

# Program of the Thirty-Second Annual ACM Symposium on Theory of Computing

May 21-23, 2000, Portland, Oregon, USA

**Important Note** There will be a workshop on “Challenges for Theoretical Computer Science” on Saturday, May 20, the day before the STOC conference starts. Details will be posted on the SIGACT web page as they become available.

## Sunday, May 21, 2000

**Session 1A** Chair: *Frances Yao*

**8:30 am** Extractors and pseudo-random generators with optimal seed length

*Russell Impagliazzo, Ronen Shaltiel, and Avi Wigderson*

**8:55 am** Pseudo-random functions and factoring

*Moni Naor, Omer Reingold, and Alon Rosen*

**9:20 am** Satisfiability of equations in free groups is in PSPACE

*Claudio Gutiérrez*

**9:45 am** Setting 2 variables at a time yields a new lower bound for random 3-SAT

*Dimitris Achlioptas*

**Sessions 1B** Chair: *Ding-Zhu Du*

**8:30 am** A new algorithmic approach to the general Lovasz Local Lemma with applications to scheduling and satisfiability problems

*Artur Czumaj and Christian Scheideler*

**8:55 am** A deterministic polynomial-time algorithm for approximating mixed discriminant and mixed volume

*Leonid Gurvits and Alex Samorodnitsky*

**9:20 am** Randomized metarounding

*Robert Carr and Santosh Vempala*

**9:45 am** Isomorphism testing for embeddable graphs through definability

*Martin Grohe*

**Coffee Break 10:10 am - 10:30 am**

**Session 2A** Chair: *Frances Yao*

**10:30 am** Circuit minimization problem

*Valentine Kabanets and Jin-Yi Cai*

**10:55 am** On the efficiency of local decoding procedures for error-correcting codes

*Jonathan Katz and Luca Trevisan*

**11:20 am** Statistical mechanics, three-dimensionality and NP-completeness

*Sorin Istrail*

**Session 2B** Chair: *Ding-Zhu Du*

**10:30 am** A combinatorial, strongly polynomial-time algorithm for minimizing submodular functions

*Satoru Iwata and Lisa Fleischer and Satoru Fujishige*

**10:55 am** Improved algorithms for submodular function minimization and submodular flow

*Lisa Fleischer and Satoru Iwata*

**11:20 am** On dual minimum cost flow algorithms

*Jens Vygen*

**Lunch 11:50 am**

**1:20 pm Invited Session:** Some Problems Related to Content Distribution

*Tom Leighton, Department of Mathematics, MIT, and Akamai Technologies*

**Session 3A** Chair: *Steven Rudich*

**2:20 pm** On the approximability of the traveling salesman problem

*Christos H Papadimitriou and Santosh Vempala*

**2:45pm** Approximating the domatic number

*Uriel Feige, Magnús M Halldórsson, and Guy Kortsarz*

**3:10 pm** The value of strong inapproximability results for clique

*Aravind Srinivasan*

**Sessions 3B** Chair: *Éva Tardos*

**2:20 pm** Compression using efficient multicasting

*Micah Adler and Tom Leighton*

**2:45 pm** The small-world phenomenon: an algorithmic perspective

*Jon Kleinberg*

**3:10 pm** A random graph model for massive graphs

*William Aiello, Fan Chung, and Linyuan Lu*

**Coffee Break 3:35 - 3:55 pm**

**Session 4A** Chair: *Steven Rudich*

**3:55 pm** List decoding algorithms for certain concatenated codes

*Venkatesan Guruswami and Madhu Sudan*

**4:20 pm** A PCP characterization of NP with optimal amortized query complexity

*Alex Samorodnitsky and Luca Trevisan*

**4:45 pm** On transformations of interactive proofs that preserve the prover's complexity

*Salil Vadhan*

**Sessions 4B** Chair: *Éva Tardos*

**3:55 pm** On the sum-of-squares algorithm for bin packing

*János Csirik, David S Johnson, Claire Kenyon, James B Orlin, Peter W Shor, and Richard R Weber*

**4:20 pm** Sharing the cost of multicast transmissions

*Joan Feigenbaum, Christos Papadimitriou, and Scott Shenker*

**4:45 pm** The risk profile problem for stock portfolio optimization

*Ming-Yang Kao and Andreas Nolte and Stephen R Tate*

**Monday, May 22, 2000**

**Session 5A** Chair: *Rafail Ostrovsky*

**8:30 am** Resettable zero-knowledge

*Ran Canetti, Oded Goldreich, Shafi Goldwasser and Silvio Micali*

**8:55 am** Complete characterization of security notions for probabilistic private-key encryption

*Jonathan Katz and Moti Yung*

**9:20 am** On zero-knowledge proofs: “from membership to decision”

*Giovanni Di Crescenzo, Kouichi Sakurai, and Moti Yung*

**9:45 am** Finding smooth integers in short intervals using CRT decoding

*Dan Boneh*

**Sessions 5B** Chair: *David Eppstein*

**8:30 am** Smoothing and cleaning up slivers

*Herbert Edelsbrunner, Xiang-Yang Li, Garry Miller, Andreas Stathopoulos, Dafna Talmor, Shang-Hua Teng, Alper Üngör, and Noel Walkington*

**8:55 am** Hard-potato routing

*Costas Busch, Maurice Herlihy, and Roger Wattenhofer*

**9:20 am** Approximation algorithms for geometric shortest path problems

*Lyudmil Aleksandrov, Anil Maheshwari, and Jörg-Rüdiger Sack*

**9:45 am** Improved approximations of crossings in graph drawings and VLSI layout areas

*Guy Even, Sudipto Guha, and Baruch Schieber*

**Coffee Break 10:10 am - 10:30 am**

**Sessions 6A** Chair: *Rafail Ostrovsky*

**10:30 am** On the decidability of accessibility problems

*Rajeev Motwani, Rina Panigrahy, Vijay Saraswat, and Suresh Venkatasubramanian*

**10:55 am** More general completeness theorems for secure two-party computation

*Joe Kilian*

**11:20 am** On the complexity of verifiable secret sharing and multiparty computation

*Ronald Cramer, Ivan Damgård, and Stefan Dziembowski*

**Session 6B:** *David Eppstein*

**10:30 am** Tight(er) worst-case bounds on dynamic searching and priority queues

*Arne Andersson and Mikkel Thorup*

**10:55 am** Near-optimal fully-dynamic graph connectivity

*Mikkel Thorup*

**11:20 am** A new NC-algorithm for finding a perfect matching in bipartite planar and small genus graphs

*Meena Mahajan and Kasturi R Varadarajan*

**Lunch 11:50 am**

**Session 7A** Chair: *Sally Goldman*

**1:20 pm** Space complexity in propositional calculus

*Michael Alekhnovich, Eli Ben-Sasson, Alexander A Razborov, and Avi Wigderson*

**1:45 pm** A new proof of the weak pigeonhole principle

*Alexis Maciel, Toniann Pitassi, and Alan R Woods*

**2:10 pm** Higher lower bounds on monotone size

*Danny Harnik and Ran Raz*

**2:35 pm** Tighter lower bounds for nearest neighbor search and related problems in the cell probe model

*Omer Barkol and Yuval Rabani*

**Sessions 7B** Chair: *Pavel Pevzner*

**1:20 pm** Compressed suffix arrays and suffix trees with applications to text indexing and string matching

*Roberto Grossi and Jeffrey Scott Vitter*

**1:45 pm** Faster suffix tree construction with missing suffix links

*Richard Cole and Ramesh Hariharan*

**2:10 pm** Approximate nearest neighbors and sequence comparison with block operations

*S Muthukrishnan and Suleyman Cenk Sahinalp*

**2:35 pm** Near optimal multiple alignment within a band in polynomial time

*Ming Li, Bin Ma, and Lusheng Wang*

**Coffee Break 3:00 - 3:20 pm**

**Sessions 8A** Chair: *Sally Goldman*

**3:20 pm** Noise-tolerant learning, the parity problem, and the statistical query model

*Avrim Blum and Adam Kalai and Hal Wasserman*

**3:45 pm** More theory revision with queries

*Judy Goldsmith and Robert H Sloan*

**4:10 pm** Are bitvectors optimal?

*H Buhrman and PB Miltersen and J Radhakrishnan and S Venkatesh*

**Sessions 8B** Chair: *Pavel Pevzner*

**3:20 pm** The program-size complexity of self-assembled squares

*Paul W K Rothmund and Erik Winfree*

**3:45 pm** Shortest path queries in planar graphs

*Danny Z Chen and Jinhui Xu*

**4:10 pm** How tall is a tree?

*Bruce Reed*

## **Tuesday, May 23, 2000**

**Session 9A** Chair: *Eli Upfal*

**8:30 am** Random walks with “back buttons”

*Ronald Fagin, Anna Karlin, Jon Kleinberg, Prabhakar Raghavan, Sridhar Rajagopalan, Ronitt Rubinfeld, Madhu Sudan, and Andrew Tomkins*

**8:55 am** From partial consistency to global broadcast

*Matthias Fitzi and Ueli Maurer*

**9:20 am** Connectivity and inference problems for temporal networks

*David Kempe, Jon Kleinberg, and Amit Kumar*

**9:45 am** Strictly non-blocking WDM cross-connects for heterogeneous networks

*April Rasala and Gordon Wilfong*

**Sessions 9B** Chair: *Sanjeev Khanna*

**8:30 am** Finding long paths and cycles in sparse Hamiltonian graphs

*Tomas Feder, Rajeev Motwani, and Carlos Subi*

**8:55 am** Approximating the minimum bisection size

*Uriel Feige, Robert Krauthgamer, and Kobbi Nissim*

**9:20 am** A matter of degree: Improved approximation algorithms for degree-bounded minimum spanning trees

*J Könemann and R Ravi*

**9:45 am** Clustering for edge-cost minimization

*Leonard J Schulman*

**Coffee Break 10:10 am - 10:30 am**

**Sessions 10A** Chair: *Eli Upfal*

**10:30 am** Exact computation of the inertia of symmetric integer matrices

*Steven Fortune*

**10:55 am**  $\epsilon$ -optimization schemes and  $L$ -bit precision: alternative perspectives in combinatorial optimization

*James B Orlin, Andreas S Schulz, and Sudipta Sengupta*

**11:20 am** Matrix-vector product for confluent Cauchy-like matrices with application to confluent rational interpolation

*Vadim Olshevsky and Amin Shokrollahi*

**Session 10B** Chair: *Sanjeev Khanna*

**10:30 am** Query strategies for priced information

*Moses Charikar, Ron Fagin, Venkatesan Guruswami, Jon Kleinberg, Prabhakar Raghavan, and Amit Sahai*

**10:55 am** A guessing game and randomized online algorithms

*Steven S Seiden*

**11:20 am** Computing the median with uncertainty

*Tomas Feder, Rajeev Motwani, Rina Panigrahy, Chris Olston, and Jennifer Widom*

**Lunch 11:50 am**

**Session 11A** Chair: *Charles Bennett*

**1:20 pm** Parallelization, amplification, and exponential time simulation of quantum interactive proof systems

*Alexei Kitaev and John Watrous*

**1:45 pm** Rapid sampling through quantum computing

*Lov K Grover*

**2:10 pm** Normal subgroup reconstruction and quantum computation using group representations

*Sean Hallgren, Alexander Russell, and Amnon Ta-Shma*

**2:35 pm** Quantum lower bounds by quantum arguments

*Andris Ambainis*

**3:00 pm** On quantum and probabilistic communication: Las Vegas and one-way protocols

*Hartmut Klauck*

**Sessions 11B** Chair: *Andrei Broder*

**1:20 pm** A constant factor approximation algorithm for a class of classification problems

*Anupam Gupta and Éva Tardos*

**1:45 pm** Polynomial-time approximation scheme for data broadcast

*Claire Kenyon, Nicolas Schabanel, and Neal Young*

**2:10 pm** Approximating permanents of complex matrices

*Martin Fürer*

**2:35 pm** Combining fairness with throughput: Online routing with multiple objectives

*Ashish Goel, Adam Meyerson, and Serge Plotkin*

**3:00 pm** Improvements in throughput maximization for real-time scheduling

*Piotr Berman and Bhaskar DasGupta*

**Coffee Break 3:25 - 3:40 pm**

**Session 12A** Chair: *Charles Bennett*

**3:40 pm** Self-testing of universal and fault-tolerant sets of quantum gates

*Wim van Dam, Frédéric Magniez, Michele Mosca, and Miklos Santha*

**4:05 pm** Computing with highly mixed states

*Andris Ambainis, Leonard J Schulman, and Umesh V Vazirani*

**4:30 pm** Quantum bit escrow

*Dorit Aharonov, Amnon Ta-Shma, Umesh Vazirani and Andrew C Yao*

**4:55 pm** A proof of security of quantum key distribution

*Eli Biham, Michel Boyer, P Oscar Boykin, Tal Mor, and Vwani Roychowdhury*

**Sessions 12B** Chair: *Andrei Broder*

**3:40 pm** Better algorithms for unfair metrical task systems and applications

*Amos Fiat and Manor Mendel*

**4:05 pm** A unified approach to approximating resource allocation and scheduling

*Amotz Bar-Noy, Reuven Bar-Yehuda, Ari Freund, Joseph (Seffi) Naor, and Baruch Schieber*

**4:30 pm** Balanced allocations: the heavily loaded case

*Petra Berenbrink, Artur Czumaj, Angelika Steger, Berthold Vöcking*

**End of Program**