

Lecture Notes in Computer Science

673

Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer



Gérard Cohen Teo Mora Oscar Moreno (Eds.)

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

10th International Symposium,AAECC-10
San Juan de Puerto Rico, Puerto Rico,
May 10-14, 1993
Proceedings

Springer-Verlag

Berlin Heidelberg New York

London Paris Tokyo

Hong Kong Barcelona

Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Gérard Cohen
Ecole Nationale Supérieure des Télécommunications
46, rue Barrault, F-75634 Paris Cedex 13, France

Teo Mora
Università di Genova, Dipartimento di Matematica
Via L. B. Alberti 4, I-16132 Genova, Italy

Oscar Moreno
University of Puerto Rico, Department of Mathematics
Rio Pedras, Puerto Rico 00931

CR Subject Classification (1991): E.3-4, I.1, G.2, F.2

ISBN 3-540-56686-4 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56686-4 Springer-Verlag New York Berlin Heidelberg

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 1993
Printed in Germany

Typesetting: Camera ready by author/editor
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

The AAEEC Symposia Series was started ten years ago by Alain Poli (Toulouse), who organized, together with R. Desq, D. Lazard and P. Camion, the first conference in the series (Toulouse, June 1983) and was in charge of most of the following editions.

AAEEC (the acronym has shifted its meaning over the years before stabilizing as "Applied Algebra, Algebraic Algorithms and Error Correcting Codes") aims to attract high-level research papers and to encourage cross-fertilization among different areas which share the use of algebraic methods and techniques for applications in the sciences of computing, communications, and engineering.

Algebra, in its broader sense, has always been viewed as a frame to describe in a formal setting both the properties of the objects giving mathematical models of reality and the rules under which they can be manipulated. Its importance for applications has grown in recent years with the introduction of technological areas (related to signal processing, error correcting codes, information processing, software engineering, etc.) in which the symbolic nature of the objects studied make the techniques of calculus and numerical analysis inapplicable. For these areas, algebra provides both a theoretical framework for the development of theories and algorithmic techniques for the concrete manipulation of objects.

While in principle covering any area related to applications of algebra to communication and computer sciences, by their previous history the AAEEC Symposia are mainly devoted to research in coding theory and computer algebra.

The theory of error-correcting codes deals with the transmission of information in the presence of noise. Coding is the systematic use of redundancy in the formation of the messages to be sent so as to enable the recovery of the information present originally after it has been corrupted by (not too much) noise in the transmission over the channel. There has been a great deal of theoretical and applied work in this subject since the famous paper of Shannon in 1949. Applications of coding range from the lowly Hamming codes used in dynamic memories to the sophisticated Reed-Solomon codes used in compact disks and in many commercial and military systems. There are also convolutional codes widely used in satellite systems.

Computer algebra is devoted to the investigation of algorithms, computational methods, software systems and computer languages, oriented to scientific computations performed on exact and often symbolic data, by manipulating formal expressions by means of the algebraic rules they satisfy. It studies such problems from three different but confluent viewpoints: a) development and analysis of algebraic algorithms (both from the viewpoint of practical performance and of theoretical complexity); b) design and analysis of software systems for symbolic manipulation; c) applications of scientific and/or technological systems. It is important to stress that the mathematical theories to which computer algebra applies are not necessarily only the algebraic ones: polynomial equations, algebraic geometry, commutative algebra and group theory have a well-established research activity using symbolic computation techniques, but the same is equally

true for analytic theories, e.g. differential equations, as shown by a couple of papers in these proceedings. Computer algebra views algebra more as a method than as an object of research.

In the past, coding has interacted with group theory, combinatorics and finite geometries (the proof of the non-existence of a projective plane of order 10 by a coding approach is a recent example). More recently it has developed remarkable and unexpected connections with algebraic geometry and number theory (Goppa's algebraic geometric codes, Serre's improvement on Weil's bound for number of points of curves over finite fields, the p-adic Serre bound, improvements on Ax and Chevalley-Waring Theorems, etc.). This connection is creating links between the two major areas represented in AAEC, coding theory and computer algebra, e.g. by the use of Gröbner bases for decoding algebraic geometric codes or other algebraic codes.

Questions of complexity are naturally linked with the computational issues of both coding theory and computer algebra and represent an important share of the area which AAEC aims to cover; the same holds for cryptography where algebraic techniques are gaining relevance.

Finally let us mention the area of sequence design or spread spectrum multiple access, represented here by an invited contribution: originally developed in the Second World War for communications in a hostile environment where the enemy tries to jam one's message, it now includes non-military applications such as mobile radio, cellular telephony, and wireless computer communications.

Except for AAEC 1 (*Discrete Mathematics*, **56**,1985) and AAEC 7 (*Discrete Applied Mathematics*, **33**,1991), the proceedings of all the symposia are published in Springer *Lecture Notes in Computer Sciences*, Vols. 228, 229, 307, 356, 357, 508, 539.

It is a policy of AAEC to maintain a high scientific standard, comparable to that of a journal, and at the same time a fast publication of the proceedings. This is made possible only thanks to the cooperation of a large body of referees.

We aimed to have each submission evaluated by at least three referees, and we failed only in 9 cases. We had 147 independent reports from 105 referees on the 47 submissions. Of these, 6 were withdrawn during the procedure, 12 were rejected, 7 accepted for oral presentation only, 22 accepted for oral presentation and inclusion in the proceedings. The proceedings also contain six invited contributions; a seventh, by G. Lachaud, was not received in time for inclusion in the proceedings.

The conference was organized by the University of Puerto Rico and sponsored by the Army Research Office Cornell MSI project and by the NSF EPSCoR of Puerto Rico project.

We express our thanks to the staff of the Gauss Laboratory of the University of Puerto Rico and especially to Tita Santos, for handling the local organization, and to the Springer-Verlag staff and especially to A. Hofmann for their help in the preparation of these proceedings.

Conference Board

Gerard Cohen (Paris), Teo Mora (Genova), Oscar Moreno (Puerto Rico)

Conference Committee

T. Beth (Karlsruhe), J. Calmet (Karlsruhe), G. Cohen (Paris), M. Giusti (Palaiseau), J. Heintz (Buenos Aires), H. Imai (Yokohama), H. Janwa (Bombay), R. Kohno (Yokohama), H. F. Mattson (Syracuse), A. Miola (Roma), T. Mora (Genova), O. Moreno (Puerto Rico), A. Poli (Toulouse), T. R. N. Rao (Lafayette, LA), S. Sakata (Toyohashi)

Referees

G. Attardi, T. Beth, E. Biglieri, D. Bini, M. Blaum, M. Bronstein, D. Brusch, G. Butler, P. Camion, J.F. Canny, H. Chabanne, I. Chakravarti, A. Chan, P. Charpin, M. Clausen, A. Cohen, G. Cohen, D. Coppersmith, J. Davenport, J.L. Dornstetter, L.A. Dunning, A. Duval, D. Duval, T. Etzion, H.J. Fell, G.L. Feng, R. Froemberg, G. Gallo, Z. Ge, W. Geiselmann, M. Giusti, S. Goldwasser, D. Gordon, M. Goresky, R. Grossman, S. Harari, J. Heintz, T. Hellese, H. Imai, H. Janwa, J. Justesen, M. Kalkbrener, E. Kaltofen, A. Kerber, N. Kobitz, R. Kohno, G. Lachaud, W. Lassner, D. Lazard, D. Lebrigand, S. Litsyn, A. Logar, I. Luengo, H.S. Maini, H.F. Mattson, H.M. Möller, T. Mora, R. Morelos-Zaragoza, O. Moreno, J. Moulin-Ollagnier, D. Mundici, H. Niederreiter, A.M. Odlyzko, F. Ollivier, G. Persiano, K.T. Phelps, V. Pless, A. Poli, C. Pomerance, T.R.N. Rao, T. Recio, J.J. Risler, L. Robbiano, F. Rodier, M.F. Roy, S. Sakata, R. Safavi-Naini, B.D. Saunders, W. Schmidt, R. Schoof, C. Scovel, J. Seberry, W. Seiler, N. Sendrier, A. Sgarro, K. Shirayanagi, M. Singer, P. Sole, H.J. Stetter, D.R. Stinson, B. Sturmfels, M. Sweedler, M. Szegedy, A. Tietavainen, H.C.A. van Tilborg, J. van Tilburg, L. Tolhuizen, C. Traverso, K. Tzeng, U. Vaccaro, F. Vatan, S. Vladut, J. Wolfmann, H. Yoshida, G. Zemor.

Contents

Invited Contributions

Sequence Based Methods for Data Transmission and Source Compression A.R. Calderbank, P.C. Fishburn (AT&T), A. Rabinovich (Stanford Univ.)	1
On the Apparent Duality of the Kerdock and Preparata Codes A. R. Hammons Jr. (Hughes Aircraft Co.), P. V. Kumar (USC, Los Angeles), A. R. Calderbank (AT&T), N.J.A. Sloane (AT&T), P. Solé (CNRS, Sophia Antipolis)	13
Bounds for Codes as Solutions of Extremum Problems for Systems of Orthogonal Polynomials V. Levenshtein (Keldysh Inst., Moscow)	25
Systems of Algebraic Equations Solved by Means of Endomorphisms H.M. Möller (Hagen Univ.)	43
Criteria for Sequence Set Design in CDMA Communications R.A. Scholtz (USC, Los Angeles)	57
Using Groebner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: Return of the Killer Tag Variables M. Sweedler (Cornell Univ.)	66

Submitted Contributions

A "Divide and Conquer" Algorithm for Hilbert-Poincaré Series, Multiplicity and Dimension of Monomial Ideals A. M. Bigatti (Univ. Genova), P. Conti (Univ. Pisa) L. Robbiano (Univ. Genova), C. Traverso (Univ. Pisa)	76
An Efficient Algorithm for the Sparse Mixed Resultant J.F. Canny, I. Emiris (Univ. California, Berkeley)	89
Some Features of Binary Block Codes for Correcting Asymmetric Errors G. Fang, H.C.A. van Tilborg, F.W. Sun (Eindhoven Univ.), I.S. Honkala (Univ. Turku)	105
Fixed-Parameter Complexity and Cryptography M.R. Fellows (Univ. Victoria, Canada), N.Koblitz (Univ. Washington, Seattle)	121
A Class of Algebraic Geometric Codes from Curves in High-Dimensional Projective Spaces G.L. Feng, T.R.N. Rao (Univ. SW Louisiana, Lafayette)	132
A New Class of Sequences: Mapping Sequences G. Gong (Fond. Bordoni, Roma)	147
A Zero-Test and an Interpolation Algorithm for the Shifted Sparse Polynomials D. Grigoriev (Pennsylvania State Univ.), M. Karpinski (Univ. Bonn)	162

Parallelization of Quantifier Elimination on a Workstation Network H. Hong (RISC, Linz)	170
Hyperplane Sections of Fermat Varieties in P^3 in Char. 2 and Some Applications to Cyclic Codes H. Janwa (Centre Adv. Studies Math. Bombay), R.M. Wilson (Caltech, Pasadena)	180
Analysis of Coppersmith's Block Wiedemann Algorithm for the Parallel Solution of Sparse Linear Systems E. Kaltofen (RPI, Troy)	195
Relations Among Lie Formal Series and Construction of Symplectic Integrators P.-V. Koseleff (Ec. Polytechnique, Palaiseau)	213
Exponential Sums as Discrete Fourier Transform with Invariant Phase Functions G. Lachaud (CNRS, Luminy)	231
Application of Finite Fields to Memory Interleaving A. Lempel, G. Seroussi (Hewlett-Packard, Palo Alto)	244
An Elementary Proof of a Partial Improvement to the Ax-Katz Theorem O. Moreno (Univ. Puerto Rico), C.J. Moreno (CUNY, N. Salem) ...	257
Energy Functions Associated with Error-Correcting Codes C. Rentería (IPN, Mexico), H. Tapia-Recillas (UAM, Mexico)	269
On Determining All Codes in Semi-Simple Group Rings R. E. Sabin (Loyola Coll., Baltimore)	279
On Hyperbolic Cascaded Reed-Solomon Codes K. Saints, C. Heegard (Cornell Univ., Ithaca)	291
Peak-Shift and Bit Error-Correction with Channel Side Information in Runlength-Limited Sequences Y. Saitoh, I. Ibe (Yokohama Univ.), H. Imai (Univ. Tokyo)	304
On a Third Order Differential Equation whose Differential Galois Group is the Simple Group of 168 Elements M.F. Singer, F. Ulmer (NCSU, Raleigh)	316
Approximating the Number of Error Locations within a Constant Ratio is NP-complete J. Stern (ENS, Paris)	325
Two Chosen Plaintext Attacks on the Li-Wang Joint Authentication and Encryption Scheme J. van Tilburg (PTT, Leidschendam)	332
Some Constructions of Perfect Binary Codes A. Vardy (IBM, San Jose), T. Etzion (Technion, Haifa)	344
Authors' Index	355