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
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 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 Bozta¸s (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
Invited Contributions

List Decoding and Pseudorandom Constructions .......................... 1
Venkatesan Guruswami

A Survey of Recent Attacks on the Filter Generator .................... 7
Sondre Rønjom, Guang Gong, and Tor Helleseth

Iterative List Decoding of LDPC Codes .................................. 18
Tom Høholdt and Jørn Justesen

Inverted Edwards Coordinates ............................................. 20
Daniel J. Bernstein and Tanja Lange

Spectra of Boolean Functions, Subspaces of Matrices, and Going Up
Versus Going Down ....................................................... 28
Gary McGuire

Efficient List Decoding of Explicit Codes with Optimal Redundancy .. 38
Atri Rudra

Algebraic Structure Theory of Tail-Biting Trellises .................... 47
Priti Shankar

Nice Codes from Nice Curves ............................................. 48
Henning Stichtenoth

Regular Contributions

Generalized Sudan’s List Decoding for Order Domain Codes .......... 50
Olav Geil and Ryutaroh Matsumoto

Bent Functions and Codes with Low Peak-to-Average Power Ratio for
Multi-Code CDMA ......................................................... 60
Jianqin Zhou, Wai Ho Mow, and Xiaoping Dai

Determining the Nonlinearity of a New Family of APN Functions .... 72
Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire

An Improvement of Tardos’s Collusion-Secure Fingerprinting Codes
with Very Short Lengths .................................................. 80
Koji Nuida, Satoshi Fujitsu, Manabu Hagiwara, Takashi Kitagawa,
Hajime Watanabe, Kazuto Ogawa, and Hideki Imai
Space-Time Codes from Crossed Product Algebras of Degree 4 .......................... 90
Grégoire Berhuy and Frédérique Oggier

On Non-randomness of the Permutation After RC4 Key Scheduling .................. 100
Goutam Paul, Subhamoy Maitra, and Rohit Srivastava

Correctable Errors of Weight Half the Minimum Distance Plus One for the First-Order Reed-Muller Codes ................................................................. 110
Kenji Yasunaga and Toru Fujiwara

Fault-Tolerant Finite Field Computation in the Public Key Cryptosystems .......................... 120
Silvana Medoš and Serdar Boztaş

A Note on a Class of Quadratic Permutations over \(\mathbb{F}_{2^n}\) .......................... 130
Yann Laigle-Chapuy

Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields ................................................................. 138
B.A. Sethuraman and Frédérique Oggier

Quaternary Plotkin Constructions and Quaternary Reed-Muller Codes .......................... 148
J. Pujol, J. Rifà, and F.I. Solov’eva

Joint Source-Cryptographic-Channel Coding Based on Linear Block Codes .......................... 158
Haruhiko Kaneko and Eiji Fujiwara

On the Key-Privacy Issue of McEliece Public-Key Encryption .......................... 168
Shigenori Yamakawa, Yang Cui, Kazukuni Kobara, Manabu Hagiwara, and Hideki Imai

Lattices for Distributed Source Coding: Jointly Gaussian Sources and Reconstruction of a Linear Function ................................................................. 178
Dinesh Krithivasan and S. Sandeep Pradhan

Linear Complexity and Autocorrelation of Prime Cube Sequences .................. 188
Young-Joon Kim, Seok-Yong Jin, and Hong-Yeop Song

The “Art of Trellis Decoding” Is NP-Hard .......................................................... 198
Navin Kashyap

On the Structure of Inversive Pseudorandom Number Generators .................. 208
Harald Niederreiter and Arne Winterhof

Subcodes of Reed-Solomon Codes Suitable for Soft Decoding .......................... 217
Safitha J. Raj and Andrew Thangaraj
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normalized Minimum Determinant Calculation for Multi-block and Asymmetric Space-Time Codes</td>
<td>227</td>
</tr>
<tr>
<td>Camilla Hollanti and Hsiao-feng (Francis) Lu</td>
<td></td>
</tr>
<tr>
<td>On the Computation of Non-uniform Input for List Decoding on Bezerra-Garcia Tower</td>
<td>237</td>
</tr>
<tr>
<td>M. Prem Laxman Das and Kripasindhu Sikdar</td>
<td></td>
</tr>
<tr>
<td>Dense MIMO Matrix Lattices—A Meeting Point for Class Field Theory and Invariant Theory</td>
<td>247</td>
</tr>
<tr>
<td>Jyrki Lahtonen and Roope Vehkalahti</td>
<td></td>
</tr>
<tr>
<td>Secure Cross-Realm Client-to-Client Password-Based Authenticated Key Exchange Against Undetectable On-Line Dictionary Attacks</td>
<td>257</td>
</tr>
<tr>
<td>Kazuki Yoneyama, Haruki Ota, and Kazuo Ohta</td>
<td></td>
</tr>
<tr>
<td>Links Between Discriminating and Identifying Codes in the Binary Hamming Space</td>
<td>267</td>
</tr>
<tr>
<td>Irène Charon, Gérard Cohen, Olivier Hudry, and Antoine Lobstein</td>
<td></td>
</tr>
<tr>
<td>Construction of Rotation Symmetric Boolean Functions on Odd Number of Variables with Maximum Algebraic Immunity</td>
<td>271</td>
</tr>
<tr>
<td>Sumanta Sarkar and Subhamoy Maitra</td>
<td></td>
</tr>
<tr>
<td>A Path to Hadamard Matrices</td>
<td>281</td>
</tr>
<tr>
<td>P. Embury and A. Rao</td>
<td></td>
</tr>
<tr>
<td>The Tangent FFT</td>
<td>291</td>
</tr>
<tr>
<td>Daniel J. Bernstein</td>
<td></td>
</tr>
<tr>
<td>Novel Algebraic Structure for Cyclic Codes</td>
<td>301</td>
</tr>
<tr>
<td>Dang Hoai Bac, Nguyen Binh, and Nguyen Xuan Quynh</td>
<td></td>
</tr>
<tr>
<td>Distribution of Trace Values and Two-Weight, Self-orthogonal Codes over $GF(p,2)$</td>
<td>311</td>
</tr>
<tr>
<td>N. Pinnawala, A. Rao, and T.A. Gulliver</td>
<td></td>
</tr>
<tr>
<td>Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions – 9 Variable Boolean Functions with Nonlinearity 242</td>
<td>321</td>
</tr>
<tr>
<td>Selçuk Kavut and Melek Diker Yücel</td>
<td></td>
</tr>
<tr>
<td>On Quasi-cyclic Codes over Integer Residue Rings</td>
<td>330</td>
</tr>
<tr>
<td>Maheshanand and Siri Krishan Wasan</td>
<td></td>
</tr>
<tr>
<td>Extended Norm-Trace Codes with Optimized Correction Capability</td>
<td>337</td>
</tr>
<tr>
<td>Maria Bras-Amorós and Michael E. O'Sullivan</td>
<td></td>
</tr>
<tr>
<td>On Generalized Hamming Weights and the Covering Radius of Linear Codes</td>
<td>347</td>
</tr>
<tr>
<td>H. Janwa and A.K. Lal</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

Homomorphic Encryptions of Sums of Groups .......................... 357
   Akihiro Yamamura

Author Index ....................................................... 367