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

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

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

http://www.springer.de

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 Vucetic, 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 Boztaş (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 Boztaş	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

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

Sponsoring Institutions

Australian Mathematical Society

Table of Contents

Invited Contributions

Block Codes

Code Constructions

Codes and Algebra: Rings and Fields

Codes and Algebra: Algebraic Geometry Codes

Sequences

Cryptography

Algorithms

Algorithms: Decoding