PROCEEDINGS OF THE TWENTY-NINTH
ANNUAL ACM SYMPOSIUM ON
THEORY OF COMPUTING

El Paso, Texas
May 4-6, 1997
SPONSORED BY
THE ACM SPECIAL INTEREST GROUP FOR
ALGORITHMS AND COMPUTATION THEORY
**TABLE OF CONTENTS**

**Sunday, May 4**

**Session 1A**
Some Optimal Inapproximability Results ................................................................. 1  
Johan Håstad
A Complete Classification of the Approximability of Maximization Problems Derived from Boolean  
Constraint Satisfaction ................................................................. 11  
Sanjeev Khanna, Madhu Sudan and David P. Williamson
When Hamming Meets Euclid: The Approximability of Geometric TSP and MST ............. 21  
Luca Trevisan

**Session 1B**
Approximate Complex Polynomial Evaluation in Near Constant Work per Point .................. 30  
John H. Reif
Fast and Precise Computations of Discrete Fourier Transforms Using Cyclotomic Integers ...... 40  
Joe Buhler, M. Amin Shokrollahi and Volker Stemann
Quantum Computation of Fourier Transforms over Symmetric Groups .......................... 48  
Robert Beals

**Session 2A**
General Techniques for Comparing Unrooted Evolutionary Trees ................................... 54  
Ming-Yang Kao, Tak-Wah Lam, Teresa M. Przytycka, Wing-Kin Sung and Hing-Fung Ting
Tree Pattern Matching and Subset Matching in Randomized $O(n \log^3 m)$ Time .............. 66  
Richard Cole and Ramesh Hariharan

**Session 2B**
Randomized $\Omega(n^2)$ Lower Bound for Knapsack ................................................. 76  
Dima Grigoriev and Marek Karpinski
Exponential Lower Bounds for Depth 3 Boolean Circuits ........................................... 86  
Ramamohan Paturi, Michael E. Saks and Francis Zane

**Invited Session I**
Algorithmic Complexity in Coding Theory and the Minimum Distance Problem ................ 92  
Alexander Vardy

**Session 3A**
Approximating Total Flow Time on Parallel Machines .............................................. 110  
Stefano Leonardi and Danny Raz
Non-Clairvoyant Multiprocessor Scheduling of Jobs with Changing Execution Characteristics 120  
Jeff Edmonds, Donald D. Chinn, Tim Brecht and Xiaotie Deng
Better Bounds for Online Scheduling ................................................. 130
  Susanne Albers
Optimal Time-Critical Scheduling via Resource Augmentation ................ 140
  Cynthia A. Phillips, Cliff Stein, Eric Torng and Joel Wein

Session 3B
Practical Loss-Resilient Codes .................................................... 150
  Michael G. Luby, Michael Mitzenmacher, M. Amin Shokrollahi, Daniel A. Spielman and
  Volker Stemann
Spectral Techniques for Expander Codes ........................................... 160
  John D. Lafferty and Daniel N. Rockmore
Faster Solution of the Key Equation for Decoding BCH Error-Correcting Codes .................................................. 168
  Victor Y. Pan
Fault Tolerant Quantum Computation with Constant Error ........................ 176
  Dorit Aharonov and Michael Ben-Or

Session 4A
On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited .................................................. 189
  Moni Naor and Omer Reingold
Reducing Randomness via Irrational Numbers ...................................... 200
  Zhi-Zhong Chen and Ming-Yang Kao
Is There an Algebraic Proof for P ≠ NC? ........................................... 210
  Ketan Mulmuley
P = BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma .................................................. 220
  Russell Impagliazzo and Avi Wigderson
SL ⊆ L 3/2 ................................................................. 230
  Roy Armoni, Amnon Ta-Shma, Avi Wigderson and Shiyou Zhou

Session 4B
Using Random Sampling to Find Maximum Flows in Uncapacitated Undirected Graphs .................................................. 240
  David Karger
Combinatorial Complexity of the Central Curve .................................... 250
  Peter A. Beling and Sushil Verma
Approximation of k-Set Cover by Semi-Local Optimization ...................... 256
  Rong-chih Duh and Martin Füre
Approximation Algorithms for Facility Location Problems ........................ 265
  David B. Shmoys, Éva Tardos and Karen Aardal
Covering Points in the Plane by k-Tours: Towards a Polynomial Time Approximation Scheme for
General k ........................................................................... 275
  Tetsuo Asano, Naoki Katoh, Hisao Tamaki and Takeshi Tokuyama

Monday, May 5

Session 5A
A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence .......... 284
  Miklós Ajtai and Cynthia Dwork
Private Information Storage ............................................................. 294
  Rafail Ostrovsky and Victor Shoup
Computationally Private Information Retrieval ........................................... 304
Benny Chor and Niv Gilboa

Session 5B

Approximating Hyper-Rectangles: Learning and Pseudo-Random Sets .................. 314
Peter Auer, Philip M. Long and Aravind Srinivasan

A Composition Theorem for Learning Algorithms with Applications to Geometric Concept Classes .... 324
Shai Ben-David, Nader H. Bshouty and Eyal Kushilevitz

Using and Combining Predictors that Specialize ............................................. 334
Yoav Freund, Robert E. Schapire, Yoram Singer and Manfred K. Warmuth

Session 6A

On-Line Algorithms for Steiner Tree Problems .................................................. 344
Piotr Berman and Chris Coulston

Online Algorithms for Selective Multicast and Maximal Dense Trees ...................... 354
Baruch Awerbuch and Tripurari Singh

Session 6B

Direct Product Results and the GCD Problem, in Old and New Communication Models .......... 363
Itzhak Parnafes, Ran Raz and Avi Wigderson

The Linear-Array Problem in Communication Complexity Resolved .......................... 373
Martin Dietzfelbinger

Invited Session II

László Babai

Session 7A

Permanents, Pfaffian Orientations, and Even Directed Circuits .............................. 402
William McCuaig, Neil Robertson, P. D. Seymour and Robin Thomas

Property Testing in Bounded Degree Graphs ...................................................... 406
Oded Goldreich and Dana Ron

Exploring Unknown Environments ......................................................................... 416
Susanne Albers and Monika R. Henzinger

On Floorplans of Planar Graphs ............................................................................. 426
Xin He

Session 7B

Linear Zero-Knowledge — A Note on Efficient Zero-Knowledge Proofs and Arguments .... 436
Ronald Cramer and Ivan Damgård

Commodity-Based Cryptography ............................................................................ 446
Donald Beaver

Oblivious Data Structures: Applications to Cryptography ........................................ 456
Daniele Micciancio

Is Linear Hashing Good? ......................................................................................... 465
Noga Alon, Martin Dietzfelbinger, Peter Bro Miltersen, Erez Petrank and Gábor Tardos
Session 8A
A Sub-Constant Error-Probability Low-Degree Test, and a Sub-Constant Error-Probability PCP
Characterization of NP ................................. 475
Ran Raz and Shmuel Safra
Improved Low Degree Testing and its Applications ....................... 485
Sanjeev Arora and Madhu Sudan
Probabilistically Checkable Proofs with Zero Knowledge .................. 496
Joe Kilian, Erez Petrank and Gábor Tardos
Making Games Short .................................... 506
Uriel Feige and Joe Kilian

Session 8B
Improved Routing and Sorting on Multibutterflies ....................... 517
Bruce M. Maggs and Berthold Vöcking
Static and Dynamic Path Selection on Expander Graphs: A Random Walk Approach .................... 531
Andrei Z. Broder, Alan M. Frieze and Eli Upfal
On Sorting Strings in External Memory ................................ 540
Lars Arge, Paolo Ferragina, Roberto Grossi and Jeffrey Scott Vitter
Pointer Jumping Requires Concurrent Read ............................ 549
Noam Nisan and Ziv Bar-Yossef

Tuesday, May 6

Session 9A
Lower Bounds for Distributed Coin-Flipping and Randomized Consensus ....................... 559
James Aspnes
Byzantine Quorum Systems .................................. 569
Dahlia Malkhi and Michael Reiter
All of Us Are Smarter Than Any of Us: Wait-Free Hierarchies Are Not Robust .................. 579
Wai-Kau Lo and Vassos Hadzilacos
The Decidability of Distributed Decision Tasks ......................... 589
Maurice Herlihy and Sergio Rajsbaum

Session 9B
Two Algorithms for Nearest-Neighbor Search in High Dimensions ............ 599
Jon M. Kleinberg
Nearest Neighbor Queries in Metric Spaces ............................ 609
Kenneth L. Clarkson
Locality-Preserving Hashing in Multidimensional Spaces .................. 618
Piotr Indyk, Rajeev Motwani, Prabhakar Raghavan and Santosh Vempala
Incremental Clustering and Dynamic Information Retrieval ................ 626
Moses Charikar, Chandra Chekuri, Tomás Feder and Rajeev Motwani

Session 10A
A Constant-Factor Approximation Algorithm for Packet Routing, and Balancing Local vs. Global Criteria .......................... 636
Aravind Srinivasan and Chung-Piaw Teo
Universal $O(\text{congestion}+\text{dilation}+\log^{1+\epsilon}(N))$ Local Control Packet Switching Algorithms .......................... 644  
Rafail Ostrovsky and Yuval Rabani

Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web ................................................................. 654  
David Karger, Eric Lehman, Tom Leighton, Matthew Levine, Daniel Lewin and Rina Panigrahy

Allocating Bandwidth for Bursty Connections ......................................................... 664  
Jon Kleinberg, Yuval Rabani and Éva Tardos

Session 10B

The Swendsen-Wang Process Does Not Always Mix Rapidly ................................. 674  
Vivek K. Gore and Mark R. Jerrum

Approximately Counting up to Four ................................................................. 682  
Michael Luby and Eric Vigoda

An Interruptible Algorithm for Perfect Sampling via Markov Chains ....................... 688  
James Allen Fill

Sampling Lattice Points ..................................................................................... 696  
Ravi Kannan and Santosh Vempala

Session 11A

Page Replacement with Multi-Size Pages and Applications to Web Caching ............... 701  
Sandy Irani

A Polylog(n)-Competitive Algorithm for Metrical Task Systems .............................. 711  
Yair Bartal, Avrim Blum, Carl Burch and Andrew Tomkins

Session 11B

On $\text{ACC}^0[p^k]$ Frege Proofs ............................................................................. 720  
Alexis Maciel and Toniann Pitassi

Reducing the Complexity of Reductions .................................................................. 730  
Manindra Agrawal, Eric Allender, Russell Impagliazzo, Toniann Pitassi and Steven Rudich

Read-Once Branching Programs, Rectangular Proofs of the Pigeonhole Principle and the Transversal Calculus ................................................................. 739  
Alexander Razborov, Avi Wigderson and Andrew Yao

Errata

Eigenvalues, Flows and Separators of Graphs ...................................................... 749  
F. R. K. Chung and S.-T. Yau

Retraction of “Probabilistic Computation and Linear Time” .................................... 750  
Lance Fortnow and Michael Sipser

Author Index ........................................................................................................... 751