

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](mailto: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](mailto: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 .....	1
<i>Johan Håstad</i>	
A Complete Classification of the Approximability of Maximization Problems Derived from Boolean Constraint Satisfaction .....	11
<i>Sanjeev Khanna, Madhu Sudan and David P. Williamson</i>	
When Hamming Meets Euclid: The Approximability of Geometric TSP and MST .....	21
<i>Luca Trevisan</i>	

#### Session 1B

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

#### Session 2A

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

#### Session 2B

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

#### Invited Session I

Algorithmic Complexity in Coding Theory and the Minimum Distance Problem .....	92
<i>Alexander Vardy</i>	

#### Session 3A

Approximating Total Flow Time on Parallel Machines .....	110
<i>Stefano Leonardi and Danny Raz</i>	
Non-Clairvoyant Multiprocessor Scheduling of Jobs with Changing Execution Characteristics .....	120
<i>Jeff Edmonds, Donald D. Chinn, Tim Brecht and Xiaotie Deng</i>	

4	Better Bounds for Online Scheduling .....	130
	<i>Susanne Albers</i>	
	Optimal Time-Critical Scheduling via Resource Augmentation .....	140
	<i>Cynthia A. Phillips, Cliff Stein, Eric Torng and Joel Wein</i>	
	<b>Session 3B</b>	
	Practical Loss-Resilient Codes .....	150
	<i>Michael G. Luby, Michael Mitzenmacher, M. Amin Shokrollahi, Daniel A. Spielman and Volker Stemann</i>	
	Spectral Techniques for Expander Codes .....	160
	<i>John D. Lafferty and Daniel N. Rockmore</i>	
	Faster Solution of the Key Equation for Decoding BCH Error-Correcting Codes .....	168
	<i>Victor Y. Pan</i>	
	Fault Tolerant Quantum Computation with Constant Error .....	176
	<i>Dorit Aharonov and Michael Ben-Or</i>	
	<b>Session 4A</b>	
	On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited .....	189
	<i>Moni Naor and Omer Reingold</i>	
	Reducing Randomness via Irrational Numbers .....	200
	<i>Zhi-Zhong Chen and Ming-Yang Kao</i>	
	Is There an Algebraic Proof for $P \neq NC$ ? .....	210
	<i>Ketan Mulmuley</i>	
	$P = BPP$ if $E$ Requires Exponential Circuits: Derandomizing the XOR Lemma .....	220
	<i>Russell Impagliazzo and Avi Wigderson</i>	
	$SL \subseteq L^{\frac{4}{3}}$ .....	230
	<i>Roy Armoni, Amnon Ta-Shma, Avi Wigderson and Shiyu Zhou</i>	
	<b>Session 4B</b>	
	Using Random Sampling to Find Maximum Flows in Uncapacitated Undirected Graphs .....	240
	<i>David Karger</i>	
	Combinatorial Complexity of the Central Curve .....	250
	<i>Peter A. Beling and Sushil Verma</i>	
	Approximation of $k$ -Set Cover by Semi-Local Optimization .....	256
	<i>Rong-chii Duh and Martin Fürer</i>	
	Approximation Algorithms for Facility Location Problems .....	265
	<i>David B. Shmoys, Éva Tardos and Karen Aardal</i>	
	Covering Points in the Plane by $k$ -Tours: Towards a Polynomial Time Approximation Scheme for General $k$ .....	275
	<i>Tetsuo Asano, Naoki Katoh, Hisao Tamaki and Takeshi Tokuyama</i>	
	<b>Monday, May 5</b>	
	<b>Session 5A</b>	
	A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence .....	284
	<i>Miklós Ajtai and Cynthia Dwork</i>	
	Private Information Storage .....	294
	<i>Rafail Ostrovsky and Victor Shoup</i>	

5	Computationally Private Information Retrieval . . . . .	304
	<i>Benny Chor and Niv Gilboa</i>	
<b>Session 5B</b>		
	Approximating Hyper-Rectangles: Learning and Pseudo-Random Sets . . . . .	314
	<i>Peter Auer, Philip M. Long and Aravind Srinivasan</i>	
	A Composition Theorem for Learning Algorithms with Applications to Geometric Concept Classes . . . . .	324
	<i>Shai Ben-David, Nader H. Bshouty and Eyal Kushilevitz</i>	
	Using and Combining Predictors that Specialize . . . . .	334
	<i>Yoav Freund, Robert E. Schapire, Yoram Singer and Manfred K. Warmuth</i>	
<b>Session 6A</b>		
	On-Line Algorithms for Steiner Tree Problems . . . . .	344
	<i>Piotr Berman and Chris Coulston</i>	
	Online Algorithms for Selective Multicast and Maximal Dense Trees . . . . .	354
	<i>Baruch Awerbuch and Tripurari Singh</i>	
<b>Session 6B</b>		
	Direct Product Results and the GCD Problem, in Old and New Communication Models . . . . .	363
	<i>Itzhak Parnafes, Ran Raz and Avi Wigderson</i>	
	The Linear-Array Problem in Communication Complexity Resolved . . . . .	373
	<i>Martin Dietzfelbinger</i>	
<b>Invited Session II</b>		
	Paul Erdős (1913–1996): His Influence on the Theory of Computing . . . . .	383
	<i>László Babai</i>	
<b>Session 7A</b>		
	Permanents, Pfaffian Orientations, and Even Directed Circuits . . . . .	402
	<i>William McCuaig, Neil Robertson, P. D. Seymour and Robin Thomas</i>	
	Property Testing in Bounded Degree Graphs . . . . .	406
	<i>Oded Goldreich and Dana Ron</i>	
	Exploring Unknown Environments . . . . .	416
	<i>Susanne Albers and Monika R. Henzinger</i>	
	On Floorplans of Planar Graphs . . . . .	426
	<i>Xin He</i>	
<b>Session 7B</b>		
	Linear Zero-Knowledge — A Note on Efficient Zero-Knowledge Proofs and Arguments . . . . .	436
	<i>Ronald Cramer and Ivan Damgård</i>	
	Commodity-Based Cryptography . . . . .	446
	<i>Donald Beaver</i>	
	Oblivious Data Structures: Applications to Cryptography . . . . .	456
	<i>Daniele Micciancio</i>	
	Is Linear Hashing Good? . . . . .	465
	<i>Noga Alon, Martin Dietzfelbinger, Peter Bro Miltersen, Erez Petrank and Gábor Tardos</i>	

# 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.