Lecture Notes in Computer Science 2643
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Marc Fossorier Tom Høholdt
Alain Poli (Eds.)

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

15th International Symposium, AAECC-15
Toulouse, France, May 12-16, 2003
Proceedings

Springer

Volume Editors

Marc Fossorier
University of Hawaii, Department of Electrical Engineering
2540 Dole Street, Holmes Hall 455, Honolulu, HI 96822, USA
E-mail: marc@spectra.eng.hawaii.edu

Tom Høholdt
The Technical University of Denmark, Department of Mathematics
Bldg. 303, DK-2800 Lyngby, Denmark
E-mail: T.Hoeholdt@mat.dtu.dk

Alain Poli
IRIT - Université Paul Sabatier
31602 Toulouse cédex, France
E-mail: poli@cict.fr

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek.
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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

ISSN 0302-9743
ISBN 3-540-40111-3 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 PTP-Berlin GmbH
Printed on acid-free paper SPIN: 10930380 06/3142 5 4 3 2 1 0

Preface

The AAECC symposium was started in June 1983 by Alain Poli (Toulouse), who, together with Roger Desq, Daniel Lazard, and Paul Camion, organized the first conference. The meaning of the acronym AAECC changed from "Applied Algebra and Error Correcting Codes" to "Applied Algebra, Algebraic Algorithms, and Error Correcting Codes." One reason for this was the increasing 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 was slightly more oriented to algebraic geometry codes, finite fields, complexity, polynomials, and graphs.

For AAECC-15 the main subjects covered were:

- Block codes.
- Algebra and codes: rings, fields, AG codes.
- Cryptography.
- Sequences.
- Algorithms, decoding algorithms.
- Algebra: constructions in algebra, Galois groups, differential algebra, polynomials.

The talks of the six invited speakers characterized the aims of AAECC-15:

- P. Sole ("Public Key Cryptosystems Based on Rings").
- S. Lin ("Combinatorics Low Density Parity Check Codes").
- J. Stern ("Cryptography and the Methodology of Provable Security").
- D. Costello ("Graph-Based Convolutional LDPC Codes").
- I. Shparlinsky ("Dynamical Systems Generated by Rational Functions").
- A. Lauder ("Algorithms for Multivariate Polynomials over Finite Fields").

Except for AAECC-1 (published in the journal Discrete Mathematics, 56, 1985) and AAECC-7 (Discrete Mathematics, 33, 1991), the proceedings of all the symposia have been published in Springer-Verlag's Lecture Notes in Computer Science series (vols. 228, 229, 307, 356, 357, 508, 673, 948, 1255, 1719, 2227). It is the policy of AAECC to maintain a high scientific standard. This has been made possible thanks to the many referees involved. Each submitted paper was evaluated by at least two international researchers.

AAECC-15 received 40 submissions; 25 were selected for publication in these proceedings while 8 additional works were contributed to the symposium as oral presentations.

The symposium was organized by Marc Fossorier, Tom Høholdt, and Alain Poli, with the help of the 'Centre Baudis' in Toulouse.

We express our thanks to Jinghu Chen and Juntan Zhang of the University of Hawaii for their dedicated work on these proccedings, to the Springer-Verlag staff, especially Alfred Hofmann and Anna Kramer, and to the referees.

February 2003 M. Fossorier, T. Høholdt, A. Poli

Organization

Steering Committee

Conference General Chairman:	Alain Poli (Univ. of Toulouse, France)
Conference Co-chairman:	Tom Høholdt (Technical Univ. of Denmark, Denmark)
Publication:	Marc Fossorier, Jinghu Chen and Juntan Zhang (Univ. of Hawaii, USA)
Local Arrangements:	Marie-Claude Gennero, Geneviève Cluzel (Univ. of Toulouse, France)

Conference Committee

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

Program Committee

T. Berger
E. Biglieri
J. Calmet
C. Carlet
D. Costello
T. Ericson
P. Farrell
M. Fossorier
J. Hagenauer
S. Harari
T. Helleseth
E. Kaltofen
T. Kasami
L.R. Knudsen
S. Litsyn
R.J. McEliece
R. Morelos-Zaragoza
H. Niederreiter
P. Sole
H. Tilborg

Table of Contents