

2008 49th Annual Symposium on Foundations of Computer Science

(FOCS 2008)

**Philadelphia, Pennsylvania
25-28 October 2008**



IEEE Catalog Number: CFP08053-PRT
ISBN: 978-1-4244-3248-6

2008 49th Annual IEEE Symposium on Foundations of Computer Science

FOCS 2008

Table of Contents

Foreword
Committees
Reviewers

Tutorial 1 (Session Chair: Harry Buhrman)

The Polynomial Method in Quantum and Classical Computing1
Scott Aaronson

Tutorial 2 (Session Chair: Mohammad Mahdian)

Theory of Sponsored Search Auctions2
Gagan Aggarwal and S. Muthukrishnan

Tutorial 3 (Session Chair: Emanuele Viola)

Average-case Complexity3
Luca Trevisan

Session 1A (Session Chair: Mohammad Mahdian)

Truthful Approximation Schemes for Single-Parameter Agents4
Peerapong Dhangwatnotai, Shahar Dobzinski, Shaddin Dughmi, and Tim Roughgarden

Discretized Multinomial Distributions and Nash Equilibria in Anonymous
Games14
Constantinos Daskalakis and Christos H. Papadimitriou

Approximation Algorithms for Single-minded Envy-free Profit-maximization
Problems with Limited Supply24
Maurice Cheung and Chaitanya Swamy

Market Equilibria in Polynomial Time for Fixed Number of Goods or Agents34
Nikhil R. Devanur and Ravi Kannan

Session 1B (Session Chair: Emanuele Viola)

The Sign-Rank of AC^0	43
<i>Alexander A. Razborov and Alexander A. Sherstov</i>	
Arithmetic Circuits: A Chasm at Depth Four	53
<i>Manindra Agrawal and V. Vinay</i>	
Dense Subsets of Pseudorandom Sets	62
<i>Omer Reingold, Luca Trevisan, Madhur Tulsiani, and Salil Vadhan</i>	
Almost-Natural Proofs	72
<i>Timothy Y. Chow</i>	

Session 2A (Session Chair: Artur Czumaj)

Dynamic Connectivity: Connecting to Networks and Geometry	78
<i>Timothy M. Chan, Mihai Patrascu, and Liam Roditty</i>	
Algorithms for Single-Source Vertex Connectivity	88
<i>Julia Chuzhoy and Sanjeev Khanna</i>	
A Polynomial-Time Approximation Scheme for Euclidean Steiner Forest	98
<i>Glencora Borradaile, Philip N. Klein, and Claire Mathieu</i>	
Degree Bounded Network Design with Metric Costs	108
<i>Yuk Hei Chan, Wai Shing Fung, Lap Chi Lau, and Chun Kong Yung</i>	

Session 2B (Session Chair: Toniann Pitassi)

Matrix Sparsification for Rank and Determinant Computations via Nested Dissection	118
<i>Raphael Yuster</i>	
Fast Modular Composition in any Characteristic	127
<i>Kiran S. Kedlaya and Christopher Umans</i>	
Gaussian Bounds for Noise Correlation of Functions and Tight Analysis of Long Codes	137
<i>Elchanan Mossel</i>	
Worst Case to Average Case Reductions for Polynomials	147
<i>Tali Kaufman and Shachar Lovett</i>	

Session 3A (Session Chair: Jeff Erickson)

On the Union of Cylinders in Three Dimensions	157
<i>Esther Ezra</i>	
Spherical Cubes and Rounding in High Dimensions	167
<i>Guy Kindler, Ryan O'Donnell, Anup Rao, and Avi Wigderson</i>	
Near-Optimal Sparse Recovery in the L1 Norm	177
<i>Piotr Indyk and Milan Ruzic</i>	

Session 3B (Session Chair: Avrim Blum)

On Basing Lower-Bounds for Learning on Worst-Case Assumptions	186
<i>Benny Applebaum, Boaz Barak, and David Xiao</i>	
The Bayesian Learner is Optimal for Noisy Binary Search (and Pretty Good for Quantum as Well)	196
<i>Michael Ben-Or and Avinatan Hassidim</i>	
Hardness of Minimizing and Learning DNF Expressions	206
<i>Subhash Khot and Rishi Saket</i>	

Session 4A (Session Chair: Yossi Azar)

Elections Can be Manipulated Often	216
<i>Ehud Friedgut, Gil Kalai, and Noam Nisan</i>	
On the Hardness of Being Truthful	223
<i>Christos Papadimitriou, Michael Schapira, and Yaron Singer</i>	
Multi-unit Auctions with Budget Limits	233
<i>Shahar Dobzinski, Ron Lavi, and Noam Nisan</i>	

Session 4B (Session Chair: Yevgeniy Dodis)

Multilinear Formulas, Maximal-Partition Discrepancy and Mixed-Sources Extractors	243
<i>Ran Raz and Amir Yehudayoff</i>	
On the Impossibility of Basing Identity Based Encryption on Trapdoor Permutations	253
<i>Dan Boneh, Periklis Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, and Brent Waters</i>	
Leakage-Resilient Cryptography	263
<i>Stefan Dziembowski and Krzysztof Pietrzak</i>	

Session 5 (Session Chair: R. Ravi)

Succincter	273
<i>Mihai Patrascu</i>	
Two Query PCP with Sub-Constant Error	282
<i>Dana Moshkovitz and Ran Raz</i>	

Session 6A (Session Chair: Yury Makarychev)

Constant-Time Approximation Algorithms via Local Improvements	292
<i>Huy N. Nguyen and Krzysztof Onak</i>	
Some Results on Greedy Embeddings in Metric Spaces	302
<i>Ankur Moitra and Tom Leighton</i>	
Set Covering with our Eyes Closed	312
<i>Fabrizio Grandoni, Anupam Gupta, Stefano Leonardi, Pauli Miettinen, Piotr Sankowski, and Mohit Singh</i>	

Minimizing Movement in Mobile Facility Location Problems	322
<i>Zachary Friggstad and Mohammad R. Salavatipour</i>	

Session 6B (Session Chair: Sampath Kannan)

A Counterexample to Strong Parallel Repetition	332
<i>Ran Raz</i>	
Rounding Parallel Repetitions of Unique Games	337
<i>Boaz Barak, Moritz Hardt, Ishay Haviv, Anup Rao, Oded Regev, and David Steurer</i>	
The Unbounded-Error Communication Complexity of Symmetric Functions	347
<i>Alexander A. Sherstov</i>	
Lower Bounds for Noisy Wireless Networks using Sampling Algorithms	357
<i>Chinmoy Dutta and Jaikumar Radhakrishnan</i>	

Session 7A (Session Chair: Jeff Erickson)

Inapproximability for Metric Embeddings into \mathbb{R}^d	366
<i>Jiri Matousek and Anastasios Sidiropoulos</i>	
A Geometric Approach to Lower Bounds for Approximate Near-Neighbor Search and Partial Match	375
<i>Rina Panigrahy, Kunal Talwar, and Udi Wieder</i>	
Hardness of Nearest Neighbor under L_∞	385
<i>Alexandr Andoni, Dorian Croitoru, and Mihai Patrascu</i>	
(Data) STRUCTURES	395
<i>Mihai Patrascu</i>	

Session 7B (Session Chair: Scott Aaronson)

Entangled Games are Hard to Approximate	405
<i>Julia Kempe, Hirota Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick</i>	
Unique Games with Entangled Provers are Easy	415
<i>Julia Kempe, Oded Regev, and Ben Toner</i>	
Quantum Multi Prover Interactive Proofs with Communicating Provers	425
<i>Michael Ben Or, Avinatan Hassidim, and Haran Pilpel</i>	
A Hypercontractive Inequality for Matrix-Valued Functions with Applications to Quantum Computing and LDCs	435
<i>Avraham Ben-Aroya, Oded Regev, and Ronald de Wolf</i>	

Session 8A (Session Chair: Artur Czumaj)

Sketching and Streaming Entropy via Approximation Theory	445
<i>Nicholas J.A. Harvey, Jelani Nelson, and Krzysztof Onak</i>	
On the Value of Multiple Read/Write Streams for Approximating Frequency Moments	455
<i>Paul Beame and Dang-Trinh Huynh-Ngoc</i>	

Clock Synchronization with Bounded Global and Local Skew	465
<i>Christoph Lenzen, Thomas Locher, and Roger Wattenhofer</i>	
Shallow-Low-Light Trees, and Tight Lower Bounds for Euclidean Spanners	475
<i>Yefim Dinitz, Michael Elkin, and Shay Solomon</i>	
Session 8B (Session Chair: Yishay Mansour)	
What Can We Learn Privately?	485
<i>Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith</i>	
Learning Geometric Concepts via Gaussian Surface Area	495
<i>Adam R. Klivans, Ryan O'Donnell, and Rocco A. Servedio</i>	
Isotropic PCA and Affine-Invariant Clustering	505
<i>Spencer Charles Brubaker and Santosh Vempala</i>	
Approximate Kernel Clustering	515
<i>Subhash Khot and Assaf Naor</i>	
Session 9A (Session Chair: Yossi Azar)	
Beating the Random Ordering is Hard: Inapproximability of Maximum Acyclic Subgraph	525
<i>Venkatesan Guruswami, Rajsekar Manokaran, and Prasad Raghavendra</i>	
(Acyclic) Job Shops are Hard to Approximate	535
<i>Monaldo Mastrolilli and Ola Svensson</i>	
Linear Level Lasserre Lower Bounds for Certain k-CSPs	545
<i>Grant Schoenebeck</i>	
The Power of Reordering for Online Minimum Makespan Scheduling	555
<i>Matthias Englert, Deniz Özmen, and Matthias Westermann</i>	
Locally Testing Direct Product in the Low Error Range	565
<i>Irit Dinur and Elazar Goldenberg</i>	
Session 9B (Session Chair: Valerie King)	
Makeya Sets, New Mergers and Old Extractors	575
<i>Zeev Dvir and Avi Wigderson</i>	
A Dichotomy Theorem for the Resolution Complexity of Random Constraint Satisfaction Problems	584
<i>Siu On Chan and Michael Molloy</i>	
Holographic Algorithms by Fibonacci Gates and Holographic Reductions for Hardness	594
<i>Jin-Yi Cai, Pinyan Lu, and Mingji Xia</i>	
Network Extractor Protocols	604
<i>Yael Tauman Kalai, Xin Li, Anup Rao, and David Zuckerman</i>	

Session 10A (Session Chair: Yury Makarychev)

Isomorphism of Hypergraphs of Low Rank in Moderately Exponential Time	614
<i>Laszlo Babai and Paolo Codenotti</i>	
Computing the Tutte Polynomial in Vertex-Exponential Time	624
<i>Andreas Björklund, Thore Husfeldt, Petteri Kaski, and Mikko Koivisto</i>	
On the Approximability of Budgeted Allocations and Improved Lower Bounds for Submodular Welfare Maximization and GAP	634
<i>Deeparnab Chakrabarty and Gagan Goel</i>	
Submodular Approximation: Sampling-based Algorithms and Lower Bounds	644
<i>Zoya Svitkina and Lisa Fleischer</i>	

Session 10B (Session Chair: Jonathan Katz)

Short Proofs May Be Spacious: An Optimal Separation of Space and Length in Resolution	654
<i>Eli Ben-Sasson and Jakob Nordström</i>	
Noise Tolerance of Expanders and Sublinear Expander Reconstruction	664
<i>Satyen Kale, Yuval Peres, and C. Seshadhri</i>	
Sequence Length Requirement of Distance-Based Phylogeny Reconstruction: Breaking the Polynomial Barrier	674
<i>Sébastien Roch</i>	
Size Bounds and Query Plans for Relational Joins	684
<i>Albert Atserias, Martin Grohe, and Dániel Marx</i>	

Session 11A (Session Chair: Rafail Ostrovsky)

Eigenvalue Bounds, Spectral Partitioning, and Metrical Deformations via Flows	694
<i>Punyashloka Biswal, James R. Lee, and Satish Rao</i>	
Embeddings of Topological Graphs: Lossy Invariants, Linearization, and 2-Sums	704
<i>Amit Chakrabarti, Alexander Jaffe, James R. Lee, and Justin Vincent</i>	
A Simpler Linear Time Algorithm for Embedding Graphs into an Arbitrary Surface and the Genus of Graphs of Bounded Tree-Width	714
<i>Ken-ichi Kawarabayashi, Bojan Mohar, and Bruce Reed</i>	
Nearly Tight Low Stretch Spanning Trees	724
<i>Ittai Abraham, Yair Bartal, and Ofer Neiman</i>	

Session 11B (Session Chair: Harry Buhrman)

Algorithmic Barriers from Phase Transitions	734
<i>Dimitris Achlioptas and Amin Coja-Oghlan</i>	
Mixing Time of Exponential Random Graphs	744
<i>Shankar Bhamidi, Guy Bresler, and Allan Sly</i>	

k-Wise Independent Random Graphs	754
<i>Noga Alon and Asaf Nussboim</i>	
Broadcasting with Side Information	764
<i>Noga Alon, Eyal Lubetzky, Uri Stav, Amit Weinstein, and Avinatan Hassidim</i>	