Lecture Notes in Computer Science 539

Edited by G. Goos and J. Hartmanis

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

H. F. Mattson T. Mora
T. R. N. Rao (Eds.)

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes

9th International Symposium, AAECC-9
New Orleans, LA, USA, October 7-11, 1991
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Volume Editors

Harold F. Mattson
School of Computer and Information Science 4-110
Center for Science and Technology, Syracuse University
Syracuse, NY 13244-4100, USA

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

T. R. N. Rao
Center for Advanced Computing Studies
University of Southwestern Louisiana
P.O. Box 44330, Lafayette, LA 70504-4330, USA

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

ISBN 3-540-54522-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-54522-0 Springer-Verlag New York Berlin Heidelberg

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

Foreword

The Ninth International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC 9) held in New Orleans, October 7-11, 1991 was organized by a Conference Committee of 15 members and a Conference Board consisting of H. F. Mattson, Jr., T. Mora, and General Chair T.R.N. Rao. T. Mora was in charge, with the assistance of H.F. Mattson, of the refereeing procedure. The local organization was the care of W. R. Edwards and W. Patterson.

The aim of AAECC 9 was 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 concepts and theories and algorithmic techniques for the concrete manipulation of objects.

While in principle covering each area related to applications of algebra to communication and computer sciences, by their previous history the AAECC Symposia are mainly devoted to research themes 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. Interestingly coding has not only taken from mathematics but it has contributed to mathematics: the nonexistence of the projective plane of order 10 is the latest result in mathematics which owes its proof to a coding approach.

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 view points: 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.

AAECC Symposia (the acronym has shifted meaning from year to year) began in 1983 under the leadership of Alain Poli (Toulouse) who organized, together with R. Desq, D. Lazard and P. Camion, the first International Colloquium on "Algebra and Error Correcting Codes: Theory and Applications", held in Toulouse, France, in June 1983 and whose proceedings are collected in *Discrete Mathematics*, Vol. 56 (1985).

A second AAECC Symposium was again held in Toulouse, October 1984. The proceedings appeared as Lecture Notes in Computer Science (LNCS), Vol. 228, edited by A. Poli, 1986.

The third, held in Grenoble, France, July 1985, was chaired by J. Calmet. The proceedings appeared as LNCS 229, edited by J. Calmet, 1986. Here it appeared that the series was filling a communication gap among researchers in error correcting codes, applied algebra and algebraic algorithms. It was then decided that the AAECC Symposia were to be held in different countries annually. A permanent organizing committee was set up, consisting of: T. Beth, J. Calmet, A. C. Hearn, J. Heintz, H. Imai, H. Lüneburg, H.F. Mattson Jr., A. Poli.

Subsequent Symposia were:

AAECC 4, Karlsruhe, FRG, September 1986, chaired by T. Beth and H. Lüneburg, LNCS 307, edited by T. Beth and M. Clausen, 1988.

AAECC 5, Mahon, Menorca Island, Spain, June 1987, chaired by L. Huguet and A. Poli, LNCS 356, edited by L. Huguet, 1989.

AAECC 6, Rome, Italy, July 1988, chaired by A. Miola and A. Poli, LNCS, 357, edited by T. Mora, 1989. (This Symposium was held jointly with the International Symposium on Symbolic and Algebraic Computation ISSAC'88)

AAECC 7, Toulouse, France, June 1989, chaired by A. Poli, *Discrete Applied Mathematics*, edited by H. F. Mattson, Jr. and T. Mora, 1991.

AAECC 8, Tokyo, Japan, August 1990, chaired by H. Imai and A. Poli, LNCS, 508, edited by S. Sakata, 1991 (again held jointly with the ISSAC'90 Symposium).

Because of the increasing success of the Conference, its broader audience and wider scope, the need was felt for a reorganization, in order to obtain a better integration of the different research areas contributing to it and a faster, while still high-level, refereeing and editorial procedure.

To this end a meeting of the AAECC 8 Organizing Committee, held in Tokyo, on August 23rd, 1990, took several decisions. We report here excerpts of the Minutes of that meeting:

Officers of the Conference

(...) the officers of AAECC are a Conference Committee of 12-15 members, a local organizer, and a Conference Board consisting of three persons. Their roles are as follows:

the Conference Committee consists of 12-15 persons to stay in charge for one conference; it is responsible for the scientific management of the Conference. (...) Its tasks are to appoint the next Conference Committee and, among its members, the next Conference Board; to fix the topics of the conference; to appoint the place and the local organizer of the conference 2 years in advance; to contribute to the selection process (...); to suggest invited speakers. (...)

The Conference Committee chooses three persons among the appointed members of the next Conference Committee to act as Conference Board. (...) Its task is to organize the referee procedure, to organize the editorial procedure, to edit the Proceedings, to choose invited speakers (together with the local organizer), to support the local organizer for any problem which could arise.

Referee and Editorial Procedure

(...) full papers only (perhaps in a draft form, but not extended abstracts) approximately 12 pages long, together with an abstract, are to be submitted to the Conference Board (...); submissions are distributed to three referees each (...) All decisions related to the referee and editorial procedure are a joint task and the exclusive responsibility of the Conference Board.

Deadlines for the Editorial Procedures

(...) The O.C. (...) suggested that Proceedings be usually available at the conference.

Periodicity of the Conference

(...) it was agreed to hold the Conference every second year in the odd years.

Official Language of the Conference

English is the only official language of the Conference and the Proceedings, to guarantee maximum communication among participants.

We express our thanks to the Local Organization and to the Conference Committee for their contribution to the organization of AAECC 9, to the Springer-Verlag staff and especially to A. Hofmann for their help in the preparation of these proceedings.

H. F. Mattson, Jr., T. Mora, T.R.N. Rao
Conference Board Members

July 1991

Preface

Each of the full papers submitted to AAECC 9 was evaluated by at least two international referees (the average number of referees per paper being 2.88). Out of the 78 contributions, 40 were accepted for inclusion in the Proceedings and oral presentation at the conference, and 19 more were accepted for oral presentation only. The Proceedings contain five invited contributions, which also underwent a referee screening. A sixth invited talk, *Algebra as an Organizing Principle in Parallel Processing*, by M. R. Fellows, was not received in time for inclusion in the Proceedings.

The topics of the symposium were:

- Error Correcting Codes, Theory and Applications
- Algebraic Algorithms
- Computational Methods and Complexity Issues in Computational Algebra and Geometry
- Cryptography and Security
- Applications of Information Theory to Computing

Handling the refereeing procedure for a conference of such broad scope would not have been possible without the involvement and the dedication of a large body of scientists with different competencies; 135 persons contributed to the procedure, either acting as referees themselves, or by suggesting and procuring suitable referees. Their names are listed below; while apologizing for any involuntary omission, I want to express to all of them my most sincere thanks for their precious help.

The considerable expenses required by the procedure were mostly covered by the Mathematics Department of the University of Genova.

There is a person without whom the refereeing procedure would not have been completed; he not only edited himself some of the papers, including the toughest ones, he was a constant source of advice and encouragement and only his support allowed me to overcome the many difficulties I met: it is a pleasure to thank Skip Mattson for his invaluable role in the refereeing procedure.

Teo Mora

July 1991

Conference Officers

Conference Board

Harold F. Mattson (Syracuse), Teo Mora (Genova), T. R. N. Rao (Lafayette, LA)

Conference Committee

T. Beth (Karlsruhe), J. Calmet (Karlsruhe), G. Cohen (Paris), M. Giusti (Palaiseau), W. Edwards (Lafayette, LA), J. Heintz (Buenos Aires), H. Imai (Yokohama), R. Kohno (Yokohama), H. F. Mattson (Syracuse), A. Miola (Roma), T. Mora (Genova), W. Patterson (New Orleans), A. Poli (Toulouse), T. R. N. Rao (Lafayette, LA), S. Sakata (Toyohashi)

Local Arrangement Committee

Wayne Patterson (New Orleans), William R. Edwards (Lafayette, LA)

Referees

M.E. Alonso, F. Annexstein, T. Becker, G. Beenker, R. Benedetti, E.R. Berlekamp, J.C. Bermond, E. Biglieri, I.F. Blake, M. Blaum, M. Bronstein, A.E. Brouwer, J. Calmet, P. Camion, J. Canny, G. Carrà Ferro, I. Chakravarti, M. Chardin, P. Charpin, F. Chung, G. Clark, M. Clausen, G. Cohen, A.M. Colla, J.H. Davenport, J. Delladora, A. Di Porto, L.A. Dunning, A. Dür, W.R. Edwards, H.J. Fell, M. Fellows, G.L. Feng, A. Ferro, T. Fuja, M. Galbiati, A. Galligo, G. Garibotto, J. von zur Gathen, C. Ghezzi, M. Giusti, M. Goto, D. Grigor'ev, C. Günther, H.E. Heatherly, J. Heintz, T. Helleseth, J.P.G. Henry, K. Hole, X. Hou, H. Imai, K. Iwamura, H. Janwa, M. Kalkbrener, W. Kantor, K. Karplus, R. Kohno, T. Krick, G. Lachaud, E. Lander, D. Lazard, P. Lescanne, S. Litsyn, A. Lobstein, A. Loeliger, A. Logar, I. Luengo, J.B. Marston, J.L. Massey, H.F. Mattson, M. MacCallum, M. Merle, M. Mignotte, A. Miola, H.M. Möller, C. Moreno, O. Moreno, V. Morgavi, J. Morgenstern, M. Morii, D. Mundici, A. Nückel, A. Odlyzko, F. Ollivier, I. van Overveld, C. Park, A. Pethö, V. Pless, A. Poli, L. Pottier, P. Rabizzoni, M. Raimondo, T.R.N. Rao, T. Recio, S. Ridella, J.J. Risler, R. Rivest, L. Robbiano, M.F. Roy, R. Rueppel, Y. Saitoh, S. Sakata, R. Schoof, G. Seroussi, A. Sgarro, M. Singer, M. Sipser, J. Snyders, P. Solé, P. Solerno, B. Teissier, A. Tietavainen, H. van Tilborg, J. van Tilburg, A. Tognoli, L. Tolhuizen, C. Traverso, V. Trevisan, K. Tzeng, U. Vaccaro, A. Valibouze, G. Valla, B. Vallée, W. Vasconcelos, A.T. Vasquez, R. Vilareal, J. Villard, P. Wang, V.K. Wei, V. Weispfenning, J. Wolfmann, W. Wolfowicz, K. Yamaguchi, Ø. Ytrehus, G. Zémor.

Contents

Invited Contributions

Submitted Contributions