

Proceedings

**36th Annual Symposium on
Foundations of Computer Science**

October 23 - 25, 1995

Milwaukee, Wisconsin

Sponsored by

**IEEE Computer Society Technical Committee on
Mathematical Foundations of Computing**



IEEE Computer Society Press
Los Alamitos, California

Washington • Brussels • Tokyo

Table of Contents

36th Annual Symposium on Foundations of Computer Science

| | |
|-----------------|------|
| Foreword..... | xi |
| Referrees..... | xii |
| Committees..... | xiii |

Session 1

Chair: Steve Cook

| | |
|--|---|
| Invited Talk: Cognitive Computation..... | 2 |
| <i>Leslie G. Valiant, Harvard University</i> | |

Session 2A

Chair: László Babai

| | |
|---|----|
| Spectral Methods for Matrix Rigidity with Applications to Size-Depth Tradeoffs and Communication Complexity..... | 6 |
| <i>S.V. Lokam</i> | |
| Lower Bounds on Arithmetic Circuits via Partial Derivatives..... | 16 |
| <i>N. Nisan and A. Wigderson</i> | |
| Pseudorandom Generators, Measure Theory, and Natural Proofs..... | 26 |
| <i>K.W. Regan, D. Sivakumar, and J.-Y. Cai</i> | |
| Counting Bottlenecks to Show Monotone $P \neq NP$ | 36 |
| <i>A. Haken</i> | |
| Private Information Retrieval..... | 41 |
| <i>B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan</i> | |

Session 2B

Chair: Serge Plotkin

| | |
|---|----|
| Disjoint Paths in Densely Embedded Graphs..... | 52 |
| <i>J. Kleinberg and É. Tardos</i> | |
| Divide-and-Conquer Approximation Algorithms via Spreading Metrics..... | 62 |
| <i>G. Even, J. Naor, S. Rao, and B. Schieber</i> | |
| The Loading Time Scheduling Problem..... | 72 |
| <i>R. Bhatia, S. Khuller, and J. Naor</i> | |
| Approximability of Flow Shop Scheduling..... | 82 |
| <i>L.A. Hall</i> | |
| A Representation of Cuts within $6/5$ Times the Edge Connectivity with Applications..... | 92 |
| <i>A.A. Benczúr</i> | |

Session 3A**Chair: Nicholas Pippenger**

| | |
|--|-----|
| Contention Resolution with Bounded Delay | 104 |
| <i>M. Paterson and A. Srinivasan</i> | |
| Tight Bounds for a Distributed Selection Game with Applications to Fixed-Connection Machines..... | 114 |
| <i>C.G. Plaxton</i> | |
| Efficient Parallel Solution of Sparse Eigenvalue and Eigenvector Problems | 123 |
| <i>J.H. Reif</i> | |

Session 3B**Chair: Umesh Vazirani**

| | |
|--|-----|
| Approximating the Volume of Definable Sets | 134 |
| <i>P. Koiran</i> | |
| An Optimal Algorithm for Monte Carlo Estimation | 142 |
| <i>P. Dagum, R. Karp, M. Luby, and S. Ross</i> | |
| Markov Chain Algorithms for Planar Lattice Structures..... | 150 |
| <i>M. Luby, D. Randall, and A. Sinclair</i> | |

Session 4A**Chair: Steven Rudich**

| | |
|---|-----|
| Derandomizing Semidefinite Programming Based Approximation Algorithms | 162 |
| <i>S. Mahajan and H. Ramesh</i> | |
| Synthesizers and their Application to the Parallel Construction of Pseudo-Random Functions | 170 |
| <i>M. Naor and O. Reingold</i> | |
| Splitters and Near-Optimal Derandomization..... | 182 |
| <i>M. Naor, L.J. Schulman, and A. Srinivasan</i> | |

Session 4B**Chair: Edith Cohen**

| | |
|--|-----|
| A Unified Analysis of Paging and Caching..... | 194 |
| <i>E. Torng</i> | |
| Application-Controlled Paging for a Shared Cache | 204 |
| <i>R.D. Barve, E.F. Grove, and J.S. Vitter</i> | |
| Speed is as Powerful as Clairvoyance | 214 |
| <i>B. Kalyanasundaram and K. Pruhs</i> | |

Session 5**Chair: Andrew C.-C. Yao**

| | |
|--|-----|
| Invited Talk: Perspectives on Database Theory | 224 |
| <i>Mihalis Yannakakis, AT&T Bell Laboratories</i> | |

Session 6A**Chair: Pankaj Agarwal**

| | |
|---|-----|
| Algebraic Decomposition of Non-Convex Polyhedra | 248 |
| <i>H. Edelsbrunner</i> | |
| Improved Lower Bound on Testing Membership to a Polyhedron by Algebraic Decision Trees | 258 |
| <i>D. Grigoriev, M. Karpinski, and N. Vorobjov</i> | |
| Optimal Algorithms for Curves on Surfaces | 266 |
| <i>T.K. Dey and S. Guha</i> | |
| Integral Geometry of Higher-Dimensional Polytopes and the Average Case in Combinatorial Optimization | 275 |
| <i>A.I. Barvinok</i> | |
| Finding Points on Curves Over Finite Fields | 284 |
| <i>J. von zur Gathen and I. Shparlinski</i> | |

Session 6B**Chair: John Canny**

| | |
|---|-----|
| Learning Polynomials with Queries: The Highly Noisy Case | 294 |
| <i>O. Goldreich, R. Rubinfeld, and M. Sudan</i> | |
| Simple Learning Algorithms for Decision Trees and Multivariate Polynomials | 304 |
| <i>N.H. Bshouty and Y. Mansour</i> | |
| Tracking the Best Disjunction | 312 |
| <i>P. Auer and M.K. Warmuth</i> | |
| Gambling in a Rigged Casino: The Adversarial Multi-Armed Bandit Problem | 322 |
| <i>P. Auer, N. Cesa-Bianchi, Y. Freund, and R.E. Schapire</i> | |
| Efficient Algorithms for Learning to Play Repeated Games Against Computationally Bounded Adversaries | 332 |
| <i>Y. Freund, M. Kearns, Y. Mansour, D. Ron, R. Rubinfeld, and R.E. Schapire</i> | |

Session 7A**Chair: Uri Feige**

| | |
|---|-----|
| $RSPACE(S) \subseteq DSPACE(S^{3/2})$ | 344 |
| <i>M. Saks and S. Zhou</i> | |

| | |
|---|-----|
| Sparse P-Hard Sets Yield Space-Efficient Algorithms | 354 |
| <i>M. Ogihara</i> | |
| The Resolution of a Hartmanis Conjecture | 362 |
| <i>J.-Y. Cai and D. Sivakumar</i> | |

Session 7B

Chair: Martin Dyer

| | |
|--|-----|
| A Scheduling Model for Reduced CPU Energy | 374 |
| <i>F. Yao, A. Demers, and S. Shenker</i> | |
| Load Balancing in the L_p Norm | 383 |
| <i>B. Awerbuch, Y. Azar, E.F. Grove, M.-Y. Kao, P. Krishnan, and J.S. Vitter</i> | |
| Competitive Access Time via Dynamic Storage Rearrangement | 392 |
| <i>A. Fiat, Y. Mansour, A. Rosén, and O. Waarts</i> | |

Session 8A

Chair: Uri Feige

| | |
|---|-----|
| Reductions, Codes, PCPs, and Inapproximability | 404 |
| <i>S. Arora</i> | |
| Improved Hardness Results for Approximating the Chromatic Number | 414 |
| <i>M. Fürer</i> | |
| Free Bits, PCPs, and Non-Approximability — Towards Tight Results | 422 |
| <i>M. Bellare, O. Goldreich, and M. Sudan</i> | |
| Linearity Testing in Characteristic Two | 432 |
| <i>M. Bellare, D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan</i> | |

Session 8B

Chair: Edith Cohen

| | |
|--|-----|
| 3-Coloring in Time $O(1.3446^n)$: A No-MIS Algorithm | 444 |
| <i>R. Beigel and D. Eppstein</i> | |
| Computing Simulations on Finite and Infinite Graphs | 453 |
| <i>M.R. Henzinger, T.A. Henzinger, and P.W. Kopke</i> | |
| Minimum Coloring Random and Semi-Random Graphs in Polynomial Expected Time | 463 |
| <i>C.R. Subramanian</i> | |
| Improved Algorithms and Analysis for Secretary Problems and Generalizations | 473 |
| <i>M. Ajtai, N. Megiddo, and O. Waarts</i> | |

Session 9**Chair: John Canny**

| | |
|---|-----|
| Invited Talk: Controllability, Recognizability, and Complexity Issues in Robot Motion Planning | 484 |
| <i>Jean-Claude Latombe, Stanford University</i> | |

Session 10A**Chair: Steven Rudich**

| | |
|--|-----|
| Coding for Computing | 502 |
| <i>A. Orlitsky and J.R. Roche</i> | |
| Linear Time Erasure Codes with Nearly Optimal Recovery | 512 |
| <i>N. Alon, J. Edmonds, and M. Luby</i> | |
| Using Autoreducibility to Separate Complexity Classes | 520 |
| <i>H. Buhrman, L. Fortnow, and L. Torenvliet</i> | |
| On One-Dimensional Quantum Cellular Automata | 528 |
| <i>J. Watrous</i> | |
| Hard-Core Distributions for Somewhat Hard Problems | 538 |
| <i>R. Impagliazzo</i> | |

Session 10B**Chair: Cynthia Dwork**

| | |
|--|-----|
| Efficient Access to Optical Bandwidth | 548 |
| <i>M. Mihail, C. Kaklamanis, and S. Rao</i> | |
| Routing on Butterfly Networks with Random Faults | 558 |
| <i>R. Cole, B. Maggs, and R. Sitaraman</i> | |
| Fault Diagnosis in a Flash | 571 |
| <i>R. Beigel, W. Hurwood, and N. Kahale</i> | |
| Transforming Men into Mice (Polynomial Algorithm for Genomic Distance Problem) | 581 |
| <i>S. Hannenhalli and P.A. Pevzner</i> | |
| Algorithms for Matrix Groups and the Tits Alternative | 593 |
| <i>R. Beals</i> | |

Session 11A**Chair: Martin Dyer**

| | |
|---|-----|
| Optimal On-Line Search and Sublinear Time Update in String Matching | 604 |
| <i>P. Ferragina and R. Grossi</i> | |
| Reconstructing Strings from Substrings in Rounds | 613 |
| <i>D. Margaritis and S.S. Skiena</i> | |

| | |
|---|-----|
| The Bit Vector Intersection Problem..... | 621 |
| <i>R.M. Karp, O. Waarts, and G. Zweig</i> | |
| Faster Algorithms for the Construction of Parameterized Suffix Trees | 631 |
| <i>S.R. Kosaraju</i> | |

Session 11B

Chair: Pankaj Agarwal

| | |
|---|-----|
| An Approximation Scheme for Planar Graph TSP | 640 |
| <i>M. Grigni, E. Koutsoupias, and C. Papadimitriou</i> | |
| Amortization, Lazy Evaluation, and Persistence: Lists with Catenation via Lazy Linking | 646 |
| <i>C. Okasaki</i> | |
| Sublogarithmic Searching Without Multiplications | 655 |
| <i>A. Andersson</i> | |
| Fully Dynamic Biconnectivity and Transitive Closure | 664 |
| <i>M.R. Henzinger and V. King</i> | |

Session 12A

Chair: László Babai

| | |
|---|-----|
| Lower Bounds for Monotone Span Programs | 674 |
| <i>A. Beimel, A. Gál, and M. Paterson</i> | |
| On Computing Boolean Functions by Sparse Real Polynomials | 682 |
| <i>M. Krause and P. Pudlák</i> | |
| Improved Depth Lower Bounds for Small Distance Connectivity | 692 |
| <i>P. Beame, R. Impagliazzo, and T. Pitassi</i> | |

Session 12B

Chair: Cynthia Dwork

| | |
|---|-----|
| Tight Fault Locality | 704 |
| <i>S. Kutten and D. Peleg</i> | |
| Faster Approximate Agreement with Multi-Writer Registers | 714 |
| <i>E. Schenk</i> | |
| Resolving Message Complexity of Byzantine Agreement and Beyond | 724 |
| <i>Z. Galil, A. Mayer, and M. Yung</i> | |

| | |
|---------------------------|-----|
| Author Index | 734 |
|---------------------------|-----|