**Committees**

**PROGRAM COMMITTEE**
Scott Baden  
University of California at San Diego  
Giandomenico Ciardo  
College of William and Mary  
Chita Das  
Purdue University  
Peter Denning  
University of Southern California  
David Dewitt  
University of Wisconsin  
Carla Fisk  
Duke University  
Atle Perregaard  
University of Vienna  
Richard Fujimoto  
Georgia Institute of Technology  
Bruno Guajardo  
INRIA  
Ed Griswold  
North Carolina State University  
Robert Gräub  
Clemson University  
Garth Gibson  
 Carnegie Mellon University  
Albert Greenberg  
AVL/Tokai Bell Laboratories  
Nagesh Gupta  
Stanford University  
Peter Harrison  
Imperial College  
Philip Heidelberger  
IBM Research  
Graham Horton  
University of Edinburgh  
Robert Joplin  
Rice University  
Harry Jordan  
University of Colorado  
David Kets  
Dartmouth College  
Wii Leland  
Bell Communications Research  
Scott Luntz  
University of Dortmund  
Miron Livny  
University of Wisconsin  
Dick Monta  
University of California at Los Angeles  
Vernon Rege  
Purdue University  
Jed Saltz  
University of Maryland  
Sanjeev Satia  
George Mason University  
Ken Sevick  
University of Toronto  
Rahul Simha  
College of William and Mary  
Billy Stewart  
North Carolina State University  
Mark Squillante  
IBM Research  
Xin He Su  
Louisiana State University  
Den Towsley  
University of Massachusetts  
Rabie Trivedi  
Duke University  
David Wood  
University of Wisconsin

---

**28th Annual ACM Symposium on Theory of Computing (STOC)**

**Plenary Invited Speaker**  
**Daily**  
8:00 am — 9:00 am  
**Room:** Salon F  
**Grand Ballroom**

Registration for the 28th Annual ACM Symposium on Theory of Computing includes a reception, SIGACT business meeting, an evening excursion, two lunches, continental breakfasts, coffee breaks, and conference proceedings. Student registration fee includes all at the above except the evening excursion. The conference is sponsored by the ACM Special Interest Group on Algorithms and Computation Theory (SIGACT).

---

**Sessions**

**R**

**Reception**  
Tuesday, May 21, 1996  
7:00 pm – 10:00 pm

**$S1 A$**

**Session 1A**  
Wednesday, May 22, 1996  
9:30 am – 10:55 am  
Jin-Yi Cai, Chair  
SUNY Buffalo

**9:20 am**  
The Linear Array Conjecture of Communication Complexity is False  
Eyal Kushilevitz  
Technion  
Nathan Linial  
Hebrew Institute  
Rafael Ostrovsky  
Bellcore

**9:45 am**  
Testing the Long Code and Hardness for Clique  
Johan Håstad  
Royal Institute of Technology

**10:10 am**  
The Space Complexity of Approximating the Frequency Moments  
Noga Alon  
Tel Aviv Univ.  
Yosi Matias and Mario Szegedy  
AT&T Bell Laboratories

**10:35 am**  
Deterministic Restrictions in Circuit Complexity  
Shiva Chaudhuri  
Max Planck Institut für Informatik  
Jukka R. Kämäräinen  
TITS Institute of Fundamental Research

**$S1 B$**

**Session 1B**  
Wednesday, May 22, 1996  
9:30 am – 10:55 am  
Manfred R. Hennig, Chair  
Cornell

**9:30 am**  
Fast Algorithms for $k$-Node Connectivity Augmentation and Related Problems  
Joseph Cheriyan  
Univ. of Waterloo

**9:45 am**  
Ramakrishna Thurimella  
Univ. of Denver

**9:50 am**  
Approximating $k$-Minimum Cuts in $n^{o(k)}$ time  
Andreas A. Benczur and David R. Karger  
MIT

**10:05 am**  
Minimum Cuts in Near-Linear Time  
David R. Karger  
MIT

**10:35 am**  
Deterministic $(\log n)$ Time Edge-Splitting in Undirected Graphs  
Hiroshi Nagamochi and Toshihiko Ibaraki  
Kyoto Univ.

**11:25 am**  
Coffee Break

**S2 A**

**Session 2A**  
Wednesday, May 22, 1996  
11:25 am – 12:25 pm  
Jin-Yi Cai, Chair  
SUNY Buffalo

**11:25 am**  
Evaluation may be Easier than Generation  
Mond Nuer  
Wetware Institute

**11:50 am**  
The PL Hierarchy Collapses  
Mutsunori Ogihara  
Univ. of Rochester

**12:15 pm**  
Convergence Complexity of Optimistic Rate Based Flow Control Algorithms  
Yehuda Ahits  
Yeshaya Mansour  
and Zvi Oshri  
Tel Aviv Univ.

**S2 B**

**Session 2B**  
Wednesday, May 22, 1996  
11:25 am – 12:35 pm  
ShangHua Teng, Chair  
Univ. of Minnesota

**11:25 am**  
Generating Hard Instances of Lattice Problems  
M. Ajtai  
IBM Almaden
0

Sessions

11:50 am
Translational Polygon Containment and Minimal Enclosure Using Linear Programming Based Restriction
Victor J. Milenkovic
Univ. of Miami

12:15 pm
Pushing Disks Together—the Continuous-motion Case
Marshall Bern
Xerox PARC
Amir A. Aghasi
UC Berkeley

L

12:35 pm – 2:00 pm
Lunch

Session 3A
Wednesday, May 22, 1996
2:00 pm – 3:35 pm
Bevett Rubenfield, Chair
Cornell/MIT

2:00 pm
Computing Roadmaps of Semi-algebraic Sets
Saugata Basu and Richard Pollack
Courant Institute
Marie-Francoise Roy
INRIA, Universite de Rennes

2:50 pm
Using the Greedy Basis Algorithm to Find Proofs of Unsatisfiability
Matthew Clegg
UCSD
Jeffery Edmonds
York Univ.
Rudolf Impagliazzo
UCSD

3:35 pm
Efficient Algorithms for Inverting Evolution
Martin Farach
Rutgers
Sanath Kannan
Univ. of Pennsylvania

3:35 pm
Coffee Break

Session 4A
Wednesday, May 22, 1996
4:05 pm – 5:40 pm
Monika R. Hetzinger, Chair
Cornell

4:05 pm
Efficient 3-d Range Searching in External Memory
Darren V. Breslow
Brown
Jeffery Scott Vitter
Duke

4:30 pm
Purely Functional Representations of Catenable Sorted Lists
Haim Kaplan and Robert E. Tarjan
Princeton

10:35 am
An (Ω(logn))-Size Fault-Tolerant Scheduling Network
Yuan Ma
Stanford

Session 5B
Thursday, May 23, 1996
9:20 am – 10:55 am
Abdul S. Slobod, Chair
UC Berkeley

9:20 am
On Extracting Randomness From Weak Random Sources
Annan Ta-Shma
Hebrew Univ.

9:45 am
Randomness-Optimal Sampling, Extractors, and Constructive Leader Election
David Zuckerman
Univ. of Texas, Austin

10:10 am
Generating Random Spanning Trees More Quickly than the Cover Time
David Bruce Wilson
MIT

10:35 am
Towards an Analysis of Local Optimization Algorithms
Tassos Dimitriou and Russell Impagliazzo
UCSD

10:55 am Coffee Break

Knuth Prize Lecture
Thursday, May 23, 1996
11:30 am – 12:30 pm
Andrew C. C. Yao
Princeton

L

12:30 pm – 2:00 pm
Lunch

Session 7A
Thursday, May 23, 1996
2:00 pm – 3:35 pm
Michel Goemans, Chair
MIT
## Sessions

### 2:00 pm
A Threshold of ln n for Approximating Set Cover
Uriel Feige
Weizmann Institute

### 2:25 pm
Fast Algorithms for Parametric Scheduling come from Extensions to Parametric Maximum Flow
S. Thomas McCormick
UBC

### 3:05 pm
Efficient Approximation Algorithms for MAX-CUT and COLORING
Philip Klein and Hsueh-I Lu
Brown

### 3:30 pm
Embedding Graphs in an Arbitrary Surface in Linear Time
Dapun Mohar
University of Ljubljana

### 4:30 pm
How Good is the Goemans-Williamson MAX CUT Algorithm?
Howard J. Karloff
Georgia Tech

### 5:05 pm
A Tight Analysis of the Greedy Algorithm for Set Cover
Petra Slavik
SUNY Buffalo

### 5:35 pm
SIGACT Business Meeting
Thursday, May 23, 1996
5:00 pm

### 2:25 pm
Universal Algorithms for Store-and-Forward and Wormhole Routing
Robert Cypher
Johns Hopkins
Friedhelm Meyer auf der Heide, Christian Schindelhauer and Berthold Vocking
Univ. of Paderborn

### 3:05 pm
Distributed Packet Switching in Arbitrary Networks
Yuvol Rabani and Eyal Tardos
Cornell

### 3:15 pm
Adversarial Queuing Theory
Allan Brodsky
Univ. of Toronto
Jen Kleinberg
MIT

### 4:30 pm
On the Boosting Ability of Top-Down Decision Tree Learning Algorithms
Baruch Awerbuch
Johns Hopkins
Yehuda Mansour
Tel Aviv Univ.

### 5:05 pm
Making Commitments in the Face of Uncertainty: How to Pick a Winner Almost Every Time
Baruch Awerbuch
Johns Hopkins
Yehuda Mansour
Tel Aviv Univ.

### 2:25 pm
Efficient Approximation and Nonapproximability Results for Minimizing Total Flow Time on a Single Machine
Hausi Koller
Universität Graz
Thomas Tustemhahn
Universität Magdeburg
Gerhard J. Woeginger
Radboud University

### 9:20 am
Correlated Pseudorandomness and the Complexity of Private Computations
Donald Beaver
Transarc Corp.

### 9:45 am
Digital Signatures for Protection of Digital Information
Cynthia Dwork and J. Jeffery Liptespaech
IBM Almaden

### 10:10 am
Witness-Based Cryptographic Program Checking and Robust Function Sharing
Yair Frankel and Peter Gemmell
Sorbon National Labs
M. Li
IBM T.J. Watson

### 10:30 am
SIGACT Business Meeting
Thursday, May 23, 1996
5:00 pm
28th Annual ACM Symposium on Theory of Computing (STOC)

Sessions

11:00 am
Characterizing Linear Size Circuits in Terms of Privacy
Eyal Kushilevitz
Technion
Rafail Ostrovsky
Bellore
Adi Rosenc
Tel Aviv Univ.

11:25 am
Nondeterministic Communication with a Limited Number of Advice Bits
Juraj Hromkovic
Universitaet zu Kiel
Georg Schnitzer
Joanneum Wolfgang Goethe-Universität

11:50 am
Public vs. Private Coin Flips in One Round Communication Games
Ian Newman
Haifa Univ.
Matth Saegedy
AT&T Bell Laboratories

2:50 pm
Faster Isomorphism Testing of Strongly Regular Graphs
David A. Spielman
UC Berkeley

3:15 pm
Node-Dissipant Paths on the Mesh and a New Trade-off in VLSI Layout
Alek Aggarwal and David P. Williamson
IBM Research
Jon M. Kleinberg
MIT

3:35 pm Coffee Break

3:50 pm
Adaptive Zero Knowledge and Computational Equivocation
Donald Beaver
Transarc Corp.

4:30 pm
Adaptively Secure Multiparty Computation
Ran Canetti
MIT

5:15 pm
On Relationships between Statistical Zero-Knowledge Proofs
Tatsuaki Okamoto
NTT Labs.

Committees

David S. Johnson
AT&T Research
General Chair

Gary L. Miller
Carnegie-Mellon University
Program Chair

Alek Aggarwal
IBM Research
Finance Chair

PROGRAM COMMITTEE
Sanjeev Arora
Princeton
Jin-Yi Cai
SUNY Buffalo
Alan Frieze
CMU

Erich Kaltofen
IBM
Joe Kilian
NEC

Michel Goemans
MIT
Monika R. Henzinger
Cornell

Maurice Herlihy
Brown
Thomas Leighton
MIT

Gary L. Miller
CMU
Noam Nisan
Hebrew Univ.

Exhibits
Wednesday – Sunday
9:00 am – 6:00 pm
Room: Franklin Hall