

**2000 IEEE 41st Annual Symposium on  
Foundations of Computer Science**

Proceedings

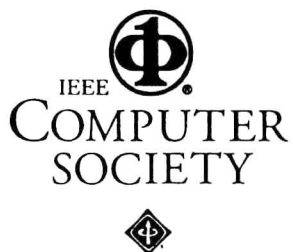
# **41<sup>st</sup> Annual Symposium on Foundations of Computer Science**

**12-14 November 2000**

**Redondo Beach, California**

*Sponsored by*

IEEE Computer Society Technical Committee on  
Mathematical Foundations of Computing



Los Alamitos, California

Washington · Brussels · Tokyo

---

Copyright © 2000 by The Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

*The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.*

IEEE Computer Society Order Number PR00850

ISBN 0-7695-0850-2

ISBN 0-7695-0851-0 (case)

ISBN 0-7695-0852-9 (microfiche)

ISSN 0272-5428

*Additional copies may be ordered from:*

IEEE Computer Society  
Customer Service Center  
10662 Los Vaqueros Circle  
P.O. Box 3014  
Los Alamitos, CA 90720-1314  
Tel: +1 714 821 8380  
Fax: +1 714 821 4641  
<http://computer.org/>  
[csbooks@computer.org](mailto:csbooks@computer.org)

IEEE Service Center  
445 Hoes Lane  
P.O. Box 1331  
Piscataway, NJ 08855-1331  
Tel: +1 732 981 0060  
Fax: +1 732 981 9667  
[http://shop.ieee.org/store/](http://shop.ieee.org/store/customer-service@ieee.org)  
[customer-service@ieee.org](mailto:customer-service@ieee.org)

IEEE Computer Society  
Asia/Pacific Office  
Watanabe Bldg., 1-4-2  
Minami-Aoyama  
Minato-ku, Tokyo 107-0062  
JAPAN  
Tel: +81 3 3408 3118  
Fax: +81 3 3408 3553  
[tokyo.ofc@computer.org](mailto:tokyo.ofc@computer.org)

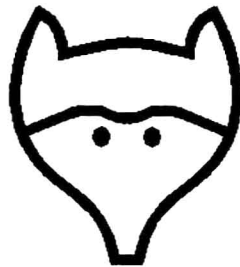
Editorial production by Danielle C. Young

Cover art production by Alex Torres

Printed in the United States of America by The Printing House



# **FOCS 2000**



## Foreword

The papers in these proceedings were presented at the 41st Annual Symposium on Foundations of Computer Science (FOCS '00), sponsored by the IEEE Computer Society Technical Committee on Mathematical Foundations of Computing. The Conference was held in Redondo Beach, CA, November 12-14, 2000.

The program committee consisted of Sanjeev Arora (Princeton), Avrim Blum (Carnegie Mellon), Faith Fich (University of Toronto), Leslie Ann Goldberg (Warwick), Michael Goodrich (Johns Hopkins), Monika Henzinger (Google), Joe Kilian (NECI), Yishay Mansour (Tel-Aviv), R. Ravi (Carnegie Mellon), Leonard Schulman (Georgia Tech & Caltech), Michael Sipser (MIT), Mario Szegedy (Institute for Advanced Studies), Umesh Vazirani (UC Berkeley), David Williamson (IBM Watson), and David Zuckerman (UT Austin & UC Berkeley).

The program committee met on June 23-24, 2000 and selected 66 papers from 206 detailed abstracts submitted. The submissions were not refereed, and many of them represent reports of continuing research. It is expected that most of these papers will appear in a more complete and polished form in scientific journals in the future. In addition to the regular program, Jeff Ullman gave his Donald E. Knuth Prize lecture at the conference.

The committee selected the paper "Stable Distributions, Pseudorandom Generators, Embeddings and Data Stream Computation" by Piotr Indyk to receive the Machtey Award for best student-authored paper. There were many excellent candidates for this award.

The committee wishes to thank all of those who submitted papers for consideration, as well as those who helped with the process of evaluating the submissions. A list of the latter individuals appears in these proceedings under the heading "Reviewers". The program committee also wishes to thank Joe Kilian for his help with the electronic submission server and Danielle Young for the production of these proceedings.

***Avrim Blum***

***Program Committee Chair***

## **Committees**

### **General Conference and Technical Committee Chair**

Alok Aggarwal, IBM Research

### **Local Arrangements and Finance Chair**

Marek Chrobak and Tao Jiang, University of California at Riverside

### **Program Committee Chair**

Avrim Blum, Carnegie Mellon University

### **Program Committee**

|                     |                  |
|---------------------|------------------|
| Sanjeev Arora       | R. Ravi          |
| Avrim Blum          | Leonard Schulman |
| Faith Fich          | Michael Sipser   |
| Leslie Ann Goldberg | Mario Szegedy    |
| Michael Goodrich    | Umesh Vazirani   |
| Monika Henzinger    | David Williamson |
| Joe Kilian          | David Zuckerman  |
| Yishay Mansour      |                  |

### **Corporate Sponsors**

IBM Research

Akamai Technologies

### **Machtley Award**

“Stable Distributions, Pseudorandom Generators, Embeddings  
and Data Stream Computation”

Piotr Indyk

### **Knuth Prize**

Jeff Ullman

<http://www-db.stanford.edu/~ullman/pub/focs00.html>

## Reviewers

|                  |                     |                   |                    |
|------------------|---------------------|-------------------|--------------------|
| Dorit Aharonov   | Alan Frieze         | Arjen Lenstra     | Amin Shokrollahi   |
| Susanne Albers   | Hal Gabow           | Nati Linial       | Alistair Sinclair  |
| Eric Allender    | Naveen Garg         | Philip Long       | Danny Sleator      |
| Noga Alon        | Leszek Gasieniec    | Dominic Mayers    | Warren Smith       |
| Nina Amenta      | Ashish Goel         | David McAllester  | Joel Spencer       |
| Lars Arge        | Michel Goemans      | M. Mitzenmacher   | Dan Spielman       |
| Hagit Attiya     | Paul Goldberg       | Michael Molloy    | Aravind Srinivasan |
| Yossi Azar       | Oded Goldreich      | Yoram Moses       | Angelika Steger    |
| Laci Babai       | M. Grigni           | Ian Munro         | Cliff Stein        |
| David Barrington | Leo Guibas          | S. Muthukrishnan  | Alexander Stolyar  |
| A. Barvinok      | Vassos Hadzilacos   | Ashwin Nayak      | Martin Strauss     |
| Saugata Basu     | Peter Hajnal        | Peter Neumann     | Bernd Sturmfels    |
| Paul Beame       | Ramesh Hariharan    | Shmuel Onn        | Benny Sudakov      |
| Jozsef Beck      | George Havas        | Rafail Ostrovsky  | Madhu Sudan        |
| Mihir Bellare    | Xin He              | Janos Pach        | Ondrej Sykora      |
| Petra Berenbrink | Dan Hirschberg      | C. Papadimitriou  | Christian Szegedy  |
| Dan Boneh        | Mike Hutton         | Boaz Patt-Shamir  | Amnon Ta-Shma      |
| Julian Bradfield | Neil Immerman       | David Peleg       | E. Ternovskaia     |
| Nader Bshouty    | Russell Impagliazzo | Enoch Peserico    | Prasad Tetali      |
| Peter BuerGISser | Piotr Indyk         | Erez Petrank      | Denis Therien      |
| Ran Canetti      | Yuval Ishai         | Maurizio Pizzonia | Mikkel Thorup      |
| N. Cesa-Bianchi  | Andreas Jakoby      | Pavel Pudlak      | Alexandre Tiskin   |
| Bernard Chazelle | Mark Jerrum         | Yuval Rabani      | Andrew Tomkins     |
| Ed Coffman       | Erich Kaltofen      | Uri Rabinovich    | Luca Trevisan      |
| Edith Cohen      | Ravi Kannan         | Charlie Rackoff   | Chris Umann        |
| Richard Cole     | Sampath Kannan      | P. Raghavan       | Alisdair Urquhart  |
| Steve Cook       | Haim Kaplan         | S. Rajagopalan    | Maresh V           |
| Gene Cooperman   | George Karakostas   | R. Rajaraman      | Salil Vadhan       |
| Derek Corneil    | Richard Karp        | Dana Randall      | Moshe Vardi        |
| Felipe Cucker    | Leonid Khachiyan    | Satish Rao        | Vijay Vazirani     |
| Sanjoy Dasgupta  | Sanjeev Khanna      | Ran Raz           | Boban Velickovich  |
| Luc Devroye      | Valerie King        | A. Razborov       | Santosh Vempala    |
| Shlomi Dolev     | Ralf Klasing        | Bruce Reed        | Eric Vigoda        |
| Jeff Edmonds     | Phil Klein          | Oded Regev        | Uzi Vishkin        |
| Noam Elkies      | Jon Kleinberg       | Omer Reingold     | Nicolai Vorobjov   |
| Ioannis Emiris   | M. Klugerman        | Dana Ron          | John Watrous       |
| David Eppstein   | Pascal Koiran       | Ronitt Rubinfeld  | Avi Wigderson      |
| William Evans    | Elias Koutsoupias   | Steven Rudich     | Peter Winkler      |
| M. Farach-Colton | Matthias Krause     | Amit Sahai        | G. Woeginger       |
| Uriel Feige      | Oliver Kullmann     | Cenk Sahinalp     | Neal Young         |
| Eldar Fischer    | Andre Kundgen       | Michael Saks      | Uri Zwick          |
| Lance Fortnow    | Orna Kupferman      | Raimund Seidel    |                    |
| Ehud Friedgut    | Eyal Kushilevitz    | David Shmoys      |                    |



## Table of Contents

41<sup>st</sup> Annual Symposium on Foundations of Computer Science

|                  |      |
|------------------|------|
| Foreword.....    | xii  |
| Committees ..... | xiii |
| Reviewers .....  | xiv  |

### Session 1

---

Chair: David Zuckerman

|                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------|----|
| Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree<br>Expanders and Extractors ..... | 3  |
| <i>O. Reingold, S. Vadhan, and A. Wigderson</i>                                                     |    |
| Universality and Tolerance .....                                                                    | 14 |
| <i>N. Alon, M. Capalbo, Y. Kohayakawa, V. Rödl, A. Ruciński,<br/>and E. Szemerédi</i>               |    |
| Extracting Randomness via Repeated Condensing.....                                                  | 22 |
| <i>O. Reingold, R. Shaltiel, and A. Wigderson</i>                                                   |    |
| Extracting Randomness from Samplable Distributions.....                                             | 32 |
| <i>L. Trevisan and S. Vadhan</i>                                                                    |    |
| Pseudorandom Generators in Propositional Proof Complexity .....                                     | 43 |
| <i>M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson</i>                                 |    |

### Session 2

---

Chair: David Williamson

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| Stochastic Models for the Web Graph .....                                                | 57 |
| <i>R. Kumar, P. Raghavan, S. Rajagopalan, D. Sivakumar, A. Tomkins,<br/>and E. Upfal</i> |    |
| Optimization Problems in Congestion Control .....                                        | 66 |
| <i>R. Karp, E. Koutsoupias, C. Papadimitriou, and S. Shenker</i>                         |    |

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| Fairness Measures for Resource Allocation .....                              | 75 |
| <i>A. Kumar and J. Kleinberg</i>                                             |    |
| On the Approximability of Trade-offs and Optimal Access of Web Sources ..... | 86 |
| <i>C. Papadimitriou and M. Yannakakis</i>                                    |    |
| How Bad is Selfish Routing? .....                                            | 93 |
| <i>T. Roughgarden and É. Tardos</i>                                          |    |

### Session 3

---

Chair: Sanjeev Arora

|                                                                                     |     |
|-------------------------------------------------------------------------------------|-----|
| A Polylogarithmic Approximation of the Minimum Bisection .....                      | 105 |
| <i>U. Feige and R. Krauthgamer</i>                                                  |     |
| Approximability and In-Approximability Results for No-Wait Shop<br>Scheduling ..... | 116 |
| <i>M. Sviridenko and G. Woeginger</i>                                               |     |
| Nested Graph Dissection and Approximation Algorithms .....                          | 126 |
| <i>S. Guha</i>                                                                      |     |
| Approximating the Single Source Unsplittable Min-Cost Flow Problem .....            | 136 |
| <i>M. Skutella</i>                                                                  |     |

### Session 4

---

Chair: Michael Sipser

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| Hardness of Approximate Hypergraph Coloring .....                                 | 149 |
| <i>V. Guruswami, J. Håstad, and M. Sudan</i>                                      |     |
| “Soft-Decision” Decoding of Chinese Remainder Codes .....                         | 159 |
| <i>V. Guruswami, A. Sahai, and M. Sudan</i>                                       |     |
| Super-Linear Time-Space Tradeoff Lower Bounds for Randomized<br>Computation ..... | 169 |
| <i>P. Beame, M. Saks, X. Sun, and E. Vee</i>                                      |     |
| On the Hardness of Graph Isomorphism .....                                        | 180 |
| <i>J. Torán</i>                                                                   |     |

## Session 5

---

Chair: R. Ravi

|                                                                                                |     |
|------------------------------------------------------------------------------------------------|-----|
| Stable Distributions, Pseudorandom Generators, Embeddings and Data<br>Stream Computation ..... | 189 |
| <i>P. Indyk</i>                                                                                |     |
| New Data Structures for Orthogonal Range Searching .....                                       | 198 |
| <i>S. Alstrup, G. Brodal, and T. Rauhe</i>                                                     |     |
| Nearly Optimal Expected-Case Planar Point Location .....                                       | 208 |
| <i>S. Arya, T. Malamatos, and D. Mount</i>                                                     |     |
| On Levels in Arrangements of Curves .....                                                      | 219 |
| <i>T. Chan</i>                                                                                 |     |

## Session 6

---

Chair: Avrim Blum

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| Detecting a Network Failure .....                                  | 231 |
| <i>J. Kleinberg</i>                                                |     |
| Testing of Clustering.....                                         | 240 |
| <i>N. Alon, S. Dar, M. Parnas, and D. Ron</i>                      |     |
| Testing of Function That Have Small Width Branching Programs ..... | 251 |
| <i>I. Newman</i>                                                   |     |
| Testing That Distributions Are Close .....                         | 259 |
| <i>T. Batu, L. Fortnow, R. Rubinfeld, W. Smith, and P. White</i>   |     |
| Using Upper Confidence Bounds for Online Learning .....            | 270 |
| <i>P. Auer</i>                                                     |     |

## Session 7

---

Chair: Joe Kilian

|                                   |     |
|-----------------------------------|-----|
| Zaps and Their Applications ..... | 283 |
| <i>C. Dwork and M. Naor</i>       |     |

|                                                                                                             |     |
|-------------------------------------------------------------------------------------------------------------|-----|
| Randomizing Polynomials: A New Representation with Applications to Round-Efficient Secure Computation ..... | 294 |
| <i>Y. Ishai and E. Kushilevitz</i>                                                                          |     |
| Lower Bounds on the Efficiency of Generic Cryptographic Constructions .....                                 | 305 |
| <i>R. Gennaro and L. Trevisan</i>                                                                           |     |
| Concurrent Oblivious Transfer .....                                                                         | 314 |
| <i>J. Garay and P. MacKenzie</i>                                                                            |     |
| The Relationship between Public Key Encryption and Oblivious Transfer .....                                 | 325 |
| <i>Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan</i>                                    |     |

## Session 8

---

Chair: Leonard Schulman

|                                                                           |     |
|---------------------------------------------------------------------------|-----|
| The Online Median Problem .....                                           | 339 |
| <i>R. Mettu and C. Plaxton</i>                                            |     |
| Polynomial Time Approximation Schemes for Geometric $k$ -Clustering ..... | 349 |
| <i>R. Ostrovsky and Y. Rabani</i>                                         |     |
| Clustering Data Streams .....                                             | 359 |
| <i>S. Guha, N. Mishra, R. Motwani, and L. O'Callaghan</i>                 |     |
| On Clusterings — Good, Bad and Spectral .....                             | 367 |
| <i>R. Kannan, S. Vempala, and A. Vetta</i>                                |     |

## Session 9

---

Chair: Leonard Schulman

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Fully Dynamic Transitive Closure: Breaking through the $O(n^2)$ Barrier ..... | 381 |
| <i>C. Demetrescu and G. Italiano</i>                                          |     |
| Opportunistic Data Structures with Applications .....                         | 390 |
| <i>P. Ferragina and G. Manzini</i>                                            |     |
| Cache-Oblivious B-Trees .....                                                 | 399 |
| <i>M. Bender, E. Demaine, and M. Farach-Colton</i>                            |     |

|                                                         |     |
|---------------------------------------------------------|-----|
| Using Expander Graphs to Find Vertex Connectivity ..... | 410 |
| <i>H. Gabow</i>                                         |     |

## Session 10

---

Chair: Mario Szegedy

|                                                                                     |     |
|-------------------------------------------------------------------------------------|-----|
| On the Boundary Complexity of the Union of Fat Triangles .....                      | 423 |
| <i>J. Pach and G. Tardos</i>                                                        |     |
| Straightening Polygonal Arcs and Convexifying Polygonal Cycles .....                | 432 |
| <i>R. Connelly, E. Demaine, and G. Rote</i>                                         |     |
| A Combinatorial Approach to Planar Non-Colliding Robot Arm Motion<br>Planning ..... | 443 |
| <i>I. Streinu</i>                                                                   |     |
| Topological Persistence and Simplification.....                                     | 454 |
| <i>H. Edelsbrunner, D. Letscher, and A. Zomorodian</i>                              |     |

## Session 11

---

Chair: Leslie Goldberg

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| The Cover Time, the Blanket Time, and the Matthews Bound.....                             | 467 |
| <i>J. Kahn, J. Kim, L. Lovász, and V. Vu</i>                                              |     |
| The Product Replacement Algorithm is Polynomial .....                                     | 476 |
| <i>I. Pak</i>                                                                             |     |
| Efficient Algorithms for Universal Portfolios .....                                       | 486 |
| <i>A. Kalai and S. Vempala</i>                                                            |     |
| Sampling Adsorbing Staircase Walks Using a New Markov Chain<br>Decomposition Method ..... | 492 |
| <i>R. Martin and D. Randall</i>                                                           |     |
| The Randomness Recycler: A New Technique for Perfect Sampling .....                       | 503 |
| <i>J. Fill and M. Huber</i>                                                               |     |

## Session 12

---

Chair: Umesh Vazirani

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| An Improved Quantum Fourier Transform Algorithm and Applications ..... | 515 |
| <i>L. Hales and S. Hallgren</i>                                        |     |
| Fast Parallel Circuits for the Quantum Fourier Transform .....         | 526 |
| <i>R. Cleve and J. Watrous</i>                                         |     |
| Succinct Quantum Proofs for Properties of Finite Groups .....          | 537 |
| <i>J. Watrous</i>                                                      |     |
| Private Quantum Channels .....                                         | 547 |
| <i>A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf</i>                  |     |
| The Quantum Complexity of Set Membership .....                         | 554 |
| <i>J. Radhakrishnan, P. Sen, and S. Venkatesh</i>                      |     |

## Session 13

---

Chair: Leslie Goldberg

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| Randomized Rumor Spreading .....                                   | 565 |
| <i>R. Karp, C. Schindelhauer, S. Shenker, and B. Vöcking</i>       |     |
| Fast Broadcasting and Gossiping in Radio Networks .....            | 575 |
| <i>M. Chrobak, L. Gąsieniec, and W. Rytter</i>                     |     |
| Linear Waste of Best Fit Bin Packing on Skewed Distributions ..... | 582 |
| <i>C. Kenyon and M. Mitzenmacher</i>                               |     |
| Optimal Myopic Algorithms for Random 3-SAT .....                   | 590 |
| <i>D. Achlioptas and G. Sorkin</i>                                 |     |

## Session 14

---

Chair: David Williamson

|                                                          |     |
|----------------------------------------------------------|-----|
| Hierarchical Placement and Network Design Problems ..... | 603 |
| <i>S. Guha, A. Meyerson, and K. Munagala</i>             |     |

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| Building Steiner Trees with Incomplete Global Knowledge.....             | 613 |
| <i>D. Karger and M. Minkoff</i>                                          |     |
| COST-DISTANCE: Two Metric Network Design .....                           | 624 |
| <i>A. Meyerson, K. Munagala, and S. Plotkin</i>                          |     |
| Combinatorial Feature Selection Problems .....                           | 631 |
| <i>M. Charikar, V. Guruswami, R. Kumar, S. Rajagopalan, and A. Sahai</i> |     |

## Session 15

---

Chair: Michael Sipser

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| The Common Fragment of CTL and LTL.....                                                | 643 |
| <i>M. Maidl</i>                                                                        |     |
| On the Existence of Booster Types .....                                                | 653 |
| <i>M. Herlihy and E. Ruppert</i>                                                       |     |
| Existential Second-Order Logic over Graphs: Charting the Tractability<br>Frontier..... | 664 |
| <i>G. Gottlob, P. Kolaitis, and T. Schwentick</i>                                      |     |
| On Computing the Determinant and Smith Form of an Integer Matrix .....                 | 675 |
| <i>W. Eberly, M. Giesbrecht, and G. Villard</i>                                        |     |
| <b>Author Index</b> .....                                                              | 687 |

## **Session 1**

---

Chair: David Zuckerman



# Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors

EXTENDED ABSTRACT

Omer Reingold\*

Salil Vadhan†

Avi Wigderson‡

## Abstract

*The main contribution of this work is a new type of graph product, which we call the **zig-zag product**. Taking a product of a large graph with a small graph, the resulting graph inherits (roughly) its size from the large one, its degree from the small one, and its expansion properties from both! Iteration yields simple explicit constructions of constant-degree expanders of every size, starting from one constant-size expander.*

*Crucial to our intuition (and simple analysis) of the properties of this graph product is the view of expanders as functions which act as “entropy wave” propagators — they transform probability distributions in which entropy is concentrated in one area to distributions where that concentration is dissipated. In these terms, the graph product affords the constructive interference of two such waves.*

*A variant of this product can be applied to extractors, giving the first explicit extractors whose seed length depends (poly)logarithmically on only the entropy deficiency of the source (rather than its length) and that extract almost all the entropy of high min-entropy sources. These high min-entropy extractors have several interesting applications, including the first constant-degree explicit expanders which beat the “eigenvalue bound.”*

## 1 Introduction

### 1.1 Expanders

Expanders are graphs which are sparse but nevertheless highly connected. Such graphs have been used to address many fundamental problems in computer science, on topics including network design (e.g. [Pip87, PY82, AKS83]), complexity theory ([Val77, Sip88, Urq87]), derandomization ([NN93, INW94, IW97]), coding theory ([SS96, Spi96]), and cryptography ([GIL<sup>+</sup>90]). Standard probabilistic arguments ([Pin73]) show that almost every constant-degree ( $\geq 3$ ) graph is an expander. However, explicitly constructing such graphs seemed to be much harder and this led to an exciting and extensive body of research, developed mainly by mathematicians intrigued by this computer science challenge.

Most of this work was guided by the sufficient<sup>1</sup> condition for the expansion of (infinite families of constant-degree regular) graphs discovered by Tanner [Tan84] (see also [AM85]): the second largest eigenvalue of the adjacency matrix should be strictly smaller than the degree. This naturally led researchers to consider algebraic constructions, where this eigenvalue can be estimated. The celebrated sequence of papers [Mar73, GG81, AM85, AGM87, JM87, LPS88, Mar88, Mor94] provided such constant-degree expanders. All these graphs are extremely simple to describe: given the name of a vertex (in binary), its neighbors can be computed in polynomial time (or even logarithmic space). This level of explicitness is essential for many of the applications. However, the analysis bounding the eigenvalue is quite sophisticated (and often based on deep mathematical results). Thus, it is hard to intuitively understand why these graphs are expanders.

A deviation from this path was taken by Ajtai [Ajt94], who proposed a combinatorial construction of cubic expanders. It starts with an arbitrary cubic  $N$ -vertex graph and applies a sequence of polynomially many local opera-

<sup>1</sup>This condition turned out to be necessary as well [Alo86].

\*AT&T Labs - Research, Room A243, 180 Park Avenue, Bldg. 103, Florham Park, NJ, 07932, USA. E-mail: omer@research.att.com. Part of this research was performed while visiting the Institute for Advanced Study, Princeton, NJ.

†Institute for Advanced Study, Princeton, NJ, and Harvard University, Cambridge, MA. E-mail: salil@deas.harvard.edu. Work done while at MIT, supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

‡Institute for Advanced Study, Princeton and the Hebrew University, Jerusalem. Address: Institute for Advanced Study, School of Mathematics, Einstein Drive, Princeton, NJ 08540. E-mail: avi@ias.edu. Partially supported by Israel - US Binational Science Foundation grant number 97-00188.