Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

311

G. Cohen P. Godlewski (Eds.)

Coding Theory and Applications

2nd International Colloquium
Cachan-Paris, France, November 24–26, 1986
Proceedings

Springer-Verlag

Editors

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

Philippe Godlewski
Département Réseaux
Ecole Nationale Supérieure des Télécommunications
46, rue Barrault, F-75634 Paris Cedex 13, France

CR Subject Classification (1987): E.4, G.2.1, F.2.1

ISBN 3-540-19368-5 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-19368-5 Springer-Verlag New York Berlin Heidelberg

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

Preface

The colloquium *"Trois Journées sur le Codage"* , held in Cachan near Paris, France from 24th to 26th November 1986, was the second one of this type. It aimed at gathering together approximately one hundred scientists and engineers, mostly from France. With its broad spectrum, ranging from algebraic geometry to implementation of coding algorithms, it was a unique opportunity for contact between university and industry on the topics of information and coding theory.

It is a great pleasure to acknowledge the efforts of Professor Goutelard who played a great part in making the organization of these "3 journées" a success.

We would like to thank the organizing institutions for their help: DRET, LETTI and BULL s.a., the Advisory Board, the Scientific Committee, the Sponsoring Committee, Editors and referees of Springer-Verlag, and our own referees (see "List of Referees") with a special mention for Gilles Zemor.

These contributed papers allow a survey of "hexagonal" research (cf. fig. 1) in coding. The purpose of this introduction is to provide a quick first visit. It has its drawbacks as do most tourist guides: simplifications or information of a local or anecdotal type ... but it mainly aims at giving a taste of French production, in a area different from cookery or wine.

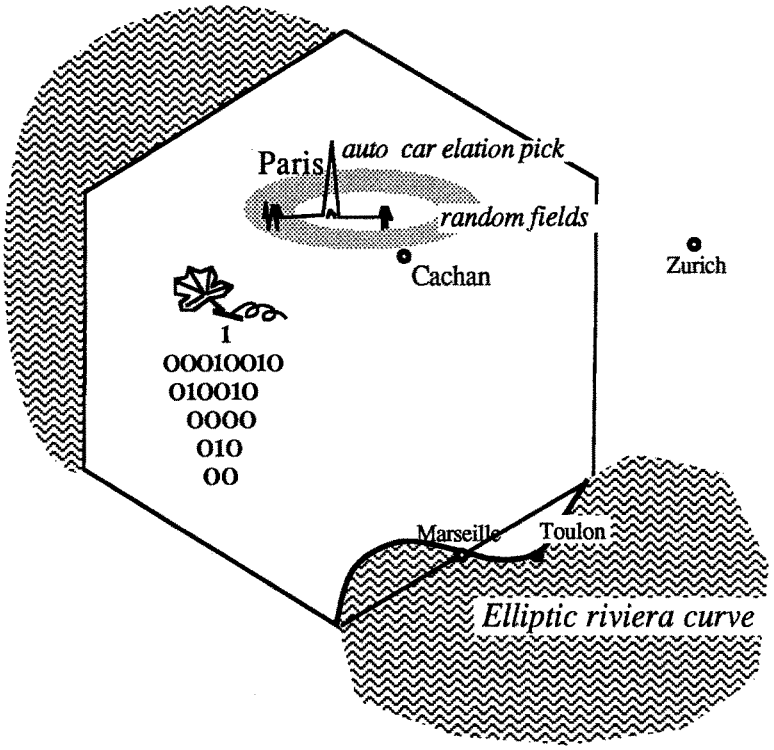

Fig. 1 : French Hexagon

The proceedings begin with the texts of two "almost French" invited speakers: Toby Berger, at that time on sabbatical at ENST, and James Massey, from ETH, Zürich.

The first invited address was on "Information Theory in Random Fields". A random field is a family of random variables with multidimensional parameter set. Random fields provide mathematical models for distributed sources of information. Channels that link an input and an output random field are also of interest.

The second one, entitled "Linear Complexity in Coding Theory", connected different problems: Blahut's Theorem on algebraic decoding, linear complexity of periodic sequences and minimum distance bounds of cyclic codes. These enlightening

connections allow the various generalizations of the BCH bound to be gathered into a unified presentation .

1. CODING AND COMBINATORICS

Links between Coding and Combinatorics are well known now, e.g. between designs and perfect codes. The goal of this session was to further investigate them.

The paper by G. Roux is an extension of a "design-like" property from sequences over a finite alphabet to permutations. The problem considered here is of covering type: find the minimum number p(n,k) of rows in an array with n columns and elements from {1,2,...n} such that every extracted subarray of k columns contains as rows the k! permutations of the column indices. In particular, for k fixed and n large enough, the order of magnitude of p(n,k) is found to be n^{k-1}.

A more classical covering problem is studied in the paper by M. Beveraggi and G. Cohen, namely the minimal possible density μ_n for a covering of the binary n-dimensional Hamming space by spheres of radius one. It is shown that $\mu_n \leq 3/2$. Another fruitful interaction between Coding and Combinatorics occurred through algebra and association schemes. Initiated by P. Delsarte (see reference 9 in P. Solé's paper), it is extended from the Hamming case to the Lee one by P. Solé, with a generalization of Lloyd's theorem.

Another step off the classical Hamming path in Coding is taken by A. Lobstein in his paper "On Modular Weights in Arithmetic Codes". These codes are used for detecting and correcting errors in computer computations. The weight of these errors can be measured by two types of "modular distances" which do not necessarily satisfy the triangular inequality. The author investigates when these distances coincide.

2. VARIABLE LENGTH CODES

Two schools of unequal importance coexist in France. They differ from the usual approach, based on source coding problems, which can be found in most books on information theory.

The first one studies "questionnaires", following C.F. Picard. The point of view is often pragmatic and does not exclude probabilities.

The second one deals with combinatorics on the free monoid, as considered by Schützenberger; a recent book "Theory of Codes" (cf. reference 2 in A. Bertrand's paper) is characteristic of that trend. The approach is mathematical. In fact "Theory of Codes" deals with variable length codes endowed with algebraic, especially non-commutative, structures. The book has very little in common with error-correcting codes, even with "algebraic theory" as considered by, e.g. Berlekamp.

The first article by Toby Berger and Raymond Yeung studies "Optimum 1-Ended Binary Prefix Codes". Such codes can find applications for conflict resolution in a multiple access protocol where active stations are identified by a sequence of answers to queries, represented by a binary variable: 0 no transmission, 1 at least one transmission. To solve the conflict in an efficient way, the last answer should be a "1" corresponding to a successful transmission. A last "0" answer would be a revealing but time-wasting silence.

The second article by H. Akdag and B. Bouchon deals with right leaning trees (or prefix coding) that allow terminal nodes (code words) to be ordered according to their probabilities.

The paper by A. Bertrand investigates the noiseless source coding problem (i.e. how to minimize the average length for a source with given entropy) in a non-classical setting, which is connected to those emerging from constraint channel or line code problems.

3. CODING AND ALGEBRAIC GEOMETRY

Quite recently, concepts of algebraic geometry have been successfully applied to Coding, starting with the following very general idea due to Goppa (reference G in Le Brigand): take a projective algebraic curve X over a finite field K, i.e. an algebraic variety of dimension one in the projective m-space $P^m(K)$ over K; choose n rational points (i.e. with coordinates in K) on X, say $P_1, P_2, \ldots P_n$, and another rational point Q. For a fixed integer t, consider the linear space L of rational functions f(.) such that the pole of f(.) in Q is at most t. Then

$$C = \{ (f(P_1), f(P_2), \ldots, f(P_m)), f \in L\}$$

is a linear code over K. Its dimension and minimum distance can be estimated with the Riemann-Roch theorem. This very powerful technique has produced a large class of codes. Some of them lie above the Varshamov-Gilbert bound (see references 11 and 12 in the paper by Michon and Driencourt). For example, the classical definition of Reed-Solomon Codes as

$$E = \{ (f(\alpha_0), f(\alpha_1) \ldots f(\alpha_{q-1})), f \in M\},$$

where $\{ \alpha_0, \alpha_1, \ldots, \alpha_{q-1}\} = F_q$ and M = {polynomials over F_q of degree at most k-1}, can be put into the framework of Goppa codes as follows: take for X the projective line over F_q, with $P_i = (\alpha_i, 1)$, $0 \le i \le q-1$, and point Q being the point at infinity (1,0). Then choose for L the set of rational functions with no poles on the P_i's and a pole of order at most k-1 on Q.

A few extensions of these codes are studied in this book:

- One idea is to replace the curve X in Goppa codes by a variety of higher dimension (e.g. projective spaces): this in done in Lachaud's paper, where he gets projective r^{th} order Reed-Muller codes, attaining Plotkin bound for r = 1.
- Starting with the singular curve $F(X,Y,Z) = Y^2 Z^3+YZ^4+X^5 = 0$ over F_{16}, Le Brigand gets a code with parameters [n=32, k=17, d=14].

- One of Goppa's constructions involved the Hermitian curves $X_0^{s+1} + X_1^{s+1} + X_2^{s+1}$ over $PG(2,s^2)$. By embedding it for s = 2 in PG(5,4), this gave a [9,3,6] code over F_4.

- By embedding the Hermitian surface $X_0^3 + X_1^3 + X_2^3 + X_3^3 = 0$ of PG(3,4) in PG (9,4), Chakravarti obtains a [45,35,4] code over F_4.

- One goal was to improve the tables of best known codes by ad hoc constructions like concatenation. This is done in detail by Driencourt and Michon, following Barg, Katsman and Tsfasman: they use outer geometric codes on elliptic curves over F_8 or F_{16} concatenated with inner binary codes. For example, one can get a [104,32,35] binary code, decreasing the best known redundancy for such n and d by 2.

4. DECODING IN REAL SPACE

In many engineering applications, it is important to embed discrete space into real space. This can be done to improve performances of a decoding process (cf. soft or weighted decoding algorithms) or in the conception of communication systems with high spectral efficiency.

Since Ungerboeck's work, it is customary to consider codes matched to specific constellations of points in real space. These codes are adapted to Viterbi decoding which operates on a trellis. In an article "A Lower Bound on the Minimum Euclidian Distance of Trellis Codes", Marc Rouanne and Daniel J. Costello obtain a random coding bound over the set of non-linear time-varying trellis codes, which provides a means of comparing asymptotic performances of different modulation schemes.

Soft decoding algorithms have been studied for more than 25 years. With respect to the general complexity of this problem, no significant breakthrough, comparable to the

Berlekamp-Massey algorithm in the hard decoding case, has been made for a large class of codes. For general linear codes the problem is NP-complete as underlined by J. Fang et al. An interesting approach initialized by G. Battail consists of using cross-entropy minimization under the following artificial constraint: the a posteriori probability distribution is separable (i.e. the random variables corresponding to the decoded symbols are independent). Such a method can be of interest in a concatenated scheme where it is important to have weighted symbols at the input of the second decoder. The complete paper will appear in French in *Annales des Télécommunications*. J.C. Belfiore, using the same assumption on the a posteriori distribution, obtains a decoding algorithm for binary convolutional codes which belongs to the same family.

5. APPLICATIONS

Roger Alexis studies sequences with periodic autocorrelation equal to zero on 2n points round the central peak. Such sequences, called CAZAC (for Constant Amplitude and Zero Autocorrelation), are used for synchronization purposes or for estimating the transfer function of a transmission channel by sounding. The author obtains by a shortened exhaustive search all binary sequences for small length N, $N \leq 20$ and for $N = 32$, and quaternary sequences for $N \leq 12$. To transmit information over a deeply distorted and noisy channel like an underwater channel, one can use a set of sequences with suitable correlation properties. For such a channel, Gaspard Hakizimana, G. Jourdain and G. Loubet compare two signalling sets. The first one, called pseudo-orthogonal coset code, consists of sequences with small cross-correlation and out-of-phase autocorrelation (e.g. Gold Sequences). The second one, due to Yates and Holgate, involves sequences with multi-peak autocorrelation; it is more sensitive to the distribution of channel path delays but leads to simpler receivers.

Francisco Garcia-Ulgade compares 3 variants of the algebraic decoding method and gives the processing time of the corresponding algorithms implemented on a 16-bit microprocessor (M68000) for [15,9,7] and [31,25,7] Reed Solomon codes.

Paris, April 1988 Gérard Cohen and Philippe Godlewski

LIST OF REFEREES

M. Beveraggi, J.C. Bic, B. Bouchon, P. Camion, G. Cohen, J.L. Dornstetter, P. Godlewski, C. Goutelard, A. Lobstein, P. Solé, R. Vallet, J. Wolfmann, G. Zemor

COLLOQUE INTERNATIONAL

"TROIS JOURNEES SUR LE CODAGE"

PARRAINAGE SCIENTIFIQUE
ADVISORY BOARD

J.-C. BERMOND
Directeur de Recherche CNRS
P. CAMION
Directeur de Recherche CNRS-INRIA
P. FAURRE
Directeur Général de la SAGEM
Membre de l'Institut
C. GUEGUEN
Professeur à l'ENST
Directeur de l'UA 820 du CNRS
P. LALLEMAND
Directeur scientifique de la DRET
D. LAZARD
Professeur à l'Université Paris VI
Directeur du Greco "Calcul formel"
D. LOMBARD
Directeur du CNET Paris B
D. PERRIN
Professeur à l'Université Paris VII, LITP
B. PICINBONO
Professeur à l'Université Paris-Sud, Orsay
Directeur du LSS, Gif sur Yvette

COMITE D'ORGANISATION
ORGANIZING COMMITTEE

C. GOUTELARD (LETTI)
L. RIZZI (DRET)
P. GODLEWSKI (ENST)
S. HARARI (GECT)

COMITE DE PROGRAMME ET PUBLICATIONS
PROGRAM COMMITTEE

G. COHEN (ENST)
P. GODLEWSKI (ENST)
C. GOUTELARD (LETTI)

COMITE SCIENTIFIQUE
SCIENTIFIC COMMITTEE

G. BATTAIL (ENST),
J. C. BIC (CNET)
B. BOUCHON (CNRS),
P. CAMION (CNRS),
M. CHARBIT (ENST, LSS),
P. CHARPIN (Paris VI),
G. COHEN (ENST),
J. CONAN (Polytec. de Montréal),
B. COURTEAU (Univer. de Sherbrooke),
J. L. DORNSTETTER (LCT),
Y. DRIENCOURT (Paris-VII),
P. GODLEWSKI (ENST),
C. GOUTELARD (LETTE),
D. HACCOUN (Polytec. de Montréal),
S. HARARI (GECT),
P. LAURENT (THOMSON-CSF DTC),
S. LEBEL (SCCST),
J. F. MICHON (Paris VII),
A. OISEL (BULL),
D. PERRIN (Paris-VII),
P. PIRET (PHILIPS R. L.),
A. POLI (AAECC),
J. WOLFMANN (GECT).

PATRONAGE :
SPONSORS :

- Groupe d'Etudes de Codage de la Direction des Recherches, Etudes et Techniques (DRET)
- Laboratoire d'Etudes des Transmissions Ionosphériques (LETTI)
- Bull S.A.
- Equipe "Traitement de l'information discrète" de l'ENS des Télécommunications
- Groupe d'Etudes du Codage de Toulon (GECT, Université de Toulon)
- Laboratoire d'Algèbre Appliquée et Codes Correcteurs (AAECC, Université Paul-Sabatier de Toulouse)
- Equipe "Théorie de l'information" du groupe de recherches "Claude-François Picard", CNRS
- Groupe d'études de Codage de l'Université Paris VII

CONTENTS

CODING AND ALGEBRAIC GEOMETRY

DECODING IN REAL SPACE

APPLICATIONS