Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

229

Algebraic Algorithms and Error-Correcting Codes

3rd International Conference, AAECC-3
Grenoble, France, July 15–19, 1985
Proceedings

Edited by Jacques Calmet

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Editor

Jacques Calmet
LIFIA, BP 68
38402 Saint Martin d'Hères Cédex, France

CR Subject Classifications (1985): E.4, I.1

ISBN 3-540-16776-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-16776-5 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2145/3140-543210

PREFACE

The AAECC conferences began in Toulouse in 1983. The proceedings of AAECC-1 were published as a special issue of Discrete Mathematics. The proceedings of AAECC-2 are also published by Springer-Verlag as a volume in the Lecture Notes in Computer Science series. This third conference was organized by the "Laboratoire d'Informatique Fondamentale et d'Intelligence Artificielle" (LIFIA) in Grenoble on July 15-19, 1985. It was held in the building of the "Ecole Nationale Supérieure d'Ingénieurs en Informatique et Mathématiques Appliquées" of the National Polytechnic Institute of Grenoble.

The main motivation for this series of conferences was to gather researchers in error-correcting codes, applied algebra and algebraic algorithms. The latter topic has been extended to computer algebra in general. Applied algebra must be understood as applied to computer science. After three conferences, it appears that they fill a communication gap. It is thus natural that the AAECC conferences are going to be held annually in different countries. For this reason, a permanent organizing committee has been set up. It consists of: Thomas Beth, Jacques Calmet, Anthony C. Hearn, Joos Heintz, Hideki Imai, Heinz Lüneburg, H.F. Mattson Jr. and Alain Poli. The next conferences will be held in Karlsruhe (1986), Barcelona (1987), Pisa or Roma (1988), Toulouse (1989) and Yokohama (1990).

I am very grateful to the following institutions and organizations for their generous funding of the conference:

. DRET (Direction des Recherches, Etudes et Techniques du Ministère de la Défense)
. CNRS (Centre National de la Recherche Scientifique)
. SMF (Société Mathématique de France)
. INPG (Institut National Polytechnique de Grenoble)
. Mairie de Grenoble
. Conseil Général de l'Isère.

No conference is successful without many people contributing their time and efforts in its preparation. The referees did an excellent job in reading and evaluating many papers in a very short amount of time, both before and after the meeting was held. The session chairpersons were very efficient in keeping the conference on tracks. A special thanks is deserved by Alain Poli who made available to me his experience of organizing the previous AAECC conferences.
The local organization ran smoothly because of the help of Ph. Chatelin. Isabelle Michel has been a very efficient and pleasant conference secretary. G. Veillon, the ENSIMAG director, provided us with all the help we required. I extend my warmest thanks to all of them.

Jacques Calmet
May 1986

ORGANIZING COMMITTEE

Th. BETH, University of London, England and University of Karlsruhe, FRG
J. CALMET, LIFIA, Grenoble, France **(Conference Chairman)**
A.C. HEARN, The Rand Corporation, Santa Monica, USA
H. LÜNEBURG, University of Kaiserslautern, FRG
A. POLI, University Paul Sabatier, Toulouse, France

SCIENTIFIC COMMITTEE

B. BUCHBERGER, University J. Kepler, Linz, Austria
P. CAMION, INRIA, Rocquencourt, France
B.F. CAVINESS, University of Delaware, Newark, USA
G.E. COLLINS, University of Wisconsin at Madison, USA
B. COURTEAU, Sherbrooke University, Canada
J.H. DAVENPORT, University of Bath, England
E. ENGELER, ETH, Zürich, Switzerland
J. HEINTZ, Univ. Frankfurt and IAM, Buenos Aires, Argentina
L. HUGUET, Autonomous University of Barcelona, Spain
H. IMAI, Yokohama National University, Japan
D. LAZARD, University of Paris VI, France
R. LOOS, University of Karlsruhe, FRG
H.F. MATTSON Jr., Syracuse University, USA
A. MIOLA, IASI-CNR, Roma, Italy
Ph. PIRET, Philips Research Lab., Brussels, Belgium
C.C. SIMS, Rutgers University, New Brunswick, USA
H. ZASSENHAUS, Ohio State University, Colombus, USA

LOCAL ORGANIZATION: J. CALMET and Ph. CHATELIN, LIFIA, Grenoble, France

List of Referees

J.A. Abbott, Th. Beth, B. Buchberger, R. Caferra, J. Calmet, P. Camion, B.F. Caviness, G. Cohen, G.E. Collins, B. Courteau, J.H. Davenport, K. Dittenberger, E. Engeler, R. Gebauer, K.O. Geddes, A.C. Hearn, J. Heintz, L. Huguet, H. Imai, D. Lazard, A. Leitsch, R. Loos, H. Lüneburg, H.F. Mattson Jr., A. Miola, F. Mora, J. Padget, Ph. Piret, A. Poli, C.C. Sims, J. Smit, F. Winkler, H. Zassenhaus.

Session chairpersons

M. Bergman, B.Buchberger, P. Camion, B. Courteau, K.O. Geddes, C. Goutelard, A.C. Hearn, J. Heintz, L. Huguet, H. Imai, H. Lüneburg, T. Matsumoto, H.F. Mattson Jr., A. Miola, F. Mora, M.F. Newman, A. Poli, V. Weispfenning, J. Wolfmann.

TABLE OF CONTENTS

Introduction

This volume includes 42 of the talks presented at the AAECC-3 conference and an abstract of an invited lecture. The topics of the conference were: error-correcting codes, applied algebra, algebraic algorithms and symbolic computation. In addition to the papers selected for this volume, informal talks and demonstrations were also part of the conference. These proceedings do not reflect the 19 sessions which took place since many communications are not part of them. They are organized according to the three main topics covered by AAECC-3 in the following ordering: error-correcting codes, applied algebra and computer algebra. What is still respected is the order of presentation of the talks within each of these topics.
It was intended by the organizers to cover not only the algebraic parts of error-correcting coding theory and computer algebra, but also to present the aspects of these fields concerned by applications and their link with and impact on technology. We do hope that these proceedings illustrate this aim.
Another goal of this series of conferences is to stimulate communication and cooperation between scientists working in domains which have many common features but using different approaches. It looks like this goal has also been achieved. We expect to see an illustration of this statement in the proceedings of the forthcoming conferences.

A last introductory remark is that this volume may be seen as an illustration of the present trend integrating computer science and communication theory. In this present example,the computer algebra field of computer science and security of communications are investigated. Applied algebra is by no mean foreign to this integration: it is the common language.