

Proceedings of the

48th Annual IEEE Symposium on Foundations of Computer Science

October 20-23, 2007, Providence, Rhode Island



Los Alamitos, California

Washington • Tokyo



Foundations of Computer Science

FOCS 2007

TABLE OF CONTENTS

Foreword
Conference Organization
Reviewers

TUTORIAL 1

CHAIR: LUCA TREVISAN

Structure and Randomness in Combinatorics 1
Terence Tao

TUTORIAL 2

CHAIR: DANIELE MICCIANCIO

A Brief Look at Pairings Based Cryptography..... 14
Dan Boneh

TUTORIAL 3

CHAIR: ALISTAIR SINCLAIR

Spectral Graph Theory and its Applications 22
Daniel A. Spielman

SESSION 1

CHAIR: ADAM KLIVANS

Pseudorandom Bits for Polynomials 32
Andrej Bogdanov, Emanuele Viola

Extractors and Rank Extractors for Polynomial Sources..... 43
Zeev Dvir, Ariel Gabizon, Avi Wigderson

Polylogarithmic Independence Can Fool DNF Formulas..... 54
Louay M.J. Bazzi

Derandomization of Sparse Cyclotomic Integer Zero Testing 65
Qi Cheng

SESSION 2

CHAIR: KAMAL JAIN

Computing Equilibria in Anonymous Games	72
<i>Constantinos Daskalakis, Christos Papadimitriou</i>	
Mechanism Design via Differential Privacy.....	83
<i>Frank McSherry, Kunal Talwar</i>	
Balloon Popping With Applications to Ascending Auctions.....	93
<i>Nicole Immorlica, Anna R. Karlin, Mohammad Mahdian, Kunal Talwar</i>	
On the Complexity of Nash Equilibria and Other Fixed Points (Extended Abstract)	102
<i>Kousha Etessami, Mihalis Yannakakis</i>	
Paths Beyond Local Search: A Tight Bound for Randomized Fixed-Point Computation	113
<i>Xi Chen, Shang-Hua Teng</i>	

SESSION 3

CHAIR: T.S. JAYRAM

Exponential Time/Space Speedups for Resolution and the PSPACE-completeness of Black-White Pebbling.....	124
<i>Philipp Hertel, Toniann Pitassi</i>	
Parameterized Proof Complexity.....	137
<i>Stefan Dantchev, Barnaby Martin, Stefan Szeider</i>	
Non-linear Index Coding Outperforming the Linear Optimum.....	148
<i>Eyal Lubetzky, Uri Stav</i>	
Can you beat treewidth?	156
<i>Daniel Marx</i>	

SESSION 4

CHAIR: ALISTAIR SINCLAIR

Adaptive Simulated Annealing: A Near-optimal Connection between Sampling and Counting	167
<i>Daniel Stefankovic, Santosh Vempala, Eric Vigoda</i>	
Reconstruction for Models on Random Graphs.....	178
<i>Antoine Gerschenfeld, Andrea Montanari</i>	
Mixing Time Power Laws at Criticality.....	189
<i>Yun Long, Asaf Nachmias, Yuval Peres</i>	
Near Optimal Bounds for Collision in Pollard Rho for Discrete Log	199
<i>Jeong Han Kim, Ravi Montenegro, Prasad Tetali</i>	

SESSION 5

CHAIR: DANIELE MICCIANCIO

Intrusion-Resilient Secret Sharing	208
<i>Stefan Dziembowski, Krzysztof Pietrzak</i>	
Covert Multi-party Computation	219
<i>Nishanth Chandran, Vipul Goyal, Rafail Ostrovsky, Amit Sahai</i>	
Cryptography from Sunspots: How to Use an Imperfect Reference String.....	230
<i>Ran Canetti, Rafael Pass, Abhi Shelat</i>	

SESSION 6

CHAIR: PIOTR INDYK

Planning for Fast Connectivity Updates	241
<i>Mihai Patrascu, Mikkel Thorup</i>	
Strongly History-Independent Hashing with Applications	250
<i>Guy E. Blelloch, Daniel Golovin</i>	
Smooth Histograms for Sliding Windows	261
<i>Vladimir Braverman, Rafail Ostrovsky</i>	
Lower Bounds on Streaming Algorithms for Approximating the Length of the Longest Increasing Subsequence.....	272
<i>Anna Gal, Parikshit Gopalan</i>	

SESSION 7

CHAIR: JAMES LEE

Towards Sharp Inapproximability For Any 2-CSP	283
<i>Per Austrin</i>	
Linear Equations Modulo 2 and the L1 Diameter of Convex Bodies	294
<i>Subhash Khot, Assaf Naor</i>	
Inapproximability Results for Sparsest Cut, Optimal Linear Arrangement, and Precedence Constrained Scheduling	305
<i>Christoph Ambuhl, Monaldo Mastrolilli, Ola Svensson</i>	
On the Optimality of Planar and Geometric Approximation Schemes.....	314
<i>Daniel Marx</i>	
Hardness of Reconstructing Multivariate Polynomials over Finite Fields.....	325
<i>Parikshit Gopalan, Subhash Khot, Rishi Saket</i>	

SESSION 8

CHAIR: ALEXANDER RAZBOROV

Any AND-OR Formula of Size N Can be Evaluated in Time $N^{1/2+o(1)}$ on a Quantum Computer	336
<i>Andris Ambainis, Andrew M. Childs, Ben W. Reichardt, Shengyu Zhang</i>	
The Power of Quantum Systems on a Line	346
<i>Dorit Aharonov, Daniel Gottesmant, Sandy Iran, Julia Kempe</i>	

Simulating Quantum Correlations with Finite Communication	357
<i>Oded Regev, Ben Toner</i>	
Quantum Algorithms for Hidden Nonlinear Structures	368
<i>Andrew M. Childs, Leonard J. Schulman, Umesh V. Vazirani</i>	

SESSION 9

CHAIR: CHRIS UMANS

Refuting Smoothed 3CNF Formulas	378
<i>Uriel Feige</i>	
Hardness Amplification for Errorless Heuristics.....	389
<i>Andrej Bogdanov, Muli Safra</i>	
One-way Multi-party Communication Lower Bound for Pointer Jumping with Applications.....	398
<i>Emanuele Viola, Avi Wigderson</i>	
A Lower Bound for the Size of Syntactically Multilinear Arithmetic Circuits	409
<i>Ran Raz, Amir Shpilka, Amir Yehudayoff</i>	
Discrepancy and the Power of Bottom Fan-in in Depth-three Circuits	420
<i>Arkadev Chattopadhyay</i>	

SESSION 10

CHAIR: JULIA CHUZHUY

Maximizing Non-monotone Submodular Functions.....	430
<i>Uriel Feige, Vahab S. Mirrokni, Jan Vondrak</i>	
On the Hardness and Smoothed Complexity of Quasi-Concave Minimization	441
<i>Jonathan A. Kelner, Evdokia Nikolova</i>	
Approximation Algorithms for Partial-information based Stochastic Control with Markovian Rewards	452
<i>Sudipto Guha, Kamesh Munagala</i>	
Beating Simplex for Fractional Packing and Covering Linear Programs	463
<i>Christos Koufogiannakis, Neal E. Young</i>	

SESSION 11

CHAIR: ROBERT KLEINBERG

A Primal-Dual Randomized Algorithm for Weighted Paging.....	474
<i>Nikhil Bansal, Niv Buchbinder, Joseph Naor</i>	
Finding Disjoint Paths in Expanders Deterministically and Online.....	485
<i>Noga Alon, Michael Capalbo</i>	
Almost Tight Bound for the Union of Fat Tetrahedra in Three Dimensions	492
<i>Esther Ezra, Micha Sharir</i>	
Inferring Local Homology from Sampled Stratified Spaces	503
<i>Paul Bendich, David Cohen-Steiner, Herbert Edelsbrunner, John Harer, Dmitriy Morozov</i>	

SESSION 12

CHAIR: LUCA TREVISAN

Testing for Concise Representations	514
<i>Ilias Diakonikolas, Homin K. Lee, Kevin Matulef, Krzysztof Onak, Ronitt Rubinfeld, Rocco A. Servedio, Andrew Wan</i>	
Strong Lower Bounds for Approximating Distribution Support Size and the Distinct Elements Problem	524
<i>Sofya Raskhodnikova, Dana Ron, Amir Shpilka, Adam Smith</i>	
Testing Expansion in Bounded-Degree Graphs	535
<i>Artur Czumaj, Christian Sohler</i>	
Approximate Hypergraph Partitioning and Applications.....	544
<i>Eldar Fischer, Arie Matsliah, Asaf Shapira</i>	
Sparse Random Linear Codes are Locally Decodable and Testable	555
<i>Tali Kaufman, Madhu Sudan</i>	

SESSION 13

CHAIR: JULIA CHUZHAY

Minimizing Average Flow-time : Upper and Lower Bounds	566
<i>Naveen Garg, Amit Kumar</i>	
Non-Preemptive Min-Sum Scheduling with Resource Augmentation.....	577
<i>Nikhil Bansal, Ho-Leung Chan, Rohit Khandekar, Kirk Pruhs, Baruch Schieber, Cliff Stein</i>	
On the Advantage over Random for Maximum Acyclic Subgraph	588
<i>Moses Charikar, Konstantin Makarychev, Yury Makarychev</i>	
Buy-at-Bulk Network Design with Protection	597
<i>Spyridon Antonakopoulos, Chandra Chekuri, Bruce Shepherd, Lisa Zhang</i>	

SESSION 14

CHAIR: ANNA LYSYANSKAYA

Space-Efficient Identity Based Encryption Without Pairings.....	608
<i>Dan Boneh, Craig Gentry, Michael Hamburg</i>	
Round Complexity of Authenticated Broadcast with a Dishonest Majority	619
<i>Juan A. Garay, Jonathan Katz, Chiu-Yuen Koo, Rafail Ostrovsky</i>	
Finding Collisions in Interactive Protocols – A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments.....	630
<i>Iftach Haitner, Jonathan J. Hoch, Omer Reingold, Gil Segev</i>	
Lower Bounds on Signatures From Symmetric Primitives	641
<i>Boaz Barak, Mohammad Mahmoody-Ghidary</i>	
Approximation Algorithms Using Hierarchies of Semidefinite Programming Relaxations	650
<i>Eden Chlamtac</i>	
Integrality Gaps of 2 - $\epsilon(1)$ for Vertex Cover SDPs in the Lovasz-Schrijver Hierarchy.....	661
<i>Konstantinos Georgiou, Avner Magen, Toniann Pitassi, Iannis Tzoulakis</i>	

Local Global Tradeoffs in Metric Embeddings 672
Moses Charikar, Konstantin Makarychev, Yury Makarychev

The Computational Hardness of Estimating Edit Distance 683
Alexandr Andoni, Robert Krauthgamer

Author Index