ACM Symposium on Theory of Computing Proceedings of the ... annual ACM Symposium on Theory of Computing S&E Stacks
UC San Diego
Received on: 06-09-98



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



The Association for Computing Machinery 1515 Broadway New York New York 10036

Copyright 1997 by the Association for Computing Machinery, Inc.(ACM). Permission to make digital or hard work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists requires prior specific permission and/or a fee. Request permission to republish from: Publications Dept. ACM, Inc. Fax +1 (212) 869-0481 or permissions@acm.org> For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

ACM ISBN: 0-89791-888-6

Additional copies may be ordered prepaid from:

ACM Order Department

PO Box 12114 Church Street Station New York, NY 10257

Phone: 1-800-342-6626 (US and Canada) +1-212-626-0500 (all other countries) Fax: +1-212-944-1318 E-mail: acmpubs@acm.org ACM European Service Center 108 Cowley Road Oxford OX 4 1 JF UK

Phone: +44-1-865-382338 Fax: +44-1-865-381338 E-Mail: acm_europe@acm.org URL:http://www.acm.org

ACM Order Number: 508970

Printed in the USA



Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing

May 4 – 6, 1997, El Paso, Texas

TABLE OF CONTENTS

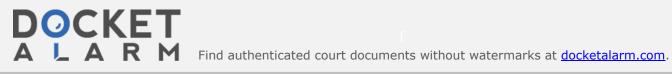
Sunday, May 4

Session 1A

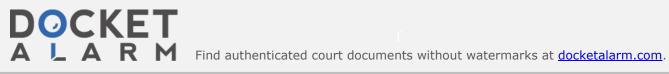
Some Optimal Inapproximability Results
A Complete Classification of the Approximability of Maximization Problems Derived from Boolean Constraint Satisfaction
When Hamming Meets Euclid: The Approximability of Geometric TSP and MST
Session 1B
Approximate Complex Polynomial Evaluation in Near Constant Work per Point
Fast and Precise Computations of Discrete Fourier Transforms Using Cyclotomic Integers
Quantum Computation of Fourier Transforms over Symmetric Groups
Session 2A
General Techniques for Comparing Unrooted Evolutionary Trees
Tree Pattern Matching and Subset Matching in Randomized $O(n \log^3 m)$ Time
Session 2B
Randomized $\Omega(n^2)$ Lower Bound for Knapsack
Exponential Lower Bounds for Depth 3 Boolean Circuits
Invited Session I
Algorithmic Complexity in Coding Theory and the Minimum Distance Problem
Session 3A
Approximating Total Flow Time on Parallel Machines
Non-Clairvoyant Multiprocessor Scheduling of Jobs with Changing Execution Characteristics



Better Bounds for Online Scheduling	. 130
Optimal Time-Critical Scheduling via Resource Augmentation	. 140
Session 3B	
Practical Loss-Resilient Codes	. 150
Spectral Techniques for Expander Codes	. 160
Faster Solution of the Key Equation for Decoding BCH Error-Correcting Codes	. 168
Fault Tolerant Quantum Computation with Constant Error Dorit Aharonov and Michael Ben-Or	176
Session 4A	
On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited	. 189
Reducing Randomness via Irrational Numbers	. 200
Is There an Algebraic Proof for $P \neq NC$?	210
P = BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma	220
$SL\subseteq L^{\frac{4}{3}}$	230
Session 4B	
Using Random Sampling to Find Maximum Flows in Uncapacitated Undirected Graphs	240
Combinatorial Complexity of the Central Curve Peter A. Beling and Sushil Verma	250
Approximation of k-Set Cover by Semi-Local Optimization	256
Approximation Algorithms for Facility Location Problems	265
Covering Points in the Plane by k -Tours: Towards a Polynomial Time Approximation Scheme for General k	275
Monday, May 5	
Session 5A	
A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence	284
Private Information Storage	294



Computationally Private Information Retrieval	04
Session 5B	
Approximating Hyper-Rectangles: Learning and Pseudo-Random Sets	14
A Composition Theorem for Learning Algorithms with Applications to Geometric Concept Classes 32 Shai Ben-David, Nader H. Bshouty and Eyal Kushilevitz	24
Using and Combining Predictors that Specialize	34
Session 6A	
On-Line Algorithms for Steiner Tree Problems	344
Online Algorithms for Selective Multicast and Maximal Dense Trees	354
Session 6B	
Direct Product Results and the GCD Problem, in Old and New Communication Models	363
The Linear-Array Problem in Communication Complexity Resolved	373
Invited Session II	
Paul Erdős (1913–1996): His Influence on the Theory of Computing	383
Session 7A	
Permanents, Pfaffian Orientations, and Even Directed Circuits	402
Property Testing in Bounded Degree Graphs	40€
Exploring Unknown Environments 4 Susanne Albers and Monika R. Henzinger	
On Floorplans of Planar Graphs	426
Session 7B	
Linear Zero-Knowledge — A Note on Efficient Zero-Knowledge Proofs and Arguments	430
Commodity-Based Cryptography	440
Oblivious Data Structures: Applications to Cryptography	450
Is Linear Hashing Good?	46:



DOCKET

Explore Litigation Insights



Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time** alerts and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

