

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

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 AAEEC 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 AAEEC 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 AAEEC-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 AAEEC-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 AAEEC-17:

- Ralf Koetter, “Error Correction for Network Coding Channels”
- Tor Hellesteth, “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 AAEEC-1 (*Discrete Mathematics* 56, 1985) and AAEEC-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 AAEEC 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 Committee

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

List Decoding and Pseudorandom Constructions	1
<i>Venkatesan Guruswami</i>	
A Survey of Recent Attacks on the Filter Generator	7
<i>Sondre Rønjom, Guang Gong, and Tor Hellesest</i>	
Iterative List Decoding of LDPC Codes	18
<i>Tom Høholdt and Jørn Justesen</i>	
Inverted Edwards Coordinates	20
<i>Daniel J. Bernstein and Tanja Lange</i>	
Spectra of Boolean Functions, Subspaces of Matrices, and Going Up Versus Going Down	28
<i>Gary McGuire</i>	
Efficient List Decoding of Explicit Codes with Optimal Redundancy	38
<i>Atri Rudra</i>	
Algebraic Structure Theory of Tail-Biting Trellises	47
<i>Priti Shankar</i>	
Nice Codes from Nice Curves	48
<i>Henning Stichtenoth</i>	

Regular Contributions

Generalized Sudan's List Decoding for Order Domain Codes	50
<i>Olav Geil and Ryutaroh Matsumoto</i>	
Bent Functions and Codes with Low Peak-to-Average Power Ratio for Multi-Code CDMA	60
<i>Jianqin Zhou, Wai Ho Mow, and Xiaoping Dai</i>	
Determining the Nonlinearity of a New Family of APN Functions	72
<i>Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire</i>	
An Improvement of Tardos's Collusion-Secure Fingerprinting Codes with Very Short Lengths	80
<i>Koji Nuida, Satoshi Fujitsu, Manabu Hagiwara, Takashi Kitagawa, Hajime Watanabe, Kazuto Ogawa, and Hideki Imai</i>	

Space-Time Codes from Crossed Product Algebras of Degree 4	90
<i>Grégory Berhuy and Frédérique Oggier</i>	
On Non-randomness of the Permutation After RC4 Key Scheduling	100
<i>Goutam Paul, Subhamoy Maitra, and Rohit Srivastava</i>	
Correctable Errors of Weight Half the Minimum Distance Plus One for the First-Order Reed-Muller Codes	110
<i>Kenji Yasunaga and Toru Fujiwara</i>	
Fault-Tolerant Finite Field Computation in the Public Key Cryptosystems	120
<i>Silvana Medoš and Serdar Boztaş</i>	
A Note on a Class of Quadratic Permutations over \mathbb{F}_{2^n}	130
<i>Yann Laigle-Chapuy</i>	
Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields	138
<i>B.A. Sethuraman and Frédérique Oggier</i>	
Quaternary Plotkin Constructions and Quaternary Reed-Muller Codes	148
<i>J. Pujol, J. Rifà, and F.I. Solov'eva</i>	
Joint Source-Cryptographic-Channel Coding Based on Linear Block Codes	158
<i>Haruhiko Kaneko and Eiji Fujiwara</i>	
On the Key-Privacy Issue of McEliece Public-Key Encryption	168
<i>Shigenori Yamakawa, Yang Cui, Kazukuni Kobara, Manabu Hagiwara, and Hideki Imai</i>	
Lattices for Distributed Source Coding: Jointly Gaussian Sources and Reconstruction of a Linear Function	178
<i>Dinesh Krithivasan and S. Sandeep Pradhan</i>	
Linear Complexity and Autocorrelation of Prime Cube Sequences	188
<i>Young-Joon Kim, Seok-Yong Jin, and Hong-Yeop Song</i>	
The “Art of Trellis Decoding” Is NP-Hard	198
<i>Navin Kashyap</i>	
On the Structure of Inversive Pseudorandom Number Generators	208
<i>Harald Niederreiter and Arne Winterhof</i>	
Subcodes of Reed-Solomon Codes Suitable for Soft Decoding	217
<i>Safitha J. Raj and Andrew Thangaraj</i>	

Normalized Minimum Determinant Calculation for Multi-block and Asymmetric Space-Time Codes	227
<i>Camilla Hollanti and Hsiao-feng (Francis) Lu</i>	
On the Computation of Non-uniform Input for List Decoding on Bezerra-Garcia Tower	237
<i>M. Prem Laxman Das and Kripasindhu Sikdar</i>	
Dense MIMO Matrix Lattices—A Meeting Point for Class Field Theory and Invariant Theory	247
<i>Jyrki Lahtonen and Roope Vehkalahti</i>	
Secure Cross-Realm Client-to-Client Password-Based Authenticated Key Exchange Against Undetectable On-Line Dictionary Attacks	257
<i>Kazuki Yoneyama, Haruki Ota, and Kazuo Ohta</i>	
Links Between Discriminating and Identifying Codes in the Binary Hamming Space	267
<i>Irène Charon, Gérard Cohen, Olivier Hudry, and Antoine Lobstein</i>	
Construction of Rotation Symmetric Boolean Functions on Odd Number of Variables with Maximum Algebraic Immunity	271
<i>Sumanta Sarkar and Subhamoy Maitra</i>	
A Path to Hadamard Matrices	281
<i>P. Embury and A. Rao</i>	
The Tangent FFT	291
<i>Daniel J. Bernstein</i>	
Novel Algebraic Structure for Cyclic Codes	301
<i>Dang Hoai Bac, Nguyen Binh, and Nguyen Xuan Quynh</i>	
Distribution of Trace Values and Two-Weight, Self-orthogonal Codes over $GF(p, 2)$	311
<i>N. Pinnawala, A. Rao, and T.A. Gulliver</i>	
Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions – 9 Variable Boolean Functions with Nonlinearity 242	321
<i>Selçuk Kavut and Melek Diker Yücel</i>	
On Quasi-cyclic Codes over Integer Residue Rings	330
<i>Maheshanand and Siri Krishan Wasan</i>	
Extended Norm-Trace Codes with Optimized Correction Capability	337
<i>Maria Bras-Amorós and Michael E. O’Sullivan</i>	
On Generalized Hamming Weights and the Covering Radius of Linear Codes	347
<i>H. Janwa and A.K. Lal</i>	

Homomorphic Encryptions of Sums of Groups	357
<i>Akihiro Yamamura</i>	
Author Index	367