30th Annual Symposium On Foundations Of Computer Science

30th Annual

Symposium On Foundations of Computer Science

October 30 - November 1, 1989 *Research Triangle Park, NC*

IEEE Computer Society Press
Los Alamitos, CA

Washington • Los Alamitos • Brussels • Tokyo

IEEE COMPUTER SOCIETY

IEEE THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and are published as presented and without change, in the interests of timely dissemination. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society Press, or The Institute of Electrical and Electronics Engineers, Inc.

Published by

IEEE Computer Society Press
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1264

Cover designed by Alvy Ray Smith

Printed in the United States of America

IEEE Computer Society Order Number 1982
Library of Congress Catalog Number 80-646634
IEEE Catalog Number 89CH2808-4
ISBN 0-8186-1982-1 (case)
0-8186-5982-3 (microfiche)
ISSN 0272-5428
SAN 264-620-X

Additional copies may be ordered from:

IEEE Computer Society
Order Department
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-2578

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331

IEEE Computer Society
13, Avenue de l'Aquilon
B-1200 Brussels
BELGIUM

IEEE Computer Society
Ooshima Building
2-19-1 Minami-Aoyama,
Minato-Ku
Tokyo 107, JAPAN

IEEE

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

Foreword

The papers in this volume were presented at the 30th Annual Symposium on Foundations of Computer Science, held October 30 - November 1, 1989, in the Research Triangle Park, North Carolina. The Symposium was sponsored by the IEEE Technical Committee on Mathematical Foundations of Computing.

The program committee met on June 15-16, 1989 and selected these 100 papers from 273 abstracts submitted in response to the Call for Papers. The selection was based on originality, quality, and relevance to theoretical computer science. The submissions were not refereed, and many of them represent reports of continuing research. It is anticipated that most of these papers will appear in more polished and complete form in scientific journals.

There may be some overlap between some papers appearing in these proceedings and papers either in these proceedings or elsewhere; since the program committee had only extended abstracts to work with, they have in most cases chosen not to make any decisions about priority or independence, but rather to judge the abstracts solely on their technical merits.

The program committee wishes to thank all who submitted papers for consideration.

Alok Aggarwal
Eric Bach
Zvi Galil, *Chair*
Juris Hartmanis
Charles Leiserson
Rohit Parikh
Nicholas Pippenger
Charles Rackoff
Ray Strong
Robert Tarjan
Mihalis Yannakakis
Frances Yao

Machtey Award

The Michael Machtey Award is awarded in recognition of the most outstanding paper written solely by a student or students, as judged by the program committee. The 1989 Machtey Award was presented to

Simulating ($\log^c n$)-wise Independence in NC
by Bonnie Berger and John Rompel

Industrial Sponsors

Academic Press Inc.
Addison-Wesley Publishing Company
AT&T Bell Laboratories
Bell Communications Research
Computer Science Press, Inc.
Digital Equipment Corporation, Systems Research Center
Hewlett-Packard Laboratories, Palo Alto
IBM Almaden Research Center
IBM Thomas J. Watson Research Center
Instituto di Analisi dei Sistemi ed Informatica (Rome, Italy)
John Wiley & Sons Inc.
Morgan Kaufmann Publishers, Inc.
Springer-Verlag New York Inc.
Xerox Palo Alto Research Center

Conference Organization

Conference Chair
Christos Papadimitriou
University of California, San Diego

Program Chair
Zvi Galil
Columbia University & Tel Aviv University

Local Arrangements Chair
John Reif
Duke University

Publicity Chair
David Bray
Clarkson University

Symposium Coordinator
Greg Frederickson
Purdue University

30th Annual

Symposium On
Foundations of Computer Science

Table of Contents

Foreword v

Machtey Award vi

Industrial Sponsors vii

Conference Organization viii

Session 1A
Chair: Zvi Galil

Simulating ($\log^c n$)-wise Independence in NC 2
B. Berger and J. Rompel

The Probabilistic Method Yields Deterministic
Parallel Algorithms 8
R. Motwani, J. Naor, and M. Naor

Dispersers, Deterministic Amplification, and Weak
Random Sources 14
A. Cohen and A. Wigderson

On Universal Classes of Fast High Performance Hash Functions,
Their Time-Space Tradeoff, and Their Applications 20
A. Siegel

Session 1B
Chair: Mihalis Yannakakis

The Strength of Weak Learnability 28
R.E. Schapire

A Theory of Learning Simple Concepts Under Simple Distributions and Average Case Complexity for the Universal Distribution 34
M. Li and P.M.B. Vitanyi
Generalizing the PAC Model: Sample Size Bounds From Metric Dimension-based Uniform Convergence Results 40
D. Haussler
Learning Binary Relations and Total Orders 46
S.A. Goldman, R.L. Rivest, and R.E. Schapire

Session 2A
Chair: Alok Aggarwal

Efficient NC Algorithms for Set Cover with Applications to Learning and Geometry 54
B. Berger, J. Rompel, and P.W. Shor
Fast Matching Algorithms for Points on a Polygon 60
O. Marcotte and S. Suri
Ensemble Motion Planning on Trees 66
G.N. Frederickson and D.J. Guan
An Upper Bound on the Number of Planar k-Sets 72
J. Pach, W. Steiger, and E. Szemerédi

Session 2B
Chair: Eric Bach

The Inverse of Automorphism in Polynomial Time 82
M. Dickerson
Testing for Permutation Polynomials 88
J. von zur Gathen
Computing Irreducible Representations of Finite Groups 93
L. Babai and L. Rónyai
Galois Groups and Factoring Polynomials Over Finite Fields 99
L. Rónyai

Session 3A
Chair: Robert Tarjan

Efficient Algorithms for Independent Assignment on Graphic and Linear Matroids 106
H. Gabow and Y. Xu

Sorting on a Parallel Pointer Machine with Applications to Set Expression Evaluation 190
M.T. Goodrich and S.R. Kosaraju
Recursive *-Tree Parallel Data-Structure 196
O. Berkman and U. Vishkin

Session 4B
Chair: Juris Hartmanis

Computational Complexity of Roots of Real Functions 204
K. Ko
On the Complexity of Fixed Parameter Problems 210
K. Abrahamson and J. Ellis
Structure in Locally Optimal Solutions 216
M. Krentel
Decision Versus Search Problems in Super-Polynomial Time 222
R. Impagliazzo and G. Tardos

Session 5A
Chair: Charles Rackoff

One-way Functions are Essential for Complexity Based Cryptography 230
R. Impagliazzo and M. Luby
Efficient Cryptographic Schemes Provably as Secure as Subset Sum 236
R. Impagliazzo and M. Naor
Lower Bounds for Pseudorandom Number Generators 242
M. Kharitonov, A. Goldberg, and M. Yung
How to Recycle Random Bits 248
R. Impagliazzo and D. Zuckerman

Session 5B
Chair: Rohit Parikh

The Weighted Majority Algorithm 256
N. Littlestone and M. Warmuth
On the Complexity of Learning from Counterexamples 262
W. Maass and G. Turán
The Equivalence and Learning of Probabilistic Automata 268
W.-G. Tzeng
Planning and Learning in Permutation Groups 274
A. Fiat, S. Moses, A. Shamir, I. Shimshoni, and G. Tardos

Flow in Planar Graphs with Multiple Sources and Sinks 112
G.L. Miller and J. Naor
A Randomized Maximum Flow Algorithm 118
J. Cheriyan and T. Hagerup
Graph Products and Chromatic Numbers 124
N. Linial and U. Vazirani
Lower Bounds for the Stable Marriage Problem
and its Variants 129
C. Ng
Approximation Schemes for Constrained Scheduling Problems 134
L.A. Hall and D. Shmoys

Session 3B
Chair: Rohit Parikh

Datalog vs. First-Order Logic 142
M. Ajtai and Y. Gurevich
Decidability and Expressiveness for First-Order
Logics of Probability 148
M. Abadi and J. Halpern
Characterizations of the Basic Feasible Functionals of
Finite Type 154
S. Cook and B. Kapron
The 0-1 Law Fails for the Class of Existential
Second Order Gödel Sentences with Equality 160
L. Pacholski and W. Szwast
A Really Temporal Logic 164
R. Alur and T. Henzinger
Full Abstraction for Nondeterministic Dataflow Networks 170
J. Russell

Session 4A
Chair: Charles Leiserson

Efficient Tree Pattern Matching 178
S.R. Kosaraju
Pipelining Computations in a Tree of Processors 184
S.R. Kosaraju

Session 6A
Chair: Alok Aggarwal

An Optimal Parallel Algorithm for Graph Planarity 282
V. Ramachandran and J. Reif
Efficient Parallel Algorithms for Testing Connectivity and
Finding Disjoint *s-t* Paths in Graphs 288
S. Khuller and B. Schieber
The Parallel Complexity of the Subgraph
Connectivity Problem 294
L. Kirousis, M. Serna, and P. Spirakis
Processor Efficient Parallel Algorithms for the Two Disjoint
Paths Problem, and for Finding a Kuratowski Homeomorph 300
S. Khuller, S. Mitchell, and V. Vazirani

Session 6B
Chair: Nicholas Pippenger

Lower Bounds for Algebraic Computation Trees with Integer Inputs 308
A.C. Yao
Simplification of Nested Radicals 314
S. Landau
Generalizing the Continued Fraction Algorithm to
Arbitrary Dimensions 320
B. Just
The Complexity of Approximating the Square Root 325
Y. Mansour, B. Schieber, and P. Tiwari

Session 7A
Chair: Zvi Galil

Speeding-up Linear Programming Using Fast Matrix Multiplication 332
P. Vaidya
A New Algorithm for Minimizing Convex Functions Over
Convex Sets 338
P. Vaidya
Asymptotically Fast Algorithms for Spherical and
Related Transforms 344
J. Driscoll and D. Healy, Jr.
Interior-Point Methods in Parallel Computation 350
A. Goldberg, S. Plotkin, D. Shmoys, and E. Tardos

Session 7B

Chair: Ray Strong

Polynomial End-To-End Communication 358
B. Awerbuch, Y. Mansour, N. Shavit
Network Decomposition and Locality in Distributed Computation 364
B. Awerbuch, M. Luby, A. Goldberg, and S. Plotkin
Upper and Lower Bounds for Routing Schemes in Dynamic Networks 370
M. Ricklin and Y. Afek
The Synchronization of Nonuniform Networks of Finite Automata 376
T. Jiang

Session 8A

Chair: Charles Leiserson

Expanders Might Be Practical: Fast Algorithms for Routing
Around Faults on Multibutterflies 384
T. Leighton and B. Maggs
Efficient Simulations of Small Shared Memories on
Bounded Degree Networks 390
K. Herley
On the Network Complexity of Selection 396
C.G. Plaxton
Power of Fast VLSI Models Is Insensitive to Wires' Thinness 402
G. Itkis and L. Levin

Session 8B

Chair: Mihalis Yannakakis

Towards Optimal Distributed Consensus 410
P. Berman, J. Garay, and K. Perry
Privacy and Communication Complexity 416
E. Kushilevitz
Solvability in Asynchronous Environments 422
B. Chor and L. Moscovici
Miltiparty Communication Complexity 428
D. Dolev and T. Feder

Session 9A
Chair: Robert Tarjan

Incremental Planarity Testing 436
G. Di Battista and R. Tamassia
Generating Random Spanning Trees 442
A. Broder
Using Cellular Graph Embeddings in Solving All Pairs
Shortest Path Problems 448
G. Frederickson
An Efficient Parallel Algorithm for the
Minimal Elimination Ordering (MEO) of an Arbitrary Graph 454
E. Dahlhaus and M. Karpinski

Session 9B
Chair: Charles Rackoff

On the Complexity of Space Bounded Interactive Proofs 462
A. Condon and R. Lipton
Multiparty Computation with Faulty Majority 468
D. Beaver and S. Goldwasser
Minimum Resource Zero-Knowledge Proofs 474
J. Kilian, S. Micali, and R. Ostrovsky
On the Power of 2-Way Probablistic Finite State Automata 480
C. Dwork and L. Stockmeyer

Session 10A
Chair: Frances Yao

Dynamically Computing the Maxima of Decomposable
Functions, with Applications 488
D. Dobkin, S. Suri
Stable Maintenance of Point Set Triangulations in
Two Dimensions 494
S. Fortune
Double Precision Geometry: A General Technique for Calculating
Line and Segment Intersections Using Rounded Arithmetic 500
V. Milenkovic
Area-Optimal Three-Layer Channel Routing 506
R. Duchem, D. Wagner, and F. Wagner

Session 10B
Chair: Juris Hartmanis

On the Computational Power of PP and $\oplus$P 514
S. Toda
An Analogue of the Myhill-Nerode Theorem and Its Use in Computing Finite-Basis Characterizations 520
M. Fellows and M. Langston
Conductance and Convergence of Markov Chains — A Combinatorial Treatment of Expanders 526
M. Mihail
Lower Bounds for Constant Depth Circuits in the Presence of Help Bits 532
J.-Y. Cai

Session 11A
Chair: Eric Bach

Randomized Search Trees 540
C. Aragon and R. Seidel
On the Complexity of a Game Related to the Dictionary Problem 546
K. Mehlhorn, S. Näher, and M. Rauch
Space-efficient Static Trees and Graphs 549
G. Jacobson
Twists, Turns, Cascades, Deque Conjecture, and Scanning Theorem 555
R. Sundar

Session 11B
Chair: Nicholas Pippenger

Probabilistic Communication Complexity of Boolean Relations 562
R. Raz and A. Wigderson
Subquadratic Simulations of Circuits byBranching Programs 568
J.-Y. Cai and R. Lipton
Constant Depth Circuits, Fourier Transform and Learnability 574
N. Linial, Y. Mansour, and N. Nisan
A Note on the Power of Threshold Circuits 580
E. Allender

Session 12A
Chair: Frances Yao

An Optimal Algorithm for Intersecting Three-Dimensional Convex Polyhedra 586
B. Chazelle
On Obstructions in Relation to a Fixed Viewpoint 592
K. Mulmuley
Output-Sensitive Hidden Surface Removal 598
M. Overmars and M. Sharir
Approximation Algorithms for Geometric Embeddings in the Plane with Applications to Parallel Processing Problems 604
M. Hansen

Session 12B
Chair: Ray Strong

An Optimal Lower Bound on the Number of Variables for Graph Identification 612
N. Immerman and J.-Y. Cai
On Reversal Complexity for Alternating TMs 618
M. Liskiewicz and K. Lorys
Every Polynomial-Time 1-Degree Collapses iff P = PSPACE 624
S. Fenner, S. Kurtz, and J. Royer

Author Index 631

Session 1A

Chair: Zvi Galil
Columbia University, Tel-Aviv University