

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Maria Bras-Amorós Tom Høholdt (Eds.)

Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes

18th International Symposium, AAECC-18
Tarragona, Spain, June 8-12, 2009
Proceedings

Volume Editors

Maria Bras-Amorós
Universitat Rovira i Virgili
Departament d'Enginyeria Informàtica i Matemàtiques
Avinguda Països Catalans, 26, 43007 Tarragona, Catalonia, Spain,
E-mail: maria.bras@urv.cat

Tom Høholdt
The Technical University of Denmark
Department of Mathematics
Building 303, 2800 Lyngby, Denmark,
E-mail: tom@mat.dtu.dk

Library of Congress Control Number: Applied for

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

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN	0302-9743
ISBN-10	3-642-02180-8 Springer Berlin Heidelberg New York
ISBN-13	978-3-642-02180-0 Springer 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. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12690084 06/3180 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 stood for “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. The main topics for AAECC-18 were algebra, algebraic computation, codes and algebra, codes and combinatorics, modulation and codes, sequences, and cryptography.

The invited speakers of this edition were Iwan Duursma, Henning Stichtenoth, and Fernando Torres. We would like to express our deep regret for the loss of Professor Ralf Kötter, who recently passed away and could not be our fourth invited speaker.

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, 4851).

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-18 received and refereed 50 submissions. Of these, 22 were selected for publication in these proceedings as regular papers and 7 were selected as extended abstracts.

The symposium was organized by Maria Bras-Amorós and Tom Høholdt, with the help of Jesús Manjón, Glòria Pujol, Jordi Castellà, Antoni Martínez, and Xavier Fernández under the umbrella of the CRISES group for Cryptography and Statistical Secrecy, at the Universitat Rovira i Virgili, led by Josep Domingo-Ferrer.

It was sponsored by the Catalan Government, the UNESCO Chair in Data Privacy located at Universitat Rovira i Virgili, and the Spanish Network on Mathematics of Information Society.

We would like to dedicate these proceedings to the memory of our colleague Ralf Kötter.

June 2009

Maria Bras-Amorós
Tom Høholdt

Applied Algebra, Algebraic Algorithms, and Error Correcting Codes - AAECC-18

General Chair

Maria Bras-Amorós Universitat Rovira i Virgili, Catalonia, Spain

Co-chair

Tom Høholdt Technical University of Denmark

Program Committee

Jacques Calmet	University of Karlsruhe, Germany
Claude Carlet	University of Paris 8, France
Gerard D. Cohen	Ecole Nationale Supérieure des Télécommunications, France
Cunsheng Ding	Hong Kong University of Science and Technology, China
Gui-Liang Feng	University of Southwestern Louisiana, USA
Marc Giusti	Ecole Polytechnique, France
Guang Gong	University of Waterloo, Canada
Joos Heintz	University of Buenos Aires, Argentina and University of Cantabria, Spain
Kathy Horadam	RMIT University, Australia
Hideki Imai	University of Tokyo, Japan
Navin Kashyap	Queen's University, Canada
Shu Lin	University of California, USA
Oscar Moreno	University of Puerto Rico
Wai Ho Mow	Southwest Jiaotong University, China
Harald Niederreiter	National University of Singapore
Michael E. O'Sullivan	San Diego State University, USA
Ferruh Ozbudak	Middle East Technical University, Turkey
Udaya Parampalli	University of Melbourne, Australia
Alain Poli	University P. Sabatier, France
S. Sandeep Pradhan	University of Michigan at Ann Arbor, USA
Asha Rao	Royal Melbourne Institute of Technology, Australia
Shojiro Sakata	Technical University of Denmark
Hong-Yeop Song	Yonsei University, Korea
Chaoping Xing	Nanyang Technological University, Singapore

Organizing Committee

Jesús Manjón	Universitat Rovira i Virgili, Catalonia, Spain
Glòria Pujol	Universitat Rovira i Virgili, Catalonia, Spain
Jordi Castellà-Roca	Universitat Rovira i Virgili, Catalonia, Spain
Antoni Martínez-Ballesté	Universitat Rovira i Virgili, Catalonia, Spain
Xavier Fernández	Universitat Rovira i Virgili, Catalonia, Spain

Table of Contents

Codes

The Order Bound for Toric Codes	1
<i>Peter Beelen and Diego Ruano</i>	
An Extension of the Order Bound for AG Codes	11
<i>Iwan Duursma and Radoslav Kirov</i>	
Sparse Numerical Semigroups	23
<i>C. Munuera, F. Torres, and J. Villanueva</i>	
From the Euclidean Algorithm for Solving a Key Equation for Dual Reed–Solomon Codes to the Berlekamp–Massey Algorithm	32
<i>Maria Bras-Amorós and Michael E. O’Sullivan</i>	
Rank for Some Families of Quaternary Reed-Muller Codes	43
<i>Jaume Pernas, Jaume Pujol, and Mercè Villanueva</i>	
Optimal Bipartite Ramanujan Graphs from Balanced Incomplete Block Designs: Their Characterizations and Applications to Expander/LDPC Codes	53
<i>Tom Høholdt and Heeralal Janwal</i>	
Simulation of the Sum-Product Algorithm Using Stratified Sampling	65
<i>John Brevik, Michael E. O’Sullivan, Anya Umlauf, and Rich Wolski</i>	
A Systems Theory Approach to Periodically Time-Varying Convolutional Codes by Means of Their Invariant Equivalent	73
<i>Joan-Josep Climent, Victoria Herranz, Carmen Perea, and Virtudes Tomás</i>	
On Elliptic Convolutional Goppa Codes	83
<i>José Ignacio Iglesias Curto</i>	
The Minimum Hamming Distance of Cyclic Codes of Length $2p^s$	92
<i>Hakan Özadam and Ferruh Özbudak</i>	
There Are Not Non-obvious Cyclic Affine-invariant Codes	101
<i>José Joaquín Bernal, Ángel del Río, and Juan Jacobo Simón</i>	
On Self-dual Codes over $\mathbf{Z}_{16}$	107
<i>Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada</i>	

Cryptography

A Non-abelian Group Based on Block Upper Triangular Matrices with Cryptographic Applications	117
<i>Rafael Álvarez, Leandro Tortosa, José Vicent, and Antonio Zamora</i>	
Word Oriented Cascade Jump σ -LFSR	127
<i>Guang Zeng, Yang Yang, Wenbao Han, and Shuqin Fan</i>	
On Some Sequences of the Secret Pseudo-random Index j in RC4 Key Scheduling	137
<i>Riddhipratim Basu, Subhamoy Maitra, Goutam Paul, and Tanmoy Talukdar</i>	
Very-Efficient Anonymous Password-Authenticated Key Exchange and Its Extensions	149
<i>SeongHan Shin, Kazukuni Kobara, and Hideki Imai</i>	
Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE	159
<i>Yang Cui, Kirill Morozov, Kazukuni Kobara, and Hideki Imai</i>	

Algebra

Noisy Interpolation of Multivariate Sparse Polynomials in Finite Fields	169
<i>Álvar Ibeas and Arne Winterhof</i>	
New Commutative Semifields and Their Nuclei	179
<i>Jürgen Bierbrauer</i>	
Spreads in Projective Hjelmslev Geometries	186
<i>Ivan Landjev</i>	
On the Distribution of Nonlinear Congruential Pseudorandom Numbers of Higher Orders in Residue Rings	195
<i>Edwin D. El-Mahassni and Domingo Gomez</i>	
Rooted Trees Searching for Cocyclic Hadamard Matrices over D_{4t}	204
<i>Víctor Álvarez, José Andrés Armario, María Dolores Frau, Félix Gudiel, and Amparo Osuna</i>	

Extended Abstracts

Interesting Examples on Maximal Irreducible Goppa Codes	215
<i>Marta Giorgetti</i>	
Repeated Root Cyclic and Negacyclic Codes over Galois Rings	219
<i>Sergio R. López-Permouth and Steve Szabo</i>	

Construction of Additive Reed-Muller Codes	223
<i>J. Pujol, J. Rifà, and L. Ronquillo</i>	
Gröbner Representations of Binary Matroids	227
<i>M. Borges-Quintana, M.A. Borges-Trenard, and E. Martínez-Moro</i>	
A Generalization of the Zig-Zag Graph Product by Means of the Sandwich Product	231
<i>David M. Monarres and Michael E. O'Sullivan</i>	
Novel Efficient Certificateless Aggregate Signatures	235
<i>Lei Zhang, Bo Qin, Qianhong Wu, and Futai Zhang</i>	
Bounds on the Number of Users for Random 2-Secure Codes	239
<i>Manabu Hagiwara, Takahiro Yoshida, and Hideki Imai</i>	
Author Index	243