Can Tolerate Polynomially Many Edge Faults for Free <i>Greg Bodwin, Michael Dinitz, and Yasamin Nazari</i> .....	20:1–20:22
Opponent Indifference in Rating Systems: A Theoretical Case for Sonas <i>Greg Bodwin and Forest Zhang</i> .....	21:1–21:21
PPP-Completeness and Extremal Combinatorics <i>Romain Bourneuf, Lukáš Folwarczný, Pavel Hubáček, Alon Rosen, and Nikolaj I. Schwartzbach</i> .....	22:1–22:20
On Low-End Obfuscation and Learning <i>Elette Boyle, Yuval Ishai, Pierre Meyer, Robert Robere, and Gal Yehuda</i> .....	23:1–23:28
On the Computational Hardness Needed for Quantum Cryptography <i>Zvika Brakerski, Ran Canetti, and Luowen Qian</i> .....	24:1–24:21
Improved Monotonicity Testers via Hypercube Embeddings <i>Mark Braverman, Subhash Khot, Guy Kindler, and Dor Minzer</i> .....	25:1–25:24
Rounding via Low Dimensional Embeddings <i>Mark Braverman and Dor Minzer</i> .....	26:1–26:30
Counting Subgraphs in Somewhere Dense Graphs <i>Marco Bressan, Leslie Ann Goldberg, Kitty Meeks, and Marc Roth</i> .....	27:1–27:14
Rigidity for Monogamy-Of-Entanglement Games <i>Anne Broadbent and Eric Culf</i> .....	28:1–28:29
Quantum Majority Vote <i>Harry Buhrman, Noah Linden, Laura Mančinská, Ashley Montanaro, and Maris Ozols</i> .....	29:1–29:1
TFNP Characterizations of Proof Systems and Monotone Circuits <i>Sam Buss, Noah Fleming, and Russell Impagliazzo</i> .....	30:1–30:40
Clustering Permutations: New Techniques with Streaming Applications <i>Diptarka Chakraborty, Debarati Das, and Robert Krauthgamer</i> .....	31:1–31:24

Certificate Games <i>Sourav Chakraborty, Anna Gál, Sophie Laplante, Rajat Mittal, and Anupa Sunny</i> .....	32:1–32:24
Lifting to Parity Decision Trees via Stifling <i>Arkadev Chattopadhyay, Nikhil S. Mande, Swagato Sanyal, and Suhail Sherif</i> .....	33:1–33:20
New Lower Bounds and Derandomization for ACC, and a Derandomization-Centric View on the Algorithmic Method <i>Lijie Chen</i> .....	34:1–34:15
Black-Box Constructive Proofs Are Unavoidable <i>Lijie Chen, Ryan Williams, and Tianqi Yang</i> .....	35:1–35:24
Necessary Conditions in Multi-Server Differential Privacy <i>Albert Cheu and Chao Yan</i> .....	36:1–36:21
Quantum Algorithms and the Power of Forgetting <i>Andrew M. Childs, Matthew Coudron, and Amin Shiraz Gilani</i> .....	37:1–37:22
A New Conjecture on Hardness of 2-CSP’s with Implications to Hardness of Densest $k$ -Subgraph and Other Problems <i>Julia Chuzhoy, Mina Dalirrooyfard, Vadim Grinberg, and Zihan Tan</i> .....	38:1–38:23
Generalized Private Selection and Testing with High Confidence <i>Edith Cohen, Xin Lyu, Jelani Nelson, Tamás Sarlós, and Uri Stemmer</i> .....	39:1–39:23
Exact Completeness of LP Hierarchies for Linear Codes <i>Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones</i> .....	40:1–40:18
HappyMap: A Generalized Multicalibration Method <i>Zhan Deng, Cynthia Dwork, and Linjun Zhang</i> .....	41:1–41:23
Bit Complexity of Jordan Normal Form and Polynomial Spectral Factorization <i>Papri Dey, Ravi Kannan, Nick Ryder, and Nikhil Srivastava</i> .....	42:1–42:18
Constant-Depth Sorting Networks <i>Natalia Dobrokhotova-Maikova, Alexander Kozachinskiy, and Vladimir Podolskii</i> .....	43:1–43:19
Rigidity in Mechanism Design and Its Applications <i>Shahar Dobzinski and Ariel Shaulker</i> .....	44:1–44:21
Beeping Shortest Paths via Hypergraph Bipartite Decomposition <i>Fabien Dufoulon, Yuval Emek, and Ran Gelles</i> .....	45:1–45:24
Noisy Radio Network Lower Bounds via Noiseless Beeping Lower Bounds <i>Klim Efremenko, Gillat Kol, Dmitry Paramonov, and Raghuvansh R. Saxena</i> ....	46:1–46:20
Asymptotically Tight Bounds on the Time Complexity of Broadcast and Its Variants in Dynamic Networks <i>Antoine El-Hayek, Monika Henzinger, and Stefan Schmid</i> .....	47:1–47:21
Differentially Private Continual Releases of Streaming Frequency Moment Estimations <i>Alessandro Epasto, Jieming Mao, Andres Munoz Medina, Vahab Mirrokni, Sergei Vassilvitskii, and Peilin Zhong</i> .....	48:1–48:24

A Subpolynomial-Time Algorithm for the Free Energy of One-Dimensional Quantum Systems in the Thermodynamic Limit <i>Hamza Fawzi, Omar Fawzi, and Samuel O. Scalet</i> .....	49:1–49:6
Expander Decomposition in Dynamic Streams <i>Arnold Filtser, Michael Kapralov, and Mikhail Makarov</i> .....	50:1–50:13
On Flipping the Fréchet Distance <i>Omrit Filtser, Mayank Goswami, Joseph S. B. Mitchell, and Valentin Polishchuk</i> .....	51:1–51:22
Budget Pacing in Repeated Auctions: Regret and Efficiency Without Convergence <i>Jason Gaitonde, Yingkai Li, Bar Light, Brendan Lucier, and Aleksandrs Slivkins</i> .....	52:1–52:1
Quantum Space, Ground Space Traversal, and How to Embed Multi-Prover Interactive Proofs into Unentanglement <i>Sevag Gharibian and Dorian Rudolph</i> .....	53:1–53:23
Algorithms with More Granular Differential Privacy Guarantees <i>Badih Ghazi, Ravi Kumar, Pasin Manurangsi, and Thomas Steinke</i> .....	54:1–54:24
Private Counting of Distinct and $k$ -Occurring Items in Time Windows <i>Badih Ghazi, Ravi Kumar, Jelani Nelson, and Pasin Manurangsi</i> .....	55:1–55:24
Is Untrusted Randomness Helpful? <i>Uma Girish, Ran Raz, and Wei Zhan</i> .....	56:1–56:18
Consensus Division in an Arbitrary Ratio <i>Paul Goldberg and Jiawei Li</i> .....	57:1–57:18
An Algorithmic Bridge Between Hamming and Levenshtein Distances <i>Elazar Goldenberg, Tomasz Kociumaka, Robert Krauthgamer, and Barna Saha</i> ...	58:1–58:23
On Interactive Proofs of Proximity with Proof-Oblivious Queries <i>Oded Goldreich, Guy N. Rothblum, and Tal Skverer</i> .....	59:1–59:16
Loss Minimization Through the Lens Of Outcome Indistinguishability <i>Parikshit Gopalan, Lunjia Hu, Michael P. Kim, Omer Reingold, and Udi Wieder</i> .....	60:1–60:20
List Agreement Expansion from Coboundary Expansion <i>Roy Gottlib and Tali Kaufman</i> .....	61:1–61:23
Asynchronous Multi-Party Quantum Computation <i>Vipul Goyal, Chen-Da Liu-Zhang, Justin Raizes, and João Ribeiro</i> .....	62:1–62:22
Unsplittable Euclidean Capacitated Vehicle Routing: A $(2 + \epsilon)$ -Approximation Algorithm <i>Fabrizio Grandoni, Claire Mathieu, and Hang Zhou</i> .....	63:1–63:13
Low-Stabilizer-Complexity Quantum States Are Not Pseudorandom <i>Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang</i> .....	64:1–64:20
Look Before, Before You Leap: Online Vector Load Balancing with Few Reassignments <i>Varun Gupta, Ravishankar Krishnaswamy, Sai Sandeep, and Janani Sundaresan</i> .....	65:1–65:17

Incompressibility and Next-Block Pseudoentropy <i>Iftach Haitner, Noam Mazon, and Jad Silbak</i> .....	66:1–66:18
Downward Self-Reducibility in TFNP <i>Prahladh Harsha, Daniel Mitropolsky, and Alon Rosen</i> .....	67:1–67:17
Symmetric Formulas for Products of Permutations <i>William He and Benjamin Rossman</i> .....	68:1–68:23
A Combinatorial Cut-Toggling Algorithm for Solving Laplacian Linear Systems <i>Monika Henzinger, Billy Jin, Richard Peng, and David P. Williamson</i> .....	69:1–69:22
Learning Versus Pseudorandom Generators in Constant Parallel Time <i>Shuichi Hirahara and Mikito Nanashima</i> .....	70:1–70:18
Secure Distributed Network Optimization Against Eavesdroppers <i>Yael Hitron, Merav Parter, and Eylon Yogev</i> .....	71:1–71:20
Comparative Learning: A Sample Complexity Theory for Two Hypothesis Classes <i>Lunjia Hu and Charlotte Peale</i> .....	72:1–72:30
Recovery from Non-Decomposable Distance Oracles <i>Zhuangfei Hu, Xinda Li, David P. Woodruff, Hongyang Zhang, and Shufan Zhang</i> .....	73:1–73:22
Karchmer-Wigderson Games for Hazard-Free Computation <i>Christian Ikenmeyer, Balagopal Komarath, and Nitin Saurabh</i> .....	74:1–74:25
Learning Reserve Prices in Second-Price Auctions <i>Yaonan Jin, Pinyan Lu, and Tao Xiao</i> .....	75:1–75:24
The Complexity of Infinite-Horizon General-Sum Stochastic Games <i>Yujia Jin, Vidya Muthukumar, and Aaron Sidford</i> .....	76:1–76:20
Random Max-CSPs Inherit Algorithmic Hardness from Spin Glasses <i>Chris Jones, Kunal Marwaha, Jusspreet Singh Sandhu, and Jonathan Shi</i> .....	77:1–77:26
Garland’s Technique for Posets and High Dimensional Grassmannian Expanders <i>Tali Kaufman and Ran J. Tessler</i> .....	78:1–78:22
Making Decisions Under Outcome Performativity <i>Michael P. Kim and Juan C. Perdomo</i> .....	79:1–79:15
Characterizing the Multi-Pass Streaming Complexity for Solving Boolean CSPs Exactly <i>Gillat Kol, Dmitry Paramonov, Raghuvansh R. Saxena, and Huacheng Yu</i> .....	80:1–80:15
False Consensus, Information Theory, and Prediction Markets <i>Yuqing Kong and Grant Schoenebeck</i> .....	81:1–81:23
Depth-Bounded Quantum Cryptography with Applications to One-Time Memory and More <i>Qipeng Liu</i> .....	82:1–82:18
Vertex Sparsification for Edge Connectivity in Polynomial Time <i>Yang P. Liu</i> .....	83:1–83:15

Fractional Certificates for Bounded Functions <i>Shachar Lovett and Jiapeng Zhang</i> .....	84:1–84:13
Improved Inapproximability of VC Dimension and Littlestone’s Dimension via (Unbalanced) Biclique <i>Pasin Manurangsi</i> .....	85:1–85:18
Resilience of 3-Majority Dynamics to Non-Uniform Schedulers <i>Uri Meir, Rotem Oshman, Ofer Shayevitz, and Yuval Volkov</i> .....	86:1–86:19
Proofs of Quantumness from Trapdoor Permutations <i>Tomoyuki Morimae and Takashi Yamakawa</i> .....	87:1–87:14
Extremal Combinatorics, Iterated Pigeonhole Arguments and Generalizations of PPP <i>Amol Pasarkar, Christos Papadimitriou, and Mihalis Yannakakis</i> .....	88:1–88:20
The Strength of Equality Oracles in Communication <i>Toniann Pitassi, Morgan Shirley, and Adi Shraibman</i> .....	89:1–89:19
Quantum Proofs of Deletion for Learning with Errors <i>Alexander Poremba</i> .....	90:1–90:14
Online Pen Testing <i>Mingda Qiao and Gregory Valiant</i> .....	91:1–91:26
Decision-Making Under Miscalibration <i>Guy N. Rothblum and Gal Yona</i> .....	92:1–92:20
Beyond Worst-Case Budget-Feasible Mechanism Design <i>Aviad Rubinfeld and Junyao Zhao</i> .....	93:1–93:22
Is It Easier to Count Communities Than Find Them? <i>Cynthia Rush, Fiona Skerman, Alexander S. Wein, and Dana Yang</i> .....	94:1–94:23
An Improved Lower Bound for Matroid Intersection Prophet Inequalities <i>Raghuvansh R. Saxena, Santhoshini Velusamy, and S. Matthew Weinberg</i> .....	95:1–95:20
Unitary Property Testing Lower Bounds by Polynomials <i>Adrian She and Henry Yuen</i> .....	96:1–96:17
What Can Cryptography Do for Decentralized Mechanism Design? <i>Elaine Shi, Hao Chung, and Ke Wu</i> .....	97:1–97:22
Efficient Algorithms for Certifying Lower Bounds on the Discrepancy of Random Matrices <i>Prayaag Venkat</i> .....	98:1–98:12
On Oracles and Algorithmic Methods for Proving Lower Bounds <i>Nikhil Vyas and Ryan Williams</i> .....	99:1–99:26
The Time Complexity of Consensus Under Oblivious Message Adversaries <i>Kyrill Winkler, Ami Paz, Hugo Rincon Galeana, Stefan Schmid, and Ulrich Schmid</i> .....	100:1–100:28
Exponential Separations Using Guarded Extension Variables <i>Emre Yolcu and Marijn J. H. Heule</i> .....	101:1–101:22