

# **2010 IEEE 51st Annual Symposium on Foundations of Computer Science**

**(FOCS 2010)**

**Las Vegas, Nevada, USA  
23 – 26 October 2010**



**IEEE Catalog Number: CFP10053-PRT  
ISBN: 978-1-4244-8525-3**

# 2010 IEEE 51st Annual Symposium on Foundations of Computer Science

## *FOCS 2010*

# Table of Contents

Foreword.....	xii
Organizing Committee.....	xiii
Program Committee.....	xiv
Reviewers.....	xv

---

### **Session 1A**

Constructive Algorithms for Discrepancy Minimization .....	3
<i>Nikhil Bansal</i>	
Bounded Independence Fools Degree-2 Threshold Functions .....	11
<i>Ilias Diakonikolas, Daniel M. Kane, and Jelani Nelson</i>	
From Sylvester-Gallai Configurations to Rank Bounds: Improved Black-Box Identity Test for Depth-3 Circuits .....	21
<i>Nitin Saxena and C. Seshadhri</i>	
The Coin Problem and Pseudorandomness for Branching Programs .....	30
<i>Joshua Brody and Elad Verbin</i>	
Pseudorandom Generators for Regular Branching Programs .....	40
<i>Mark Braverman, Anup Rao, Ran Raz, and Amir Yehudayoff</i>	

### **Session 1B**

Boosting and Differential Privacy .....	51
<i>Cynthia Dwork, Guy N. Rothblum, and Salil Vadhan</i>	
A Multiplicative Weights Mechanism for Privacy-Preserving Data Analysis .....	61
<i>Moritz Hardt and Guy N. Rothblum</i>	
Impossibility of Differentially Private Universally Optimal Mechanisms .....	71
<i>Hai Brenner and Kobbi Nissim</i>	
The Limits of Two-Party Differential Privacy .....	81
<i>Andrew McGregor, Ilya Mironov, Toniann Pitassi, Omer Reingold, Kunal Talwar, and Salil Vadhan</i>	

## Session 2A

Settling the Polynomial Learnability of Mixtures of Gaussians .....	93
<i>Ankur Moitra and Gregory Valiant</i>	
Polynomial Learning of Distribution Families .....	103
<i>Mikhail Belkin and Kaushik Sinha</i>	
Agnostically Learning under Permutation Invariant Distributions .....	113
<i>Karl Wimmer</i>	
Corrigendum: A Random Sampling Algorithm for Learning an Intersection of Halfspaces .....	123
<i>Santosh S. Vempala</i>	
Learning Convex Concepts from Gaussian Distributions with PCA .....	124
<i>Santosh S. Vempala</i>	

## Session 2B

Deciding First-Order Properties for Sparse Graphs .....	133
<i>Zdeněk Dvořák, Daniel Král, and Robin Thomas</i>	
Logspace Versions of the Theorems of Bodlaender and Courcelle .....	143
<i>Michael Elberfeld, Andreas Jakoby, and Till Tantau</i>	
A Separator Theorem in Minor-Closed Classes .....	153
<i>Ken-ichi Kawarabayashi and Bruce Reed</i>	
Optimal Stochastic Planarization .....	163
<i>Anastasios Sidiropoulos</i>	

## Session 3A

Determinant Sums for Undirected Hamiltonicity .....	173
<i>Andreas Björklund</i>	
Fighting Perebor: New and Improved Algorithms for Formula and QBF Satisfiability .....	183
<i>Rahul Santhanam</i>	
The Monotone Complexity of k-clique on Random Graphs .....	193
<i>Benjamin Rossman</i>	
The Complexity of Distributions .....	202
<i>Emanuele Viola</i>	
Hardness of Finding Independent Sets in Almost 3-Colorable Graphs .....	212
<i>Irit Dinur, Subhash Khot, Will Perkins, and Muli Safra</i>	

## Session 3B

Solving Linear Systems through Nested Dissection .....	225
<i>Noga Alon and Raphael Yuster</i>	
Approaching Optimality for Solving SDD Linear Systems .....	235
<i>Ioannis Koutis, Gary L. Miller, and Richard Peng</i>	

Fast Approximation Algorithms for Cut-Based Problems in Undirected Graphs .....	245
<i>Aleksander Madry</i>	
Metric Extension Operators, Vertex Sparsifiers and Lipschitz Extendability .....	255
<i>Konstantin Makarychev and Yury Makarychev</i>	
Vertex Sparsifiers and Abstract Rounding Algorithms .....	265
<i>Moses Charikar, Tom Leighton, Shi Li, and Ankur Moitra</i>	
<b>Session 4</b>	
Approximation Algorithms for the Edge-Disjoint Paths Problem via Raecke Decompositions .....	277
<i>Matthew Andrews</i>	
Computational Transition at the Uniqueness Threshold .....	287
<i>Allan Sly</i>	
<b>Session 5A</b>	
Clustering with Spectral Norm and the k-Means Algorithm .....	299
<i>Amit Kumar and Ravindran Kannan</i>	
Stability Yields a PTAS for k-Median and k-Means Clustering .....	309
<i>Pranjal Awasthi, Avrim Blum, and Or Sheffet</i>	
The Geometry of Manipulation: A Quantitative Proof of the Gibbard-Satterthwaite Theorem .....	319
<i>Marcus Isaksson, Guy Kindler, and Elchanan Mossel</i>	
Efficient Volume Sampling for Row/Column Subset Selection .....	329
<i>Amit Deshpande and Luis Rademacher</i>	
<b>Session 5B</b>	
A Non-linear Lower Bound for Planar Epsilon-Nets .....	341
<i>Noga Alon</i>	
The Sub-exponential Upper Bound for On-Line Chain Partitioning .....	347
<i>Bartłomiej Bosek and Tomasz Krawczyk</i>	
Improved Bounds for Geometric Permutations .....	355
<i>Natan Rubin, Haim Kaplan, and Micha Sharir</i>	
On the Queue Number of Planar Graphs .....	365
<i>Giuseppe Di Battista, Fabrizio Frati, and János Pach</i>	
<b>Session 6A</b>	
Polylogarithmic Approximation for Edit Distance and the Asymmetric Query Complexity .....	377
<i>Alexandr Andoni, Robert Krauthgamer, and Krzysztof Onak</i>	
Information Cost Tradeoffs for Augmented Index and Streaming Language Recognition .....	387
<i>Amit Chakrabarti, Graham Cormode, Ranganath Kondapally, and Andrew McGregor</i>	

New Constructive Aspects of the Lovasz Local Lemma .....	397
<i>Bernhard Haeupler, Barna Saha, and Aravind Srinivasan</i>	
The Geometry of Scheduling .....	407
<i>Nikhil Bansal and Kirk Pruhs</i>	
<b>Session 6B</b>	
Strong Fault-Tolerance for Self-Assembly with Fuzzy Temperature .....	417
<i>David Doty, Matthew J. Patitz, Dustin Reishus, Robert T. Schweller, and Scott M. Summers</i>	
Holographic Algorithms with Matchgates Capture Precisely Tractable Planar #CSP .....	427
<i>Jin-Yi Cai, Pinyan Lu, and Mingji Xia</i>	
A Decidable Dichotomy Theorem on Directed Graph Homomorphisms with Non-negative Weights .....	437
<i>Jin-Yi Cai and Xi Chen</i>	
<b>Session 7A</b>	
Sublinear Optimization for Machine Learning .....	449
<i>Kenneth L. Clarkson, Elad Hazan, and David P. Woodruff</i>	
Estimating the Longest Increasing Sequence in Polylogarithmic Time .....	458
<i>Michael Saks and C. Seshadhri</i>	
Testing Properties of Sparse Images .....	468
<i>Gilad Tsur and Dana Ron</i>	
A Unified Framework for Testing Linear-Invariant Properties .....	478
<i>Arnab Bhattacharyya, Elena Grigorescu, and Asaf Shapira</i>	
Optimal Testing of Reed-Muller Codes .....	488
<i>Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman</i>	
<b>Session 7B</b>	
Overcoming the Hole in the Bucket: Public-Key Cryptography Resilient to Continual Memory Leakage .....	501
<i>Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, and Vinod Vaikuntanathan</i>	
Cryptography against Continuous Memory Attacks .....	511
<i>Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs</i>	
On the Insecurity of Parallel Repetition for Leakage Resilience .....	521
<i>Allison Lewko and Brent Waters</i>	
Black-Box, Round-Efficient Secure Computation via Non-malleability Amplification .....	531
<i>Hoeteck Wee</i>	
Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions .....	541
<i>Ran Canetti, Huijia Lin, and Rafael Pass</i>	

## Session 8

Bounds on Monotone Switching Networks for Directed Connectivity .....	553
<i>Aaron Potechin</i>	
Subexponential Algorithms for Unique Games and Related Problems .....	563
<i>Sanjeev Arora, Boaz Barak, and David Steurer</i>	

## Session 9A

Dependent Randomized Rounding via Exchange Properties of Combinatorial Structures .....	575
<i>Chandra Chekuri, Jan Vondrák, and Rico Zenklusen</i>	
Minimum-Cost Network Design with (Dis)economies of Scale .....	585
<i>Matthew Andrews, Spyridon Antonakopoulos, and Lisa Zhang</i>	
One Tree Suffices: A Simultaneous $O(1)$ -Approximation for Single-Sink Buy-at-Bulk .....	593
<i>Ashish Goel and Ian Post</i>	
Min st-cut Oracle for Planar Graphs with Near-Linear Preprocessing Time .....	601
<i>Glencora Borradaile, Piotr Sankowski, and Christian Wulff-Nilsen</i>	

## Session 9B

On the Computational Complexity of Coin Flipping .....	613
<i>Hemanta K. Maji, Manoj Prabhakaran, and Amit Sahai</i>	
Sequential Rationality in Cryptographic Protocols .....	623
<i>Ronen Gradwohl, Noam Livne, and Alon Rosen</i>	
An Efficient Test for Product States with Applications to Quantum Merlin-Arthur Games .....	633
<i>Aram W. Harrow and Ashley Montanaro</i>	

## Session 10A

Subcubic Equivalences between Path, Matrix and Triangle Problems .....	645
<i>Virginia Vassilevska Williams and Ryan Williams</i>	
Replacement Paths via Fast Matrix Multiplication .....	655
<i>Oren Weimann and Raphael Yuster</i>	
All-Pairs Shortest Paths in $O(n^2)$ Time with High Probability .....	663
<i>Yuval Peres, Dmitry Sotnikov, Benny Sudakov, and Uri Zwick</i>	
Approximating Maximum Weight Matching in Near-Linear Time .....	673
<i>Ran Duan and Seth Pettie</i>	

## Session 10B

A Fourier-Analytic Approach to Reed-Muller Decoding .....	685
<i>Parikshit Gopalan</i>	
Pseudorandom Generators for $CC^0[p]$ and the Fourier Spectrum of Low-Degree Polynomials over Finite Fields .....	695
<i>Shachar Lovett, Partha Mukhopadhyay, and Amir Shpilka</i>	
Matching Vector Codes .....	705
<i>Zeev Dvir, Parikshit Gopalan, and Sergey Yekhanin</i>	
Local List Decoding with a Constant Number of Queries .....	715
<i>Avraham Ben-Aroya, Klim Efremenko, and Amnon Ta-Shma</i>	
Codes for Computationally Simple Channels: Explicit Constructions with Optimal Rate .....	723
<i>Venkatesan Guruswami and Adam Smith</i>	

## Session 11A

Pure and Bayes-Nash Price of Anarchy for Generalized Second Price Auction .....	735
<i>Renato Paes Leme and Éva Tardos</i>	
Frugal and Truthful Auctions for Vertex Covers, Flows and Cuts .....	745
<i>David Kempe, Mahyar Salek, and Cristopher Moore</i>	
Frugal Mechanism Design via Spectral Techniques .....	755
<i>Ning Chen, Edith Elkind, Nick Gravin, and Fedor Petrov</i>	
Budget Feasible Mechanisms .....	765
<i>Yaron Singer</i>	
Black-Box Randomized Reductions in Algorithmic Mechanism Design .....	775
<i>Shaddin Dughmi and Tim Roughgarden</i>	

## Session 11B

Backyard Cuckoo Hashing: Constant Worst-Case Operations with a Succinct Representation .....	787
<i>Yuriy Arbitman, Moni Naor, and Gil Segev</i>	
A Lower Bound for Dynamic Approximate Membership Data Structures .....	797
<i>Shachar Lovett and Ely Porat</i>	
Lower Bounds on Near Neighbor Search via Metric Expansion .....	805
<i>Rina Panigrahy, Kunal Talwar, and Udi Wieder</i>	
Distance Oracles beyond the Thorup–Zwick Bound .....	815
<i>Mihai Pătraşcu and Liam Roditty</i>	

<b>Author Index</b> .....	824
---------------------------	-----