



**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

## Series Editors

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

## Volume Editors

Marc Fosserier  
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

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 2003  
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 proceedings, 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	R. Kohno
G. Cohen	H.W. Lenstra Jr.
S.D. Cohen	S. Lin
G.L. Feng	O. Moreno
M. Giusti	H. Niederreiter
J. Heintz	A. Poli
T. Høholdt	T.R.N. Rao
H. Imai	S. Sakata
H. Janwa	P. Sole
J.M. Jensen	

## Program Committee

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

# Table of Contents

Cryptography and the Methodology of Provable Security . . . . .	1
<i>Jacques Stern</i>	
Dynamical Systems Generated by Rational Functions . . . . .	6
<i>Harald Niederreiter, Igor E. Shparlinski</i>	
Homotopy Methods for Equations over Finite Fields . . . . .	18
<i>Alan G.B. Lauder</i>	
Three Constructions of Authentication/Secrecy Codes . . . . .	24
<i>Cunsheng Ding, Arto Salomaa, Patrick Solé, Xiaojian Tian</i>	
The Jacobi Model of an Elliptic Curve and Side-Channel Analysis . . . . .	34
<i>Olivier Billet, Marc Joye</i>	
Fast Point Multiplication on Elliptic Curves through Isogenies . . . . .	43
<i>Eric Brier, Marc Joye</i>	
Interpolation of the Elliptic Curve Diffie–Hellman Mapping . . . . .	51
<i>Tanja Lange, Arne Winterhof</i>	
An Optimized Algebraic Method for Higher Order Differential Attack . . .	61
<i>Yasuo Hatano, Hidema Tanaka, Toshinobu Kaneko</i>	
Fighting Two Pirates . . . . .	71
<i>Hans Georg Schaathun</i>	
Copyright Control and Separating Systems . . . . .	79
<i>Sylvia Encheva, Gérard Cohen</i>	
Unconditionally Secure Homomorphic Pre-distributed Commitments . . . .	87
<i>Anderson C.A. Nascimento, Akira Otsuka, Hideki Imai, Joern Mueller-Quade</i>	
A Class of Low-Density Parity-Check Codes Constructed Based on Reed–Solomon Codes with Two Information Symbols . . . . .	98
<i>Ivana Djurdjevic, Jun Xu, Khaled Abdel-Ghaffar, Shu Lin</i>	
Relative Duality in MacWilliams Identity . . . . .	108
<i>L.S. Kazarin, V.M. Sidelnikov, Igor B. Gashkov</i>	
Good Expander Graphs and Expander Codes: Parameters and Decoding .	119
<i>H. Janwa</i>	
On the Covering Radius of Certain Cyclic Codes . . . . .	129
<i>Oscar Moreno, Francis N. Castro</i>	



Unitary Error Bases: Constructions, Equivalence, and Applications . . . . .	139
<i>Andreas Klappenecker, Martin Rötteler</i>	
Differentially 2-Uniform Cocycles – The Binary Case . . . . .	150
<i>K.J. Horadam</i>	
The Second and Third Generalized Hamming Weights of Algebraic Geometry Codes . . . . .	158
<i>Domingo Ramirez-Alzola</i>	
Error Correcting Codes over Algebraic Surfaces . . . . .	169
<i>Thanasis Bouganis</i>	
A Geometric View of Decoding AG Codes . . . . .	180
<i>Thanasis Bouganis, Drue Coles</i>	
Performance Analysis of M-PSK Signal Constellations in Riemannian Varieties . . . . .	191
<i>Rodrigo Gusmão Cavalcante, Reginaldo Palazzo Jr.</i>	
Improvements to Evaluation Codes and New Characterizations of Arf Semigroups . . . . .	204
<i>Maria Bras-Amorós</i>	
Optimal 2-Dimensional 3-Dispersion Lattices . . . . .	216
<i>Moshe Schwartz, Tuvi Etzion</i>	
On $g$ -th MDS Codes and Matroids . . . . .	226
<i>Keisuke Shiromoto</i>	
On the Minimum Distance of Some Families of $\mathbb{Z}_{2^k}$ -Linear Codes . . . . .	235
<i>Fabien Galand</i>	
Quasicyclic Codes of Index $\ell$ over $F_q$ Viewed as $F_q[x]$ -Submodules of $F_{q^\ell}[x]/\langle x^m - 1 \rangle$ . . . . .	244
<i>Kristine Lally</i>	
Fast Decomposition of Polynomials with Known Galois Group . . . . .	254
<i>Andreas Enge, François Morain</i>	
Author Index . . . . .	265