Twentieth Annual ACM Symposium on Theory of Computing

May 2–4, 1988
Hilton Hyde Park
University of Chicago

TECHNICAL PROGRAM

Sunday, May 1, 1988

Reception: 7:30—10:30 pm, at the Hilton.

Monday, May 2, 1988

Session 1: 9—10:20 am. Chair: Andrew Odlyzko

Completeness Theorem's for Non-Cryptographic Fault-Tolerant Distributed Computation. Michael Ben-Or, Hebrew University, Shafi Goldwasser, MIT, and Avi Wigderson, Hebrew University.

Multiparty Unconditionally Secure Protocols. David Chaum, Centre for Mathematics and Computer Science, Claude Crepeau, MIT, and Ivaa Damgard, Aarhus Universitet.

On the Power of Oblivious Transfer. Joe Kilian, MIT.

How to Sign Given Any Trapdoor Function. Mihir Bellare and Silvio Micali, MIT.

Coffee Break: 10:20—10:50 am

Session 2: 10:50 am—12:30 pm. Chair: Nancy Lynch

A Tradeoff Between Space and Efficiency for Routing Tables. David Peleg, Stanford University, and Eli Upfal, IBM Almaden.

Reasoning About Knowledge and Time in Asynchronous Systems. Joseph Halpern and Moshe Vardi, IBM Almaden.

Investigations of Fault-Tolerant Networks of Computers. Piotr Berman, Penn State University, and János Simon, University of Chicago.

Toward a Non-Atomic Era: l-Exclusion as a Test Case. Danny Dolev, IBM Almaden and Hebrew University, Eli Gafni, UCLA, and Nir Shavit, Hebrew University.

A Time-Randomness Tradeoff for Oblivious Routing. Danny Krizanc, Harvard University, David Peleg, Stanford University, and Eli Upfal, IBM Almaden.

Lunch: 12:30—2 pm

Session 3: 2—5:30 pm. Chair: TBA

Non-Interactive Zero-Knowledge and its Applications. Manuel Blum, University of California, Berkeley, Paul Feldman and Silvio Micali, MIT.

Multi-Prover Interactive Proofs: How to Remove Intractability. Michael Ben-Or, Hebrew University, Shafi Goldwasser, MIT, Joe Kilian, MIT, and Avi Widgerson, Hebrew University.

A Knowledge-Based Analysis of Zero Knowledge. Joseph Halpern, IBM Almaden, Yoram Moses, Weizmann Institute, and Mark Tuttle, MIT.

From Scratch to Byzantine Agreement in Constant Expected Time. Paul Feldman and Silvio Micali, MIT.

Coffee Break: 3:20—3:50 pm

Session 4: 3:50—5:30 pm. Chair: TBA

On Different Modes of Communication. Bernd Halstenberg and Rudiger Reischuk, Technische Hochschule Darmstadt.

Virtual Memory Algorithms. Alok Aggarwal and Ashok Chandra, IBM Yorktown Heights.

On the Communication Complexity of Graph Properties. András Hajnal, University of Illinois at Chicago and Hungarian Academy of Sciences, Wolfgang Maass, University of Illinois at Chicago, and György Turán, University of Illinois at Chicago and Hungarian Academy of Sciences.

Optimal Simulations by Butterfly Networks. Sandeep Bhatt, Yale University, Fan Chung, BellCore, Jia-Wei Hong, Beijing Computer Institute and Courant Institute of NYU, Tom Leighton, MIT, and Arnold Rosenberg, University of Massachusetts at Amherst.

Energy Consumption in VLSI Circuits. Alok Aggarwal, Ashok Chandra, and Prabhakar Raghavan, IBM Yorktown Heights.

Business Meeting: 8:30 pm, at the Hilton.

Tuesday, May 3, 1988

Session 5: 9—10:20 am. Chair: TBA

Random Instances of a Graph Coloring Problem are Hard. Ramarathnam Venkatesan and Leonid Levin, Boston University.

Expressing Combinatorial Optimization Problems by Linear Programs. Mihalis Yannakakis, AT&T Bell Labs, Murray Hill.

Optimization, Approximation, and Complexity Classes. Christos Papadimitriou, University of California, San Diego, and Mihalis Yannakakis, AT&T Bell Labs, Murray Hill.

Conductance and the Rapid Mixing Property for Markov Chains: the Approximation of the Permanent Resolved. Mark Jerrum and Alistair Sinclair, University of Edinburgh.

Coffee Break: 10:20—10:50 am

Session 6: 10:50 am—12:30 pm. Chair: TBA

Relativized Polynomial Time Hierarchies Having Exactly K Levels. Ker-I Ko, SUNY at Stony Brook.

Computing Algebraic Formulas with a Constant Number of Registers. Richard Cleve, University of Toronto.

On the Power of White Pebbles. Balasubramanian Kalyanasundaram and George Schnitger, Penn State University.

Learning in the Presence of Malicious Errors. Michael Kearns and Ming Li, Harvard University.

Nondeterministic Linear Tasks May Require Substantially Nonlinear Deterministic Time in the Case of Sublinear Work Space. Yuri Gurevich and Saharon Shelah, University of Michigan.

Lunch: 12:30—2 pm

Session 7: 2—3:20 pm. Chair: TBA

A Randomized Parallel Branch-and-Bound Procedure. Richard Karp and Yanjun Zhang, University of California, Berkeley.

Randomized Algorithms and Pseudorandom Numbers. Howard Karloff, University of Chicago, and Prabhakar Raghavan, IBM Yorktown Heights.

A Deterministic Algorithm for Sparse Multivariate Polynomial Interpolation. Michael Ben-Or, Hebrew University, and Prasoon Tiwari, IBM Yorktown Heights.

Competitive Algorithms for On-line Problems. Mark Manasse, DEC Systems Research Center, Lyle McGeoch, Amherst College, and Daniel Sleator, Carnegie-Mellon University.

Coffee Break: 3:20—3:50 pm

Session 8: 3:50—5:30 pm. Chair: Herbert Edelsbrunner

Implicit Representation of Graphs. Sampath Kannan, Moni Naor, and Steven Rudich, University of California, Berkeley.

Storing and Searching a Multikey Table. Amos Fiat and Moni Naor, University of California, Berkeley, Alexandro Schäffer, Stanford University, Jeanette Schmidt and Alan Siegel, Courant Institute of NYU.

More Analysis of Double Hashing. George Lueker and Mariko Molodowitch, University of California, Irvine.

Linearity and Unprovability of Set Union Problem. Martin Loebl and Jaroslav Nešetřil, Charles University and Universität Bonn.

Non-Oblivious Hashing. Amos Fiat and Moni Naor, University of California, Berkeley, Jeanette Schmidt and Alan Siegel, Courant Institute of NYU.

Blues Concert: 8—11pm, Mandel Hall, Univ. of Chicago.

Wednesday, May 4, 1988

Session 9: 9—10:20 am. Chair: Greg Frederickson

A Faster Strongly Polynomial Minimum Cost Flow Algorithm. James Orlin, MIT.

Finding Minimum-Cost Circulations by Canceling Negative Cycles. Andrew Goldberg, Stanford University, and Robert Tarjan, Princeton University and AT&T Bell Labs, Murray Hill.

Detecting Cycles in Dynamic Graphs in Polynomial Time. S. Rao Kosaraju and Gregory Sullivan, Johns Hopkins University.

An Efficient Matroid Partitioning Algorithm and Applications. Harold Gabow and Herbert Westermann, University of Colorado at Boulder.

Coffee Break: 10:20—10:50 am

Session 10: 10:50 am—12:30 pm. Chair: John Reif

Geometry Helps in Matching. Pravin Vaidya, AT&T Bell Labs, Murray Hill.

Small Sets Supporting Fary Embeddings of Planar Graphs. Hubert de Fraysseix, CNRS, János Pach, Hungarian Academy of Sciences, and Richard Pollack, Courant Institute of NYU.

Optimal Algorithms for Approximate Clustering. Tomás Feder, Stanford University, and Daniel Greene, Xerox PARC.

Planning Constrained Motion. Steven Fortune and Gordon Wilfong, AT&T Bell Labs, Murray Hill.

Some Algebraic and Geometric Computations in P-SPACE. John Canny, University of California, Berkeley.

Lunch: 12:30—2 pm

Session 11: 2—3:20 pm. Chair: Jeffrey Ullman

Lower Bounds on the Complexity of Graph Properties. Valerie King, University of California, Berkeley.

Decidable Optimization Problems for Database Logic Programs. Stavros Cosmadakis, IBM Yorktown Heights, Haim Gaifman, Hebrew University, Paris Kanellakis, Brown University, and Moshe Vardi, IBM Almaden.

Polynomial Universal Traversing Sequences for Cycles Are Constructible. Sorin Istrail, Wesleyan University.

Two Infinite Sets of Primes with Fast Primality Tests. János Pintz, Hungarian Academy of Sciences, William Steiger, Rutgers University, and Endre Szemerédi, Rutgers University and Hungarian Academy of Sciences.

Coffee Break: 3:20—3:50 pm

Session 12: 3:50—5:10 pm. Chair: Richard Cole

Towards an Architecture-Independent Analysis of Parallel Algorithms. Christos Papadimitriou, University of California, San Diego, and Mihalis Yannakakis, AT&T Bell Labs, Murray Hill.

Almost-Optimum Speed-ups of Algorithms for Matching and Related Problems. Harold Gabow, University of Colorado at Boulder, and Robert Tarjan, Princeton University and AT&T Bell Labs, Murray Hill.

Using Smoothness to Achieve Parallelism. Leonard Adleman and Kireeti Kompella, University of Southern California.

Monotone Circuits for Connectivity Require Super-logarithmic Depth. Mauricio Karchmer and Avi Wigderson, Hebrew University.