Lecture Notes in Computer Science 4851

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Serdar Boztaş Hsiao-Feng (Francis) Lu (Eds.)

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

17th International Symposium, AAECC-17
Bangalore, India, December 16-20, 2007
Proceedings

Springer

Volume Editors

Serdar Boztaş
RMIT University, School of Mathematical and Geospatial Sciences
GPO Box 2476V, Melbourne 3001, Australia
E-mail: serdar.boztas@ems.rmit.edu.au

Hsiao-Feng (Francis) Lu
National Chung-Cheng University, Department of Communications Engineering
168 University Rd., Min-Hsiung, Chia-Yi, Taiwan
E-mail: francis@ccu.edu.tw

Library of Congress Control Number: 2007940905

CR Subject Classification (1998): E.4, I.1, E.3, G.2, F.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-77223-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77223-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12202058 06/3180 5 4 3 2 1 0

Preface

The AAECC Symposia Series was started in 1983 by Alain Poli (Toulouse), who, together with R. Desq, D. Lazard and P. Camion, organized the first conference. Originally the acronym AAECC meant "Applied Algebra and Error-Correcting Codes." Over the years its meaning has shifted to "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes," reflecting the growing importance of complexity, particularly for decoding algorithms. During the AAECC-12 symposium the conference committee decided to enforce the theory and practice of the coding side as well as the cryptographic aspects. Algebra was conserved, as in the past, but slightly more oriented to algebraic geometry codes, finite fields, complexity, polynomials, and graphs.

For AAECC-17 the main subjects covered were:

- Block codes, including list-decoding algorithms
- Algebra and codes: rings, fields, algebraic geometry codes
- Algebra: rings and fields, polynomials, permutations, lattices
- Cryptography: cryptanalysis and complexity
- Computational algebra: algebraic algorithms and transforms
- Sequences and boolean functions

Seven invited speakers characterize the aim of AAECC-17:

- Ralf Koetter, "Error Correction for Network Coding Channels"
- Tor Helleseth, "New Attacks on the Filter Generator"
- Tanja Lange, "Arithmetic on Edwards Curves"
- Gary McGuire, "Spectra of Boolean Functions, Subspaces of Matrices, and Going up Versus Going Down"
- Priti Shankar, "Algebraic Structure Theory of Tail-biting Trellises"
- Henning Stichtenoth, "Nice Codes from Nice Curves"
- Manindra Agrawal, "Determinant versus Permanent"

In addition, an Invited List Decoding Session was organized by Madhu Sudan:

- Venkatesan Guruswami, "List Decoding and Pseudorandom Constructions"
- Tom Høholdt, "Iterative List decoding of LDPC Codes"
- Ralf Koetter, "Optimizing Multivariate Interpolation"
- Atri Rudra, "Efficient List Decoding of Explicit Codes with Optimal Redundancy"

Except for AAECC-1 (*Discrete Mathematics* 56, 1985) and AAECC-7 (*Discrete Applied Mathematics* 33, 1991), the proceedings of all the symposia have been published in Springer's *Lecture Notes in Computer Science* (Vols. 228, 229, 307, 356, 357, 508, 539, 673, 948, 1255, 1719, 2227, 2643, 3857). It is a policy of AAECC to maintain a high scientific standard, comparable to that of a journal.

This was made possible thanks to the many referees involved. Each submitted paper was evaluated by at least two international researchers.

AAECC-17 received and refereed 61 submissions. Of these, 1 was withdrawn and 33 were selected for publication in these proceedings.

The symposium was organized by P. Vijay Kumar, Tom Høholdt, Heeralal Janwa, Serdar Boztaş and Hsiao-feng (Francis) Lu, with the help of Govindar Rangarajan, C.E. Veni Madhavan and Priti Shankar, under the Indian Institute of Science Mathematics Initiative (IMI). It was sponsored by the Department of Science and Technology, India; the Defence Research and Development Organization, India; and Microsoft Research India.

We express our thanks to the Springer staff, especially Alfred Hofmann, for their help in the preparation of these proceedings.

October 2007

Serdar Boztaş
Hsiao-Feng (Francis) Lu

Organization

Steering Commitee

Conference Co-chairs	P. Vijay Kumar (Univ. of Southern California, USA)
	Tom Høholdt (Technical Univ. of Denmark, Denmark)
	Heeralal Janwa (Univ. of Puerto Rico, Puerto Rico)
Program Co-chairs	Serdar Boztaş (RMIT Univ., Australia)
	Hsiao-feng (Francis) Lu (National Chung Cheng University, Taiwan)

Conference Committee

J. Calmet	K. Horadam	O. Moreno
G. Cohen	H. Imai	H. Niederreiter
G.L. Feng	H. Janwa	A. Poli
M. Giusti	R. Kohno	T.R.N. Rao
J. Heintz	H.W. Lenstra, Jr.	S. Sakata
T. Høholdt	S. Lin	P. Solé

Program Committee

I.F. Blake	J. Heintz	F. Özbudak
J. Calmet	K. Horadam	A. Poli
C. Carlet	H. Imai	S.S. Pradhan
G. Cohen	N. Kashyap	A. Rao
C. Ding	S. Lin	S. Sakata
G-L. Feng	O. Moreno	H-Y. Song
M. Giusti	W.H. Mow	P. Udaya
G. Gong	H. Niederreiter	C. Xing

Local Organizing Committee

Govindar Rangarajan C.E. Veni Madhavan Priti Shankar

Sponsoring Institutions

Department of Science and Technology, India
Defence Research and Development Organization, India
Microsoft Research India

Table of Contents

Invited Contributions

Regular Contributions