

Lecture Notes in Computer Science      2227  
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

**Springer**  
*Berlin*  
*Heidelberg*  
*New York*  
*Barcelona*  
*Hong Kong*  
*London*  
*Milan*  
*Paris*  
*Tokyo*

Serdar Boztaş Igor E. Shparlinski (Eds.)

# Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

14th International Symposium, AAECC-14  
Melbourne, Australia, November 26-30, 2001  
Proceedings



Springer

**Series Editors**

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

**Volume Editors**

Serdar Boztaş  
RMIT University, Department of Mathematics  
GPO Box 2476V, Melbourne 3001, Australia  
E-mail: serdar@rmit.edu.au  
Igor E. Shparlinski  
Macquarie University, Department of Computing  
NSW 2109, Australia  
E-mail: igor@comp.mq.edu.au

**Cataloging-in-Publication Data applied for**

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Applied algebra, algebraic algorithms and error correcting codes : 14th  
international symposium ; proceedings / AAECC 14, Melbourne, Australia,  
November 26 - 30, 2001. Serdar Boztaş ; Igor E. Shparlinski (ed.). - Berlin ;  
Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo :  
Springer, 2002  
(Lecture notes in computer science ; Vol. 2227)  
ISBN 3-540-42911-5

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

**ISSN 0302-9743**

**ISBN 3-540-42911-5 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Steingräber Satztechnik GmbH, Heidelberg  
Printed on acid-free paper      SPIN: 10840981      06/3142      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 in both decoding algorithms and computational algebra.

AAECC aims to encourage cross-fertilization between algebraic methods and their applications in computing and communications. The algebraic orientation is towards finite fields, complexity, polynomials, and graphs. The applications orientation is towards both theoretical and practical error-correction coding, and, since AAECC 13 (Hawaii, 1999), towards cryptography. AAECC was the first symposium with papers connecting Gröbner bases with E-C codes. The balance between theoretical and practical is intended to shift regularly; at AAECC-14 the focus was on the theoretical side.

The main subjects covered were:

- Codes: iterative decoding, decoding methods, block codes, code construction.
- Codes and algebra: algebraic curves, Gröbner bases, and AG codes.
- Algebra: rings and fields, polynomials.
- Codes and combinatorics: graphs and matrices, designs, arithmetic.
- Cryptography.
- Computational algebra: algebraic algorithms.
- Sequences for communications.

Six invited speakers covered the areas outlined:

- Robert Calderbank, “Combinatorics, Quantum Computers, and Cellular Phones”
- James Massey, “The Ubiquity of Reed-Muller Codes”
- Graham Norton, “Gröbner Bases over a Principal Ideal Ring”
- Vera Pless, “Self-dual Codes – Theme and Variations”
- Amin Shokrollahi, “Design of Differential Space-Time Codes Using Group Theory”
- Madhu Sudan, “Ideal Error-Correcting Codes: Unifying Algebraic and Number-Theoretic Algorithms”.

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-Verlag’s *Lecture Notes in Computer Science* (Vols. 228, 229, 307, 356, 357, 508, 539, 673, 948, 1255, 1719).

It is a policy of AAECC to maintain a high scientific standard, comparable to that of a journal. This has been made possible thanks to the many referees involved. Each submitted paper was evaluated by at least two international researchers.

AAECC-14 received and refereed 61 submissions. Of these, 1 was withdrawn, 36 were selected for publication in these proceedings, while 7 additional works contributed to the symposium as oral presentations. Unrefereed talks were presented in a “Recent Results” session.

The symposium was organized by Serdar Boztaş, Tom Høholdt, Kathy Horadam, Igor E. Shparlinski, and Branka Vučetić, with the help of Asha Baliga, Pride Conference Management (Juliann Smith), and the Department of Mathematics, RMIT University. It was sponsored by the Australian Mathematical Society.

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

August 2001

Serdar Boztaş and Igor E. Shparlinski

## Organization

## Steering Committee

General Chair: Kathy Horadam (RMIT Univ., AUS)  
Conference Co-chair: Tom Høholdt (Technical Univ. of Denmark, DK)  
Program Chair: Igor Shparlinski (Macquarie Univ., AUS)  
Program Co-chair: Branka Vucetic (Sydney Univ., AUS)  
Publication: Serdar Boztas (RMIT Univ., AUS)

## Conference Committee

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

## Program Committee

I.F. Blake	M. Giusti	S. Litsyn
J. Calmet	J. Gutierrez	A. Nechaev
C. Carlet	J. Heintz	H. Niederreiter
P. Charpin	T. Helleseth	D. Panario
M. Clausen	H. Imai	S. Sakata
P.G. Farrell	E. Kaltofen	P. Solé
M. Fossorier	T. Kasami	H. van Tilborg
M. Giesbrecht	L. Knudsen	C. Xing

## **Local Organizing Committee**

Asha Baliga      Serdar Boztas      Kathy Horadam

## Referees

D. Augot N. Boston C. Carlet  
A. Baliga F. Boulier P. Charpin  
I.F. Blake S. Boztaş M. Clausen  
A. Bonnecaze J. Calmet G. Cohen

## VIII Organization

R. Cramer	C. Hao	S. Murphy
I. Damgård	T. Hashimoto	V.K. Murty
M. Dichtl	J. Heintz	A. Nechaev
C. Ding	T. Helleseth	H. Niederreiter
I. Duursma	K. Horadam	D. Panario
P.G. Farrell	X-D. Hou	L. Pecquet
G-L. Feng	H. Imai	V. Rijmen
H.C. Ferreira	J. Jensen	S. Sakata
M. Fossorier	G. Kabatiansky	P. Sarkar
T. Fujiwara	E. Kaltofen	H.G. Schaathun
P. Gaborit	T. Kasami	I. Shparlinski
J. Galati	F. Keqin	B. Shung
S. Galbraith	T. Kløve	A. Silverberg
S. Gao	L. Knudsen	P. Solé
V.P. Gerdt	L. Kulesz	B. Stevens
M. Giesbrecht	T. Laihonen	H. van Tilborg
M. Giusti	S. Ling	B. Vučetić
F. Griffin	S. Litsyn	J.L. Walker
J. Gutierrez	F. Morain	K. Yang
Y.S. Han	R. Morelos-Zaragoza	C. Xing

## Sponsoring Institutions

Australian Mathematical Society

# Table of Contents

## Invited Contributions

The Ubiquity of Reed-Muller Codes .....	1
<i>J.L. Massey (ETH-Zürich and Lund Univ.)</i>	
Self-dual Codes-Theme and Variations .....	13
<i>V. Pless (Univ. of Illinois)</i>	
Design of Differential Space-Time Codes Using Group Theory .....	22
<i>A. Shokrollahi (Digital Fountain)</i>	
Ideal Error-Correcting Codes:	
Unifying Algebraic and Number-Theoretic Algorithms .....	36
<i>M. Sudan (MIT)</i>	

## Block Codes

Self-dual Codes Using Image Restoration Techniques .....	46
<i>A. Baliga (RMIT Univ.) and J. Chua (Monash Univ.)</i>	
Low Complexity Tail-Biting Trellises of Self-dual Codes of Length 24, 32 and 40 over $GF(2)$ and $\mathbb{Z}_4$ of Large Minimum Distance .....	57
<i>E. Cadic (France Telecom R&amp;D), J.C. Carlach (France Telecom R&amp;D), G. Olocco (Univ. Paris-Sud), A. Otmani (Univ. Limoges), and J.P. Tillich (Univ. Paris-Sud)</i>	
$F_q$ -Linear Cyclic Codes over $F_{q^m}$ : DFT Characterization .....	67
<i>B.K. Dey and B.S. Rajan (Indian Inst. of Science)</i>	

## Code Constructions

Cyclic Projective Reed-Muller Codes .....	77
<i>T.P. Berger and L. de Maximy (Univ. Limoges)</i>	
Codes Identifying Sets of Vertices .....	82
<i>T. Laihonen and S. Ranto (Univ. Turku)</i>	
Duality and Greedy Weights of Linear Codes and Projective Multisets ....	92
<i>H.G. Schaathun (Univ. Bergen)</i>	

## **Codes and Algebra: Rings and Fields**

Type II Codes over $\mathbb{F}_{2^r}$ .....	102
<i>K. Betsumiya (Nagoya Univ.), M. Harada (Yamagata Univ.), and A. Munemasa (Kyushu Univ.)</i>	
On Senary Simplex Codes .....	112
<i>M.K. Gupta (Univ. Canterbury), D.G. Glynn (Univ. Canterbury), and T.A. Gulliver (Univ. Victoria)</i>	
Optimal Double Circulant $\mathbb{Z}_4$ -Codes .....	122
<i>T.A. Gulliver (Univ. Victoria) and M. Harada (Yamagata Univ.)</i>	
Constructions of Codes from Number Fields .....	129
<i>V. Guruswami (MIT)</i>	
On Generalized Hamming Weights for Codes over Finite Chain Rings .....	141
<i>H. Horimoto (Kumamoto Nat'l. Coll. of Tech.) and K. Shiromoto (Kumamoto Univ.)</i>	
Information Rates and Weights of Codes in Structural Matrix Rings .....	151
<i>A. Kelarev (Univ. Tasmania) and O. Sokratova (Univ. Tartu)</i>	

## **Codes and Algebra: Algebraic Geometry Codes**

On Hyperbolic Codes .....	159
<i>O. Geil (Aalborg Univ.) and T. Høholdt (Tech. Univ. of Denmark)</i>	
On Fast Interpolation Method for Guruswami-Sudan List Decoding of One-Point Algebraic-Geometry Codes .....	172
<i>S. Sakata (Univ. Electro-Communications)</i>	
Computing the Genus of a Class of Curves .....	182
<i>M.C. Rodríguez-Palánquer, L.J. García-Villalba, and I. Luengo-Velasco (UCM Madrid)</i>	

## **Sequences**

Iterations of Multivariate Polynomials and Discrepancy of Pseudorandom Numbers .....	192
<i>J. Gutierrez and D. Gomez-Perez (Univ. Cantabria)</i>	
Even Length Binary Sequence Families with Low Negaperiodic Autocorrelation .....	200
<i>M.G. Parker (Univ. Bergen)</i>	
On the Non-existence of (Almost-)Perfect Quaternary Sequences .....	210
<i>P. Parraud (Écoles Militaires St Cyr-Coëtquidan)</i>	

Maximal Periods of $x^2 + c$ in $\mathbb{F}_q$ . . . . .	219
<i>A. Peinado (Univ. Málaga), F. Montoya (CSIC), J. Muñoz (CSIC), and A.J. Yuste (Univ. Jaen)</i>	

On the Aperiodic Correlation Function of Galois Ring $m$ -Sequences . . . . .	229
<i>P. Udaya (Univ. Melbourne) and S. Boztas (RMIT Univ.)</i>	

Euclidean Modules and Multisequence Synthesis . . . . .	239
<i>L. Wang (Univ. Sci. and Tech. of China)</i>	

## Cryptography

On Homogeneous Bent Functions . . . . .	249
<i>C. Charnes (Univ. Melbourne and Univ. Karlsruhe), M. Rötteler (Univ. Karlsruhe), and T. Beth (Univ. Karlsruhe)</i>	

Partially Identifying Codes for Copyright Protection . . . . .	260
<i>S. Encheva (HSH, Norway) and G. Cohen (ENST)</i>	

On the Generalised Hidden Number Problem and Bit Security of XTR . . . . .	268
<i>I.E. Shparlinski (Macquarie Univ.)</i>	

CRYPTIM: Graphs as Tools for Symmetric Encryption . . . . .	278
<i>V. Ustimenko (Univ. South Pacific)</i>	

## Algorithms

An Algorithm for Computing Cocyclic Matrices Developed over Some Semidirect Products . . . . .	287
<i>V. Álvarez, J.A. Armario, M.D. Frau, and P. Real (Univ. Sevilla)</i>	

Algorithms for Large Integer Matrix Problems . . . . .	297
<i>M. Giesbrecht (Univ. Western Ontario), M. Jacobson, Jr. (Univ. Manitoba), and A. Storjohann (Univ. Western Ontario)</i>	

On the Identification of Vertices and Edges Using Cycles . . . . .	308
<i>I. Honkala (Univ. Turku), M.G. Karpovsky (Boston Univ.), and S. Litsyn (Tel-Aviv Univ.)</i>	

## Algorithms: Decoding

On Algebraic Soft Decision Decoding of Cyclic Binary Codes . . . . .	315
<i>V.B. Balakirsky (Eindhoven Univ. of Technology)</i>	

Lifting Decoding Schemes over a Galois Ring . . . . .	323
<i>E. Byrne (Nat'l. Univ. Ireland, Cork)</i>	

XII      Table of Contents

Sufficient Conditions on Most Likely Local Sub-codewords in Recursive Maximum Likelihood Decoding Algorithms . . . . .	333
<i>T. Kasami (Hiroshima City Univ.), H. Tokushige (Hiroshima City     Univ.), and Y. Kaji (Nara Inst. Science and Technology)</i>	
A Unifying System-Theoretic Framework for Errors-and-Erasures Reed-Solomon Decoding . . . . .	343
<i>M. Kuijper (Univ. Melbourne), M. van Dijk (Philips Research),     H. Hollmann (Philips Research), and J. Oostveen (Philips Research)</i>	
An Algorithm for Computing Rejection Probability of MLD with Threshold Test over BSC . . . . .	353
<i>T. Wadayama (Okayama Prefectural Univ.)</i>	
<b>Algebraic Constructions</b>	
Cartan's Characters and Stairs of Characteristic Sets . . . . .	363
<i>F. Boulier and S. Neut (Univ. Lille I)</i>	
On the Invariants of the Quotients of the Jacobian of a Curve of Genus 2 . . . . .	373
<i>P. Gaudry and É. Schost (École Polytechnique)</i>	
Algebraic Constructions for PSK Space-Time Coded Modulation . . . . .	387
<i>A.M. Guidi (Inst. Telecommunications Research), A.J. Grant (Inst. Telecommunications Research), and S.S. Pietrobon (Small World Communications)</i>	
<b>Author Index</b> . . . . .	397