



**PROCEEDINGS OF THE THIRTIETH
ANNUAL ACM SYMPOSIUM ON
THEORY OF COMPUTING**

Dallas, Texas

May 23-26, 1998

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 1998 by the Association for Computing Machinery, Inc.(ACM).
Permission to make digital or hard copies of all or part of this work for
personal or classroom use is granted without fee provided that 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. 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: 0-89791-962-9

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 11414
Church Street Station
New York, NY 10286

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 Order Number: 508980
Printed in the USA

Conference Organization

QA
75.5
A14
1998

SIGACT Chair

Jeffrey Vitter

Conference Chairs

Wolf Bein

Steve Tate

Program Chairs

Fan Chung Graham

Treasurer

Lawrence Larmore

Publicity Chair

Ian Parberry

SIGACT Institutional Sponsors

Academic Press, Inc.

A T & T Laboratories

IBM Corporation — TJ Watson Research Center

International Thomson Publishing

Lucent Technologist-Bell Laboratories

Microsoft Research

PWS Publishing Co.

Xerox Corporation - Palo Alto Research Center

**Proceedings of the Thirtieth
Annual ACM Symposium on Theory of Computing**
May 23 – 26, 1998, Dallas, Texas, USA

TABLE OF CONTENTS

Sunday, May 24

Session 1A

- On the Limits of Non-Approximability of Lattice Problems 1
Oded Goldreich and Shafi Goldwasser
- The Shortest Vector Problem in L_2 is NP-Hard for Randomized Reductions 10
Miklós Ajtai
- Quantum Circuits with Mixed States 20
Dorit Aharonov, Alexei Kitaev and Noam Nisan

Session 1B

- Exact Sampling and Approximate Counting Techniques 31
Mark L. Huber
- A Polynomial Approximation Algorithm for the Minimum Fill-In Problem 41
Assaf Natanzon, Ron Shamir and Roded Sharan
- Improved Approximation Algorithms for MULTIWAY CUT 48
Gruia Călinescu, Howard Karloff and Yuval Rabani

Session 2A

- A Framework for Fast Quantum Mechanical Algorithms 53
Lov K. Grover
- Quantum vs. Classical Communication and Computation 63
Harry Buhrman, Richard Cleve and Avi Wigderson

Session 2B

- Finding Maximum Flows in Simple Undirected Graphs is Easier Than Bipartite Matching 69
David R. Karger and Matthew S. Levine
- Poly-logarithmic Deterministic Fully-dynamic Algorithms for Connectivity, Minimum Spanning tree, 2-edge and Biconnectivity 79
Jacob Holm, Kristian de Lichtenberg and Mikkel Thorup

Invited Session I

- Developments in Quantum Computing
Peter Shor

Session 3A	
Approximating the Bandwidth via Volume Respecting Embeddings	90
<i>Uriel Feige</i>	
Semi-definite Relaxations for Minimum Bandwidth and Other Vertex-ordering Problems	100
<i>Avrim Blum, Goran Konjevod, R. Ravi and Santosh Vempala</i>	
Approximation Schemes for the Euclidean k -medians and Related Problem.	106
<i>Sanjeev Arora, Prabhakar Raghavan and Satish Rao</i>	
Rounding via Tree: Deterministic Approximation Algorithms for Group Steiner Trees and k -median	114
<i>M. Charikar, C. Chekuri, A. Goel and S. Guha</i>	
Session 3B	
One Help-bit Doesn't Help	124
<i>Richard Beigel and Tirza Hirst</i>	
Perfect One-Way Probabilistic Hash Functions	131
<i>Ran Canetti, Daniele Micciancio and O. Reingold</i>	
Non-Interactive and Non-Malleable Commitment	141
<i>Giovanni Di Crescenzo, Yuval Ishai and Rafail Ostrovsky</i>	
Protecting Data Privacy in Private Information Retrieval Schemes	151
<i>Yael Gertner, Yuval Ishai, Eyal Kushilevitz and Tal Malkin</i>	
Session 4A	
On Approximating Arbitrary Metrics by Tree Metrics	161
<i>Yair Bartal</i>	
Trees and Euclidean Metrics	169
<i>Nathan Linial, Avner Magen and Michael Saks</i>	
Random Generation of Embedded Graphs and an Extension to Dobrushin Uniqueness	176
<i>Marcus Peinado and Thomas Lengauer</i>	
Efficient Algorithms for Constructing Fault Tolerant Geometric Spanners	186
<i>Christos Levcopoulos, Giri Narasimhan and Michiel Smid</i>	
Almost Optimal Dispersers	196
<i>Amnon Ta-Shma</i>	
Session 4B	
NP Might Not Be As Easy As Detecting Unique Solutions	203
<i>Richard Beigel, Harry Buhrman and Lance Fortnow</i>	
The Random Oracle Methodology, Revisited	209
<i>Ran Canetti, Oded Goldreich and Shai Halevi</i>	
Randomized Complexity Lower Bounds	219
<i>D. Grigoriev</i>	
Weak Alternating Automata and Tree Automata Emptiness	224
<i>Orna Kupferman and Moshe Vardi</i>	
Over Words, Two Variables Are as Powerful as One Quantifier Alternation: $FO^2 = \Sigma_2 \cap \Pi_2$...	234

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.