15th Annual ACM Symposium on Theory of Computing
April 25-27, 1983
57 Park Plaza Hotel
Boston, Massachusetts

Conference Information

PREREGISTRATION FORM

Use this form or a facsimile to preregister. Advance registration closes April 10. Preregistration by mail after April 10 is subject to a late fee. Registration after April 21 or at the conference site is subject to a larger* late fee.

Please mail form with check (drawn on US bank) or money order (in US funds) payable to 1983 ACM STOC to:

STOC REGISTRATION
c/o Professor Albert R. Meyer
M.I.T. Laboratory for Computer Science
545 Technology Square, NE43-801
Cambridge, MA 02139

Rates for registration:

Member of ACM, SIGACT, or IEEE Computer Society $110.00
Non-Member 135.00
Author or Committee Member 100.00
Student** 30.00
Extra banquet tickets @$27.00 30.00
Non-student late fee (after April 10 until April 21)* 30.00
Student late fee (after April 10) 10.00

Total enclosed

*NOTE: Registration fee at the conference site is $170 for all non-student registrants.

I would like assistance with day care

yes   no

Name_________________________ (Print last name first)

Affiliation__________________________________________________________

Address__________________________________________________________

City________________________ State________ Zip__________

Country (if other than USA)_______________________________________

**Student registration includes technical sessions, conference proceedings, reception, and coffee breaks; does not include luncheons or banquet.

Requests for special dietary considerations should accompany this registration form. Requests for refunds will be honored until April 21.

HOTEL RESERVATION FORM

Mail before April 4, 1983 to:

1983 ACM STOC
The 57 Park Plaza Hotel/Howard Johnson
57 Building
200 Stuart Street
Boston, MA 02116

Reservation Desk Phone: (617) 482-7352 (or 3)

Please reserve a room for me at the 15th Annual ACM-SIGACT Symposium on Theory of Computing, Sunday April 24 through Wednesday April 27, 1983.

____ Single $75.00 per day
____ Double $85.00 per day

(Rates subject to 5.7% sales tax.)

Arrival date______________ time________
Departure date______________ time________

Send me confirmation at:

Name_________________________ (Please print full name)

Address__________________________________________________________

City________________________ State________ Zip__________

Country (if other than USA)_______________________________________

For arrivals after 6PM, the hotel requests that arrival be guaranteed by providing a major credit card number, company name, or personal check for one night’s deposit.
Program - 15th STOC

Sunday April 24
- Registration 5:00 pm - 10:00 pm (6th Floor)
- Reception 7:30 pm - 10:30 pm (Ballroom 1, Mezzanine)

Session I: Monday Morning, 9:20AM - 12:30PM
Convention Hall A, 6th floor
Chair: W. L. Ruzzo, Univ. of Washington

9:20 An O(nlog n) Sorting Network
M. Ajtai, J. Komlos, E. Szemeredi
Budapest Academy of Sciences, UC San Diego, Univ. of South Carolina

9:40 A Logarithmic Time Sort for Linear Size Networks
J.H. Reif, L.G. Valiant - Harvard Univ.

10:00 Parallel Algorithms for Algebraic Problems
J. von zur Gathen - Univ. of Toronto

10:20 COFFEE BREAK
Convention Hall B, 6th floor

10:50 Topological Matching
Q. F. Stout - SUNY Binghamton

11:10 Reliable Computation with Cellular Automata
P. Gacs - Univ. of Rochester

11:30 Superconcentrators, Generalizers and Generalized Connectors with Limited Depth
D. Dolev, C. Dwork, N. Pippenger, A. Wigderson
Hebrew Univ., Cornell Univ., IBM San Jose, Princeton Univ.

11:50 Unbounded Fan-In Circuits and Associative Functions
A. K. Chandra, S. Fortune, R. Lipton
IBM Yorktown Hts., IBM Yorktown Hts., Princeton Univ.

12:10 Borel Sets and Circuit Complexity
M. Sipser - MIT

12:30 LUNCH
Ballrooms 1 and 2, located on the Mezzanine

Session II: Monday Afternoon, 2:00PM - 5:30PM
Convention Hall A, 6th floor
Chair: M. L. Fredman, UC San Diego

2:00 A Polynomial Linear Search Algorithm for the n-Dimensional Knapsack Problem
F. Meyer auf der Heide - Johann Wolfgang Goethe Univ.

2:20 Lower Bounds for Algebraic Computation Trees
M. Ben-Or - MIT and Hebrew Univ.

2:40 Bounds for Width-Two Branching Programs
A. Borodin, D. Dolev, F. Fich, W. Paul
Univ. of Toronto, Hebrew Univ., IBM San Jose, IBM San Jose

3:00 Multi-Party Protocols
A. K. Chandra, M. L. Furst, R. J. Lipton

3:20 New Bounds for Parallel Prefix Circuits
F. Fich - UC Berkeley and IBM San Jose

3:40 COFFEE BREAK
Convention Hall B, 6th floor

4:10 Exponential Lower Bounds for Restricted Monotone Formulae
L. G. Valiant - Harvard Univ.

4:30 The Complexity of Approximate Counting
L. Stockmeyer - IBM San Jose

4:50 Two Nonlinear Lower Bounds
P. Dursa, Z. Galil, W. Paul, R. Reischuk
Slovak Academy of Science, Columbia Univ. and Tel-Aviv Univ., IBM San Jose, Univ. of the Saarlandes

5:10 On Notions of Information Transfer in VLSI Circuits
A. V. Aho, J. D. Ullman, M. Yannakakis
Bell Labs Murray Hill, Stanford Univ., Bell Labs Murray Hill

5:30 End of Session

9:00 BUSINESS MEETING
Convention Hall A, 6th floor
Session III: Tuesday Morning, 9:00 AM - 12:30 PM
Convention Hall A, 6th floor
Chair: D.S. Johnson, Bell Labs, Murray Hill

9:00 Solvability by Radicals is in Polynomial Time
S. Landau, G. L. Miller - MIT

9:20 On the Diameter of Permutation Groups

9:40 Normal Forms for Trivalent Graphs
M. Furer, W. Schnyder, E. Specker
Univ. Zurich, ETH Zurich, ETH Zurich

10:00 Canonical Labeling of Graphs

10:20 COFFEE BREAK
Convention Hall B, 6th floor

10:50 How to Generate Random Integers with Known Factorization
E. Bach - UC Berkeley

11:10 Factoring Multivariate Polynomials over a Finite Field
A. K. Lenstra - Mathematical Centrum

11:30 Improved Algorithms for Integer Programming and Related Lattice Problems
R. Kannan - MIT

11:50 Retraction: A New Approach to Motion-Planning
C. O'Dunlaing, M. Sharir, C. K. Yap
NY Univ., Tel-Aviv Univ., NY Univ.

12:10 Primitives for the Manipulation of Planar Subdivisions and the Computation of Voronoi Diagrams
L. J. Guibas, J. Stolfi - Xerox PARC, Stanford Univ.

12:30 LUNCH
Ballrooms 1 and 2, located on the Mezzanine

Session IV: Tuesday Afternoon, 2:00 PM - 5:50 PM
Convention Hall A, 6th floor
Chair: D. Harel, Weizmann Institute

2:00 Self-Adjusting Binary Trees
D. D. Sleator, R. E. Tarjan - Bell Labs Murray Hill

2:20 A Linear-Time Algorithm for a Special Case of Disjoint Set Union
H. N. Gabow, R. E. Tarjan
Univ. of Colorado, Bell Labs Murray Hill

2:40 Data Structures for On-Line Updating of Minimum Spanning Trees
G. N. Frederickson - Purdue Univ.

3:00 New Results on Range Queries
F. F. Yao - Xerox PARC

3:20 Unary Inclusion Dependencies Have Polynomial Time Inference Problems
P. C. Kanellakis, S. S. Cosmadakis, M. Y. Vardi
Brown Univ., MIT, Stanford Univ.

3:40 COFFEE BREAK
Convention Hall B, 6th floor

4:10 On the Extremely Fair Treatment of Probabilistic Algorithms
A. Pnueli - Weizmann Institute and Harvard Univ.

4:30 A Probabilistic PDL
D. Kozen - IBM Yorktown Hts.

4:50 A Decidable Propositional Probabilistic Dynamic Logic
Y. A. Feldman - Weizmann Institute

5:10 A Logic to Reason about Likelihood
J. Y. Halpern, M. O. Rabin
IBM San Jose, Harvard Univ. and Hebrew Univ.

5:30 A Characterization of Hoare's Logic for Programs with Pascal-Like Procedures
E-R. Olderog - Univ. Kiel

5:50 End of session

6:30 Buses depart from hotel for the BANQUET at the New England Aquarium
Session VI: Wednesday Morning, 9:00AM - 12:30PM  Convention Hall A, 6th floor
Chair: J. Seiferas, Univ. of Rochester

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00</td>
<td>A Complexity Theoretic Approach to Randomness</td>
<td>M. Sipser - MIT</td>
</tr>
<tr>
<td>9:20</td>
<td>Speedups of Deterministic Machines by Synchronous Parallel Machines</td>
<td>P. W. Dymond, M. Tompa</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UC San Diego and Univ. of Waterloo, Univ. of Washington</td>
</tr>
<tr>
<td>9:40</td>
<td>Alternation and the Power of Nondeterminism</td>
<td>R. Kannan - MIT</td>
</tr>
<tr>
<td>10:00</td>
<td>Languages which Capture Complexity Classes</td>
<td>N. Immerman - Tufts Univ.</td>
</tr>
<tr>
<td>10:20</td>
<td>COFFEE BREAK</td>
<td>Convention Hall B, 6th floor</td>
</tr>
<tr>
<td>10:50</td>
<td>The Random Access Hierarchy</td>
<td>D. Myers - Univ. of Hawaii</td>
</tr>
<tr>
<td>11:10</td>
<td>Iterated Pushdown Automata and Complexity Classes</td>
<td>J. Engelfriet - Twente Univ. of Technology</td>
</tr>
<tr>
<td>11:50</td>
<td>On Sparse Sets in NP-P: EXPTIME vs NEXPTIME</td>
<td>J. Hartmanis, N. Immerman, V. Sewelson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cornell Univ., Tufts Univ., Cornell Univ.</td>
</tr>
<tr>
<td>12:10</td>
<td>Some Structural Properties of Polynomial Reducibilities and Sets in NP</td>
<td>P. Young - Purdue Univ.</td>
</tr>
<tr>
<td>12:30</td>
<td>LUNCH</td>
<td>Convention Hall B and C, 6th floor</td>
</tr>
</tbody>
</table>

Session VI: Wednesday Afternoon, 2:00PM - 5:30PM  Convention Hall A, 6th floor
Chair: R. L. Rivest, MIT

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:00</td>
<td>On Breaking the Iterated Merkle-Hellman Public Key Cryptosystem</td>
<td>L. M. Adleman - Univ. of Southern California and MIT</td>
</tr>
<tr>
<td>2:40</td>
<td>On the Cryptographic Security of Single RSA Bits</td>
<td>M. Ben-Or, B. Chor, A. Shamir</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MIT, MIT, Weizmann Institute</td>
</tr>
<tr>
<td>3:00</td>
<td>Strong Signature Schemes and Authentications</td>
<td>S. Goldwasser, S. Micali, A. Yao</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UC Berkeley, Univ. of Toronto, Stanford Univ.</td>
</tr>
<tr>
<td>3:20</td>
<td>How to Exchange (Secret) Keys</td>
<td>M. Blum - UC Berkeley</td>
</tr>
<tr>
<td>3:40</td>
<td>COFFEE BREAK</td>
<td>Convention Hall B, 6th floor</td>
</tr>
<tr>
<td>4:10</td>
<td>An Efficient Reduction Technique for Degree-Constrained Subgraph and Bidirected Network Flow Problems</td>
<td>H. N. Gabow - Univ. of Colorado</td>
</tr>
<tr>
<td>4:30</td>
<td>Transitive Orientation in O(n^2) Time</td>
<td>J. Siparud - Georgia Institute of Technology</td>
</tr>
<tr>
<td>4:50</td>
<td>Probabilistic Analysis of Bandwidth Minimization Algorithms</td>
<td>J. Turner - Bell Labs Naperville</td>
</tr>
<tr>
<td>5:10</td>
<td>An Approximation Algorithm for Manhattan Routing</td>
<td>B. S. Baker, S. N. Bhatt, F. T. Leighton</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bell Labs Murray Hill, MIT, MIT</td>
</tr>
</tbody>
</table>