2000 IEEE 41st Annual Symposium on Foundations of Computer Science

Proceedings

41st 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

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

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/
customer-service@ieee.org

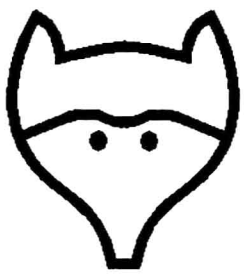
IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

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

Corporate Sponsors

IBM Research

Akamai Technologies

Machtey 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
Susanne Albers
Eric Allender
Noga Alon
Nina Amenta
Lars Arge
Hagit Attiya
Yossi Azar
Laci Babai
David Barrington
A. Barvinok
Saugata Basu
Paul Beame
Jozsef Beck
Mihir Bellare
Petra Berenbrink
Dan Boneh
Julian Bradfield
Nader Bshouty
Peter Buergisser
Ran Canetti
N. Cesa-Bianchi
Bernard Chazelle
Ed Coffman
Edith Cohen
Richard Cole
Steve Cook
Gene Cooperman
Derek Corneil
Felipe Cucker
Sanjoy Dasgupta
Luc Devroye
Shlomi Dolev
Jeff Edmonds
Noam Elkies
Ioannis Emiris
David Eppstein
William Evans
M. Farach-Colton
Uriel Feige
Eldar Fischer
Lance Fortnow
Ehud Friedgut

Alan Frieze
Hal Gabow
Naveen Garg
Leszek Gasieniec
Ashish Goel
Michel Goemans
Paul Goldberg
Oded Goldreich
M. Grigni
Leo Guibas
Vassos Hadzilacos
Peter Hajnal
Ramesh Hariharan
George Havas
Xin He
Dan Hirschberg
Mike Hutton
Neil Immerman
Russell Impagliazzo
Piotr Indyk
Yuval Ishai
Andreas Jakoby
Mark Jerrum
Erich Kaltofen
Ravi Kannan
Sampath Kannan
Haim Kaplan
George Karakostas
Richard Karp
Leonid Khachiyan
Sanjeev Khanna
Valerie King
Ralf Klasing
Phil Klein
Jon Kleinberg
M. Klugerman
Pascal Koiran
Elias Koutsoupias
Matthias Krause
Oliver Kullmann
Andre Kundgen
Orna Kupferman
Eyal Kushilevitz

Arjen Lenstra
Nati Linial
Philip Long
Dominic Mayers
David McAllester
M. Mitzenmacher
Michael Molloy
Yoram Moses
Ian Munro
S. Muthukrishnan
Ashwin Nayak
Peter Neumann
Shmuel Onn
Rafail Ostrovsky
Janos Pach
C. Papadimitriou
Boaz Patt-Shamir
David Peleg
Enoch Peserico
Erez Petrank
Maurizio Pizzonia
Pavel Pudlak
Yuval Rabani
Uri Rabinovich
Charlie Rackoff
P. Raghavan
S. Rajagopalan
R. Rajaraman
Dana Randall
Satish Rao
Ran Raz
A. Razborov
Bruce Reed
Oded Regev
Omer Reingold
Dana Ron
Ronitt Rubinfeld
Steven Rudich
Amit Sahai
Cenk Sahinalp
Michael Saks
Raimund Seidel
David Shmoys

Amin Shokrollahi
Alistair Sinclair
Danny Sleator
Warren Smith
Joel Spencer
Dan Spielman
Aravind Srinivasan
Angelika Steger
Cliff Stein
Alexander Stolyar
Martin Strauss
Bernd Sturmfels
Benny Sudakov
Madhu Sudan
Ondrej Sykora
Christian Szegedy
Amnon Ta-Shma
E. Ternovskaia
Prasad Tetali
Denis Therien
Mikkel Thorup
Alexandre Tiskin
Andrew Tomkins
Luca Trevisan
Chris Umann
Alisdair Urquhart
Mahesh V
Salil Vadhan
Moshe Vardi
Vijay Vazirani
Boban Velickovich
Santosh Vempala
Eric Vigoda
Uzi Vishkin
Nicolai Vorobjov
John Watrous
Avi Wigderson
Peter Winkler
G. Woeginger
Neal Young
Uri Zwick

Table of Contents

41st Annual Symposium on Foundations of Computer Science

Session 1

Chair: David Zuckerman

Session 2

Chair: David Williamson

Session 3

Chair: Sanjeev Arora

Session 4

Chair: Michael Sipser

Session 5

Chair: R. Ravi

Session 6

Chair: Avrim Blum

Session 7

Chair: Joe Kilian

Session 8

Chair: Leonard Schulman

Session 9

Chair: Leonard Schulman

Session 10

Chair: Mario Szegedy

Session 11

Chair: Leslie Goldberg

Session 12

Chair: Umesh Vazirani

Session 13

Chair: Leslie Goldberg

Session 14

Chair: David Williamson

Session 15

Chair: Michael Sipser

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."

*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.

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+90]). Standard probabilistic arguments ([Pin73]) show that almost every constant-degree (≥ 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[1] 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-

[1] This condition turned out to be necessary as well [Alo86].

0-7695-0850-2/00 $10.00 © 2000 IEEE