Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

388

G. Cohen J. Wolfmann (Eds.)

Coding Theory and Applications

3rd International Colloquium
Toulon, France, November 2–4, 1988
Proceedings

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

Editors

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

Jacques Wolfmann
G.E.C.T., Université de Toulon
F-83130 La Garde, France

Scientific Committee

G. Battail (ENST, Paris)
J. C. Bic (CNET, Paris)
B. Bouchon (CNRS)
P. Camion (CNRS)
P. Charpin (Paris VI)
G. Cohen (ENST, Paris)
J. Conan (Polytechnic of Montreal)
B. Courteau (University of Sherbrooke)
J. L. Dornstetter (LCT, Paris)
Y. Driencourt (Luminy)
P. Farrel (Manchester)
P. Godlewski (ENST, Paris)
C. Goutelard (LETTI, Paris)
D. Haccoun (Polytechnic of Montreal)
S. Harari (GECT, Toulon)
G. Lachaud (CIRM, Luminy)
P. Laurent (Thomson CSF DTC)
S. Lebel (SCCST)
J. F. Michon (Paris VII)
M. Minoux (DEI)
A. Oisel (Bull)
D. Perrin (Paris VII)
P. Piret (Philips Res. Bruxelles)
A. Poli (AAECC, Toulose)
J. Wolfmann (GECT, Toulon)

CR Subject Classification (1987): E.4, E.3

ISBN 3-540-51643-3 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-51643-3 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210 – Printed on acid-free paper

PREFACE

The colloquium "Trois Journées sur le Codage" held in Toulon, France, from 2nd to 4th November 1988 was the third one of this type. The previous one took place in Cachan, France in 1986 ; its proceedings appear in Lecture Notes in Computer Science, Volume 311 (G. Cohen, P. Godlewski, Eds).

The Toulon meeting gathered approximately one hundred scientists and engineers, mostly from France, but also from Belgium, Finland, Holland, Germany, USA.

These colloquia are characterized by a very broad spectrum, ranging from algebraic geometry to implementation of coding algorithms. The proceedings have been divided into four parts, each one introduced by an invited address.

1. CODING AND ALGEBRAIC GEOMETRY

Since the appearance, about ten years ago, of the work by Goppa on his construction of geometric codes, interest was growing on the links between codes and algebraic curves on finite fields. One of the main tools in this last area is the use of character sums. In his invited paper A. Tietäväinen shows how character sums can give bounds on covering radius and minimum distance. In the paper by Caral, Rotillon, Thiong Ly, the Goppa construction is applied to Artin -Schreier curve parameters and generator matrices of the corresponding codes are given. Improving an asymptotic bound concerning the number of points of algebraic curves, M. Perret introduces new families of codes exceeding the Varshamov-Gilbert bound. In her paper D. Le Brigand presents an algorithm to factorize polynomials F(x,y) over a perfect field. The main idea is to use a generalization of the Brill-Noether algorithm already used to obtain generator matrices of the Goppa geometric codes . The work by J. Wolfmann is devoted to deriving new bounds on cyclic codes from bounds on algebraic curves, which may themselves be found in the contribution of G. Lachaud on special equations over finite fields obtained by using deep results in algebraic geometry.

2. INFORMATION THEORY, DECODING AND CRYPTOGRAPHY

This section starts with an invited survey paper by P. Piret on a postal channel involving three users : a sender E transmits information to a receiver G through a mailbox operated by a postman F. The problem has an information-theoretic or cryptographic flavour, according to the degree of cooperation between E and F to inform G.In some intermediate "pacific" situations, E and F should clearly agree on a strategy for transmitting. Piret shows a simple case where time-sharing is not optimal, and conjectures that it is never optimal !

The paper by S. Harari presents an authentication algorithm based on the NP-completeness of the problem of finding codewords of a given weight in a general linear code. Some modified versions are given allowing identification and signature. The parameters of the system should be chosen cautiously, as stressed in the paper by J. Stern, which describes a probabilistic algorithm for finding small weight codewords in codes.

Another NP-complete problem is the complete decoding of linear block codes. Variations on this theme are the topic of the following four papers. G. Cohen et al. elaborate on the concept of projecting set. This set will be of "small" size (though exponentially increasing with the dimension), while retaining the property of being an "exhaustive summary" of the code, allowing maximum-likelihood decoding. G. Battail discusses weighted decoding of linear block codes by solving a system of implicit equations, where coefficients are obtained from the generator matrix and prior algebraic values associated with received bits. Simulation results are given in the AWGN case for the Golay [23,12,7], the [31,16,7] and [63,36,11] BCH codes.

In a similar vein, R. Sfez and J.C. Belfiore consider suboptimum symbol-by-symbol weighted-output decoding and specify some optimality/complexity trade-offs.

Y. Zhu and P. Godlewski deal with generalized minimum distance decoding for codes of rate 0.5. This generalized distance incorporates the reliability of code symbols and decoding is with maximum likelihood. Computer simulations are given for concatenated schemes with AWGN.

3. COMBINATORIAL AND ALGEBRAIC ASPECTS

The invited paper by H.C.A van Tilborg is devoted to a survey of recent methods concerning burst-correcting codes possessing interesting combinatorial or algebraic structures with respect to correcting properties and complexity. A description of two new methods for computing the minimum polynomial of an element in a finite field is given by J.A. Thiong Ly. The paper by P. Solé contains a construction of a quaternary cyclic code analogous to the cyclic simplex binary code. In his presentation C. Carlet obtains a new description of the Kerdock codes. The note by P. Rabizzoni gives rise to a bound on the weight of the q-ary image of a linear code over an extension field of GF(q). A semi-distributed self-diagnostic algorithm for Hypercube networks is proposed by A. Ghafoor and P. Solé. Recently the non-existence of a projective plane of order 10 was proved by using a powerful computer ; a contribution to a logical proof is given by J.F. Maurras who investigates configurations and designs associated with such a plane. P. Fitzpatrick and C.H. Norton consider linear recurring sequences with entries from a factorial domain and give algorithms generalizing the extended Euclidian algorithm and the Berlekamp-Massey algorithm .

4. APPLICATIONS

The invited paper by J.L. Dornstetter describes briefly the main features of the GSM mobile radio system, the future European standard. Emphasis is placed on transmission aspects and channel coding.

G. El Zein et al. present the conception and realization of a direct-sequence spread-spectrum digital mobile radio transmission at 910 MHz. J.L. Dalmau et al. design error-correcting schemes to evaluate the HF digital mobile radio channel (3-30 MHz), focusing on burst errors. They have carried out simulations using various concatenated schemes and compared their performances.

Jamming is the concern of the following two contributions. C. Schlegel and D. Costello discuss bandwidth efficient data transmission using trellis coded modulation (TCM) on channels with jamming and impulse noise, an extension of the AWGN case. New TCM are given and evaluated, which behave better than those designed for the AWGN channel.

P. Sadot and J.L. Politano propose a new treatment against high energy partial time jammers, based on codes correcting errors and erasures, instead of the classical spread spectrum + ECC scheme. In a similar environment - very noisy channel - P. Camion and J.L. Politano evaluate a coding design for erasure and error correction based on a RS [14,7] concatenated with a binary [8,4] Hamming code. Finally, C. Narçon proposes a solution for designing and implementing an asynchronous transmission process by code division multiple access.

The book ends with a note by G. Battail "Is minimal distance a good criterion ?" and two open problems by P. Solé : "Covering radius of the circuit code" and "Cyclic codes over rings and p-adic fields" .

Gérard Cohen Jacques Wolfmann

LIST OF REFEREES

G. BATTAIL, J.C. BELFIORE, J.C. BIC, P. CAMION, P. CHARPIN, G. CHASSE, G. COHEN, J.L. DORNSTETTER, Y. DRIENCOURT, S. HARARI, G. LACHAUD, P. LE BRIGAND, A. LOBSTEIN, B. PONSARD, C. RODRIGUEZ, J. STERN, A. THIONG LY, J. WOLFMANN, G. ZEMOR.

CONTENTS

1. CODING AND ALGEBRAIC GEOMETRY 1

2. INFORMATION THEORY, DECODING AND CRYPTOGRAPHY 77

3. COMBINATORIAL AND ALGEBRAIC ASPECTS 163