

47th Annual IEEE Symposium on Foundations
of Computer Science

FOCS 2006

21-24 October 2006

Berkeley, California



Los Alamitos, California

Washington • Tokyo

Table of Contents

47th Annual IEEE Symposium on Foundations of Computer Science

FOCS 2006

Foreword.....	xi
Organizing Committees	xii
Reviewers.....	xiii

Session 1A

Statistical Zero-Knowledge Arguments for NP from Any One-Way Function.....	3
<i>Minh-Huyen Nguyen, Shien Jin Ong, and Salil Vadhan</i>	
Fault-Tolerant Distributed Computing in Full-Information Networks	15
<i>Shafi Goldwasser, Elan Pavlov, and Vinod Vaikuntanathan</i>	
Explicit Exclusive Set Systems with Applications to Broadcast Encryption.....	27
<i>Craig Gentry, Zulfikar Ramzan, and David P. Woodruff</i>	

Session 1B

A Simple Condition Implying Rapid Mixing of Single-Site Dynamics on Spin Systems.....	39
<i>Thomas P. Hayes</i>	
Heat Flow and a Faster Algorithm to Compute the Surface Area of a Convex Body	47
<i>Mikhail Belkin, Hariharan Narayanan, and Partha Niyogi</i>	
Fast Algorithms for Logconcave Functions: Sampling, Rounding, Integration and Optimization	57
<i>László Lovász and Santosh Vempala</i>	

Session 2A

A Local Switch Markov Chain on Given Degree Graphs with Application in Connectivity of Peer-to-Peer Networks	69
<i>Tomas Feder, Adam Guetz, Milena Mihail, and Amin Saberi</i>	
Strategic Network Formation through Peering and Service Agreements	77
<i>Elliot Anshelevich, Bruce Shepherd, and Gordon Wilfong</i>	
Towards Secure and Scalable Computation in Peer-to-Peer Networks	87
<i>Valerie King, Jared Saia, Vishal Sanwalani, and Erik Vee</i>	

Session 2B

L_p Metrics on the Heisenberg Group and the Goemans-Linial Conjecture.....	99
<i>James R. Lee and Assaf Naor</i>	
Ramsey Partitions and Proximity Data Structures	109
<i>Manor Mendel and Assaf Naor</i>	
Algorithms on Negatively Curved Spaces	119
<i>Robert Krauthgamer and James R. Lee</i>	

Session 3A

Beyond Hirsch Conjecture: Walks on Random Polytopes and Smoothed Complexity of the Simplex Method.....	133
<i>Roman Vershynin</i>	
Improved Approximation Algorithms for Large Matrices via Random Projections	143
<i>Tamás Sarlós</i>	
Worst-Case and Smoothed Analysis of the ICP Algorithm, with an Application to the k -Means Method	153
<i>David Arthur and Sergei Vassilvitskii</i>	
The Effectiveness of Lloyd-Type Methods for the k -Means Problem.....	165
<i>Rafail Ostrovsky, Yuval Rabani, Leonard Schulman, and Chaitanya Swamy</i>	

Session 3B

Better Lossless Condensers through Derandomized Curve Samplers	177
<i>Amnon Ta-Shma and Christopher Umans</i>	
Approximately List-Decoding Direct Product Codes and Uniform Hardness Amplification	187
<i>Russell Impagliazzo, Ragesh Jaiswal, and Valentine Kabanets</i>	
Index Coding with Side Information	197
<i>Ziv Bar-Yossef, Yitzhak Birk, T.S. Jayram, and Tomer Kol</i>	
Subspace Polynomials and List Decoding of Reed-Solomon Codes.....	207
<i>Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan</i>	

Session 4A

SDP Gaps and UGC-Hardness for MaxCutGain	217
<i>Subhash Khot and Ryan O'Donnell</i>	
Correlated Algebraic-Geometric Codes: Improved List Decoding over Bounded Alphabets.....	227
<i>Venkatesan Guruswami and Anindya Patthak</i>	

Session 4B

- Cryptography from Anonymity 239
Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai
- Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority..... 249
*Michael Ben-Or, Claude Crepeau, Daniel Gottesman, Avinatan Hassidim,
and Adam Smith*

Session 5A

- Settling the Complexity of Two-Player Nash Equilibrium..... 261
Xi Chen and Xiaotie Deng

Session 6A

- Minimum Bounded Degree Spanning Trees..... 273
Michel Goemans
- Approximate Min-Max Theorems of Steiner Rooted-Orientations of Hypergraphs 283
Tamás Király and Lap Chi Lau
- Improved Bounds for Online Routing and Packing via a Primal-Dual Approach..... 293
Niv Buchbinder and Seffi Naor

Session 6B

- Improved Dynamic Planar Point Location..... 305
Lars Arge, Gerth Stolting Brodal, and Loukas Georgiadis
- Coresets for Weighted Facilities and their Applications..... 315
Dan Feldman, Amos Fiat, and Micha Sharir
- Planar Point Location in Sublogarithmic Time..... 325
Mihai Patrascu
- Point Location in $o(\log n)$ Time, Voronoi Diagrams in $o(n \log n)$ time, and Other
Transdichotomous Results in Computational Geometry 333
Timothy M. Chan

Session 7A

- Concurrent Non-Malleable Zero Knowledge 345
Boaz Barak, Manoj Prabhakaran, and Amit Sahai
- Succinct Non-Interactive Zero-Knowledge Proofs with Preprocessing for LOGSNP 355
Yael Tauman Kalai and Ran Raz

Input-Indistinguishable Computation	367
<i>Silvio Micali, Rafael Pass, and Alon Rosen</i>	
Session 7B	
Generalization of Binary Search: Searching in Trees and Forest-Like Partial Orders	379
<i>Krzysztof Onak and Pawel Parys</i>	
Lower Bounds for Additive Spanners, Emulators, and More	389
<i>David P. Woodruff</i>	
Solving Evacuation Problems Efficiently—Earliest Arrival Flows with Multiple Sources	399
<i>Nadine Baumann and Martin Skutella</i>	
Session 8A	
New Limits on Fault-Tolerant Quantum Computation	411
<i>Harry Buhrman, Richard Cleve, Monique Laurent, Noah Linden, Alexander Schrijver, and Falk Unger</i>	
Postselection Threshold against Biased Noise	420
<i>Ben W. Reichardt</i>	
On the Quantum Query Complexity of Local Search in Two and Three Dimensions	429
<i>Xiaoming Sun and Andrew C. Yao</i>	
On the Time Complexity of 2-Tag Systems and Small Universal Turing Machines	439
<i>Damien Woods and Turlough Neary</i>	
Session 8B	
On the Optimality of the Dimensionality Reduction Method	449
<i>Alexandr Andoni, Piotr Indyk, and Mihai Patrascu</i>	
Near-Optimal Hashing Algorithms for Approximate Nearest Neighbor in High Dimensions	459
<i>Alexandr Andoni and Piotr Indyk</i>	
Points on Computable Curves	469
<i>Xiaoyang Gu, Jack H. Lutz, and Elvira Mayordomo</i>	
Local Graph Partitioning using PageRank Vectors	475
<i>Reid Andersen, Fan Chung, and Kevin Lang</i>	
Session 9A	
Norm of the Inverse of a Random Matrix	487
<i>Mark Rudelson</i>	

Witnesses for Non-Satisfiability of Dense Random 3CNF Formulas.....	497
<i>Uriel Feige, Jeong Han Kim, and Eran Ofek</i>	

Session 9B

Accidental Algorithms	509
<i>Leslie Valiant</i>	

The Kesten-Stigum Reconstruction Bound is Tight for Roughly Symmetric Binary Channels.....	518
<i>Christian Borgs, Jennifer Chayes, Elchanan Mossel, and Sebastien Roch</i>	

Session 10A

Algebraic Structures and Algorithms for Matching and Matroid Problems	531
<i>Nicholas J.A. Harvey</i>	

Session 11A

Hardness of Learning Halfspaces with Noise	543
<i>Venkatesan Guruswami and Prasad Raghavendra</i>	

Cryptographic Hardness for Learning Intersections of Halfspaces	553
<i>Adam R. Klivans and Alexander A. Sherstov</i>	

New Results for Learning Noisy Parities and Halfspaces	563
<i>Vitaly Feldman, Parikshit Gopalan, Subhash Khot, and Ashok Kumar Ponnuswami</i>	

Session 11B

Inclusion-Exclusion Algorithms for Counting Set Partitions	575
<i>Andreas Björklund and Thore Husfeldt</i>	

An $O^*(2^n)$ Algorithm for Graph Coloring and Other Partitioning Problems via Inclusion-Exclusion	583
<i>Mikko Koivisto</i>	

Faster Algorithms for Approximate Distance Oracles and All-Pairs Small Stretch Paths	591
<i>Surender Baswana and Telikepalli Kavitha</i>	

Session 12A

Computing Nash Equilibria: Approximation and Smoothed Complexity	603
<i>Xi Chen, Xiaotie Deng and Shang-Hua Teng</i>	

On the Impact of Combinatorial Structure on Congestion Games.....	613
<i>Heiner Ackermann, Heiko Roeglin, and Berthold Voeking</i>	

Balanced Allocations of Cake.....	623
<i>Jeff Edmonds and Kirk Pruhs</i>	
Session 12B	
On a Geometric Generalization of the Upper Bound Theorem	635
<i>Uli Wagner</i>	
Higher Lower Bounds for Near-Neighbor and Further Rich Problems	646
<i>Mihai Patrascu and Mikkel Thorup</i>	
Planar Earthmover is not in L_1	655
<i>Assaf Naor and Gideon Schechtman</i>	
Session 13A	
Approximation Algorithms for Allocation Problems: Improving the Factor of $1-1/e$	667
<i>Uriel Feige and Jan Vondrak</i>	
Approximation Algorithms for Non-Uniform Buy-at-Bulk Network Design	677
<i>Chandra Chekuri, Mohammad Taghi Hajiaghayi, Guy Kortsarz, and Mohammad R. Salavatipour</i>	
How to Play Unique Games Using Embeddings	687
<i>Eden Chlamtac, Konstantin Makarychev, and Yury Makarychev</i>	
Improved Approximation Algorithms for Multidimensional Bin Packing Problems.....	697
<i>Nikhil Bansal, Alberto Caprara, and Maxim Sviridenko</i>	
Session 13B	
Lower Bounds for Circuits with MOD_m Gates	709
<i>Arkadev Chattopadhyay, Navin Goyal, Pavel Pudlak, and Denis Therien</i>	
On the Compressibility of NP Instances and Cryptographic Applications.....	719
<i>Danny Harnik and Moni Naor</i>	
Dispersion of Mass and the Complexity of Randomized Geometric Algorithms.....	729
<i>Luis Rademacher and Santosh Vempala</i>	
An $\Omega(n^{1/3})$ Lower Bound for Bilinear Group Based Private Information Retrieval	739
<i>A.A. Razborov and S. Yekhanin</i>	
Author Index	749