2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS 2016)

New Brunswick, New Jersey, USA
9 – 11 October 2016

IEEE Catalog Number:	CFP16053-POD
ISBN:	978-1-5090-3934-0

Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16053-POD
ISBN (Print-On-Demand):	978-1-5090-3934-0
ISBN (Online):	978-1-5090-3933-3
ISSN:	1523-8288

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2016 IEEE 57th Annual Symposium on Foundations of Computer Science

FOCS 2016

Table of Contents

Preface.....xiii

Organizing Committee and Sponsors.....xiv

Program Committee.....xv

External Reviewers.....xvi

Awards.....xix

Session 1.1A

Bounded-Communication Leakage Resilience via Parity-Resilient Circuits 1
Vipul Goyal, Yuval Ishai, Hemanta K. Maji, Amit Sahai, and Alexander A. Sherstov

Indistinguishability Obfuscation from DDH-Like Assumptions
on Constant-Degree Graded Encodings 11
Huijia Lin and Vinod Vaikuntanathan

Breaking the Three Round Barrier for Non-malleable Commitments 21
Vipul Goyal, Dakshita Khurana, and Amit Sahai

Zero-Knowledge Proof Systems for QMA 31
Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous

Session 1.1B

Strong Fooling Sets for Multi-player Communication with Applications
to Deterministic Estimation of Stream Statistics 41
Amit Chakrabarti and Sagar Kale

Edit Distance: Sketching, Streaming, and Document Exchange 51
Djamal Belazzougui and Qin Zhang

Heavy Hitters via Cluster-Preserving Clustering 61
Kasper Green Larsen, Jelani Nelson, Huy L. Nguyễn, and Mikkel Thorup

Optimal Quantile Approximation in Streams 71
Zohar Karnin, Kevin Lang, and Edo Liberty

Session 1.2A

An Average-Case Depth Hierarchy Theorem for Higher Depth 79
Johan Håstad

A Better-Than-3n Lower Bound for the Circuit Complexity of an Explicit Function 89
Magnus Gausdal Find, Alexander Golovnev, Edward A. Hirsch, and Alexander S. Kulikov

Depth-Reduction for Composites 99
Shiteng Chen and Periklis A. Papakonstantinou

A Deterministic Polynomial Time Algorithm for Non-commutative Rational Identity Testing 109
Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson

Session 1.2B

The Salesman's Improved Paths: A 3/2+1/34 Approximation 118
András Sebo and Anke Van Zuylen

Hopsets with Constant Hopbound, and Applications to Approximate Shortest Paths 128
Michael Elkin and Ofer Neiman

Better Unrelated Machine Scheduling for Weighted Completion Time via Random Offsets from Non-uniform Distributions 138
Sungjin Im and Shi Li

Online Algorithms for Covering and Packing Problems with Convex Objectives 148
Yossi Azar, Niv Buchbinder, T-H. Hubert Chan, Shahar Chen, Ilan Reuven Cohen, Anupam Gupta, Zhiyi Huang, Ning Kang, Viswanath Nagarajan, Joseph (Seffi) Naor, and Debmalya Panigrahi

Session 1.3A

Explicit Non-malleable Extractors, Multi-source Extractors, and Almost Optimal Privacy Amplification Protocols 158
Eshan Chattopadhyay and Xin Li

Improved Two-Source Extractors, and Affine Extractors for Polylogarithmic Entropy 168
Xin Li

Extractors for Near Logarithmic Min-Entropy 178
Gil Cohen and Leonard J. Schulman

Making the Most of Advice: New Correlation Breakers and Their Applications 188
Gil Cohen

The Hilbert Function, Algebraic Extractors, and Recursive Fourier Sampling 197
Zachary Remscrim

Session 1.3B

Computational Efficiency Requires Simple Taxation 209
Shahar Dobzinski

Learning in Auctions: Regret is Hard, Envy is Easy 219
Constantinos Daskalakis and Vasilis Syrgkanis

On the Communication Complexity of Approximate Fixed Points 229
Tim Roughgarden and Omri Weinstein

Informational Substitutes 239
Yiling Chen and Bo Waggoner

Constrained Submodular Maximization: Beyond 1/e 248
Alina Ene and Huy L. Nguyễn

Session 1.4 Best Papers

Settling the Complexity of Computing Approximate Two-Player Nash Equilibria 258
Aviad Rubinstein

Fast Learning Requires Good Memory: A Time-Space Lower Bound for Parity
Learning 266
Ran Raz

Ramanujan Graphs in Polynomial Time 276
Michael B. Cohen

Session 2.1A

Structure of Protocols for XOR Functions 282
Hamed Hatami, Kaave Hosseini, and Shachar Lovett

The Multiparty Communication Complexity of Interleaved Group Products 289
W.T. Gowers and Emanuele Viola

How Limited Interaction Hinders Real Communication (and What It Means
for Proof and Circuit Complexity) 295
Susanna F. de Rezende, Jakob Nordström, and Marc Vinyals

Amortized Dynamic Cell-Probe Lower Bounds from Four-Party
Communication 305
Omri Weinstein and Huacheng Yu

Session 2.1B

Decremental Single-Source Reachability and Strongly Connected Components in $\tilde{O}(m\sqrt{n})$ Total Update Time 315
Shiri Chechik, Thomas Dueholm Hansen, Giuseppe F. Italiano, Jakub Łącki, and Nikos Parotsidis

Fully Dynamic Maximal Matching in Constant Update Time 325
Shay Solomon

On Fully Dynamic Graph Sparsifiers 335
Ittai Abraham, David Durfee, Ioannis Koutis, Sebastian Krinninger, and Richard Peng

Linear Hashing Is Awesome 345
Mathias Bæk Tejs Knudsen

Session 2.2

Local Search Yields Approximation Schemes for k-Means and k-Median in Euclidean and Minor-Free Metrics 353
Vincent Cohen-Addad, Philip N. Klein, and Claire Mathieu

Local Search Yields a PTAS for k-Means in Doubling Metrics 365
Zachary Friggstad, Mohsen Rezapour, and Mohammad R. Salavatipour

Truly Sub-cubic Algorithms for Language Edit Distance and RNA-Folding via Fast Bounded-Difference Min-Plus Product 375
Karl Bringmann, Fabrizio Grandoni, Barna Saha, and Virginia Vassilevska Williams

Session 2.3

Knuth Prize Lecture: Complexity of Communication in Markets 385
Noam Nisan

Session 2.4

No Occurrence Obstructions in Geometric Complexity Theory 386
Peter Bürgisser, Christian Ikenmeyer, and Greta Panova

Rectangular Kronecker Coefficients and Plethysms in Geometric Complexity Theory 396
Christian Ikenmeyer and Greta Panova

Exponential Lower Bounds for Monotone Span Programs 406
Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A. Cook

A Discrete and Bounded Envy-Free Cake Cutting Protocol for Any Number of Agents 416
Haris Aziz and Simon Mackenzie

Session 2.5A

A Nearly Tight Sum-of-Squares Lower Bound for the Planted Clique Problem 428
Boaz Barak, Samuel B. Hopkins, Jonathan Kelner, Pravesh Kothari, Ankur Moitra, and Aaron Potechin

Polynomial-Time Tensor Decompositions with Sum-of-Squares 438
Tengyu Ma, Jonathan Shi, and David Steurer

Towards Strong Reverse Minkowski-Type Inequalities for Lattices 447
Daniel Dadush and Oded Regev

Session 2.5B

Which Regular Expression Patterns Are Hard to Match? 457
Arturs Backurs and Piotr Indyk

Polynomial Representations of Threshold Functions and Algorithmic Applications 467
Josh Alman, Timothy M. Chan, and Ryan Williams

Popular Conjectures as a Barrier for Dynamic Planar Graph Algorithms 477
Amir Abboud and Søren Dahlgaard

Session 2.6A

Max-Information, Differential Privacy, and Post-selection Hypothesis Testing 487
Ryan Rogers, Aaron Roth, Adam Smith, and Om Thakkar

Lipschitz Extensions for Node-Private Graph Statistics and the Generalized Exponential Mechanism 495
Sofya Raskhodnikova and Adam Smith

Session 2.6B

The Constant Inapproximability of the Parameterized Dominating Set Problem 505
Yijia Chen and Bingkai Lin

Subexponential Parameterized Algorithms for Planar and Apex-Minor-Free Graphs via Low Treewidth Pattern Covering 515
Fedor V. Fomin, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michał Pilipczuk, and Saket Saurabh

Testing Assignments to Constraint Satisfaction Problems 525
Hubie Chen, Matt Valeriote, and Yuichi Yoshida

Session 3.1A

Compressing Interactive Communication under Product Distributions 535
Alexander A. Sherstov

Decidability of Non-interactive Simulation of Joint Distributions 545
Badih Ghazi, Pritish Kamath, and Madhu Sudan

Separations in Communication Complexity Using Cheat Sheets
and Information Complexity 555
*Anurag Anshu, Aleksandrs Belovs, Shalev Ben-David, Mika Göös, Rahul Jain,
Robin Kothari, Troy Lee, and Miklos Santha*

Extension Complexity of Independent Set Polytopes 565
Mika Göös, Rahul Jain, and Thomas Watson

Session 3.1B

Approximate Gaussian Elimination for Laplacians - Fast, Sparse, and Simple 573
Rasmus Kyng and Sushant Sachdeva

Faster Algorithms for Computing the Stationary Distribution, Simulating
Random Walks, and More 583
*Michael B. Cohen, Jonathan Kelner, John Peebles, Richard Peng,
Aaron Sidford, and Adrian Vladu*

Computing Maximum Flow with Augmenting Electrical Flows 593
Aleksander Madry

Optimizing Star-Convex Functions 603
Jasper C.H. Lee and Paul Valiant

Session 3.2A

An Exponential Separation between Randomized and Deterministic
Complexity in the LOCAL Model 615
Yi-Jun Chang, Tsvi Kopelowitz, and Seth Pettie

Local Conflict Coloring 625
Pierre Fraigniaud, Marc Heinrich, and Adrian Kosowski

A Fast and Simple Unbiased Estimator for Network (Un)reliability 635
David R. Karger

A New Framework for Distributed Submodular Maximization 645
Rafael Da Ponte Barbosa, Alina Ene, Huy L. Nguyễn, and Justin Ward

Session 3.2B

Robust Estimators in High Dimensions without the Computational Intractability 655
Ilias Diakonikolas, Gautam Kamath, Daniel M. Kane, Jerry Li, Ankur Moitra, and Alistair Stewart

Agnostic Estimation of Mean and Covariance 665
Kevin A. Lai, Anup B. Rao, and Santosh Vempala

Noisy Population Recovery in Polynomial Time 675
Anindya De, Michael Saks, and Sijian Tang

A New Approach for Testing Properties of Discrete Distributions 685
Ilias Diakonikolas and Daniel M. Kane

Session 3.3A

How to Determine if a Random Graph with a Fixed Degree Sequence Has a Giant Component 695
Felix Joos, Guillem Perarnau, Dieter Rautenbach, and Bruce Reed

Convergence of MCMC and Loopy BP in the Tree Uniqueness Region for the Hard-Core Model 704
Charilaos Efthymiou, Thomas P. Hayes, Daniel Štefankovic, Eric Vigoda, and Yitong Yin

Simulated Quantum Annealing Can Be Exponentially Faster Than Classical Simulated Annealing 714
Elizabeth Crosson and Aram W. Harrow

The Number of Solutions for Random Regular NAE-SAT 724
Allan Sly, Nike Sun, and Yumeng Zhang

Session 3.3B

Accelerated Newton Iteration for Roots of Black Box Polynomials 732
Anand Louis and Santosh S. Vempala

Fourier-Sparse Interpolation without a Frequency Gap 741
Xue Chen, Daniel M. Kane, Eric Price, and Zhao Song

Robust Fourier and Polynomial Curve Fitting 751
Venkatesan Guruswami and David Zuckerman

NP-Hardness of Reed-Solomon Decoding and the Prouhet-Tarry-Escott Problem 760
Venkata Gandikota, Badih Ghazi, and Elena Grigorescu

Session 3.4A

Amplification and Derandomization without Slowdown ...770
Ofer Grossman and Dana Moshkovitz

Commutativity in the Algorithmic Lovász Local Lemma ...780
Vladimir Kolmogorov

An Algorithm for Komlós Conjecture Matching Banaszczyk's Bound ...788
Nikhil Bansal, Daniel Dadush, and Shashwat Garg

Session 3.4B

Universal Simulation of Directed Systems in the Abstract Tile Assembly Model Requires Undirectedness ...800
Jacob Hendricks, Matthew J. Patitz, and Trent A. Rogers

A PTAS for the Steiner Forest Problem in Doubling Metrics ...810
T-H. Hubert Chan, Shuguang Hu, and Shaofeng H.-C. Jiang

On Approximating Maximum Independent Set of Rectangles ...820
Julia Chuzhoy and Alina Ene

Author Index ...830