INTERNATIONAL CENTRE FOR MECHANICAL SCIENCES

COURSES AND LECTURES - No. 258

ALGEBRAIC CODING THEORY AND APPLICATIONS

EDITED BY

G. LONGO

UNIVERSITA' DI TRIESTE

WITH A PREFACE BY

CARLOS R.P. HARTMANN

SYRACUSE UNIVERSITY

Springer-Verlag Wien GmbH

Originally published by CISM Udine in 1979.

ISBN 978-3-662-38752-8 ISBN 978-3-662-39641-4 (eBook)
DOI 10.1007/978-3-662-39641-4

FOREWORD

Ten years have elapsed now from the foundation of the International Centre for Mechanical Sciences and while collecting and editing the various contributions which appear in this book, I was planning to devote it to professor Luigi Sobrero, the founder of the Centre.

But on March 11, 1979, Luigi Sobrero died from a heart attack, and I can only devote this volume to him in memoriam.

May this be a small sign of my gratitude for his associating me to the last enterprise of his life.

Giuseppe Longo

Udine, April 1979

PREFACE

The last twenty-five years have witnessed the growth of one of the most elegant and esoteric branches of applied mathematics: Algebraic Coding Theory. *Areas of mathematics which were previously considered to be of the utmost purity have been applied to the problem of constructing error-correcting codes and their decoding algorithms. In spite of the impressive theoretical accomplishments of these twenty-five years, however, only recently has algebraic coding been put into practice.*

To present some of the latest results on the theory and applications of algebraic coding, a number of scholars who have been active in the various areas of coding research were invited to lecture at the summer school on "Algebraic Coding: Theory and Applications", organized by Giuseppe Longo at the Centre International des Sciences Mécaniques (CISM) in Udine, a picturesque city in northern Italy, for a period of two weeks in July, 1978.

The first contribution, "A Survey of Error-Control Codes", by P.G. Farrell (the University of Kent, Great Britain) is an excellent compilation and condensation of numerous results on error-correcting codes. This contribution consists of four main sections. The first introduces the reader to the basic facts about error-correcting codes, the second describes various decoding methods, the third lists some classes of error-control codes which have found practical application, and the last is devoted to the performance of such codes.

The second contribution, "The Bounds of Delsarte and Lovász, and Their Applications to Coding Theory", is by R.J. McEliece (University of Illinois, U.S.A.). In 1972, P. Delsarte developed a new powerful technique for obtaining upper bounds on the largest possible number of codewords in a code of fixed length and minimum Hamming distance. This technique is nowadays usually called the linear programming approach. In 1977, L. Lovász produced an astonishingly simple solution to a long-standing problem in information theory which was posed by C. Shannon in 1956, namely the problem of computing the zero-error capacity of a certain discrete memoryless channel having five inputs and outputs. Lovász's technique can be applied to any graph (or discrete memoryless channel), although in general it gives only an upper bound for the "Shannon capacity", rather than the true value. In his paper, McEliece offers a unified treatment of these two techniques using standard methods

of linear algebra. The result is an extremely powerful and general technique for studying combinatorial packing problems. This technique is used to obtain, as special cases, the McEliece-Rodemich-Rumsey-Welch bound for binary codes and Lovász's bound on the "Shannon capacity" of many graphs.

The third contribution, "An Introduction to Anticodes", again by P.G. Farrell, is an introduction to the construction of linear anticodes and codes derived from anticodes. The study of anticodes is important in the construction of shortened codes derived from maximum-length-sequence codes. For example, Solomon and Stiffler showed that optimum binary linear codes can be constructed by deleting certain columns of a maximum-length-sequence code array. If m columns are to be deleted, it is desirable that the maximum weight, δ, of the rows of the array of deleted columns be as small as possible, since this maximum value of row weight will determine the minimum distance of the resulting code. The array of deleted columns should yield the minimum value of δ for a given m; alternatively, for a given value of δ, the maximum value of m is sought. These properties are exactly the opposite of the properties we want for a code, thus the array of deleted columns is called a linear "anti-code".

The fourth contribution, "Array Codes", by the same author, is concerned with codes formed by generalizing or iterating one or more component codes into arrays in two or more dimensions. Both known and new array codes and decoding techniques are described. The performance of such codes is also investigated.

The next contribution, "Association Schemes", by J.-M. Goethals (MBLE Research Laboratories, Brussels, Belgium) presents a survey of the algebraic theory of association schemes as developed by P. Delsarte. The material is divided into three main sections. The first section serves as a general introduction to association schemes. The eigenmatrices P and Q which play a fundamental role in the theory are introduced. The emphasis is then on a subset Y of the point set X of an association scheme. The second section deals with the important case in which the point set X of an association scheme can be given the structure of an Abelian group. In this case a dual association scheme can be defined for which the eigenmatrices are obtained by interchanging the roles of the matrices P and Q of the original scheme. For subsets Y which are subgroups of X, the above duality has a nice interpretation in terms of dual subgroups and their inner distributions. Examples of this duality are given. The third section introduces the concept of a polynomial scheme. A scheme is P-polynomial if and only if it is a metric. In this case, Y is a code for which the concept of minimum distance and external distance are well defined. A generalization of Lloyd's theorem for perfect codes is also given.

The sixth contribution, "Generalized Quadratic-Residue Codes", is by J.H. van Lint (Eindhoven University of Technology, The Netherlands). At the 1975 CISM Summer School

on Information Theory, P. Camion introduced a generalization of quadratic-residue codes (QR-codes), and another generalization of QR-codes had been introduced one year earlier by H.N. Ward. Essentially these codes (at least in the binary case) were introduced by P. Delsarte in 1971. Recently J.H. van Lint and F.J. McWilliams showed that the methods that are used to deal with QR-codes can easily be generalized to give a completely analogous treatment of the generalized quadratic-residue codes (GQR-codes). In this paper, after a brief survey of the theory of classical QR-codes, GQR-codes are described in this way.

The seventh contribution, "Soft-Decision Detection Techniques", by P.G. Farrell, is a thorough survey of the existing soft-decision decoding techniques and contains more than fifty references. As J. Massey has pointed out, the use of hard-decision demodulation can, in overall system performance terms, cancel out most or all of the gain provided by the coding scheme. Hence soft-decision decoding should be adopted whenever possible.

The eigth contribution, "Soft-Decision Decoding", is by this writer, and presents an algebraic soft-decision decoding technique whose complexity varies inversely with the code rate. It is shown that using all of the p^{n-k} parity-checks of an (n, k) linear block code it is possible to obtain a soft-decision decoding rule which minimizes the probability of symbol error. The asymptotic performance of this decoding rule for the additive white Gaussian-noise channel is presented. A simplified soft-decision decoder for L-step orthogonalizable codes is also described. The complexity of such a decoder is comparable to that of a conventional hard-decision majority decoder. For codes in which the number of orthogonal parity checks is exactly d_H-1, where d_H is the minimum Hamming distance of the code, the performance of the soft-decision decoder is asymptotically optimum for the Gaussian channel. An iterative decoding technique is also discussed.

The ninth contribution, by R.M.F. Goodman (University of Hull, Great Britain), is divided into three main sections. The first section is entitled "Towards the maximum-likelihood Decoding of Long Convolutional Codes", and presents a new minimum-distance decoding algorithm for convolutional codes which uses a sequential decoding approach to avoid an exponential growth in complexity with increasing constraint-length. It also utilizes the distance and structural properties of convolutional codes to reduce considerably the amount of tree searching needed to find the minimum-distance path, hence making it require less computation than sequential decoding. This makes the algorithm attractive for both long and short constraint-length convolutional codes. In the second section, entitled "On the Design of Practical Minimum Distance Convolutional Decoders", the author assesses quantitatively the decoding effort required by his algorithm and shows that this is indeed much less than that required by sequential decoding. He also proposes modifications to the algorithm to further reduce the computational efforts. The last section is entitled "Soft-Decision Threshold Decoders". Coding system designers are interested in threshold

decoding for convolutional codes because of the hardware simplicity of the decoder. Unfortunately, majority-decision threshold decoding is a sub-optimum scheme and this causes a loss in the coding gain. In this section, the author introduces a new method for implementing soft-decision threshold decoding which enables some of the loss to be recovered without too great a sacrifice in hardware simplicity.

The last contribution, "Algebraic Codes in the Frequency Domain", is by R.E. Blahut (I.B.M., Owego, U.S.A.). Analysis and synthesis problems in communication theory and signal processing depend heavily on reasoning in the frequency domain. In particular, in the study of real-valued or complex-valued signals, the Fourier transform plays a basic role. Likewise, when the time variable is discrete, the discrete Fourier transform plays a parallel role. Hence these transforms are among the major tools of engineers. It is also possible to define Fourier transforms for functions of a discrete index that take values in a Galois field. Finite field transforms have recently been introduced into the subject of error-control codes as a vehicle for reducing decoder complexity. However, these transforms can be made to play a much more central role in the subject. Known ideas of coding theory can be described in a frequency domain setting. For example, cyclic codes can be defined as codes whose codewords have certain specified spectral components equal to zero. Also, the decoding of many codes (including BCH, RS and Goppa codes) can be described spectrally. This paper casts much of the subject of error-control codes in a transform setting. In this way, the author hopes to stimulate interest in, and to accelerate the development of, a spectral point of view of coding. It is his belief that the spectral formulation brings the subject much closer to the subject of signal processing and makes error-control coding more accessable to the nonspecialist in coding theory.

Carlos R.P. Hartmann

Syracuse, N.Y., April 1979.

CONTENTS

NOTICE

It is unfortunate that a contribution to the summer school by professor Rom Varshamov of the Armenian Academy of Sciences, Erevan, Soviet Union, was not included in this volume, as the author could not provide the text timely.