

13th Innovations in Theoretical Computer Science Conference

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

Edited by

Mark Braverman



Editor

Mark Braverman

Princeton University, USA

mbraverm@gmail.com

ACM Classification 2012

Mathematics of computing; Theory of computation

ISBN 978-3-95977-217-4

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

ISBN 978-3-95977-217-4

ISSN 1868-8969

<https://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*, Reykjavik University, IS and Gran Sasso Science Institute, IT)
- Christel Baier (TU Dresden, DE)
- Mikolaj Bojanczyk (University of Warsaw, PL)
- Roberto Di Cosmo (Inria and Université de Paris, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Daniel Král' (Masaryk University - Brno, CZ)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (University of Oxford, GB)
- Phillip Rogaway (University of California, Davis, US)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Raimund Seidel (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)

ISSN 1868-8969

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

■ Contents

Preface	
<i>Mark Braverman</i>	0:xiii
List of Authors	
.....	0:xv–0:xxiv

Papers

Maximizing Revenue in the Presence of Intermediaries	
<i>Gagan Aggarwal, Kshipra Bhawalkar, Guru Guruganesh, and Andres Perlroth</i>	1:1–1:22
Algebraic Restriction Codes and Their Applications	
<i>Divesh Aggarwal, Nico Döttling, Jesko Dujmovic, Mohammad Hajiabadi, Giulio Malavolta, and Maciej Obremski</i>	2:1–2:15
Improved Merlin-Arthur Protocols for Central Problems in Fine-Grained Complexity	
<i>Shyan Akmal, Lijie Chen, Ce Jin, Malvika Raj, and Ryan Williams</i>	3:1–3:25
Pre-Constrained Encryption	
<i>Prabhanjan Ananth, Abhishek Jain, Zhengzhong Jin, and Giulio Malavolta</i>	4:1–4:20
Domain Sparsification of Discrete Distributions Using Entropic Independence	
<i>Nima Anari, Michał Dereziński, Thuy-Duong Vuong, and Elizabeth Yang</i>	5:1–5:23
Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians	
<i>Anurag Anshu and Chinmay Nirkhe</i>	6:1–6:22
Near-Optimal Distributed Implementations of Dynamic Algorithms for Symmetry Breaking Problems	
<i>Shiri Antaki, Quanquan C. Liu, and Shay Solomon</i>	7:1–7:25
Secret Sharing, Slice Formulas, and Monotone Real Circuits	
<i>Benny Applebaum, Amos Beimel, Oded Nir, Naty Peter, and Toniann Pitassi</i>	8:1–8:23
An Asymptotically Optimal Algorithm for Maximum Matching in Dynamic Streams	
<i>Sepehr Assadi and Vihan Shah</i>	9:1–9:23
Sublinear Time and Space Algorithms for Correlation Clustering via Sparse-Dense Decompositions	
<i>Sepehr Assadi and Chen Wang</i>	10:1–10:20
Multi-Channel Bayesian Persuasion	
<i>Yakov Babichenko, Inbal Talgam-Cohen, Haifeng Xu, and Konstantin Zabarnyi</i> ...	11:1–11:2
Randomness Extraction from Somewhat Dependent Sources	
<i>Marshall Ball, Oded Goldreich, and Tal Malkin</i>	12:1–12:14
Prefix Discrepancy, Smoothed Analysis, and Combinatorial Vector Balancing	
<i>Nikhil Bansal, Haotian Jiang, Raghu Meka, Sahil Singla, and Makrand Sinha</i>	13:1–13:22

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman



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	
<i>Boaz Barak and Kunal Marwaha</i>	14:1–14:21
Indistinguishability Obfuscation of Null Quantum Circuits and Applications	
<i>James Bartusek and Giulio Malavolta</i>	15:1–15:13
An Efficient Semi-Streaming PTAS for Tournament Feedback Arc Set with Few Passes	
<i>Anubhav Baweja, Justin Jia, and David P. Woodruff</i>	16:1–16:23
FPT Algorithms for Finding Near-Cliques in c -Closed Graphs	
<i>Balaram Behera, Edin Husić, Shweta Jain, Tim Roughgarden, and C. Seshadhri</i> .	17:1–17:24
What Does Dynamic Optimality Mean in External Memory?	
<i>Michael A. Bender, Martín Farach-Colton, and William Kuszmaul</i>	18:1–18:23
Improved Hardness of BDD and SVP Under Gap-(S)ETH	
<i>Huck Bennett, Chris Peikert, and Yi Tang</i>	19:1–19:12
Mixing of 3-Term Progressions in Quasirandom Groups	
<i>Amey Bhangale, Prahladh Harsha, and Sourya Roy</i>	20:1–20:9
Max-3-Lin over Non-Abelian Groups with Universal Factor Graphs	
<i>Amey Bhangale and Aleksa Stanković</i>	21:1–21:21
Separating the NP-Hardness of the Grothendieck Problem from the Little-Grothendieck Problem	
<i>Vijay Bhattiprolu, Euiwoong Lee, and Madhur Tulsiani</i>	22:1–22:17
Fixed-Parameter Sensitivity Oracles	
<i>Davide Bilò, Katrin Casel, Keerti Choudhary, Sarel Cohen, Tobias Friedrich, J.A. Gregor Lagodzinski, Martin Schirneck, and Simon Wietheger</i>	23:1–23:18
Local Access to Random Walks	
<i>Amartya Shankha Biswas, Edward Pyne, and Ronitt Rubinfeld</i>	24:1–24:22
Vertex Fault-Tolerant Emulators	
<i>Greg Bodwin, Michael Dinitz, and Yasamin Nazari</i>	25:1–25:22
Bounded Indistinguishability for Simple Sources	
<i>Andrej Bogdanov, Krishnamoorthy Dinesh, Yuval Filmus, Yuval Ishai, Avi Kaplan, and Akshayaram Srinivasan</i>	26:1–26:18
Locality-Preserving Hashing for Shifts with Connections to Cryptography	
<i>Elette Boyle, Itai Dinur, Niv Gilboa, Yuval Ishai, Nathan Keller, and Ohad Klein</i>	27:1–27:24
Lattice-Inspired Broadcast Encryption and Succinct Ciphertext-Policy ABE	
<i>Zvika Brakerski and Vinod Vaikuntanathan</i>	28:1–28:20
Local Problems on Trees from the Perspectives of Distributed Algorithms, Finitary Factors, and Descriptive Combinatorics	
<i>Sebastian Brandt, Yi-Jun Chang, Jan Grebík, Christoph Grunau, Václav Rozhoň, and Zoltán Vidnyánszky</i>	29:1–29:26
PCPs and Instance Compression from a Cryptographic Lens	
<i>Liron Bronfman and Ron D. Rothblum</i>	30:1–30:19

Limits of Quantum Speed-Ups for Computational Geometry and Other Problems: Fine-Grained Complexity via Quantum Walks <i>Harry Buhrman, Bruno Loff, Subhasree Patro, and Florian Speelman</i>	31:1–31:12
Small Hazard-Free Transducers <i>Johannes Bund, Christoph Lenzen, and Moti Medina</i>	32:1–32:24
Faster Sparse Matrix Inversion and Rank Computation in Finite Fields <i>Silvia Casacuberta and Rasmus Kyng</i>	33:1–33:24
Algorithms and Lower Bounds for Comparator Circuits from Shrinkage <i>Bruno P. Cavalari and Zhenjian Lu</i>	34:1–34:21
Quantum Distributed Algorithms for Detection of Cliques <i>Keren Censor-Hillel, Orr Fischer, François Le Gall, Dean Leitersdorf, and Rotem Oshman</i>	35:1–35:25
Distributed Vertex Cover Reconfiguration <i>Keren Censor-Hillel, Yannic Maus, Shahar Romem-Peled, and Tigran Tonoyan</i> ..	36:1–36:23
Adversarially Robust Coloring for Graph Streams <i>Amit Chakrabarti, Prantar Ghosh, and Manuel Stoeckl</i>	37:1–37:23
Smaller ACC0 Circuits for Symmetric Functions <i>Brynmor Chapman and R. Ryan Williams</i>	38:1–38:19
Monotone Complexity of Spanning Tree Polynomial Re-Visited <i>Arkadev Chattopadhyay, Rajit Datta, Utsab Ghosal, and Partha Mukhopadhyay</i> ...	39:1–39:21
The Space Complexity of Sampling <i>Eshan Chattopadhyay, Jesse Goodman, and David Zuckerman</i>	40:1–40:23
On the Existence of Competitive Equilibrium with Chores <i>Bhaskar Ray Chaudhury, Jugal Garg, Peter McLaughlin, and Ruta Mehta</i>	41:1–41:13
Individual Fairness in Advertising Auctions Through Inverse Proportionality <i>Shuchi Chawla and Meena Jagadeesan</i>	42:1–42:21
Improved Decoding of Expander Codes <i>Xue Chen, Kuan Cheng, Xin Li, and Minghui Ouyang</i>	43:1–43:3
Cursed yet Satisfied Agents <i>Yiling Chen, Alon Eden, and Juntao Wang</i>	44:1–44:1
Average-Case Hardness of NP and PH from Worst-Case Fine-Grained Assumptions <i>Lijie Chen, Shuichi Hirahara, and Neekon Vafa</i>	45:1–45:16
Symmetric Sparse Boolean Matrix Factorization and Applications <i>Sitan Chen, Zhao Song, Runzhou Tao, and Ruizhe Zhang</i>	46:1–46:25
Quantum Meets the Minimum Circuit Size Problem <i>Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang</i>	47:1–47:16
Larger Corner-Free Sets from Combinatorial Degenerations <i>Matthias Christandl, Omar Fawzi, Hoang Ta, and Jeroen Zuiddam</i>	48:1–48:20
Optimal Deterministic Clock Auctions and Beyond <i>Giorgos Christodoulou, Vasilis Gkatzelis, and Daniel Schoepflin</i>	49:1–49:23

Nonlinear Repair Schemes of Reed-Solomon Codes. <i>Roni Con and Itzhak Tamo</i>	50:1–50:1
A Complete Linear Programming Hierarchy for Linear Codes <i>Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones</i>	51:1–51:22
Lower Bounds for Symmetric Circuits for the Determinant <i>Anuj Dawar and Gregory Wilsenach</i>	52:1–52:22
Convex Influences <i>Anindya De, Shivam Nadimpalli, and Rocco A. Servedio</i>	53:1–53:21
The Importance of the Spectral Gap in Estimating Ground-State Energies <i>Abhinav Deshpande, Alexey V. Gorshkov, and Bill Fefferman</i>	54:1–54:6
Mechanism Design with Moral Bidders <i>Shahar Dobzinski and Sigal Oren</i>	55:1–55:17
Small-Box Cryptography <i>Yevgeniy Dodis, Harish Karthikeyan, and Daniel Wichs</i>	56:1–56:25
Interaction-Preserving Compilers for Secure Computation <i>Nico Döttling, Vipul Goyal, Giulio Malavolta, and Justin Raizes</i>	57:1–57:18
Matroid Secretary Is Equivalent to Contention Resolution <i>Shaddin Dughmi</i>	58:1–58:23
Uniform Brackets, Containers, and Combinatorial Macbeath Regions <i>Kunal Dutta, Arijit Ghosh, and Shay Moran</i>	59:1–59:10
Multiscale Entropic Regularization for MTS on General Metric Spaces <i>Farzam Ebrahimnejad and James R. Lee</i>	60:1–60:21
Counting and Sampling Perfect Matchings in Regular Expanding Non-Bipartite Graphs <i>Farzam Ebrahimnejad, Ansh Nagda, and Shayan Oveis Gharan</i>	61:1–61:12
Embeddings and Labeling Schemes for A^* <i>Talya Eden, Piotr Indyk, and Haike Xu</i>	62:1–62:19
A Unifying Framework for Characterizing and Computing Width Measures <i>Eduard Eiben, Robert Ganian, Thekla Hamm, Lars Jaffke, and O-joung Kwon</i> ...	63:1–63:23
Reduction from Non-Unique Games to Boolean Unique Games <i>Ronen Eldan and Dana Moshkovitz</i>	64:1–64:25
Pseudorandom Self-Reductions for NP-Complete Problems <i>Reyad Abed Elrazik, Robert Robere, Assaf Schuster, and Gal Yehuda</i>	65:1–65:12
Credible, Strategyproof, Optimal, and Bounded Expected-Round Single-Item Auctions for All Distributions <i>Meryem Essaidi, Matheus V. X. Ferreira, and S. Matthew Weinberg</i>	66:1–66:19
Small Circuits Imply Efficient Arthur-Merlin Protocols <i>Michael Ezra and Ron D. Rothblum</i>	67:1–67:16
A Lower Bound on the Space Overhead of Fault-Tolerant Quantum Computation <i>Omar Fawzi, Alexander Müller-Hermes, and Ala Shayeghi</i>	68:1–68:20

On Semi-Algebraic Proofs and Algorithms <i>Noah Fleming, Mika Göös, Stefan Grosser, and Robert Robere</i>	69:1–69:25
Extremely Deep Proofs <i>Noah Fleming, Toniann Pitassi, and Robert Robere</i>	70:1–70:23
On the Download Rate of Homomorphic Secret Sharing <i>Ingerid Fosli, Yuval Ishai, Victor I. Kolobov, and Mary Wootters</i>	71:1–71:22
A Variant of the VC-Dimension with Applications to Depth-3 Circuits <i>Peter Frankl, Svyatoslav Gryaznov, and Navid Talebanfard</i>	72:1–72:19
Continuous Tasks and the Asynchronous Computability Theorem <i>Hugo Rincon Galeana, Sergio Rajsbaum, and Ulrich Schmid</i>	73:1–73:27
Correlation Detection in Trees for Planted Graph Alignment <i>Luca Ganassali, Laurent Massoulié, and Marc Lelarge</i>	74:1–74:8
On Polynomially Many Queries to NP or QMA Oracles <i>Sevag Gharibian and Dorian Rudolph</i>	75:1–75:27
Eliminating Intermediate Measurements Using Pseudorandom Generators <i>Uma Girish and Ran Raz</i>	76:1–76:18
Sample-Based Proofs of Proximity <i>Guy Goldberg and Guy N. Rothblum</i>	77:1–77:19
Testing Distributions of Huge Objects <i>Oded Goldreich and Dana Ron</i>	78:1–78:19
Omnipredictors <i>Parikshit Gopalan, Adam Tauman Kalai, Omer Reingold, Vatsal Sharan, and Udi Wieder</i>	79:1–79:21
Mixing in Non-Quasirandom Groups <i>W. T. Gowers and Emanuele Viola</i>	80:1–80:9
Time-Traveling Simulators Using Blockchains and Their Applications <i>Vipul Goyal, Justin Raizes, and Pratik Soni</i>	81:1–81:19
Online Multivalid Learning: Means, Moments, and Prediction Intervals <i>Varun Gupta, Christopher Jung, Georgy Noarov, Malleesh M. Pai, and Aaron Roth</i>	82:1–82:24
Adaptive Massively Parallel Constant-Round Tree Contraction <i>MohammadTaghi Hajiaghayi, Marina Knittel, Hamed Saleh, and Hsin-Hao Su</i> ...	83:1–83:23
Errorless Versus Error-Prone Average-Case Complexity <i>Shuichi Hirahara and Rahul Santhanam</i>	84:1–84:23
Excluding PH Pessiland <i>Shuichi Hirahara and Rahul Santhanam</i>	85:1–85:25
Nash-Bargaining-Based Models for Matching Markets: One-Sided and Two-Sided; Fisher and Arrow-Debreu <i>Mojtaba Hosseini and Vijay V. Vazirani</i>	86:1–86:20

Symbolic Determinant Identity Testing and Non-Commutative Ranks of Matrix Lie Algebras	
<i>Gábor Ivanyos, Tushant Mittal, and Youming Qiao</i>	87:1–87:21
Explicit Abelian Lifts and Quantum LDPC Codes	
<i>Fernando Granha Jeronimo, Tushant Mittal, Ryan O’Donnell, Pedro Paredes, and Madhur Tulsiani</i>	88:1–88:21
Almost-Orthogonal Bases for Inner Product Polynomials	
<i>Chris Jones and Aaron Potechin</i>	89:1–89:21
Sublinear-Time Computation in the Presence of Online Erasures	
<i>Iden Kalemaj, Sofya Raskhodnikova, and Nithin Varma</i>	90:1–90:25
Noisy Boolean Hidden Matching with Applications	
<i>Michael Kapralov, Amulya Musipatla, Jakab Tardos, David P. Woodruff, and Samson Zhou</i>	91:1–91:19
On Fairness and Stability in Two-Sided Matchings	
<i>Gili Karni, Guy N. Rothblum, and Gal Yona</i>	92:1–92:17
Optimal Bounds for Dominating Set in Graph Streams	
<i>Sanjeev Khanna and Christian Konrad</i>	93:1–93:23
Deterministic Dynamic Matching in Worst-Case Update Time	
<i>Peter Kiss</i>	94:1–94:21
More Dominantly Truthful Multi-Task Peer Prediction with a Finite Number of Tasks	
<i>Yuqing Kong</i>	95:1–95:20
Dynamic Matching Algorithms Under Vertex Updates	
<i>Hung Le, Lazar Milenković, Shay Solomon, and Virginia Vassilevska Williams</i> ...	96:1–96:24
Quantum Meets Fine-Grained Complexity: Sublinear Time Quantum Algorithms for String Problems	
<i>François Le Gall and Saeed Seddighin</i>	97:1–97:23
Optimal Sub-Gaussian Mean Estimation in Very High Dimensions	
<i>Jasper C. H. Lee and Paul Valiant</i>	98:1–98:21
Double Coverage with Machine-Learned Advice	
<i>Alexander Lindermayr, Nicole Megow, and Bertrand Simon</i>	99:1–99:18
Beating Classical Impossibility of Position Verification	
<i>Jiahui Liu, Qipeng Liu, and Luowen Qian</i>	100:1–100:11
A Gaussian Fixed Point Random Walk	
<i>Yang P. Liu, Ashwin Sah, and Mehtaab Sawhney</i>	101:1–101:10
Correlation-Intractable Hash Functions via Shift-Hiding	
<i>Alex Lombardi and Vinod Vaikuntanathan</i>	102:1–102:16
Balanced Allocations with Incomplete Information: The Power of Two Queries	
<i>Dimitrios Los and Thomas Sauerwald</i>	103:1–103:23

Lifting with Sunflowers <i>Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang</i>	104:1–104:24
Interactive Communication in Bilateral Trade <i>Jieming Mao, Renato Paes Leme, and Kangning Wang</i>	105:1–105:21
Support Recovery in Universal One-Bit Compressed Sensing <i>Arya Mazumdar and Soumyabrata Pal</i>	106:1–106:20
Keep That Card in Mind: Card Guessing with Limited Memory <i>Boaz Menuhin and Moni Naor</i>	107:1–107:28
A Spectral Approach to Polytope Diameter <i>Hariharan Narayanan, Rikhav Shah, and Nikhil Srivastava</i>	108:1–108:22
Geometric Bounds on the Fastest Mixing Markov Chain <i>Sam Olesker-Taylor and Luca Zanetti</i>	109:1–109:1
Lower Bounds on Stabilizer Rank <i>Shir Peleg, Ben Lee Volk, and Amir Shpilka</i>	110:1–110:4
Beating the Folklore Algorithm for Dynamic Matching <i>Mohammad Roghani, Amin Saberi, and David Wajc</i>	111:1–111:23
Interactive Proofs for Synthesizing Quantum States and Unitaries <i>Gregory Rosenthal and Henry Yuen</i>	112:1–112:4
Budget-Smoothed Analysis for Submodular Maximization <i>Aviad Rubinfeld and Junyao Zhao</i>	113:1–113:23
Uniform Bounds for Scheduling with Job Size Estimates <i>Ziv Scully, Isaac Grosof, and Michael Mitzenmacher</i>	114:1–114:30
$3 + \epsilon$ Approximation of Tree Edit Distance in Truly Subquadratic Time <i>Masoud Seddighin and Saeed Seddighin</i>	115:1–115:22
On Hardness Assumptions Needed for “Extreme High-End” PRGs and Fast Derandomization <i>Ronen Shaltiel and Emanuele Viola</i>	116:1–116:17
Low-Bandwidth Recovery of Linear Functions of Reed-Solomon-Encoded Data <i>Noah Shetty and Mary Wootters</i>	117:1–117:19
Efficient Reconstruction of Depth Three Arithmetic Circuits with Top Fan-In Two <i>Gaurav Sinha</i>	118:1–118:33
Polynomial Identity Testing via Evaluation of Rational Functions <i>Dieter van Melkebeek and Andrew Morgan</i>	119:1–119:24
Probing to Minimize <i>Weina Wang, Anupam Gupta, and Jalani K. Williams</i>	120:1–120:23

■ Preface

The *13th Innovations in Theoretical Computer Science (ITCS) conference* was hosted by the Simons Institute for the Theory of Computing in Berkeley. It was held from January 31 to February 3, 2022.

This year, the conference received a record 246 submissions, of which 120 were selected for presentation at the conference. The submission pool was extremely strong, and the committee felt that we had to increase the number of accepted papers to accommodate the growth in the quantity and quality of the submissions. In keeping the tradition of holding the conference as a single-track event, we increased the overall length of the program to four days.

The organizers are grateful to Google Inc. for its sponsorship of the conference. Its financial support allowed us to defray costs and thereby reduce registration costs.

The program committee awarded the Best Student Paper Award to two papers: “*Deterministic dynamic matching in worst-case update time*” by Peter Kiss, and “*A Gaussian fixed point random walk*” by Yang P. Liu, Ashwin Sah, and Mehtaab Sawhney.

The bulk of the reviewing work has been carried out by the program committee and the external reviewers. The program committee consisted of a record 58 members (in addition to the chair): Maryam Aliakbarpour (Boston University/Northeastern University); Josh Alman (Columbia University); Hagit Attiya (Technion); Omri Ben-Eliezer (MIT); Aditya Bhaskara (University of Utah); Guy Bresler (MIT); Yang Cai (Yale University); Lijie Chen (MIT); Xue Chen (George Mason University); Ken Clarkson (IBM Research); Anindya De (University of Pennsylvania); Mahsa Derakhshan (Princeton University); Talya Eden (MIT and Boston University); Kousha Etessami (University of Edinburgh); Yuval Filmus (Technion); Paul Goldberg (Oxford University); Kira Goldner (Boston University); Elena Grigorescu (Purdue University); Alex Bredariol Grilo (CNRS and Sorbonne Université); Justin Holmgren (NTT Research); Karthik C. S. (Rutgers University); Antonina Kolokolova (Memorial University of Newfoundland); Lap Chi Lau (University of Waterloo); François Le Gall (Nagoya University); Jasper Lee (University of Wisconsin-Madison); Frederic Magniez (CNRS Paris); Pasin Manurangsi (Google Research); Ruta Mehta (UIUC); Jamie Morgenstern (University of Washington); Guy Moshkovitz (CUNY); Igor Oliveira (University of Warwick); Rafael Oliveira (University of Waterloo); Rotem Oshman (Tel-Aviv University); Renato Paes Leme (Google Research); Rafael Pass (Cornell University); Sofya Raskhodnikova (Boston University); Dana Ron (Tel-Aviv University); Noga Ron-Zewi (University of Haifa); Benjamin Rossman (Duke University); Alexander Russell (University of Connecticut); Rahul Santhanam (Oxford University); Nitin Saxena (IIT Kanpur); Raghuvansh Saxena (Microsoft Research); Ariel Schwartzman (DIMACS); Max Simchowitz (UC Berkeley); Makrand Sinha (Simons Institute and UC Berkeley); Adam Smith (Boston University); Thomas Steinke (Google Research); Kunal Talwar (Apple); Dave Touchette (Université de Sherbrooke); Paul Valiant (Purdue University); Nicole Wein (DIMACS); Daniel Wichs (Northeastern University and NTT Research); James Worrell (Oxford University); Steven Wu (Carnegie Mellon University); Eylon Yogev (Bar-Ilan University); Peilin Zhong (Google Research); Standa Zivny (Oxford University).

I am grateful to the program committee and the external reviewers for the hard work of reviewing the papers in a short time-frame. I am grateful to the ITCS steering committee Executive Steering Committee executive (Irit Dinur, Oded Goldreich, Shafi Goldwasser, Ueli Maurer, Eva Tardos, and Thomas Vidick), and especially its chair Ronitt Rubinfeld, for

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman



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


their advice and support as we navigated another year of covid-related uncertainty. I am grateful to the staff of the Simons Institute, Peter Bartlett, Ashley Hasson, Drew Mason, and Quelani Penland; and Joanne Hanley from MIT, for the administrative support in organizing a remote conference.

Mark Braverman
ITCS'22 Program Committee Chair
Princeton University
Princeton, NJ, USA

■ List of Authors


Divesh Aggarwal (2)
National University of Singapore, Singapore

Gagan Aggarwal (1)
Google Research, Mountain View, CA, USA

Shyan Akmal  (3)
MIT, EECS and CSAIL, Cambridge, MA, USA

Prabhanjan Ananth (4)
University of California Santa Barbara, CA, USA

Nima Anari (5)
Stanford University, CA, USA


Anurag Anshu  (6)
Simons Institute for the Theory of Computing, Berkeley, California, USA; Challenge Institute for Quantum Computation, University of California, Berkeley, CA, USA; Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA

Shiri Antaki (7)
Tel Aviv University, Tel Aviv, Israel


Benny Applebaum (8)
Tel-Aviv University, Tel-Aviv, Israel

Sepehr Assadi (9, 10)
Department of Computer Science, Rutgers University, Piscataway, NJ, USA

Yakov Babichenko (11)
Technion - Israel Institute of Technology, Haifa, Israel

Marshall Ball  (12)
Computer Science Department, Columbia University, New York, NY, USA

Nikhil Bansal (13)
University of Michigan, Ann Arbor, MI, USA

Boaz Barak  (14)
Harvard University, Cambridge, MA, USA

James Bartusek (15)
University of California, Berkeley, CA, USA

Anubhav Baweja (16)
Carnegie Mellon University, Pittsburgh, PA, USA

Balaram Behera (17)
Georgia Institute of Technology, Atlanta, GA, USA

Amos Beimel (8)
Ben-Gurion University, Be'er-Sheva, Israel


Michael A. Bender (18)
Stony Brook University, Stony Brook, NY, USA

Huck Bennett (19)
Oregon State University, Corvallis, OR, USA

Amev Bhangale (20, 21)
University of California, Riverside, CA, USA

Vijay Bhattiprolu (22)
Institute for Advanced Study, Princeton, NJ, USA; Princeton University, NJ, USA

Kshipra Bhawalkar (1)
Google Research, Mountain View, CA, USA

Davide Bilò  (23)
Department of Humanities and Social Sciences, University of Sassari, Italy


Amartya Shankha Biswas (24)
CSAIL, MIT, Cambridge, MA, USA

Greg Bodwin (25)
University of Michigan, Ann Arbor, MI, USA

Andrej Bogdanov (26)
Department of Computer Science and Engineering and Institute of Theoretical Computer Science and Communications, The Chinese University of Hong Kong, Hong Kong


Elette Boyle (27)
IDC Herzliya, Israel; NTT Research, Sunnyvale, USA

Zvika Brakerski (28)
Weizmann Institute of Science, Rehovot, Israel

Sebastian Brandt  (29)
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

Liron Bronfman (30)
Technion, Haifa, Israel

Harry Buhrman (31)
QuSoft, CWI Amsterdam, The Netherlands; University of Amsterdam, The Netherlands

Johannes Bund  (32)
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

Sílvia Casacuberta (33)
Harvard University, Cambridge, MA, USA

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman



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

- Katrin Casel  (23)
Hasso Plattner Institute, University of Potsdam,
Germany
- Bruno P. Cavalari  (34)
University of Warwick, Coventry, UK
- Keren Censor-Hillel  (35, 36)
Technion, Haifa, Israel
- Amit Chakrabarti  (37)
Department of Computer Science, Dartmouth
College, Hanover, NH, USA
- Yi-Jun Chang  (29)
National University of Singapore, Singapore
- Brynmor Chapman (38)
Department of Electrical Engineering and
Computer Science, MIT, Cambridge, MA, USA
- Arkadev Chattopadhyay (39)
TIFR, Mumbai, India
- Eshan Chattopadhyay (40)
Cornell University, Ithaca, NY, USA
- Bhaskar Ray Chaudhury (41)
University of Illinois at Urbana Champaign, IL,
USA
- Shuchi Chawla (42)
The University of Texas at Austin, TX, USA
- Lijie Chen (3, 45)
MIT, EECS and CSAIL, Cambridge, MA, USA
- Sitan Chen (46)
University of California, Berkeley, CA, USA
- Xue Chen (43)
University of Science and Technology of China,
Anhui, China
- Yiling Chen (44)
School of Engineering and Applied Science,
Harvard University, Boston, MA, US
- Kuan Cheng (43)
Peking University, China
- Nai-Hui Chia (47)
Luddy School of Informatics, Computing, and
Engineering, Indiana University, Bloomington,
IN, USA
- Chi-Ning Chou (47)
School of Engineering and Applied Sciences,
Harvard University, Boston, MA, USA
- Keerti Choudhary  (23)
Department of Computer Science and
Engineering, Indian Institute of Technology
Delhi, India
- Matthias Christandl (48)
Department of Mathematical Sciences,
University of Copenhagen, Denmark
- Giorgos Christodoulou (49)
University of Liverpool, UK
- Sarel Cohen  (23)
School of Computer Science, Tel-Aviv-Yaffo
Academic College, Israel
- Roni Con (50)
Department of Computer Science, Tel Aviv
University, Israel
- Leonardo Nagami Coreglio (51)
Institute for Advanced Study, Princeton, NJ,
USA
- Rajit Datta (39)
Goldman-Sachs, Bangalore, India
- Anuj Dawar  (52)
Department of Computer Science and
Technology, University of Cambridge, UK
- Anindya De (53)
University of Pennsylvania, Philadelphia, PA,
USA
- Michał Dereziński (5)
University of Michigan, Ann Arbor, MI, USA
- Abhinav Deshpande  (54)
Joint Center for Quantum Information and
Computer Science and Joint Quantum Institute,
NIST/University of Maryland, College Park,
MD, USA; Institute for Quantum Information
and Matter, California Institute of Technology,
Pasadena, CA, USA
- Krishnamoorthy Dinesh (26)
Institute of Theoretical Computer Science and
Communications, The Chinese University of
Hong Kong, Hong Kong
- Michael Dinitz (25)
Johns Hopkins University, Baltimore, MD,
United States
- Itai Dinur (27)
Ben-Gurion University, Be'er Sheva, Israel
- Shahar Dobzinski (55)
Weizmann Institute of Science, Rehovot, Israel

- Yevgeniy Dodis (56)
New York University, NY, USA
- Shaddin Dughmi  (58)
Department of Computer Science, University of Southern California, Los Angeles, CA, USA
- Jesko Dujmovic (2)
Helmholtz Center for Information Security (CISPA), Saarbrücken, Germany; Saarland University, Saarbrücken, Germany
- Kunal Dutta  (59)
Department of Informatics, University of Warsaw, Poland
- Nico Döttling  (2, 57)
Helmholtz Center for Information Security (CISPA), Saarbrücken, Germany
- Farzam Ebrahimejad (60, 61)
University of Washington, Seattle, WA, USA
- Alon Eden (44)
School of Engineering and Applied Science, Harvard University, Boston, MA, US
- Talya Eden (62)
Massachusetts Institute of Technology, Cambridge, MA, USA; Boston University, MA, USA
- Eduard Eiben  (63)
Department of Computer Science, Royal Holloway, University of London, Egham, UK
- Ronen Eldan (64)
Department of Mathematics, Weizmann Institute of Science, Rehovot, Israel
- Reyad Abed Elrazik (65)
Taub Faculty of Computer Science, Technion, Haifa, Israel
- Meryem Essaidi (66)
Computer Science, Princeton University, NJ, USA
- Michael Ezra (67)
Department of Computer Science, Technion, Haifa, Israel
- Martín Farach-Colton (18)
Rutgers University, New Brunswick, NJ, USA
- Omar Fawzi (48, 68)
Univ. Lyon, ENS Lyon, UCBL, CNRS, Inria, LIP, France
- Bill Fefferman  (54)
Department of Computer Science, University of Chicago, IL, USA
- Matheus V. X. Ferreira (66)
Computer Science, Harvard University, MA, USA
- Yuval Filmus (26)
The Henry and Marylin Taub Faculty of Computer Science, Technion, Haifa, Israel
- Orr Fischer (35)
Tel-Aviv University, Israel
- Noah Fleming (69, 70)
University of California, San Diego, CA, USA; Memorial University, St. John's, Canada
- Ingerid Fosli (71)
Google, Houston, TX, USA
- Peter Frankl (72)
Rényi Institute, Budapest, Hungary
- Tobias Friedrich  (23)
Hasso Plattner Institute, University of Potsdam, Germany
- Hugo Rincon Galeana  (73)
Embedded Computing Systems Group TU Wien, Austria
- Luca Ganassali (74)
Inria, DI/ENS, PSL Research University, Paris, France
- Robert Ganian  (63)
Algorithms and Complexity Group, TU Wien, Austria
- Jugal Garg (41)
University of Illinois at Urbana Champaign, IL, USA
- Shayan Oveis Gharan (61)
University of Washington, Seattle, WA, USA
- Sevag Gharibian  (75)
Department of Computer Science and Institute for Photonic Quantum Systems (PhoQS), Paderborn University, Germany
- Utsab Ghosal (39)
Chennai Mathematical Institute, India
- Arijit Ghosh (59)
Indian Statistical Institute, Kolkata, India
- Prantar Ghosh (37)
Department of Computer Science, Dartmouth College, Hanover, NH, USA
- Niv Gilboa (27)
Ben-Gurion University, Be'er Sheva, Israel

- Uma Girish (76)
Princeton University, Princeton, NJ, USA
- Vasilis Gkatzelis (49)
Drexel University, Philadelphia, PA, USA
- Guy Goldberg  (77)
Weizmann Institute of Science, Rehovot, Israel
- Oded Goldreich  (12, 78)
Faculty of Mathematics and Computer Science,
Weizmann Institute of Science, Rehovot, Israel
- Jesse Goodman (40)
Cornell University, Ithaca, NY, USA
- Parikshit Gopalan  (79)
VMware Research, Palo Alto, California, USA
- Alexey V. Gorshkov  (54)
Joint Center for Quantum Information and
Computer Science and Joint Quantum Institute,
NIST/University of Maryland, College Park,
MD, USA
- W. T. Gowers (80)
Collège de France, Paris, France
- Vipul Goyal (57, 81)
Carnegie Mellon University, Pittsburgh, PA,
USA; NTT Research, Sunnyvale, CA, USA
- Jan Grebík (29)
University of Warwick, Coventry, UK
- Isaac Grosf  (114)
Computer Science Department, Carnegie Mellon
University, Pittsburgh, PA, USA
- Stefan Grosser (69)
McGill University, Montreal, Canada
- Christoph Grunau (29)
ETH Zürich, Switzerland
- Svyatoslav Gryaznov  (72)
Institute of Mathematics of the Czech Academy
of Sciences, Prague, Czech Republic; St.
Petersburg Department of V.A. Steklov Institute
of Mathematics of the Russian Academy of
Sciences, Russia
- Anupam Gupta (120)
Computer Science Department, Carnegie Mellon
University, Pittsburgh, PA, USA
- Varun Gupta (82)
University of Pennsylvania, Philadelphia, PA,
USA
- Guru Guruganesh (1)
Google Research, Mountain View, CA, USA
- Mika Göös (69)
EPFL, Lausanne, Switzerland
- Mohammad Hajiabadi (2)
University of Waterloo, ON, Canada
- MohammadTaghi Hajiaghayi (83)
University of Maryland, College Park, MD, USA
- Thekla Hamm  (63)
Algorithms and Complexity Group, TU Wien,
Austria
- Prahladh Harsha  (20)
Tata Institute of Fundamental Research,
Mumbai, India
- Shuichi Hirahara (45, 84, 85)
National Institute of Informatics, Tokyo, Japan
- Mojtaba Hosseini  (86)
The Paul Merage School of Business, University
of California, Irvine, CA, USA
- Edin Husić  (17)
London School of Economics and Political
Science, UK
- Piotr Indyk (62)
Massachusetts Institute of Technology,
Cambridge, MA, USA
- Yuval Ishai (26, 27, 71)
The Henry and Marilyn Taub Faculty of
Computer Science, Technion, Haifa, Israel
- Gábor Ivanyos  (87)
Institute for Computer Science and Control,
Eötvös Loránd Research Network (ELKH),
Budapest, Hungary
- Lars Jaffke  (63)
Department of Informatics, University of Bergen,
Norway
- Meena Jagadeesan (42)
University of California, Berkeley, CA, USA
- Abhishek Jain (4)
Johns Hopkins University, Baltimore, MD, USA
- Shweta Jain (17)
University of Illinois, Urbana-Champaign, IL,
USA
- Fernando Granha Jeronimo (51, 88)
Institute for Advanced Study, Princeton, NJ,
USA

- Justin Jia (16)
Carnegie Mellon University, Pittsburgh, PA, USA
- Haotian Jiang (13)
University of Washington, Seattle, WA, USA
- Ce Jin (3)
MIT, EECS and CSAIL, Cambridge, MA, USA
- Zhengzhong Jin (4)
Johns Hopkins University, Baltimore, MD, USA
- Chris Jones (51, 89)
University of Chicago, IL, USA
- Christopher Jung (82)
University of Pennsylvania, Philadelphia, PA, USA
- Adam Tauman Kalai (79)
Microsoft Research, Boston, MA, USA
- Iden Kalemaj  (90)
Department of Computer Science, Boston University, MA, USA
- Avi Kaplan (26)
The Henry and Marylin Taub Faculty of Computer Science, Technion, Haifa, Israel
- Michael Kapralov (91)
EPFL, Lausanne, Switzerland
- Gili Karni (92)
Weizmann Institute of Science, Rehovot, Israel
- Harish Karthikeyan (56)
New York University, NY, USA
- Nathan Keller (27)
Bar-Ilan University, Ramat Gan, Israel
- Sanjeev Khanna (93)
Department of Computer and Information Science, University of Pennsylvania, Philadelphia, PA, US
- Peter Kiss (94)
Department of Computer Science, University of Warwick, Coventry, UK
- Ohad Klein (27)
Bar-Ilan University, Ramat Gan, Israel
- Marina Knittel (83)
University of Maryland, College Park, MD, USA
- Victor I. Kolobov (71)
Technion, Haifa, Israel
- Yuqing Kong  (95)
The Center on Frontiers of Computing Studies, Peking University, Beijing, China
- Christian Konrad  (93)
Department of Computer Science, University of Bristol, UK
- William Kuszmaul (18)
MIT, Cambridge, MA, USA
- O-joung Kwon  (63)
Department of Mathematics, Incheon National University, South Korea; Discrete Mathematics Group, Institute for Basic Science, Daejeon, South Korea
- Rasmus Kyng (33)
ETH Zürich, Switzerland
- J.A. Gregor Lagodzinski  (23)
Hasso Plattner Institute, University of Potsdam, Germany
- François Le Gall (35, 97)
Nagoya University, Aichi, Japan
- Hung Le (96)
University of Massachusetts, Amherst, MA, USA
- Euiwoong Lee (22)
University of Michigan, Ann-Arbor, USA
- James R. Lee (60)
University of Washington, Seattle, WA, USA
- Jasper C.H. Lee (98)
University of Wisconsin-Madison, WI, USA
- Dean Leitersdorf (35)
Technion, Haifa, Israel
- Marc Lelarge (74)
Inria, DI/ENS, PSL Research University, Paris, France
- Christoph Lenzen (32)
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
- Xin Li (43)
Johns Hopkins University, Baltimore, MD, USA
- Alexander Lindermayr  (99)
Faculty of Mathematics and Computer Science, University of Bremen, Germany
- Jiahui Liu (100)
Department of Computer Science, University of Texas at Austin, TX, USA


- Qipeng Liu (100)
Simons Institute for the Theory of Computing,
Berkeley, CA, USA
- Quanquan C. Liu (7)
Massachusetts Institute of Technology,
Cambridge, MA, USA
- Yang P. Liu (101)
Department of Mathematics, Stanford
University, Stanford, CA, USA
- Bruno Loff (31)
University of Porto, Portugal; INESC-Tec,
Porto, Portugal
- Alex Lombardi (102)
Massachusetts Institute of Technology,
Cambridge, MA, USA
- Dimitrios Los (103)
Department of Computer Science & Technology,
University of Cambridge, UK
- Shachar Lovett (104)
Department of Computer Science, University of
California San Diego, CA, USA
- Zhenjian Lu (34)
University of Warwick, Coventry, UK
- Giulio Malavolta (2, 4, 15, 57)
Max Planck Institute for Security and Privacy,
Bochum, Germany
- Tal Malkin (12)
Computer Science Department, Columbia
University, New York, NY, USA
- Jieming Mao (105)
Google Research, New York, NY, USA
- Kunal Marwaha  (14)
Berkeley Center for Quantum Information and
Computation, Berkeley, CA, USA
- Laurent Massoulié (74)
MSR-Inria Joint Centre, Inria, DI/ENS, PSL
Research University, Paris, France
- Yannic Maus  (36)
Institute of Software Technology, TU Graz,
Austria
- Arya Mazumdar (106)
Halicioğlu Data Science Institute, University of
California, San Diego, CA, USA
- Peter McLaughlin (41)
University of Illinois at Urbana Champaign, IL,
USA
- Moti Medina  (32)
Faculty of Engineering, Bar-Ilan University,
Ramat Gan, Israel
- Nicole Megow  (99)
Faculty of Mathematics and Computer Science,
University of Bremen, Germany
- Ruta Mehta (41)
University of Illinois at Urbana Champaign, IL,
USA
- Raghu Meka (13, 104)
University of California, Los Angeles, CA, USA
- Boaz Menuhin (107)
Department of Computer Science and Applied
Mathematics, Weizmann Institute of Science,
Rehovot, Israel
- Ian Mertz (104)
Department of Computer Science, University of
Toronto, Canada
- Lazar Milenković (96)
Tel Aviv University, Israel
- Tushant Mittal  (87, 88)
Department of Computer Science, University of
Chicago, IL, USA
- Michael Mitzenmacher  (114)
School of Engineering and Applied Sciences,
Harvard University, Cambridge, MA, USA
- Shay Moran  (59)
Technion – Israel Institute of Technology, Haifa,
Israel; Google Research, Tel Aviv, Israel
- Andrew Morgan (119)
University of Wisconsin-Madison, Madison, WI,
USA
- Dana Moshkovitz (64)
Department of Computer Science, University of
Texas at Austin, TX, USA
- Partha Mukhopadhyay (39)
Chennai Mathematical Institute, India
- Amulya Musipatla (91)
Carnegie Mellon University, Pittsburgh, PA,
USA
- Alexander Müller-Hermes (68)
Institut Camille Jordan, Université Claude
Bernard Lyon 1, 69622 Villeurbanne cedex,
France; Department of Mathematics, University
of Oslo, Norway
- Guy N. Rothblum  (77)
Weizmann Institute of Science, Rehovot, Israel

- Shivam Nadimpalli (53)
Columbia University, New York, NY, USA
- Ansh Nagda (61)
University of Washington, Seattle, WA, USA
- Moni Naor (107)
Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel
- Hariharan Narayanan (108)
Tata Institute of Fundamental Research, Mumbai, India
- Yasamin Nazari (25)
University of Salzburg, Austria
- Oded Nir (8)
Tel-Aviv University, Tel-Aviv, Israel
- Chinmay Nirkhe  (6)
Challenge Institute for Quantum Computation, University of California, Berkeley, CA, USA; Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA
- Georgy Noarov (82)
University of Pennsylvania, Philadelphia, PA, USA
- Ryan O'Donnell (88)
Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA
- Maciej Obremski (2)
National University of Singapore, Singapore
- Sam Olesker-Taylor (109)
University of Bath, UK
- Sigal Oren  (55)
Ben-Gurion University of the Negev, Beer-Sheva, Israel
- Rotem Oshman (35)
Tel-Aviv University, Israel
- Minghui Ouyang (43)
Peking University, China
- Renato Paes Leme (105)
Google Research, New York, NY, USA
- Mallesh M. Pai (82)
Rice University, Houston, TX, USA
- Soumyabrata Pal  (106)
College of Information and Computer Sciences, University of Massachusetts Amherst, MA, USA
- Pedro Paredes (88)
Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, USA
- Subhasree Patro (31)
QuSoft, CWI Amsterdam, The Netherlands; University of Amsterdam, The Netherlands
- Chris Peikert (19)
University of Michigan, Ann Arbor, MI, USA
- Shir Peleg  (110)
Tel Aviv University, Israel
- Andres Perlroth (1)
Google Research, Mountain View, CA, USA
- Naty Peter (8)
Tel-Aviv University, Tel-Aviv, Israel
- Toniann Pitassi (8, 70, 104)
University of Toronto, Toronto, Canada; Columbia University, New York, NY, USA
- Aaron Potechin (89)
University of Chicago, IL, USA
- Edward Pyne (24)
Harvard University, Cambridge, MA, USA
- Luowen Qian (100)
Department of Computer Science, Boston University, MA, USA
- Youming Qiao  (87)
Centre for Quantum Software and Information, University of Technology Sydney, Australia
- Justin Raizes (57, 81)
Carnegie Mellon University, Pittsburgh, PA, USA
- Malvika Raj (3)
University of California Berkeley, CA, USA
- Sergio Rajsbaum  (73)
UNAM, Instituto de Matemáticas, Mexico City, Mexico
- Sofya Raskhodnikova  (90)
Department of Computer Science, Boston University, MA, USA
- Ran Raz (76)
Princeton University, Princeton, NJ, USA
- Omer Reingold (79)
Stanford University, CA, USA
- Robert Robere (65, 69, 70)
School of Computer Science, McGill University, Montreal, Canada

- Mohammad Roghani (111)
Stanford University, CA, USA;
roghani@stanford.edu
- Shahar Romem-Peled (36)
Department of Computer Science, Technion,
Haifa, Israel
- Dana Ron  (78)
School of Electrical Engineering, Tel Aviv
University, Israel
- Gregory Rosenthal  (112)
Department of Computer Science, University of
Toronto, Canada
- Aaron Roth (82)
University of Pennsylvania, Philadelphia, PA,
USA
- Guy N. Rothblum (92)
Weizmann Institute of Science, Rehovot, Israel
- Ron D. Rothblum (30, 67)
Technion, Haifa, Israel
- Tim Roughgarden (17)
Columbia University, New York, NY, USA
- Sourya Roy (20)
University of California, Riverside, CA, USA
- Václav Rozhoň  (29)
ETH Zürich, Switzerland
- Ronitt Rubinfeld (24)
CSAIL, MIT, Cambridge, MA, USA
- Aviad Rubinfeld (113)
Computer Science Department, Stanford
University, CA, USA
- Dorian Rudolph  (75)
Department of Computer Science and Institute
for Photonic Quantum Systems (PhoQS),
Paderborn University, Germany
- Amin Saberi (111)
Stanford University, CA, USA;
saberi@stanford.edu
- Ashwin Sah (101)
Department of Mathematics, Massachusetts
Institute of Technology, Cambridge, MA, USA
- Hamed Saleh (83)
University of Maryland, College Park, MD, USA
- Rahul Santhanam (84, 85)
Department of Computer Science, University of
Oxford, UK
- Thomas Sauerwald  (103)
Department of Computer Science & Technology,
University of Cambridge, UK
- Mehtaab Sawhney (101)
Department of Mathematics, Massachusetts
Institute of Technology, Cambridge, MA, USA
- Martin Schirneck (23)
Hasso Plattner Institute, University of Potsdam,
Germany
- Ulrich Schmid  (73)
Embedded Computing Systems Group TU Wien,
Austria
- Daniel Schoepflin (49)
Drexel University, Philadelphia, PA, USA
- Assaf Schuster (65)
Taub Faculty of Computer Science, Technion,
Haifa, Israel
- Ziv Scully  (114)
Computer Science Department, Carnegie Mellon
University, Pittsburgh, PA, USA
- Masoud Seddighin (115)
Institute for Research in Fundamental Sciences
(IPM), School of Computer Science, Tehran,
Iran
- Saeed Seddighin (97, 115)
Toyota Technological Institute at Chicago, IL,
USA
- Rocco A. Servedio (53)
Columbia University, New York, NY, USA
- C. Seshadhri (17)
University of California, Santa Cruz, CA, USA
- Rikhav Shah (108)
University of California Berkeley, CA, USA
- Vihan Shah (9)
Department of Computer Science, Rutgers
University, Piscataway, NJ, USA
- Ronen Shaltiel (116)
Department of computer science, University of
Haifa, Israel
- Vatsal Sharan (79)
University of Southern California, Los Angeles,
CA, USA
- Ala Shayeghi (68)
Univ Lyon, ENS Lyon, UCBL, CNRS, Inria,
LIP, F-69342, Lyon Cedex 07, France

- Amir Shpilka  (110)
Tel Aviv University, Israel
- Noah Shutty (117)
Stanford University, CA, USA
- Bertrand Simon  (99)
IN2P3 Computing Center, CNRS, Villeurbanne, France
- Sahil Singla (13)
Georgia Institute of Technology, Atlanta, GA, USA
- Gaurav Sinha (118)
Adobe Research, Bangalore, India
- Makrand Sinha (13)
Simons Institute, Berkeley, CA, USA; University of California, Berkeley, CA, USA
- Shay Solomon (7, 96)
Tel Aviv University, Tel Aviv, Israel
- Zhao Song (46)
Adobe Research, Seattle, WA, USA
- Pratik Soni (81)
Carnegie Mellon University, Pittsburgh, PA, USA
- Florian Speelman (31)
QuSoft, CWI Amsterdam, The Netherlands; University of Amsterdam, The Netherlands
- Akshayaram Srinivasan (26)
School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India
- Nikhil Srivastava (108)
University of California Berkeley, CA, USA
- Aleksa Stanković  (21)
Department of Mathematics, KTH Royal Institute of Technology, Sweden
- Manuel Stoeckl  (37)
Department of Computer Science, Dartmouth College, Hanover, NH, USA
- Hsin-Hao Su (83)
Boston College, MA, USA
- Hoang Ta (48)
Univ. Lyon, ENS Lyon, UCBL, CNRS, Inria, LIP, France
- Navid Talebanfard  (72)
Institute of Mathematics of the Czech Academy of Sciences, Prague, Czech Republic
- Inbal Talgam-Cohen (11)
Technion - Israel Institute of Technology, Haifa, Israel
- Itzhak Tamo (50)
Department of Electrical Engineering-Systems, Tel Aviv University, Israel
- Yi Tang (19)
University of Michigan, Ann Arbor, MI, USA
- Runzhou Tao (46)
Columbia University, New York, NY, USA
- Jakab Tardos (91)
EPFL, Lausanne, Switzerland
- Tigran Tonoyan  (36)
Department of Computer Science, Technion, Haifa, Israel
- Madhur Tulsiani (22, 88)
Toyota Technological Institute Chicago, IL, USA
- Neekon Vafa (45)
MIT, Boston, MA, USA
- Vinod Vaikuntanathan (28, 102)
MIT, Boston, USA
- Paul Valiant (98)
Purdue University, West Lafayette, IN, USA
- Dieter van Melkebeek (119)
University of Wisconsin-Madison, Madison, WI, USA
- Nithin Varma  (90)
Chennai Mathematical Institute, India
- Virginia Vassilevska Williams (96)
MIT, Cambridge, MA, USA
- Vijay V. Vazirani  (86)
Computer Science Department, University of California, Irvine, CA, USA
- Zoltán Vidnyánszky  (29)
California Institute of Technology, Pasadena, CA, USA
- Emanuele Viola (80, 116)
Khoury College of Computer Sciences, Northeastern University, Boston, MA, USA
- Ben Lee Volk  (110)
Reichman University, Herzliya, Israel
- Thuy-Duong Vuong (5)
Stanford University, CA, USA

David Wajc (111)
Stanford University, CA, USA;
wajc@stanford.edu

Chen Wang  (10)
Department of Computer Science, Rutgers
University, Piscataway, NJ, USA

Juntao Wang (44)
School of Engineering and Applied Science,
Harvard University, Boston, MA, US


Kangning Wang (105)
Duke University, Durham, NC, USA

Weina Wang (120)
Computer Science Department, Carnegie Mellon
University, Pittsburgh, PA, USA

S. Matthew Weinberg (66)
Computer Science, Princeton University, NJ,
USA

Daniel Wicks (56)
Northeastern University, Boston, MA, USA;
NTT Research, Sunnyvale, CA, USA

Udi Wieder (79)
VMware Research, Palo Alto, California, USA

Simon Wietheger  (23)
Hasso Plattner Institute, University of Potsdam,
Germany

Jalani K. Williams (120)
Computer Science Department, Carnegie Mellon
University, Pittsburgh, PA, USA

R. Ryan Williams (38)
Department of Electrical Engineering and
Computer Science, MIT, Cambridge, MA, USA

Ryan Williams (3)
MIT, EECS and CSAIL, Cambridge, MA, USA

Gregory Wilsenach (52)
Department of Computer Science and
Technology, University of Cambridge, UK

David P. Woodruff (16, 91)
Carnegie Mellon University, Pittsburgh, PA,
USA

Mary Wootters (71, 117)
Stanford University, CA, USA


Haifeng Xu (11)
University of Virginia, Charlottesville, VA, USA

Haike Xu (62)
Tsinghua University, Beijing, China

Elizabeth Yang (5)
UC Berkeley, CA, USA

Gal Yehuda (65)
Taub Faculty of Computer Science, Technion,
Haifa, Israel

Gal Yona (92)
Weizmann Institute of Science, Rehovot, Israel

Henry Yuen  (112)
Department of Computer Science, Columbia
University, New York, NY, USA

Konstantin Zabarnyi (11)
Technion - Israel Institute of Technology, Haifa,
Israel

Luca Zanetti (109)
University of Bath, UK

Jiapeng Zhang (104)
Department of Computer Science, University of
Southern California, Los Angeles, CA, USA

Jiayu Zhang (47)
Department of Computer Science, Boston
University, MA, USA; Computing and
Mathematical Sciences, California Institute and
Technology, Pasadena, CA, USA

Ruizhe Zhang (46, 47)
University of Texas at Austin, TX, USA

Junyao Zhao (113)
Computer Science Department, Stanford
University, CA, USA

Samson Zhou  (91)
Carnegie Mellon University, Pittsburgh, PA,
USA

David Zuckerman (40)
University of Texas at Austin, TX, USA

Jeroen Zuiddam (48)
Korteweg-de Vries Institute for Mathematics,
University of Amsterdam, The Netherlands