Joaquim Borges
Cristina Fernández-Córdoba
Jaume Pujol
Josep Rifà
Mercè Villanueva

$\mathbb{Z}_2\mathbb{Z}_4$-Linear Codes

Springer

$\mathbb{Z}_2\mathbb{Z}_4$-Linear Codes

Joaquim Borges • Cristina Fernández-Córdoba
Jaume Pujol • Josep Rifà • Mercè Villanueva

$\mathbb{Z}_2\mathbb{Z}_4$-Linear Codes

Springer

Joaquim Borges
Department of Information
and Communications Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain

Cristina Fernández-Córdoba
Department of Information
and Communications Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain

Jaume Pujol
Department of Information
and Communications Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain

Josep Rifà
Department of Information
and Communications Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain

Mercè Villanueva
Department of Information
and Communications Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain

ISBN 978-3-031-05440-2 ISBN 978-3-031-05441-9 (eBook)
https://doi.org/10.1007/978-3-031-05441-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

I am very happy that Cristina Fernández asked me to write a preface to this book coauthored with her colleagues at UAB Borges, Pujol, Rifà and Villanueva. It seems to me it was only yesterday that Cristina was my intern PhD student in Sophia Antipolis. Since then, she has become a very active coding theorist with many publications to her name.

Philippe Delsarte created the field of Algebraic combinatorics in his monumental 1973 thesis [57]. In this work, he studied codes over abelian groups. In a seminal paper [134], Rifà and Pujol characterized so-called propelinear codes over the binary field as subgroups of certain abelian groups. The groups involved in that result can only be the direct products of multiple copies of the cyclic groups of order 2 and 4 and of the quaternionic group of order 8. This result was very timely, three years after the famous $\mathbb{Z}_4$ paper [92], and the avalanche of codes over rings papers it triggered [143]. This prompted the group at UAB to study $\mathbb{Z}_2\mathbb{Z}_4$ codes, that is to say additive subgroups of $\mathbb{Z}_2^m\mathbb{Z}_4^n$ for some integers m, n. The present book which compiles a quarter century of research, is devoted to this class of codes.

At a structural level, this book contains studies on the algebraic structure of $\mathbb{Z}_2\mathbb{Z}_4$ codes (cyclicity) and also to their arithmetic structure (orthogonality, self-duality, build up construction). From a constructive standpoint it also considers special families of such codes like perfect codes and Hadamard codes, a concept introduced in [57]. Another important family is that of Reed-Muller-type codes, which are relevant to Boolean functions and cryptography. To allow for numerical experimentation, the UAB group has written a package of the software Magma, a general resource for mathematical formal computations. Most paragraphs of that book contains short programs written in that package. This is a welcome innovation in the often too abstract literature on Coding Theory.

In a last chapter several generalizations to other mixed rings alphabets have been considered. Some applications to engineering (steganography) are also considered.

To conclude, this is a deep book written by experts of the field. Its

lectorship combines mathematicians, computer scientists, and engineers. It can be the support of a short course at master level.

Patrick Solé
Directeur de Recherche au CNRS,
Institut de Mathématiques de Marseille,
Luminy, le 2 Septembre 2021

Preface

Prior to 1948, systems for the digital transmission of information already existed, such as the telegraph, where the Morse code (1830's) is used. However, it was not until 1948 that Claude Shannon developed the Information Theory that deals with the problem of the transmission of information through noisy channels. At the same time, his colleague at Bell Labs, Richard Hamming, gave the first construction of what is now known as the 1-error-correcting and 2-error-detecting binary Hamming code, and also the 1-error-correcting and 3-error-detecting extended binary Hamming code. In today's technology, the messages are transmitted in sequences of 0's and 1's and, since errors can be produced in the transmission channel, it is very necessary to use these codes that correct errors (for example, in e-mail, mobile, remote sensing, IoT, etc.). Using linear algebra, we have the remarkable Hamming codes and all linear codes constructed later, most of them binary linear and their generalizations to codes over finite fields. The most representative codes are the BCH and Reed-Solomon that can be found in many applications, from the first CDs, to Blu-ray, QR codes, WiMax, satellite communication or storage systems.

From a historical point of view, linear codes over finite fields have been the most important codes since they are easier to construct, encode, and decode. Ring theory has been the next step of coding theory. Linear codes over rings are characterized because the underlying alphabet has the structure of a finite ring. The first codes of this type are found in 1963 (E. F. Assmus and H. F. Mattson) and, later in 1979 (P. Shankar), constructions which are analogous to the BCH or Reed-Solomon codes, but over rings, are given. Also, Lee metric codes were introduced in 1968 (E. R. Berlekamp) where, instead of the usual Hamming metric, Lee's metric is considered. The first examples of codes over rings that are cyclic appeared in 1972 (I. F. Blake). In 1991 (Nechaev), it was discovered that all Kerdock codes can be considered as cyclic linear codes over $\mathbb{Z}_4$, and in 1994 (Hammons et al.) it came up the explanation that the families of the well-known codes as Preparata, Kerdock, Goethals and Goethals–Delsarte, which are non-linear, can be represented as $\mathbb{Z}_4$-linear codes. Using the Lee weight and the appropriate definition of dual-

ity, they showed the unexplained for a long time relationship of their weight enumerators, which fulfil the MacWilliams transform. Since the 1990's, there have been many papers in the literature dealing with the design of codes over $\mathbb{Z}_4$, in particular, linear and cyclic codes over $\mathbb{Z}_4$ have been studied and their structure has been analysed and researched intensively.

On the other hand, in 1987, our research group CCSG (*Combinatorics, Coding and Security Group*) started to work on the so called binary propelinear codes, that is, codes such that their group of isometries contains a regular subgroup acting transitively on the code. Later, in 1997, we realized that in the abelian case this class of codes coincides with the additive codes defined by Delsarte in 1973 in terms of association schemes for the case of the binary Hamming scheme. An additive code, in a translation association scheme, is defined as a subgroup of the underlying abelian group. In the case of a Hamming scheme, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. We refer to this class of codes as $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. After using an extended Gray map, they can be seen as binary codes (not necessarily linear) of length $n = \alpha + 2\beta$. These codes include the binary codes (when $\beta = 0$) and also the linear codes over $\mathbb{Z}_4$ (when $\alpha = 0$).

This book aims to present the basics of this class of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and it is intended for people involved in coding theory, algorithms, computer science, discrete mathematics or algebra. We have tried to make the content accessible to a wide audience, although sometimes a minimum background in coding theory or algebra is required. The first chapters are an introduction to the topic, describing the basic parameters, generator matrices, parity check matrices and studying the concept of duality, including a chapter dedicated to $\mathbb{Z}_2\mathbb{Z}_4$-additive self-dual codes. In general, after applying the Gray map, these codes are not linear over $\mathbb{Z}_2$, which makes the rank and dimension of the kernel relevant parameters to be studied. We then proceed to present families of these $\mathbb{Z}_2\mathbb{Z}_4$-additive codes which have some additional properties, such as the (extended) perfect, Hadamard, Reed-Muller, and MDS codes. In a next chapter, we study the cyclic $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and deal with the values of the rank and dimension of the kernel. In the last two chapters, we present some procedures for encoding using these codes, as well as decoding via syndrome or using the permutation decoding method. We also give an application of these codes to stenography and introduce some variants and generalizations of them that have lately appeared in the literature.

Throughout the book, there are many examples to easily follow the described concepts. There are also examples by using MAGMA functions that can be found in a MAGMA package implemented by the members of the CCSG group for the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. The latest version of this package for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes and the manual with the description of all functions

can be downloaded from the CCSG web page (http://ccsg.uab.cat).

The first step that has led us to this book was an article prepared at the request of professors Victor A. Zinoviev and Thomas Ericson in a seminar that our research group gave at the Autonomous University of Barcelona (UAB). The mentioned article was a review of the research that the CCSG group had done on the subject of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. Later, at the Academy Contact Forum "Galois geometries and applications", organized by The Royal Flemish Academy of Belgium for Science and the Arts in 2012, we presented part of the content of the book that has been revised and updated to reach the current form.

Most of the results in this book come from the research of the members of the CCSG group at the UAB with the collaboration of postdocs and professors from other research groups to whom we are indebted and to whom we would like to thank for visiting our group and/or inviting us to their respective universities: postdocs Iván Bailera, Roland Barrolleta, Nasreddine Benbelkacem, Dipak K. Bhunia, José Joaquín Bernal, Muhammad Bilal, Pere Montolio, Jaume Pernas, Lorena Ronquillo, Emilio Suárez-Canedo, Roger Ten-Valls, Carlos Vela, Fanxuan Zeng; and Professors John J. Cannon, Ángel del Rio, Steven T. Dougherty, Denis S. Krotov, Kevin T. Phelps, Helena Rifà-Pous, Faina I. Soloveva. In addition, the authors are grateful to the research fellow Adrián Torres-Martín for helpful comments on an early version of the text. The work on this book has been partially funded by the Spanish Government (grant reference PID2019-104664GB-I00/AEI/10.13039/501100011033).

We would like to end this preface with a sentence from the excellent book of error-correcting codes by Professors F. J. MacWilliams and N. J. A. Sloane: *When reading the book, if you get stuck on a section, skip it, but keep reading! Don't hesitate to skip the proof of a theorem: we often do.*

Barcelona, 2022

J. Borges
C. Fernández-Córdoba
J. Pujol
J. Rifà
M. Villanueva

Contents