

# 11th Innovations in Theoretical Computer Science Conference

ITCS 2020, January 12–14, 2020, Seattle, Washington, USA

Edited by

Thomas Vidick



*Editors*

**Thomas Vidick**

California Institute of Technology, Pasadena, CA, USA  
vidick@caltech.edu

*ACM Classification 2012*

Mathematics of computing; Theory of computation

**ISBN 978-3-95977-134-4**

PRINT ISBN: 978-1-7138-0347-8

*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/978-3-95977-134-4>.

*Publication date*

January, 2020

*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 3.0 Unported license (CC-BY 3.0):  
<https://creativecommons.org/licenses/by/3.0/legalcode>.



In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work under the following conditions, without impairing or restricting the authors' moral rights:

- Attribution: The work must be attributed to its authors.

The copyright is retained by the corresponding authors.

Digital Object Identifier: 10.4230/LIPIcs.ITCS.2020.0

ISBN 978-3-95977-134-4

ISSN 1868-8969

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

## ■ Contents

Preface	
<i>Thomas Vidick</i> .....	0:xi
ITCS 2020 Conference Organization	
.....	0:xiii–0:xvi

### Regular Papers

Hardness Amplification of Optimization Problems	
<i>Elazar Goldenberg and Karthik C. S.</i> .....	1:1–1:13
Smooth and Strong PCPs	
<i>Orr Paradise</i> .....	2:1–2:41
Approximately Strategyproof Tournament Rules: On Large Manipulating Sets and Cover-Consistence	
<i>Ariel Schwartzman, S. Matthew Weinberg, Eitan Zlatin, and Albert Zuo</i> .....	3:1–3:25
Span Programs and Quantum Space Complexity	
<i>Stacey Jeffery</i> .....	4:1–4:37
DEEP-FRI: Sampling Outside the Box Improves Soundness	
<i>Eli Ben-Sasson, Lior Goldberg, Swastik Kopparty, and Shubhangi Saraf</i> .....	5:1–5:32
On the Cryptographic Hardness of Local Search	
<i>Nir Bitansky and Idan Gerichter</i> .....	6:1–6:29
Interactive Coding with Constant Round and Communication Blowup	
<i>Klim Efremenko, Elad Haramaty, and Yael Tauman Kalai</i> .....	7:1–7:34
From Independent Sets and Vertex Colorings to Isotropic Spaces and Isotropic Decompositions: Another Bridge Between Graphs and Alternating Matrix Spaces	
<i>Xiaohui Bei, Shiteng Chen, Ji Guan, Youming Qiao, and Xiaoming Sun</i> .....	8:1–8:48
Hard Properties with (Very) Short PCPPs and Their Applications	
<i>Omri Ben-Eliezer, Eldar Fischer, Amit Levi, and Ron D. Rothblum</i> .....	9:1–9:27
Kronecker Powers of Tensors and Strassen’s Laser Method	
<i>Austin Conner, Joseph M. Landsberg, Fulvio Gesmundo, and Emanuele Ventura</i> .	10:1–10:28
Algorithms and Lower Bounds for Cycles and Walks: Small Space and Sparse Graphs	
<i>Andrea Lincoln and Nikhil Vyas</i> .....	11:1–11:17
High-Dimensional Expanders from Expanders	
<i>Siqi Liu, Sidhanth Mohanty, and Elizabeth Yang</i> .....	12:1–12:32
Approximating Cumulative Pebbling Cost Is Unique Games Hard	
<i>Jeremiah Blocki, Seunghoon Lee, and Samson Zhou</i> .....	13:1–13:27
Scheduling with Predictions and the Price of Misprediction	
<i>Michael Mitzenmacher</i> .....	14:1–14:18

11th Innovations in Theoretical Computer Science Conference (ITCS 2020).  
Editor: Thomas Vidick



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

Reducing Inefficiency in Carbon Auctions with Imperfect Competition <i>Kira Goldner, Nicole Immorlica, and Brendan Lucier</i> .....	15:1–15:21
Preference-Informed Fairness <i>Michael P. Kim, Aleksandra Korolova, Guy N. Rothblum, and Gal Yona</i> .....	16:1–16:23
On a Theorem of Lovász that $\text{hom}(\cdot, H)$ Determines the Isomorphism Type of $H$ <i>Jin-Yi Cai and Artem Govorov</i> .....	17:1–17:15
Tarski’s Theorem, Supermodular Games, and the Complexity of Equilibria <i>Kousha Etessami, Christos Papadimitriou, Aviad Rubinfeld, and Mihalis Yannakakis</i> .....	18:1–18:19
Resolution with Counting: Dag-Like Lower Bounds and Different Moduli <i>Fedor Part and Iddo Tzameret</i> .....	19:1–19:37
The Random-Query Model and the Memory-Bounded Coupon Collector <i>Ran Raz and Wei Zhan</i> .....	20:1–20:11
Strategy-Stealing Is Non-Constructive <i>Greg Bodwin and Ofer Grossman</i> .....	21:1–21:12
Distribution-Free Testing of Linear Functions on $\mathbb{R}^n$ <i>Noah Fleming and Yuichi Yoshida</i> .....	22:1–22:19
Random Sketching, Clustering, and Short-Term Memory in Spiking Neural Networks <i>Yael Hitron, Nancy Lynch, Cameron Musco, and Merav Parter</i> .....	23:1–23:31
Signed Tropical Convexity <i>Georg Loho and László A. Végh</i> .....	24:1–24:35
Distributional Property Testing in a Quantum World <i>András Gilyén and Tongyang Li</i> .....	25:1–25:19
On Local Testability in the Non-Signaling Setting <i>Alessandro Chiesa, Peter Manohar, and Igor Shinkar</i> .....	26:1–26:37
Local Access to Huge Random Objects Through Partial Sampling <i>Amartya Shankha Biswas, Ronitt Rubinfeld, and Anak Yodpinyanee</i> .....	27:1–27:65
Monotone Probability Distributions over the Boolean Cube Can Be Learned with Sublinear Samples <i>Ronitt Rubinfeld and Arsen Vasilyan</i> .....	28:1–28:34
Sample Complexity Bounds for Influence Maximization <i>Gal Sadeh, Edith Cohen, and Haim Kaplan</i> .....	29:1–29:36
On Oblivious Amplification of Coin-Tossing Protocols <i>Nir Bitansky and Nathan Geier</i> .....	30:1–30:13
A New Analysis of Differential Privacy’s Generalization Guarantees <i>Christopher Jung, Katrina Ligett, Seth Neel, Aaron Roth, Saeed Sharifi-Malvajerdi, and Moshe Shenfeld</i> .....	31:1–31:17
Robust Algorithms for the Secretary Problem <i>Domagoj Bradac, Anupam Gupta, Sahil Singla, and Goran Zuzic</i> .....	32:1–32:26

Universal Communication, Universal Graphs, and Graph Labeling <i>Nathaniel Harms</i> .....	33:1–33:27
Approaching MCSP from Above and Below: Hardness for a Conditional Variant and $AC^0[p]$ <i>Rahul Ilango</i> .....	34:1–34:26
Equivalence of Systematic Linear Data Structures and Matrix Rigidity <i>Sivaramkrishnan Natarajan Ramamoorthy and Cyrus Rashtchian</i> .....	35:1–35:20
Computationally Data-Independent Memory Hard Functions <i>Mohammad Hassan Ameri, Jeremiah Blocki, and Samson Zhou</i> .....	36:1–36:28
Learning and Testing Variable Partitions <i>Andrej Bogdanov and Baoxiang Wang</i> .....	37:1–37:22
Linear Time Subgraph Counting, Graph Degeneracy, and the Chasm at Size Six <i>Suman K. Bera, Noujan Pashanasangi, and C. Seshadhri</i> .....	38:1–38:20
Parameterization Above a Multiplicative Guarantee <i>Fedor V. Fomin, Petr A. Golovach, Daniel Lokshantov, Fahad Panolan, Saket Saurabh, and Meirav Zehavi</i> .....	39:1–39:13
Ad Hoc Multi-Input Functional Encryption <i>Shweta Agrawal, Michael Clear, Ophir Frieder, Sanjam Garg, Adam O’Neill, and Justin Thaler</i> .....	40:1–40:41
Unexpected Power of Random Strings <i>Shuichi Hirahara</i> .....	41:1–41:13
Consensus vs Broadcast, with and Without Noise <i>Andrea Clementi, Luciano Gualà, Emanuele Natale, Francesco Pasquale, Giacomo Scornavacca, and Luca Trevisan</i> .....	42:1–42:13
Testing Linear Inequalities of Subgraph Statistics <i>Lior Gishboliner, Asaf Shapira, and Henrique Stagni</i> .....	43:1–43:9
Top-Down Induction of Decision Trees: Rigorous Guarantees and Inherent Limitations <i>Guy Blanc, Jane Lange, and Li-Yang Tan</i> .....	44:1–44:44
Algorithms and Adaptivity Gaps for Stochastic $k$ -TSP <i>Haotian Jiang, Jian Li, Daogao Liu, and Sahil Singla</i> .....	45:1–45:25
Strategic Payments in Financial Networks <i>Nils Bertschinger, Martin Hoefer, and Daniel Schmand</i> .....	46:1–46:16
Fault Tolerant Subgraphs with Applications in Kernelization <i>William Lochet, Daniel Lokshantov, Pranabendu Misra, Saket Saurabh, Roohani Sharma, and Meirav Zehavi</i> .....	47:1–47:22
The Computational Cost of Asynchronous Neural Communication <i>Yael Hitron, Merav Parter, and Gur Perri</i> .....	48:1–48:47
Certified Algorithms: Worst-Case Analysis and Beyond <i>Konstantin Makarychev and Yury Makarychev</i> .....	49:1–49:14

Low Diameter Graph Decompositions by Approximate Distance Computation <i>Ruben Becker, Yuval Emek, and Christoph Lenzen</i> .....	50:1–50:29
Generalized List Decoding <i>Yihan Zhang, Amitalok J. Budkuley, and Sidharth Jaggi</i> .....	51:1–51:83
Online Computation with Untrusted Advice <i>Spyros Angelopoulos, Christoph Dürr, Shendan Jin, Shahin Kamali, and Marc Renault</i> .....	52:1–52:15
Monochromatic Triangles, Intermediate Matrix Products, and Convolutions <i>Andrea Lincoln, Adam Polak, and Virginia Vassilevska Williams</i> .....	53:1–53:18
Matching Is as Easy as the Decision Problem, in the NC Model <i>Nima Anari and Vijay V. Vazirani</i> .....	54:1–54:25
Advancing Subgroup Fairness via Sleeping Experts <i>Avrim Blum and Thodoris Lykouris</i> .....	55:1–55:24
Instance Complexity and Unlabeled Certificates in the Decision Tree Model <i>Tomer Grossman, Ilan Komargodski, and Moni Naor</i> .....	56:1–56:38
On the Impossibility of Probabilistic Proofs in Relativized Worlds <i>Alessandro Chiesa and Siqi Liu</i> .....	57:1–57:30
Lower Bounds for (Non-Monotone) Comparator Circuits <i>Anna Gál and Robert Robere</i> .....	58:1–58:13
A Tight Lower Bound For Non-Coherent Index Erasure <i>Nathan Lindzey and Ansis Rosmanis</i> .....	59:1–59:37
Optimal Single-Choice Prophet Inequalities from Samples <i>Aviad Rubinfeld, Jack Z. Wang, and S. Matthew Weinberg</i> .....	60:1–60:10
Implementation in Advised Strategies: Welfare Guarantees from Posted-Price Mechanisms When Demand Queries Are NP-Hard <i>Linda Cai, Clay Thomas, and S. Matthew Weinberg</i> .....	61:1–61:32
Toward a General Complexity Theory of Motion Planning: Characterizing Which Gadgets Make Games Hard <i>Erik D. Demaine, Dylan H. Hendrickson, and Jayson Lynch</i> .....	62:1–62:42
Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality <i>Adam Bouland, Bill Fefferman, and Umesh Vazirani</i> .....	63:1–63:2
New Query Lower Bounds for Submodular Function Minimization <i>Andrei Graur, Tristan Pollner, Vidhya Ramaswamy, and S. Matthew Weinberg</i> ...	64:1–64:16
Computation-Aware Data Aggregation <i>Bernhard Haeupler, D. Ellis Hershkowitz, Anson Kahng, and Ariel D. Procaccia</i> .	65:1–65:38
Convertible Codes: New Class of Codes for Efficient Conversion of Coded Data in Distributed Storage <i>Francisco Maturana and K. V. Rashmi</i> .....	66:1–66:26

Incentive Compatible Active Learning <i>Federico Echenique and Siddharth Prasad</i> .....	67:1–67:20
Pseudorandomness and the Minimum Circuit Size Problem <i>Rahul Santhanam</i> .....	68:1–68:26
Testing Properties of Multiple Distributions with Few Samples <i>Maryam Aliakbarpour and Sandeep Silwal</i> .....	69:1–69:41
Beyond Natural Proofs: Hardness Magnification and Locality <i>Lijie Chen, Shuichi Hirahara, Igor C. Oliveira, Ján Pich, Ninad Rajgopal, and Rahul Santhanam</i> .....	70:1–70:48
Separating Two-Round Secure Computation from Oblivious Transfer <i>Benny Applebaum, Zvika Brakerski, Sanjam Garg, Yuval Ishai, and Akshayaram Srinivasan</i> .....	71:1–71:18
Trade-Offs Between Size and Degree in Polynomial Calculus <i>Guillaume Lagarde, Jakob Nordström, Dmitry Sokolov, and Joseph Swernofsky</i> ...	72:1–72:16
Smoothed Efficient Algorithms and Reductions for Network Coordination Games <i>Shant Boodaghians, Rucha Kulkarni, and Ruta Mehta</i> .....	73:1–73:15
Local-To-Global Agreement Expansion via the Variance Method <i>Tali Kaufman and David Mass</i> .....	74:1–74:14
MPC for MPC: Secure Computation on a Massively Parallel Computing Architecture <i>T-H. Hubert Chan, Kai-Min Chung, Wei-Kai Lin, and Elaine Shi</i> .....	75:1–75:52
Choice and Bias in Random Walks <i>Agelos Georgakopoulos, John Haslegrave, Thomas Sauerwald, and John Sylvester</i> .	76:1–76:19
Graph Spanners in the Message-Passing Model <i>Manuel Fernández V, David P. Woodruff, and Taisuke Yasuda</i> .....	77:1–77:18
Computational Hardness of Certifying Bounds on Constrained PCA Problems <i>Afonso S. Bandeira, Dmitriy Kunisky, and Alexander S. Wein</i> .....	78:1–78:29
Pseudo-Deterministic Streaming <i>Shafi Goldwasser, Ofer Grossman, Sidhanth Mohanty, and David P. Woodruff</i> ...	79:1–79:25
Limits to Non-Malleability <i>Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin</i> .....	80:1–80:32
Cryptography from Information Loss <i>Marshall Ball, Elette Boyle, Akshay Degwekar, Apoorvaa Deshpande, Alon Rosen, Vinod Vaikuntanathan, and Prashant Nalini Vasudevan</i> .....	81:1–81:27
Affine Determinant Programs: A Framework for Obfuscation and Witness Encryption <i>James Bartusek, Yuval Ishai, Aayush Jain, Fermi Ma, Amit Sahai, and Mark Zhandry</i> .....	82:1–82:39
OV Graphs Are (Probably) Hard Instances <i>Josh Alman and Virginia Vassilevska Williams</i> .....	83:1–83:18

**0:x**      **Contents**

Finding Skewed Subcubes Under a Distribution <i>Parikshit Gopalan, Roie Levin, and Udi Wieder</i> .....	84:1–84:30
Combinatorial Lower Bounds for 3-Query LDCs <i>Arnab Bhattacharyya, L. Sunil Chandran, and Suprovat Ghoshal</i> .....	85:1–85:8
On the Complexity of Decomposable Randomized Encodings, Or: How Friendly Can a Garbling-Friendly PRF Be? <i>Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, and Tal Malkin</i> .....	86:1–86:22