Universitat Autònoma de Barcelona

Cyclic Codes as Submodules of Rings and Direct Product of Rings

Roger Ten Valls

Universitat Autònoma de Barcelona

Departament d'Enginyeria de la Informació i de les Comunicacions

Cyclic Codes as Submodules of Rings and Direct Product of Rings

Submitted to Universitat Autònoma de Barcelona
in partial fulfillment of the requirements for the
degree of Doctor of Philosophy in Computer Science

by Roger Ten Valls

Cerdanyola del Vallès, May 2017

Advisors: Dr. Joaquim Borges Ayats and Dr. Cristina Fernández Córdoba
Professors at Universitat Autònoma de Barcelona

We certify that we have read this thesis entitled “Cyclic Codes as Submodules of Rings and Direct Product of Rings” and that in our opinion it is fully adequate, in scope and in quality, as a dissertation for the degree of Doctor of Philosophy.

Cerdanyola del Vallès, May 2017

Dr. Joaquim Borges Ayats
(Advisor)

Dr. Cristina Fernández Córdoba
(Advisor)

Committe:

Dr. José Joaquín Bernal
Dr. Sergio López-Permouth
Dr. Mercè Villanueva
Dr. Maria Bras-Amorós (substitute)
Dr. Josep Rifà (substitute)
Dr. Patrick Solé (substitute)

Els dies bons gairebé
som invencibles!

A la meva família

Abstract

Cyclic codes are an important family in coding theory and have been a primary area of study since its inception. Until the 1990s the usual alphabet chosen by coding theorist was a finite field. Thereafter, it began the study of codes over rings.

Since the emergence of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, the research on codes over mixed ring alphabets has increased. In 2014, Abualrub *et al.* presented $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and it marked the beginning of the study of cyclic properties on codes over mixed alphabets.

This thesis aims to explore the algebraic structure of cyclic codes as submodules of direct product of finite rings. As these codes can be seen as submodules of the direct product of polynomial rings, we determine the structure of these codes giving their generator polynomials. Further, we study the concept of duality defining the corresponding polynomial operation to the inner product of vectors. This operation allows us to understand the duality in the corresponding polynomial ring. Moreover, we provide techniques to give a polynomial description for dual codes in terms of the generator polynomials of the cyclic codes and we compute them in some particular cases.

Also, we consider different metrics in the direct product of finite rings and we study their binary images under distinct distance preserving maps, called Gray maps.

Finally, we give an algebraic structure for a large family of binary quasi-cyclic codes constructing a family of commutative rings and a canonical Gray map, such that cyclic codes over this family of rings produce quasi-cyclic codes of arbitrary index in the Hamming space via the Gray map.

Resum

Els codis cíclics són una família important en la teoria de la codificació i han estat una àrea principal d'estudi des de la seva aparició. Fins a la dècada dels 90, els alfabets habitualment utilitzats en teoria de codis eren cossos finits. A partir d'aleshores, es va iniciar l'estudi de codis definits sobre anells.

Des de l'aparició dels codis $\mathbb{Z}_2\mathbb{Z}_4$-additius, la investigació de codis sobre alfabets d'anells mixtes s'ha incrementat. L'any 2014, Abualrub *et al.* van presentar els codis cíclics $\mathbb{Z}_2\mathbb{Z}_4$-additius i aquest fet va marcar l'inici de l'estudi de les propietats cícliques en codis sobre alfabets mixtes.

La present tesi té com a objectiu examinar l'estructura algebraica dels codis cíclics com a submòduls de productes directes d'anells finits. Partint del fet que aquests codis poden ser interpretats com a submòduls del producte directe d'anells de polinomis, es determina l'estructura d'aquests codis cíclics tot donant els seus polinomis generadors. A més, s'estudia el concepte de dualitat definint l'operació polinòmica corresponent al producte intern de vectors. Aquesta operació permet entendre la dualitat en l'anell de polinomis corresponent. Així mateix, es proporcionen tècniques per donar una descripció polinòmica dels codis duals en termes dels polinomis generadors dels codis cíclics i es calculen explícitament en alguns casos particulars.

També es consideren diferents mètriques en el producte directe d'anells finits i s'estudien les seves imatges binàries a través de diferents aplicacions que preserven les distàncies, anomenades aplicacions de Gray.

Finalment, es dóna una estructura algebraica per a una gran família de codis quasi-cíclics binaris tot construint una família d'anells commutatius i una aplicació de Gray canònica. De tal manera que els codis cíclics sobre aquesta família d'anells produeixen codis quasi-cíclics d'índex arbitrari en l'espai d'Hamming a través de l'aplicació de Gray.

Preface

This thesis describes much of the work that I conducted while completing my PhD degree at the Universitat Autònoma de Barcelona, in the Department of Information and Communications Engineering.

The thesis is presented as a compendium of publications, thus the most important contributions of this dissertation are appended to this document in the form of publications to journals. Despite being a compendium, I have attempted to make this document as complete and self-contained as possible. It is for this reason that I found convenient to provide the appropriate background and introduce some of the main definitions and techniques of coding theory, without giving the detailed proofs of the results, before focusing the debate on the contributions to the state of the art.

A copy of all contributions comprising this compendium is provided at the end of this document, ordered by publication date. As it is already common at the Combinatorics, Coding and Security Group (CCSG) where this thesis has been developed, the name of the authors of the contributions appended to this document appear in the corresponding documents in alphabetical order.

With Quim and Cristina, we have taken great care to read and reread the text in an attempt to eliminate errors.

This work was partially supported by the Spanish MINECO under Grants TIN2013-40524-P, TIN2016-77918-P(AEI/FEDER, UE) and MTM2015-69138-REDT, and by the Catalan AGAUR under Grants 2009SGR1224 and 2014SGR-691.

Acknowledgements

This is the most introspective and personal part of this thesis. Since it is an intimate reflection, I would like to express these acknowledgements in my own language. Thanks to allow me this moment of "privacy".

Em sento molt agraït als meus directors Quim Borges i Cristina Fernández, per haver-me dirigit amb paciència i experiència, amb confiança i dedicació, amb coneixements i consells. I també per haver-me valorat des del primer moment i haver-me deixat ales tant per fer com per viatjar lliurement.

A tots els membres del grup de recerca CCSG i de la resta del dEIC per la seva acollida i per l'aportació de coneixements durant aquests anys, i un sentit agraïment a la Mercè Villanueva i al Jaume Pujol per la seva ajuda en la implementació del paquet de MAGMA.

Per tots aquells moments de distensió, tant dins com fora del centre, vull agraïr a la resta de companys doctorands, perquè junts hem sabut "gaudir" d'aquesta beca i perquè *somos unos afortunados.* En particular vull donar les gràcies als meus companys de despatx Roland i Emilio, amb els qui he compartit gran part d'aquest viatge, per ajudar-me en els difícils inicis.

I am grateful to Steven Dougherty, who provided me with guidance and expertise along all these years. It was fantastic to have the opportunity to work with him.

I would also like to express my gratitude to Irfan Siap for welcome me and for his ideas. A special thanks to Ismail Aydogdu for his friendship and to make me feel very comfortable during my stay in Istanbul. Teşekkürler.

També agraeixo a l'Italo Dejter i a totes les persones que em van donar la seva atenció, ajuda i amistat durant la meva estada a Puerto Rico.

A tota la meva família. En especial als meus pares, a la meva germana i a la Clara, per la vostra confiança, respecte, suport i amor. Per tot el que m'heu donat, aquesta tesi va dedicada a vosaltres.

Finalment, vull donar les gràcies a la meva altra "gran família" perquè també sempre han estat al meu costat, per comprendre el que molts cops no sé dir amb paraules i per tots els bons moments viscuts.

A tots, moltes gràcies!

Contents

Abstract vii

Resum ix

Preface xi

Acknowledgements xiii

Chapter 1 Introduction 1

Chapter 2 Coding Theory 5

2.1 Linear codes . . . 7

2.2 Cyclic codes . . . 11

Chapter 3 Additive Codes and their Binary Images 19

3.1 Binary images of codes over $\mathbb{Z}_4$ . . . 19

3.2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes . . . 22

Chapter 4 Contributions 27

4.1 Duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes . . . 28

4.2 $\mathbb{Z}_2$-double cyclic codes . . . 30

4.3 On codes in a direct product of finite rings . . . 33

4.4 Quasi-cyclic codes as cyclic codes over a family of local rings . 34

Chapter 5 Conclusions 39

5.1 Summary . . . 39

5.2 Future research . . . 40

Bibliography 43

Appendices 49

Chapter A Quasi-cyclic codes as cyclic codes over a family of local rings 51

Chapter B $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes 65

Chapter C $\mathbb{Z}_2$-double cyclic codes 73

Chapter D On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes 91

Chapter E On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes103

Chapter F Magma package implementation 123

Chapter 1

Introduction

Coding theory was originated as the mathematical foundation for the transmission of messages over noisy communication channels, and deals with the problem of detecting and correcting transmission errors caused by the noise of the channel.

The mathematical background of coding theory is, for example, linear algebra, theory of groups, rings and finite fields, and other areas of discrete mathematics, such as theory of designs. Thus, coding theory has now become an active part of mathematical research.

Within the family of codes, linear codes are special codes with rich mathematical structure. One of the most studied class of linear codes is the class of cyclic codes. The algebraic structure of cyclic codes makes easier their implementation. For this reason many practically important codes are cyclic.

In 1957, cyclic codes were introduced by Prange [Pra57]. As examples of classes of cyclic codes we find the quadratic residue codes presented in [Pra58], and an earlier example of such class is the binary Golay code [Gol49]. Two important classes of cyclic codes are the BCH codes, discovered by Hocquenghem [Hoc59] and independently by Bose and Ray-Chaudhuri [BRC60], and the Reed-Solomon codes, discovered by Reed and Solomon [RS60]. The Goppa codes, presented by Goppa in [Gop70], are also cyclic codes that can be seen as a subclass of alternant codes [Hel74].

Along this thesis, cyclic codes are always linear. However, not every code satisfying the cyclic property is linear. In [Bla83], Blahut presented a non-linear binary code that satisfies the cyclic property; the non-linear code with length 15, size 2^8 and minimum distance 5 which is larger than the binary linear cyclic BCH code of the same length and minimum distance, but with size 2^7. This non-linear code with the cyclic property is comparable with the non-linear Preparata code with the same parameters. Preparata codes, [Pre68], can be very simply constructed as binary images of linear codes over $\mathbb{Z}_4$. The recognition that the Preparata codes and other families of non-linear binary codes, as Kerdock and Goethals, are images under an isometry, called Gray map, of linear codes over $\mathbb{Z}_4$ was presented by Hammons *et al.* in [HKC$^+$94]. The authors proved that all these codes are extended cyclic codes over $\mathbb{Z}_4$. The study of the structure of cyclic codes over $\mathbb{Z}_4$ was discussed by Calderbank *et al.* [CMKH96] and by Pless and Qian [PQ96].

The study of codes over rings has advanced from the middle of 90's. However, in 1963, Assmus and Mattson first considered rings as possible alphabets for codes in [AM63]. Later, Blake investigate linear codes over certain rings in [Bla72] and [Bla75]. But coding theory really gets a shock when it was discovered that the mentioned families of non-linear binary codes (Preparata, Kerdock, Goethals, etc.) can be represented as linear codes over $\mathbb{Z}_4$, see [Nec89] and [HKC$^+$94], via the Gray map. The theory of codes over rings has not been developed in depth for general rings. It has been developed principally for codes over finite chain rings since they have similar properties to those of finite fields, as it will be shown later.

Some interesting results on cyclic codes over rings were done by Carlderbank and Sloane in [CS95], who determine the structure of cyclic codes over $\mathbb{Z}_{p^m}$. Later, in [KL97] Kanwar and López-Permouth do the same, but with different proofs. In 2000, Norton and Sălăgean, in [NS00b], discussed the structure of cyclic codes over finite chain rings and later, Dinh and López-Permouth prove it in a different way in [DL04].

In Delsarte's paper [Del73], he defines additive codes as subgroups of the underlying abelian group in a translation association scheme. For the binary Hamming scheme, namely, when the underlying abelian group is of order 2^n, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. This means that the subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme, [RP97].

A $\mathbb{Z}_2\mathbb{Z}_4$-linear code is a binary image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, that is an additive subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. These $\mathbb{Z}_2\mathbb{Z}_4$-linear codes were first introduced by Rifà and Pujol in 1997 [RP97] as abelian translation-invariant propelinear codes. Later, an exhaustive description of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes was done by Borges *et al.* in [BFP$^+$10]. The structure and properties of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been intensely studied, for example in [BBDF11], [BDF12], [FPV10].

In [ASA14], Abualrub *et al.* define $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. A code in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called cyclic if the set of coordinates can be partitioned into two subsets, the set of coordinates over $\mathbb{Z}_2$ and the set of coordinates over $\mathbb{Z}_4$, such that any cyclic shift of the coordinates of both subsets leaves the code invariant. These codes can be identified as submodules of the $\mathbb{Z}_4[x]$-module $\mathbb{Z}_2[x]/\langle x^\alpha - 1\rangle \times \mathbb{Z}_4[x]/\langle x^\beta - 1\rangle$.

Recently, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are generalized to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes in [AS13], and later to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes in [AS15]. These codes are defined over the direct product of rings of integers modulo some power of a prime number. Also, we can find the direct product of other finite rings, for example, codes in $\mathbb{Z}_2^\alpha \times \left(\frac{\mathbb{Z}_2[u]}{\langle u^2\rangle}\right)^\beta$ in [AAS15] and [AAS16], codes in $\mathbb{Z}_p^\alpha \times \left(\frac{\mathbb{Z}_p[u]}{\langle u^2\rangle}\right)^\beta$ in [LZ15], and codes in $\left(\frac{\mathbb{Z}_2[u]}{\langle u^2\rangle}\right)^\alpha \times \left(\frac{\mathbb{Z}_2[u,v]}{\langle u^2, v^2-1\rangle}\right)^\beta$ in [AD16]. So, codes with sets of coordinates over different rings are widely studied in recent times.

Chapter 2 and Chapter 3 aim to give a brief introduction about the research topics of the thesis. Chapter 2 includes basic concepts and definitions of classical coding theory over finite fields and over a more general algebraic structure, finite rings. Chapter 3 discusses an alternative metric for codes over finite rings and presents the Gray map and its extensions. Afterwards, the family of additive codes over a mixed alphabet, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, is introduced.

Chapter 4 is the core of this thesis, it reviews and summarizes the results of the publications making up this dissertation, shows the storyline that links them up, and discusses their relevance. These contributions are originally presented in the following publications:

[BFT16a] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, *$\mathbb{Z}_2\mathbb{Z}_4$-Additive Cyclic Codes, Generator Polynomials, and Dual Codes*, IEEE Transactions On Information Theory **62** (2016), no. 11, 6348–6354.

[BFT17] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, *$\mathbb{Z}_2$-Double Cyclic Codes*, Designs, Codes and Cryptography (2017), 1–17.

[BFT] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, *On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-Additive Cyclic Codes*, to appear in Advances in Mathematics of Communications.

[AST] I. Aydogdu, I. Siap, R. Ten-Valls, *On the Structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-Linear and Cyclic Codes*, to appear in Finite Fields and Their Applications.

[DFT16] S. T. Dougherty, C. Fernández-Córdoba, R. Ten-Valls, *Quasi-cyclic codes as cyclic codes over a family of local rings*, Finite Fields and Their Applications **40** (2016), 138–149.

In the first contribution, [BFT16a], the parameters of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code are stated in terms of the degrees of the generator polynomials of the code, and the generator polynomials of the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code are determined in terms of the generator polynomials of the code.

The second contribution, [BFT17], presents the structure of $\mathbb{Z}_2$-double cyclic codes giving the generator polynomials of these codes and their duals, and the relations between the generator polynomials of these codes. In this contribution, the relations between $\mathbb{Z}_2$-double cyclic and other families of cyclic codes are also studied.

The results in the third article, [BFT], generalise those for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and $\mathbb{Z}_2$-double cyclic codes to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes.

The fourth article, [AST], is interested in a new family of mixed alphabet codes, namely $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes, where $\mathbb{Z}_2[u^3]$ denotes the ring $\mathbb{Z}_2[u]/\langle u^3\rangle$. It focuses on the study of the algebraic structures of linear and cyclic codes in this family, giving standard forms of generator and parity-check matrices for linear codes and later presenting the generators of cyclic codes and their duals.

The last contribution, [DFT16], is an exploration of a family of commutative rings and a canonical Gray map such that cyclic codes over this family of rings produce quasi-cyclic codes of arbitrary index in the Hamming space via the Gray map.

Finally, Chapter 5 concludes this dissertation and proposes some future lines of research.

Chapter 2

Coding Theory

The publication of Claude Shannon's paper "*A Mathematical Theory of Communication*" in 1948, [Sha48], signified the beginning of coding theory. Given a communication channel that may corrupt information sent over it, Shannon's theorems tell us that there exists a number which he identified with the capacity such that reliable communication is possible at any rate below this capacity.

According to Shannon, we want to send a message $\mathbf{m}$ of a certain length over a given alphabet. First, we encode $\mathbf{m}$ to a codeword $\mathbf{c}$ enlarging the length by adding some redundant information. Then, the encoded message $\mathbf{c}$ is sent over a noisy channel such that the symbols may be changed, under certain probabilities that are characteristic of the channel. The received vector $\mathbf{c}'$ is decoded to $\mathbf{m}'$. The idea of Shannon's theorem is that it is possible to transmit information through a noisy channel at any rate, $\mathbf{R}$, less than channel capacity, $\mathbf{C}$, with an arbitrary small probability of error. In other words, for every $\mathbf{R} < \mathbf{C}$ it is possible to find optimal encoding and decoding scheme such that the error probability that $\mathbf{m}'$ differs to $\mathbf{m}$ is arbitrarily small. And for $\mathbf{R} > \mathbf{C}$, such scheme is not possible.

Note that Shannon's theorem is a non-constructive result; it tells us the existence of an encoding and decoding scheme but it does not specify how to produce an efficient code for a given channel. The origin of research in coding theory was to construct codes in order to reduce the probability of errors according to Shannon's theorem.

We restrict ourselves to block codes, that is, the message words have a fixed length of symbols. Then, for the purpose of error control, before transmission we add a fixed number of redundant symbols to the message word. So the encoded words have also a fixed length of symbols.

Definition 2.1. *Let $\mathcal{A}$ be a set of q symbols called the alphabet. Let $\mathcal{A}^n$ be the set of all n-tuples $\mathbf{c} = (c_0, \ldots, c_{n-1})$, with entries $c_i \in \mathcal{A}$. A* block code *C of length n over $\mathcal{A}$ is a non-empty subset of $\mathcal{A}^n$. We call the elements of C* codewords*. If C contains $|C|$ codewords, then $|C|$ is called the* size *of the code. The value $n - log_q(|C|)$ is called the* redundancy*, and the* information rate *is defined as $\mathbf{R} = log_q(|C|)/n$.*

Example 2.2. *Replacing every binary symbol by a 3-fold repetition gives the possibility of correcting one error in every 3-tuple of symbols in a received word by majority. The triple repetition code has length 3 and 2 codewords, so its information rate is 1/3.*

Example 2.3. *Let C be the binary block code of length n consisting of all words with exactly two ones. The size of C is $n(n-1)/2$. In this example, the number of codewords is not a power of the size of the alphabet.*

In order to determine the error-correcting capability of the code, we need to introduce an appropriate metric on $\mathcal{A}^n$. A metric on the set $\mathcal{A}^n$ is a function $d : \mathcal{A}^n \times \mathcal{A}^n \to [0, \infty)$ that defines a distance between two elements of a set. For all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{A}^n$, it has to satisfy:

- d is non-negative, $d(\mathbf{x}, \mathbf{y}) \geq 0$, and the equality holds if and only if $\mathbf{x} = \mathbf{y}$,
- d is symmetric, $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$, and
- d satisfies the triangle inequality, $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

The principal distance used in coding theory is the *Hamming distance.* The *Hamming distance* between two elements $\mathbf{c} = (c_0, \ldots, c_{n-1})$ and $\mathbf{c}' = (c'_0, \ldots, c'_{n-1})$ in $\mathcal{A}^n$, denoted by $d_H(\mathbf{c}, \mathbf{c}')$, is defined to be the number of components in which $\mathbf{c}$ and $\mathbf{c}'$ differ; i.e., $d_H(\mathbf{c}, \mathbf{c}') = |\{i \mid c_i \neq c'_i\}|$.

Definition 2.4. *The* minimum distance *of a code C, denoted by $d(C)$, is*

$$d(C) = \min\{d_H(\mathbf{c}, \mathbf{c}') \mid \mathbf{c}, \mathbf{c}' \in C, \boldsymbol{c} \neq \mathbf{c}'\}.$$

The error-correcting capability *of a code C is $\lfloor \frac{d(C)-1}{2} \rfloor$ and we say that C is a $\lfloor \frac{d(C)-1}{2} \rfloor$-error-correcting code.*

Example 2.5. *The triple binary repetition code $C = \{000, 111\}$ has minimum distance 3. The binary code of length n consisting of all words with exactly two ones has minimum distance 2.*

A classical question on coding theory is to give optimal codes. That is, to construct a code for a given length and number of codewords with the largest possible minimum distance or, for a given length and minimum distance, to construct a code with the maximum number of codewords, or to give the minimum length for a fixed number of codewords and minimum distance. One of the most important bounds for a code is the *Singleton Bound* which relate all these parameters.

Theorem 2.6 (Singleton Bound, [Sin64]). *Let C be a code of length n over $\mathcal{A}$. Then,*

$$|C| \leq q^{n-d(C)+1}.$$

Any code with parameters which achieve the Singleton Bound is called a *Maximum Distance Separable* (MDS) code.

2.1 Linear codes

2.1.1 Linear codes over finite fields

In order to simplify the encoding and decoding methods, if we impose an additional structure to a code, then we may have many practical advantages. The most popular block codes are linear, this means that the component-wise sum of two codewords is again a codeword.

From the beginning, the most studied codes are those over finite fields. A *linear code* C over the finite field of q elements, $\mathbb{F}_q$, is defined as a k-dimensional subspace of $\mathbb{F}_q^n$, and C is called an $[n,k]$ linear code over $\mathbb{F}_q$, where n is the *length* and k is the *dimension* of the code. From linear algebra, since $\mathbb{F}_q^n$ is a vector space, we have that any subspace C has a basis that consists of k linearly independent codewords. Therefore, a *generator matrix* for a code C is defined to be any $k \times n$ matrix whose rows form a basis for C, and then $|C| = q^k$.

Giving a generator matrix is an explicit way to describe a code since every codeword can be uniquely written as a linear combination of the elements of the basis. Another way to describe a code is implicitly, that is as the null space of a set of homogeneous linear equations. Let C be an $[n,k]$ linear code over $\mathbb{F}_q$, then it is well known that there exists an $(n-k)\times n$ matrix H, with entries in $\mathbb{F}_q$ and independent rows, such that C is the null space of H, i.e., C is the set of all $\mathbf{c} \in \mathbb{F}_q^n$ such that $H\mathbf{c}^t = 0$. The matrix H is called a *parity check matrix* of C.

The *inner product* of two vectors $\mathbf{u} = (u_0, \ldots, u_{n-1}), \mathbf{v} = (v_0, \ldots, v_{n-1})$ in $\mathbb{F}_q^n$ is defined by

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=0}^{n-1} u_i v_i.$$

For an $[n, k]$ linear code C over $\mathbb{F}_q$, we define the *dual code* $C^\perp$ as

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in C\}.$$

Furthermore, if H is a parity check matrix of C, then H is a generator matrix of $C^\perp$. Therefore, $C^\perp$ is an $[n, n-k]$ linear code.

If $C \subset C^\perp$ then C is called *self-orthogonal* and, if $C = C^\perp$, then C is called *self-dual* code.

One of the most important results in coding theory are the MacWilliams Theorems. They are stated by F. J. MacWilliams in [Mac62] and [Mac63]. The *weight enumerator* of C is defined by the polynomial

$$W_C(X, Y) = \sum_{\mathbf{c} \in C} X^{n - wt(\mathbf{c})} Y^{wt(\mathbf{c})},$$

where $wt(\mathbf{c})$ is the number of non-zero coordinates of $\mathbf{c}$. The MacWilliams Theorems for finite fields state that the weight enumerator of the dual code $C^\perp$ of a linear code C is uniquely determined by a linear transformation of the weight enumerator of C.

The following theorem gives the relation, called *MacWilliams identity*, between the weight enumerator of a linear code and its dual.

Theorem 2.7 (MacWilliams identity)**.** *Let C be a linear code over $\mathbb{F}_q$ and $C^\perp$ its dual. Then,*

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(X + (q-1)Y, X - Y).$$

Note that replacing $X = Y = 1$, we can obtain the well-known identity $|C||C^\perp| = |\mathbb{F}_q^n| = q^n$.

2.1.2 Linear codes over rings

It is proven by Hammons *et al.*, [HKC$^+$94], that certain good non-linear binary codes can be seen as binary images of linear codes over $\mathbb{Z}_4$. After [HKC$^+$94], it became interesting to study codes over a larger class of alphabets with some algebraic structures. For this reason, the study of codes over rings has been developed since then. So, we shall begin to study codes over rings and give the appropriate definitions of the basic concepts of coding theory from this new point of view.

A *commutative ring* is a set R equipped with two binary operations, called addition and multiplication, such that R is an additive abelian group with identity element 0, the multiplication holds the distributive laws and it is abelian and associative. We say that R is a *ring with unit* if R has a multiplicative identity; i.e., there exist an element in R, denoted 1, such that for all $r \in R$, $1r = r$. A subset $I \subseteq R$ is an *ideal* if I is an additive subgroup of R and $ar \in I$, for all $a \in I$ and for all $r \in R$. An ideal I is a *maximal ideal* of a ring R if there does not exist any other ideal I' such that $I \subsetneq I' \subsetneq R$. If R has a unique maximal ideal, then R is known as a *local ring.*

For the remainder of the text, we will consider that all rings are finite commutative rings with unity. For further information on the topic see [McD74].

Definition 2.8. *Let R be a ring. A code over R of length n is a subset C of R^n. If C is an R-submodule of R^n, then C is a* linear code.

A *module* over a ring R, or an R-module, is a generalization of the notion of vector space over a field, wherein the corresponding scalars are the elements of the given ring and a multiplication is defined between elements of the ring and elements of the module. Since a module is an abelian group, a *submodule* of an R-module is a subgroup that is closed by the inherit scalar multiplication.

So, much of the theory of codes over rings consists of extending as many as possible the desirable properties of codes over fields. However, codes over rings can be quite a bit more complicated than codes over fields; for instance, since not all modules have a basis, then the definition of a generator matrix is not trivial.

Generally, the most studied rings in coding theory are finite chain rings. A *finite chain ring*, R, is a finite commutative local ring such that its ideals are linearly ordered by inclusion, i.e., if γ is a fixed generator of the maximal ideal of R and e is the nilpotency of γ, then the ideals of R form a chain

$$0 = \langle \gamma^e \rangle \subsetneq \langle \gamma^{e-1} \rangle \subsetneq \cdots \subsetneq \langle \gamma^1 \rangle \subsetneq \langle \gamma^0 \rangle = R.$$

The theory of linear codes over finite chain rings is more similar to the theory of linear codes over finite fields than the theory of codes over arbitrary rings. Some rings whose properties lie closest to those of finite fields are in fact finite chain rings. For example, one of these rings, that was first studied, was the ring of integers modulo p^e, denoted by $\mathbb{Z}_{p^e}$. Clearly, the submodules of $\mathbb{Z}_{p^e}^n$ may not be free, but for every submodule we can find a suitable matrix, which rows are a minimal generating set. After a permutation of coordinates and row operations, we obtain a generator matrix in the form

$$G = \left(\begin{array}{ccccccc} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \dots & A_{0,e-1} & A_{0,e} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \dots & pA_{1,e-1} & pA_{1,e} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \dots & p^2 A_{2,e-1} & p^2 A_{2,e} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e} \end{array} \right),$$

where $A_{i,j}$ are matrices over $\mathbb{Z}_{p^{e-i}}$, [CS95].

Unlike codes over finite fields, we do not have dimension for codes neither over $\mathbb{Z}_{p^e}$ nor over an arbitrary ring. Although we cannot consider the dimension of a code C over $\mathbb{Z}_{p^e}$, we can define the *type* of C as

$$(p^e)^{k_0} (p^{e-1})^{k_1} (p^{e-2})^{k_2} \dots (p)^{k_{e-1}},$$

where $|C| = \prod_{i=0}^{e-1} p^{(e-i)k_i}$.

Example 2.9 ([HKC+94]). *Any linear code over $\mathbb{Z}_4$ of length n and type $4^{k_0} 2^{k_1}$ is permutation equivalent to a quaternary linear code with generator matrix of the form*

$$\mathcal{G} = \left(\begin{array}{ccc} I_{k_0} & R & S \\ 0 & 2I_{k_1} & 2T \end{array} \right),$$

where R, T are matrices over $\{0,1\} \subset \mathbb{Z}_4$ of size $k_0 \times k_1$ and $k_1 \times (n-k_1-k_0)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $k_0 \times (n-k_1-k_0)$.

These results on generator matrices are easily generalized for codes over finite chain rings [NS00a]. So, for codes over finite chain rings it is easy to construct a generator matrix from where we can identify the type. In contrast to finite chain rings, if we just take m to be a positive integer but not a power of a prime number, then it is not easy to describe a minimal generating set for codes over $\mathbb{Z}_m$, as it is shown in [DGPW07].

We can define an inner product and the dual code in the standard way for codes over rings. Clearly, a linear code C inherently determines its dual code, $C^\perp$, and so the weight distribution of $C^\perp$ has to be implicit in C. The explicit way to show this relation is by the MacWilliams identity.

We have seen that the MacWilliams identity holds for any linear code over a finite field. So it is natural to ask which is the largest family of rings such that the MacWilliams Theorem is still true, and therefore it holds $|C||C^{\perp}| = |R|^n$, for a code C over a ring R in this family. The answer of this question is given by J. Wood [Woo99] and the family of Frobenius rings is the largest family of rings such that the strong tools given by MacWilliams remain true.

Theorem 2.10 ([Woo99]). *Let R be a finite commutative Frobenius ring. Let C be a linear code over R. Then*

$$W_{C^{\perp}}(X,Y) = \frac{1}{|C|} W_C(X + (|R|-1)Y, X - Y).$$

2.2 Cyclic codes

2.2.1 Cyclic codes over finite fields

Possibly, cyclic codes are the most studied of all codes. They are a subclass of linear codes and they include important families of codes for error correction, such as binary Hamming codes, Reed-Solomon or BCH codes. We shall begin the study of codes over finite fields, examining the strong relation between a cyclic code and an ideal of the ring of polynomials modulo $x^n - 1$.

A linear code C of length n over $\mathbb{F}_q$ is called *cyclic* if

$$(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$$

Since a cyclic code is invariant under a cyclic shift we conclude that a cyclic code contains all cyclic shifts of any codeword. We will denote by $\mathbf{c}^{(i)}$ the ith shift of $\mathbf{c} \in \mathbb{F}_q^n$.

Example 2.11. *The binary code $C = \{000, 110, 011, 101\}$ is cyclic.*

We can describe these codes in algebraic terms since any element of the vector space $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ can be identified by the residue class of the polynomial $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \pmod{x^n - 1}$ over $\mathbb{F}_q$, [MS77], by the bijection

$$\begin{array}{rcl} \mathbb{F}_q^n & \to & \mathbb{F}_q[x]/\langle x^n - 1\rangle \\ (c_0, c_1, \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}. \end{array} \tag{2.1}$$

Therefore, any codeword is identified as a vector or as a polynomial. Denote the image of a codeword $\mathbf{c}$ under the map (2.1) by $\mathbf{c}(x)$, and by C indistinctly both the code and the corresponding image. It is clear that if

C is a cyclic code and $\mathbf{c}(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in C$, then $x\mathbf{c}(x) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} \in C$. Hence, multiplying the polynomial $\mathbf{c}(x)$ by x corresponds to a right shift of the vector $\mathbf{c}$. So, under the map (2.1), it follows that cyclic codes over $\mathbb{F}_q$ are precisely the ideals of the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, and vice versa. Therefore, the study of cyclic codes over $\mathbb{F}_q$ is equivalent to the study of ideals in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

It is well-known that every ideal C of $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ is principal [LN97], i.e., C is generated by one element of the ring. More precisely, C is generated by the monic polynomial of least degree $g(x) \in C$, called the *generator polynomial.* Then, $g(x)$ is a divisor of $x^n - 1$ in $\mathbb{F}_q[x]$. Any codeword $\mathbf{c}(x) \in C$ can be uniquely written as $\mathbf{c}(x) = \lambda(x)g(x)$, where $\lambda(x)$ has degree less than $n - \deg(g(x))$ and the dimension of C is $k = n - \deg(g(x))$. This discussion gives the following theorem.

Theorem 2.12 ([HP03]). *Let C be an $[n, k]$ nonzero cyclic code in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then there exists a unique monic polynomial $g(x) \in C$ of degree $n - k$ such that $g(x)$ divides $x^n - 1$ and $C = \langle g(x)\rangle$.*

Let $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ be the generator polynomial of a code C of length n over a finite field. Then, the matrix

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & \\ & & \ddots & & & \ddots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix} \leftrightarrow \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}$$

is a generator matrix of C.

From ring theory, the annihilator of an ideal C, $Ann(C)$, is the ideal whose elements cancel out all the elements in the ideal C. In our case, let C be an $[n, k]$ cyclic code with generator polynomial $g(x)$, $C = \langle g(x)\rangle \subseteq \mathbb{F}_q[x]/\langle x^n - 1\rangle$, and let $h(x) = \frac{x^n-1}{g(x)} = h_0 + h_1x + \cdots + h_kx^k$. Then $h(x)$ is called the *parity check polynomial* and $Ann(C) = \langle h(x)\rangle$. However, as it is shown in the following example, $Ann(C)$ does not correspond to the polynomial representation of the dual code $C^\perp$.

Example 2.13. *Let C be the binary cyclic code generated by the linear combination of all cyclic shifts of the vector $(1, 1, 0, 1, 0, 0, 0)$. Clearly, $C = \langle g(x)\rangle$ where $g(x) = x^3 + x + 1$, and then $h(x) = x^4 + x^2 + x + 1$. We have that the polynomial $x^2h(x) = x^6 + x^4 + x^3 + x^2$ belongs to $Ann(C) = \langle h(x)\rangle$ but its corresponding vector $(0, 0, 1, 1, 1, 0, 1)$ is not orthogonal to $(1, 1, 0, 1, 0, 0, 0)$.*

Nevertheless, there is a close relation between the generator polynomial of the dual code and the parity check polynomial.

Definition 2.14. *Let $p(x) = p_0 + p_1x + \cdots + p_tx^t$ be a polynomial over a ring of degree t. The* reciprocal polynomial *of $p(x)$ is the polynomial*

$$p^*(x) = x^tp(x^{-1}) = p_t + p_{t-1}x + \cdots + p_0x^t.$$

Note that the polynomial representation of the reverse of a vector $\mathbf{u}$ of length n corresponds to the polynomial $x^{n-\deg(\mathbf{u}(x))-1}\mathbf{u}^*(x)$.

Example 2.15. *Let $\mathbf{u} = (1, 2, 0, 0)$. Then $\mathbf{u}(x) = 2x+1$. Clearly, $n = 4$ and $x^{n-\deg(\mathbf{u}(x))-1}\mathbf{u}^*(x) = x^2(x+2) = x^3+2x^2$ that corresponds to the polynomial representation of $(0, 0, 2, 1)$, the reverse of $\mathbf{u}$.*

The connection between the dual code and the reciprocal polynomial is clear from the following fact, given in [HP03]. Let $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1}), \mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ and suppose that $\mathbf{u}$ and all its shifts are orthogonal to $\mathbf{v}$. Then, for all i, we have that

$$\mathbf{u}^{(i)} \cdot \mathbf{v} = \sum_{j=0}^{n-1} u_jv_{j+i} = 0.$$

Since $x^{n-\deg(\mathbf{v}(x))-1}\mathbf{v}^*(x) = v_{n-1} + v_{n-2}x + \cdots + v_1x^{n-2} + v_0x^{n-1}$, we have that

$$\begin{aligned}\mathbf{u}(x)x^{n-\deg(\mathbf{v}(x))-1}\mathbf{v}^*(x) = {} & u_0v_{n-1} + (u_{n-1}v_{n-2} + \cdots + u_2v_1 + u_1v_0)x^n+ \\ & + (u_0v_{n-2} + u_1v_{n-1})x + (u_2v_0 + \ldots + u_{n-1}v_{n-3})x^{n+1} \\ & + \ldots \\ & + (u_0v_1 + \cdots + u_{n-2}v_{n-1})x^{n-2} + u_{n-1}v_0x^{2n-2} \\ & + (u_0v_0 + \cdots + u_{n-1}v_{n-1})x^{n-1} \mod (x^n - 1).\end{aligned}$$

Then,

$$\mathbf{u}(x)x^{n-\deg(\mathbf{v}(x))-1}\mathbf{v}^*(x) = \sum_{i=0}^{n-1}(\mathbf{u}^{(i)} \cdot \mathbf{v})x^{n-1-i}$$

vanishes since all $\mathbf{u}^{(i)} \cdot \mathbf{v} = 0$.

Then, the generator polynomial of the dual code $C^\perp$ is $\frac{h^*(x)}{h(0)}$. Furthermore, a generator matrix for $C^\perp$, and hence a parity check matrix for C, is

$$\begin{pmatrix} h_k & \ldots & h_1 & h_0 & & & \\ & h_k & \ldots & h_1 & h_0 & & \\ & & \ddots & & & \ddots & \\ & & & h_k & \ldots & h_1 & h_0 \end{pmatrix}.$$

Since cyclic codes have received much attention, they have been generalized in many different forms, for example, negacyclic codes, quasi-cyclic codes, skew cyclic codes,... For the following chapters, we shall briefly introduce the concept of quasi-cyclic code.

Let t be a positive integer. A linear code C is called *quasi-cyclic* if for all codeword $\mathbf{u} \in C$ we have that $\mathbf{u}^{(t)} \in C$. If t is the smallest integer, such that this property holds then C is said to be a quasi-cyclic code of *index* t. Note that we obtain cyclic codes when $t = 1$. The structure of quasi-cyclic codes has been deeply studied in [LF01], [LS01], [LS03], [LS05], [LNS06].

2.2.2 Cyclic codes over rings

As we have already seen, much of the theory of codes over rings consists of generalizing concepts and properties of codes over finite fields. Cyclic codes over rings has not been studied in depth for a general ring. For the aim of this dissertation, we shall focus primarily on codes over integer residue rings.

As usual, cyclic codes of length n over a ring R are linear codes with the property that the cyclic shift of any codeword is again a codeword. They are also identified with the ideals of $R[x]/\langle x^n - 1\rangle$ by representing the vectors as the polynomials of degree less than n. So, it is natural to ask if we can find generator polynomials of cyclic codes over rings. To do this, one must focus first on the study of the factorization of $x^n - 1$ over R.

As we have said in the previous section, finite chain rings have similar properties to those of finite fields. But some properties on cyclic codes over finite fields do not hold, for example, for cyclic codes over $\mathbb{Z}_{p^e}$. A big difference is that in $\mathbb{Z}_{p^e}[x]$ it does not exist a unique factorization on irreducible polynomials, for $e > 1$. As an example, consider the ring of polynomials over $\mathbb{Z}_4$. We have the following distinct factorizations of the polynomial $x^4 - 1$:

$$\begin{aligned} x^4 - 1 &= (x+1)(x-1)(x^2+1) \\ &= (x+1)^2(x^2+2x-1), \end{aligned}$$

This occurrence may happen on polynomials over finite chain rings. Another difference is that the degree of the product of polynomials may be smaller than the sum of the degrees of the polynomials, e.g., $(2x+1)^2 = 1$ in $\mathbb{Z}_4[x]$. Hence, determining if a polynomial is *irreducible* (i.e., if $f(x) = \lambda(x)\mu(x)$ then $\lambda(x)$ or $\mu(x)$ is a unit), is arduous since we can not assume that the degree of the factors is less than the degree of the polynomial. So, on codes over rings, we will prefer to factorize a polynomial by using a useful subfamily of irreducible polynomials, called *basic irreducible*.

Let R be a ring, consider the widely known surjective *reduction homomorphism* to the residue field of R, and denote by "$\tilde{}$" the linear extension of the reduction homomorphism for all elements of $R[x]$, [McD74]. Then, a polynomial $f(x) \in R[x]$ is *basic irreducible* if $\tilde{f}(x)$ is an irreducible polynomial over the residue field of R, and two polynomials $f(x)$ and $g(x)$ are said to be *coprime* if $\langle f(x)\rangle + \langle g(x)\rangle = R[x]$.

Nevertheless, we can not guarantee yet a unique factorization of a polynomial on basic irreducible polynomials. For example, in $\mathbb{Z}_{p^2}[x]$ we have that $x^2 = x \cdot x = (x-p)(x+p)$.

Please don't be discouraged, the next theorem gives us the key.

Theorem 2.16 ([DL04, Proposition 2.7])**.** *If $f(x)$ is a monic polynomial over a finite chain ring such that $\tilde{f}(x)$ is square free, then $f(x)$ factorizes uniquely as a product of monic basic irreducible pairwise-coprime polynomials.*

For this dissertation, we want that $x^n - 1$ factorizes uniquely in a product of pairwise-coprime basic irreducible polynomials. It is well-known that x^n-1 over $\mathbb{F}_q$, with q a power of a prime p, has no repeated roots if n and p are coprime. Therefore, if $\gcd(n,p) = 1$ then $x^n - 1$ is square free on $\mathbb{F}_q[x]$.

Corollary 2.17. *Let R be finite chain ring and let n be a positive integer coprime with the characteristic of the residue field of R. Then, $x^n - 1$ has a unique decomposition as a product of basic irreducible pairwise-coprime polynomials in $R[x]$.*

Thereupon, we assume that the length of a code over a ring is coprime with the characteristic of the residue field of the ring, unless otherwise specified. The previous Theorem 2.16 and Corollary 2.17 are based on Hensel's Lemma, which shows how to obtain a factorization of a polynomial $f(x)$ from $\tilde{f}(x)$.

Lemma 2.18 (Hensel's Lemma, [McD74])**.** *Let $f(x)$ be a polynomial over R and assume $\tilde{f}(x) = g_1(x)\cdots g_t(x)$, where $g_1(x),\dots,g_t(x)$ are pairwise-coprime polynomials over the residue field of R. Then there exist pairwise-coprime polynomials $f_1(x),\dots,f_t(x)$ over R such that $f(x) = f_1(x)\cdots f_t(x)$ and $\tilde{f}_i(x) = g_i(x)$ for $i = 1,\dots,t$.*

Summarizing, to factorize $x^n - 1$ in $R[x]$, first factorize it over the residue field and then use the Hensel's Lemma to lift the resulting irreducible polynomials.

Example 2.19. *In $\mathbb{Z}_2[x]$, $(x-1)(x^3+x+1)(x^3+x^2+1)$ is the factorization of x^7-1 into irreducible polynomials. Therefore, $(x-1)(x^3+2x^2+x+3)(x^3+3x^2+2x+3)$ is a factorization of x^7-1 into basic irreducible polynomials in $\mathbb{Z}_4[x]$.*

Once we have presented a proper scenario, we are ready to describe the ideals of $R[x]/\langle x^n-1\rangle$ that implies to describe the generator polynomials of the corresponding cyclic codes. As a first approach, we are going to center our attention on cyclic codes over $\mathbb{Z}_4$.

As it is discussed in [Bla08], cyclic codes over $\mathbb{Z}_4$ of length n can be formed by using the basic irreduccible polynomials in the factorization of x^n-1 and their products, just as it is done for cyclic codes over $\mathbb{F}_q$ in Theorem 2.12. Nevertheless, there are more possibilities. For instance, let $g(x)$ be a basic irreducible polynomial on the factorization of x^n-1 over $\mathbb{Z}_4$. Then, we can use $g(x)$ as a generator polynomial of a cyclic code of length n. But, besides this, $2g(x)$ generates a different cyclic code of length n that cannot be generated by any divisor of x^n-1. Hence, we are not able to give a complete description of the generator polynomials as in Theorem 2.12 for cyclic codes over finite fields.

So, we shall enumerate some results in order to deeper understand the algebraic structure of the ideals of $\mathbb{Z}_4[x]/\langle x^n-1\rangle$. The proofs of them can be found in [Wan97].

The next theorem is an interpretation of the *Chinese Remainder Theorem* of the direct sum decomposition of the ring $\mathbb{Z}_4[x]/\langle f(x)\rangle$, where $f(x)$ is the product of pairwise-coprime polynomials in $\mathbb{Z}_4[x]$.

Theorem 2.20 ([Wan97])**.** *Let $f_1(x), f_2(x), \ldots, f_t(x)$ be pairwise-coprime monic polynomials of degree greater than 0, and let $f(x) = f_1(x)f_2(x)\cdots f_t(x)$. Then,*

$$\mathbb{Z}_4[x]/\langle f(x)\rangle \cong \bigoplus_{i=1}^{t} \mathbb{Z}_4[x]/\langle f_i(x)\rangle.$$

As a consequence, for any ideal I of $\mathbb{Z}_4[x]/\langle f(x)\rangle$ we have that $I = I_1 + I_2 + \cdots + I_t$ for ideals $I_i \subseteq \mathbb{Z}_4[x]/\langle f_i(x)\rangle$. Since x^n-1 can be represented as a product of pairwise-coprime basic irreducible polynomials, for an odd n, we are interested on the ideals of $\mathbb{Z}_4[x]/\langle f_i(x)\rangle$, for $f_i(x)$ basic irreducible.

It is known that for a basic irreducible polynomial $f_i(x)$ over $\mathbb{Z}_4[x]$, the ring $\mathbb{Z}_4[x]/\langle f_i(x)\rangle$ has only three ideals, and they are $\langle 0\rangle$, $\langle 1\rangle$ and $\langle 2\rangle$.

Let $x^n-1 = f_1(x)f_2(x)\cdots f_t(x)$ be a representation of x^n-1 as a product of pairwise-coprime basic irreducible polynomials in $\mathbb{Z}_4[x]$ for an odd n. Then, defining $\hat{f}_i(x) = \frac{x^n-1}{f_i(x)}$, it is proved that any ideal of the ring $\mathbb{Z}_4[x]/\langle x^n-1\rangle$ is a sum of some $\langle \hat{f}_i(x)\rangle$ and $\langle 2\hat{f}_i(x)\rangle$. The following result is obtained operating with these sums of ideals.

Theorem 2.21 ([Wan97]). *Let n be an odd positive integer. Let C be and ideal of $\mathbb{Z}_4[x]/\langle x^n-1\rangle$. Then there are unique monic polynomials $f(x), g(x)$ and $h(x)$ over $\mathbb{Z}_4$ such that $C = \langle f(x)h(x), 2f(x)g(x)\rangle$, where $f(x)g(x)h(x) = x^n-1$.*

Finally, we have that these ideals are principal, as it is shown in the next theorem.

Theorem 2.22 ([Wan97]). *Let n be an odd positive integer. Then, every ideal C of $\mathbb{Z}_4[x]/\langle x^n-1\rangle$ is a principal ideal of the form $\langle f(x)h(x)+2f(x)\rangle$ and $|C| = 4^{\deg(g(x))}2^{\deg(h(x))}$, where $f(x)g(x)h(x) = x^n-1$.*

In [CS95] and [KL97], the authors generalize these results to cyclic codes over $\mathbb{Z}_{p^e}$. They proved that a cyclic code over $\mathbb{Z}_{p^e}$ of length n coprime with p has a generator polynomial of the form $g(x) = g_0(x) + pg_1(x) + \cdots + p^{m-1}g_{m-1}(x)$ where $g_0(x), g_1(x), \ldots, g_{m-1}(x)$ in $\mathbb{Z}_{p^e}[x](x)$ such that $g_{m-1}(x) \mid g_{m-2}(x) \mid \cdots \mid g_1(x) \mid g_0(x) \mid (x^n-1)$. Analogous results are obtained for cyclic codes over finite chain rings, and can be found in [NS00b] and [DL04].

Chapter 3

Additive Codes and their Binary Images

In Chapter 2, we have presented basic definitions and results about linear codes over fields and we have extended them to codes over rings. In the current chapter, we start by providing a brief review on binary images of codes over $\mathbb{Z}_4$. After that, we gather some of the most remarkable results concerning the parameters and properties of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

3.1 Binary images of codes over $\mathbb{Z}_4$

The study of codes over rings exploded with codes over $\mathbb{Z}_4$. In the seminal paper [HKC$^+$94], it is proven that certain non-linear binary codes can be regarded as images of linear codes over $\mathbb{Z}_4$ under the Gray map. The breakthrough of [HKC$^+$94] was to consider an alternative weight on the representation over $\mathbb{Z}_4$, the Lee weight. The Lee weight takes advantage of the algebraic structure of $\mathbb{Z}_4$ as a cyclic group instead of only distinguishing if an element is zero or not. In this way, the Gray map becomes an isometry between two metrics defined from these two different weight functions, the Hamming and the Lee weights. In this chapter, we shall give a very brief explanation of the Gray map from $\mathbb{Z}_4$ and use it to introduce the family of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, that are codes over a mixed alphabet.

The *Gray map* between $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$ is usually denoted by ϕ. Let $u \in \mathbb{Z}_4$, we have that an element $u \in \mathbb{Z}_4$ can be uniquely expressed in the form $u = \tilde{u}+2\hat{u}$ where $\tilde{u}, \hat{u} \in \{0, 1\}$. Then, the Gray map is defined by $\phi(u) = (\hat{u}, \tilde{u}+\hat{u})$, and therefore,

$$\begin{array}{rccc} \phi: & \mathbb{Z}_4 & \rightarrow & \mathbb{Z}_2^2 \\ & 0 & \mapsto & (0,0) \\ & 1 & \mapsto & (0,1) \\ & 2 & \mapsto & (1,1) \\ & 3 & \mapsto & (1,0). \end{array}$$

There are different permutation equivalent extensions of the Gray map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. In this dissertation, we will use the same extension as in [HKC$^+$94]. Let $\mathbf{u} = (u_0, \dots, u_{n-1})$ be an element of $\mathbb{Z}_4^n$ such that $u_i = \tilde{u}_i + 2\hat{u}_i$ with $\tilde{u}_i, \hat{u}_i \in \{0,1\}$. The Gray map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$, also denoted by ϕ, is defined by

$$\phi(\mathbf{u}) = (\hat{u}_0, \dots, \hat{u}_{n-1} \mid \tilde{u}_0 + \hat{u}_0, \dots, \tilde{u}_{n-1} + \hat{u}_{n-1}).$$

This Gray map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is a non-linear map. However, the most important property of this map is that it is a distance-preserving map or *isometry* between Lee distance and Hamming distance defined on $\mathbb{Z}_4^n$ and on $\mathbb{Z}_2^{2n}$, respectively.

If we consider the elements of $\mathbb{Z}_4$ as a cyclic group then we can define a weight function as the shortest path on the cycle from an arbitrary element to 0. This weight function is called the *Lee weight*, and it is denoted by w_L. On the elements $0, 1, 2, 3 \in \mathbb{Z}_4$ it acts as follows

$$w_L(0) = 0, w_L(1) = w_L(3) = 1, w_L(2) = 2.$$

The Lee weight of $\mathbf{u} = (u_0, \dots, u_{n-1}) \in \mathbb{Z}_4^n$ is defined to be the sum of the Lee weights of its components, $w_L(\mathbf{u}) = \sum_{i=0}^{n-1} w_L(u_i)$. The Lee weight function defines a distance between two elements $\mathbf{u}$ and $\mathbf{v}$ of $\mathbb{Z}_4^n$ as the Lee weight of their difference, $d_L(\mathbf{u}, \mathbf{v}) = w_L(\mathbf{u} - \mathbf{v})$ on $\mathbb{Z}_4$, which is called the *Lee distance.*

When we refer to the image of a code $\mathcal{C}$ over $\mathbb{Z}_4$, we will always mean its image $C = \phi(\mathcal{C})$ under the Gray map. The code C is a non-linear code in general. A binary code is called a $\mathbb{Z}_4$-*linear code* if its coordinates can be arranged so that it is the image of a linear code over $\mathbb{Z}_4$.

In [HKC$^+$94], the authors give necessary and sufficient conditions for a binary code to be $\mathbb{Z}_4$-linear, and for the binary image of a code over $\mathbb{Z}_4$ to be a linear code. In [Wol99] and [Wol01], Wolfmann studies the condition for the image of a cyclic code over $\mathbb{Z}_4$ of odd length to be linear. Moreover, he proves that the cyclic structure is preserved after a convenient permutation of coordinates.

The *Nechaev permutation* is the permutation σ on $\mathbb{Z}_2^{2n}$, with n odd, defined by

$$\sigma(v_0, v_1, \ldots, v_{2n-1}) = (v_{\tau(0)}, v_{\tau(1)}, \ldots, v_{\tau(2n-1)}),$$

where τ is the permutation on $\{0, 1, \ldots, 2n-1\}$ given by

$$(1, n+1)(3, n+3)\cdots(2i+1, n+2i+1)\cdots(n-2, 2n-2).$$

Let ψ be the map from $\mathbb{Z}_4^n$ into $\mathbb{Z}_2^{2n}$ defined by $\psi = \sigma\phi$, with n odd. This map ψ is called the *Nechaev-Gray map.*

Definition 3.1. *Let $\tilde{g}(x)$ be a divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$ and let ξ be a primitive nth root of unity over $\mathbb{Z}_2$. The polynomial $(\tilde{g} \otimes \tilde{g})(x)$ is defined as the divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$ whose roots are the products $\xi^i\xi^j$ such that ξ^i and ξ^j are roots of $\tilde{g}(x)$.*

The next theorem characterizes all linear cyclic codes over $\mathbb{Z}_4$ of odd length whose images are binary linear codes.

Theorem 3.2 ([Wol01, Theorem 20]). *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$ be a cyclic code over $\mathbb{Z}_4$ of odd length n and where $f(x)h(x)g(x) = x^n - 1$. Let ϕ be the Gray map and let ψ be the Nechaev-Gray map. The following properties are equivalent.*

1. $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ *in* $\mathbb{Z}_2[x]$*;*

2. $\phi(\mathcal{C})$ *is a binary linear code of length* $2n$*;*

3. $\psi(\mathcal{C})$ *is a binary linear cyclic code of length* $2n$ *generated by* $\tilde{f}(x)^2\tilde{h}(x)$*.*

The firsts rings studied in coding theory were the commutative rings of four elements. Since $\mathbb{F}_4$ is a finite field and $\mathbb{Z}_2[v]/\langle v^2 - v\rangle$ is ring isomorphic to $\mathbb{Z}_2^2$, the other commutative ring of four elements that is interesting to consider in coding theory, a part of $\mathbb{Z}_4$ [HKC$^+$94], is $\mathbb{Z}_2[u]/\langle u^2\rangle$. The study of codes over this ring and their binary images is given in [BU99].

The ring $\mathbb{Z}_2[u]/\langle u^2\rangle$ is generalized in two different directions. On the one hand, we have the family of chain rings $\mathbb{Z}_2[u]/\langle u^r\rangle$, and on the other hand, the commutative local ring $\mathbb{Z}_2[u_1, u_2, \ldots, u_r]/\langle u_1^2, u_2^2, \ldots, u_r^2\rangle$. Later, in Chapter 4, we present a family of rings that generalizes both, and we give the corresponding Gray map.

3.2 $\mathbb{Z}_2\mathbb{Z}_4$-additive codes

In the special case of a binary Hamming scheme, the additive codes defined by Delsarte [Del73] coincide with the abelian translation invariant properlinear codes, first defined in [RP97]. According to these results, the codes that are subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in the binary Hamming scheme. In [BFP$^+$10], Borges *et al.* give a comprehensive description of these codes, called $\mathbb{Z}_2\mathbb{Z}_4$-additive codes.

A $\mathbb{Z}_2\mathbb{Z}_4$-*additive code* $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Hence, it is isomorphic to a commutative structure of the form $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords.

Since $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, they can be seen as a generalization of codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$, when $\beta = 0$ or $\alpha = 0$, respectively. Therefore, the Gray and Nechaev-Gray maps can be also applied to the coordinates over $\mathbb{Z}_4$ of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code to obtain binary codes, that are non-linear in general.

Let $\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. We write $\mathbf{u} = (u \mid u')$ where $u = (u_0, \dots, u_{\alpha-1}) \in \mathbb{Z}_2^\alpha$ and $u' = (u'_0, \dots, u'_{\beta-1}) \in \mathbb{Z}_4^\beta$. We define the *extended Gray map* Φ and the *extended Nechaev-Gray map* Ψ as the maps from $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ to $\mathbb{Z}_2^{\alpha+2\beta}$ given by

$$\Phi(\mathbf{u}) = \Phi((u \mid u')) = (u \mid \phi(u')), \quad \Psi(\mathbf{u}) = \Psi((u \mid u')) = (u \mid \psi(u')),$$

where ϕ is the Gray map and ψ is the Nechaev-Gray map, previously defined. The weight of any element $\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ can be computed by adding the Hamming weight of the coordinates over $\mathbb{Z}_2$ and the Lee weight of the coordinates over $\mathbb{Z}_4$, i.e., $w(\mathbf{u}) = w_H(u) + w_L(u')$. This new weight function defines a metric in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, and the maps Φ and Ψ are isometries from $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ to $\mathbb{Z}_2^{\alpha+2\beta}$.

After applying the extend Gray map to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, we obtain binary codes called $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. There are several important classes of binary codes which include $\mathbb{Z}_2\mathbb{Z}_4$-linear codes, e.g., $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard codes or $\mathbb{Z}_2\mathbb{Z}_4$-linear 1-perfect codes, see [PRV06] and [BR99], respectively.

Let X (respectively Y) be the set of $\mathbb{Z}_2$ (respectively $\mathbb{Z}_4$) coordinate positions, so $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set X corresponds to the first α coordinates and Y corresponds to the last β coordinates. Let $\mathcal{C}_X$ be the binary punctured code of $\mathcal{C}$ by deleting the coordinates outside X. Define similary the quaternary code $\mathcal{C}_Y$. Let $\mathcal{C}_b$ be the subcode of $\mathcal{C}$ which contains all order two codewords and let κ be the dimension of $(\mathcal{C}_b)_X$, which is a binary linear code. For the case $\alpha = 0$, we write $\kappa = 0$. With all these parameters, we say that the code $\mathcal{C}$ is of *type* $(\alpha, \beta; \gamma, \delta; \kappa)$.

Applying the classical Singleton bound [Sin64] to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and minimum distance $d(\mathcal{C})$, the following bound is obtained:

$$\frac{d(\mathcal{C})-1}{2} \leq \frac{\alpha}{2} + \beta - \frac{\gamma}{2} - \delta. \tag{3.1}$$

According to [BBDF11], a code meeting the bound (3.1) is called *maximum distance separable with respect to the Singleton* bound, briefly MDSS.

Although a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is not a free submodule, in [BFP$^+$10] it is shown that any $\mathbb{Z}_2\mathbb{Z}_4$-additive code is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with standard generator matrix of the form

$$\mathcal{G}_S = \left(\begin{array}{cc|ccc} I_\kappa & T_b & 2T_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2T_1 & 2I_{\gamma-\kappa} & \mathbf{0} \\ \mathbf{0} & S_b & S_q & R & I_\delta \end{array}\right),$$

where I_k is the identity matrix of size $k \times k$; T_b, S_b are matrices over $\mathbb{Z}_2$; T_1, T_2, R are matrices over $\mathbb{Z}_4$ with all entries in $\{0,1\} \subset \mathbb{Z}_4$; and S_q is a matrix over $\mathbb{Z}_4$.

The concept of duality for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes is also studied in [BFP$^+$10], and the appropriate inner product for any two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is given by

$$\mathbf{u} \cdot \mathbf{v} = 2\sum_{i=0}^{\alpha-1} u_i v_i + \sum_{j=0}^{\beta-1} u'_j v'_j \in \mathbb{Z}_4, \tag{3.2}$$

where the computations are made taking the zeros and ones in the first α coordinates as zeros and ones over $\mathbb{Z}_4$, respectively. The *dual code* of $\mathcal{C}$ is defined in the standard way as $\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{u} \in \mathcal{C}\}$, and it is proven in [BFP$^+$10] that $\mathcal{C}^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$, where

$$\bar{\gamma} = \alpha + \gamma - 2\kappa, \quad \bar{\delta} = \beta - \gamma - \delta + \kappa, \quad \bar{\kappa} = \alpha - \kappa,$$

and has a generator matrix of the form

$$\left(\begin{array}{cc|ccc} T_b^t & I_{\alpha-\kappa} & \mathbf{0} & \mathbf{0} & 2S_b^t \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 2I_{\gamma-\kappa} & 2R^t \\ T_2^t & \mathbf{0} & I_{\beta+\kappa-\gamma-\delta} & T_1^t & -(S_q + RT_1)^t \end{array}\right).$$

Example 3.3. *As a simple example, consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(3, 3; 2, 1; 2)$ with generator matrix in standard form*

$$G = \left(\begin{array}{c|c} 101 & 200 \\ 011 & 220 \\ 000 & 111 \end{array}\right).$$

Then, $\mathcal{C}^\perp$ *is of type* $(3,3;1,2;1)$ *and has generator matrix*

$$H = \left(\begin{array}{c|c} 111 & 000 \\ 100 & 310 \\ 001 & 301 \end{array}\right).$$

Two structural invariants for binary codes are the rank and the dimension of the kernel. In the case of non-linear codes, these parameters tell us how far is the code from being linear. The rank of a binary code C is the dimension of $\langle C \rangle$, which is the linear span of the codewords of C; and the kernel of a binary code C, denoted by $ker(C)$, is the set of vectors that leave C invariant under translations, thus $ker(C) = \{v \mid v + C = C\}$. If C contains the zero vector, then $ker(C)$ is a binary linear subcode of C. Note that if C is a binary linear code, then the rank and the dimension of the kernel coincide with the dimension of the code C.

Any additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is associated with two other codes. The preimage of the kernel of $\Phi(\mathcal{C})$, which is defined to be the code $\mathcal{K}(\mathcal{C}) = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \Phi(\mathbf{v}) \in ker(\Phi(\mathcal{C}))\}$, and the preimage of the span of $\Phi(\mathcal{C})$, $\mathcal{R}(\mathcal{C}) = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \Phi(\mathbf{v}) \in \langle\Phi(\mathcal{C})\rangle\}$. It is clear that $\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C} \subseteq \mathcal{R}(\mathcal{C})$.

It is known that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive code, then $\langle\Phi(\mathcal{C})\rangle$ and $ker(\Phi(\mathcal{C}))$ are both $\mathbb{Z}_2\mathbb{Z}_4$-linear codes ([FPV10]). Therefore, $\mathcal{R}(\mathcal{C})$ and $\mathcal{K}(\mathcal{C})$ are both $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. For the study on rank and kernel of $\mathbb{Z}_4$-linear codes we refer to [FPV08].

In recent times, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been first generalized to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes and later to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes in [AS13] and [AS15], respectively. With the same techniques, the authors extend the results from [BFP$^+$10] to these new mixed alphabets. These codes are defined over the direct product of rings of integers modulo some power of a prime number. Moreover, there are different works on codes over mixed alphabets from other kind of finite rings. Some of these structures that we can find are $\mathbb{Z}_2^\alpha \times \left(\frac{\mathbb{Z}_2[u]}{\langle u^2 \rangle}\right)^\beta$ in [AAS15], $\mathbb{Z}_p^\alpha \times \left(\frac{\mathbb{Z}_p[u]}{\langle u^2 \rangle}\right)^\beta$ in [LZ15], or $\left(\frac{\mathbb{Z}_2[u]}{\langle u^2 \rangle}\right)^\alpha \times \left(\frac{\mathbb{Z}_2[u,v]}{\langle u^2, v^2-1 \rangle}\right)^\beta$ in [AD16]. In these papers, the authors use comparable approaches to the previously described ones to prove their results.

3.2.1 $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

Cyclic codes have been a primary area of study for coding theory. Newly, a first study that considers cyclic properties on codes with two different alphabets is done by Abualrub *et al.* in [ASA14], where the class of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is defined.

Let $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and i be an integer. We define a cyclic shift on $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ as the simultaneous cyclic shift of the set of $\mathbb{Z}_2$ and the set of $\mathbb{Z}_4$ coordinates, and we denote by

$$\mathbf{u}^{(i)} = (u^{(i)} \mid u'^{(i)}) = (u_{0-i}, u_{1-i}, \dots, u_{\alpha-1-i} \mid u'_{0-i}, u'_{1-i}, \dots, u'_{\beta-1-i})$$

the cyclic ith shift of $\mathbf{u}$, where the subscripts are read modulo α and β, respectively. We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is *cyclic* if $\mathcal{C}$ is invariant under the cyclic shift; that is, if for all codeword $\mathbf{u} \in \mathcal{C}$ then $\mathbf{u}^{(1)} \in \mathcal{C}$.

As in the normal course of events, there exists a bijection between $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}$ given by:

$$\begin{aligned}(u_0, u_1, \dots, u_{\alpha-1} \mid u'_0, \dots, u'_{\beta-1}) \mapsto& \\ &(u_0 + u_1 x + \dots + u_{\alpha-1}x^{\alpha-1} \mid u'_0 + \dots + u'_{\beta-1}x^{\beta-1}).\end{aligned}$$

Therefore, as it is common in the studies of cyclic codes, any codeword is identified as a vector or as a polynomial where $\mathbf{u} = (u \mid u')$ is represented as $\mathbf{u}(x) = (u(x) \mid u'(x))$. Using the polynomial representation, an equivalent definition of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is the following

Definition 3.4 ([ASA14])**.** *A subset $\mathcal{C} \subseteq \frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}$ is called a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code if $\mathcal{C}$ is a $\mathbb{Z}_4[x]$-submodule of $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}$.*

From [ASA14], if β is odd, we know that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code then it is of the form

$$\langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x))\rangle,$$

where $f(x)h(x)g(x) = x^\beta - 1$ in $\mathbb{Z}_4[x]$, $b(x)$ divides $x^\alpha - 1$ in $\mathbb{Z}_2[x]$, and we can assume that $deg(\ell(x)) < deg(b(x))$.

Denote by $*$ the external multiplication of elements in $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}$ by polynomials of $\mathbb{Z}_4[x]$ given by $p(x) * \mathbf{u}(x) = p(x) * (u(x) \mid u'(x)) = (\tilde{p}(x)u(x) \mid p(x)u'(x))$. The next theorem gives the spanning sets of $\mathcal{C}$ in terms of the generator polynomials of the code.

Theorem 3.5 ([ASA14, Theorem 13])**.** *Let $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where β is odd and $f(x)h(x)g(x) = x^\beta - 1$. Let*

$$S_1 = \bigcup_{i=0}^{\alpha - \deg(b(x)) - 1} \{x^i * (b(x) \mid 0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg(g(x))-1} \{x^i * (\ell(x) \mid f(x)h(x) + 2f(x))\}$$

and

$$S_3 = \bigcup_{i=0}^{\deg(h(x))-1} \{x^i * (\ell(x)\tilde{g}(x) \mid 2f(x)g(x))\}.$$

Then, $S_1 \cup S_2 \cup S_3$ forms a minimal spanning set for $\mathcal{C}$ as a $\mathbb{Z}_4$-module.

Note that S_2 generates all order 4 codewords and the subcode of codewords of order 2, $\mathcal{C}_b$, is generated by $\{S_1, 2S_2, S_3\}$. Hence, in this case we have that $|C| = 2^{\alpha-deg(b(x))}4^{deg(g(x))}2^{deg(h(x))}$.

In [ASA14], Albuarub *et al.* establish an encoding method for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and prove that the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is again cyclic. Finally, the authors present an infinite family of MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. In [BFT16a], we show that the binary image of this family is the set of all even weight vectors and the binary image of its dual is the repetition code. In fact, these are the only MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with more than one codeword and minimum distance $d(\mathcal{C}) > 1$, as can be seen in [BBDF11].

Chapter 4

Contributions

The aforementioned contributions are the publications listed below. They do not appear here in chronological order of publication, but in the order in which they were developed. In the next sections we summarize them with the aim of justifying the thematic unity of this compendium.

[BFT16a] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2\mathbb{Z}_4$-*Additive Cyclic Codes, Generator Polynomials, and Dual Codes*, IEEE Transactions On Information Theory **62** (2016), no. 11, 6348–6354.

[BFT17] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, $\mathbb{Z}_2$-*Double Cyclic Codes*, Designs, Codes and Cryptography (2017), 1–17.

[BFT] J. Borges, C. Fernández-Córdoba, R. Ten-Valls, *On* $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-*Additive Cyclic Codes*, to appear in Advances in Mathematics of Communications.

[AST] I. Aydogdu, I. Siap, R. Ten-Valls, *On the Structure of* $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-*Linear and Cyclic Codes*, to appear in Finite Fields and Their Applications.

[DFT16] S. T. Dougherty, C. Fernández-Córdoba, R. Ten-Valls, *Quasi-cyclic codes as cyclic codes over a family of local rings*, Finite Fields and Their Applications **40** (2016), 138–149.

4.1 Duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

The family of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes is defined in [ASA14]. The authors study the algebraic structure of this family of codes and determine a set of generator polynomials for this family as $\mathbb{Z}_4[x]$-submodules of the ring $\mathbb{Z}_2[x]/\langle x^\alpha - 1\rangle \times \mathbb{Z}_4[x]/\langle x^\beta - 1\rangle$. They also give a minimal spanning set of these codes as $\mathbb{Z}_4$-submodules in terms of the generator polynomials. From this set it is easy to compute γ and δ of the type of the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, but not κ. Therefore, a first important result in this contribution was the complete description of the type $(\alpha, \beta; \gamma, \delta; \kappa)$ in terms of the degrees of the generator polynomials.

Theorem 4.1 ([BFT16a, Theorem 5]). *Let β be an odd positive integer. Let $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $f(x)h(x)g(x) = x^\beta - 1$. Then,*

$$\begin{aligned}\gamma &= \alpha - \deg(b(x)) + \deg(h(x)),\\ \delta &= \deg(g(x)),\\ \kappa &= \alpha - \deg(\gcd(\ell(x)\tilde{g}(x), b(x))).\end{aligned}$$

In [ASA14], it is also proven that the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is also a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. But in their work it was not showed how the generators of the dual code and the generators of the code are linked. The primary center of attention in [BFT16a] was to find such relation. In order to do that, first we should give an equivalent polynomial operation to the inner product of a codeword and all the shifts of an element of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

First note that for a given codeword $\mathbf{u}$, we have to do $lcm(\alpha, \beta)$ number of shifts to arrive to the initial starting point, therefore there are $lcm(\alpha, \beta)$ different inner products between $\mathbf{u}$ and all the shifts of $\mathbf{v}$.

Denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$ and by $\mathfrak{m}$ the least common multiple of α and β. Then $\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha) = 1 + x^\alpha + x^{2\alpha} + \cdots + x^{\mathfrak{m}-2\alpha} + x^{\mathfrak{m}-\alpha}$ and note that if $p(x)$ is a polynomial of degree $\alpha - 1$, then $\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)p(x) = p(x) + x^\alpha p(x) + \cdots + x^{\mathfrak{m}-\alpha}p(x)$ is a polynomial whose coefficients are $\frac{\mathfrak{m}}{\alpha}$ simultaneous copies of the coefficients of $p(x)$.

From the previous remarks and the definition of the inner product defined over $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ on Equation (3.2), we define the following operation on two elements $\mathbf{u}(x)$ and $\mathbf{v}(x)$ of $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}$, where the resulting polynomial has as coefficients the inner product of $\mathbf{u}$ and all the possible shifts of $\mathbf{v}$.

Definition 4.2 ([BFT16a, Definition 8]). *Let* $\mathbf{u}(x) = (u(x) \mid u'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$ *be elements in* $\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}$. *We define the map*

$$\circ : \left(\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}\right) \times \left(\frac{\mathbb{Z}_2[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_4[x]}{\langle x^\beta - 1\rangle}\right) \longrightarrow \frac{\mathbb{Z}_4[x]}{\langle x^{\mathtt{m}} - 1\rangle},$$

such that

$$\begin{aligned}\mathbf{u}(x) \circ \mathbf{v}(x) =& 2u(x)\theta_{\frac{\mathtt{m}}{\alpha}}(x^\alpha)x^{\mathtt{m}-1-\deg(v(x))}v^*(x)\\ &+ u'(x)\theta_{\frac{\mathtt{m}}{\beta}}(x^\beta)x^{\mathtt{m}-1-\deg(v'(x))}v'^*(x) \mod (x^{\mathtt{m}} - 1),\end{aligned}$$

where the computations are made taking the binary zeros and ones in $u(x)$ *and* $v(x)$ *as zeros and ones over* $\mathbb{Z}_4$*, respectively.*

Proposition 4.3 ([BFT16a, Proposition 9]). *Let* $\mathbf{u}$ *and* $\mathbf{v}$ *be vectors in* $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ *with associated polynomials* $\mathbf{u}(x) = (u(x) \mid u'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$*. Then,* $\mathbf{u}$ *and all its shifts are orthogonal to* $\mathbf{v}$ *if and only if*

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0.$$

Since the dual $\mathcal{C}^\perp$ of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code $\mathcal{C}$ is also cyclic, we will denote

$$\mathcal{C}^\perp = \langle(\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{f}(x)\bar{h}(x) + 2\bar{f}(x))\rangle,$$

where $\bar{f}(x)\bar{h}(x)\bar{g}(x) = x^\beta - 1$ in $\mathbb{Z}_4[x]$, $\bar{b}(x), \bar{\ell}(x) \in \mathbb{Z}_2[x]/(x^\alpha - 1)$ with $\bar{b}(x)|(x^\alpha - 1)$, $deg(\bar{\ell}(x)) < deg(\bar{b}(x))$ and $\bar{b}$ divides $\frac{x^\beta - 1}{\bar{f}(x)}\bar{\ell}(x) \pmod 2$. The following theorem gives the generators of the dual code in terms of the generators of the code.

Theorem 4.4 ([BFT16a, Theorem 18]). *Let* β *be an odd positive integer. Let* $\mathcal{C} = \langle(b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x))\rangle$ *be a* $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic code of type* $(\alpha, \beta; \gamma, \delta; \kappa)$ *, where* $f(x)g(x)h(x) = x^\beta - 1$*, and with dual code* $\mathcal{C}^\perp = \langle(\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{f}(x)\bar{h}(x) + 2\bar{f}(x))\rangle$*, where* $\bar{f}(x)\bar{g}(x)\bar{h}(x) = x^\beta - 1$*. Let* $\rho(x) = \frac{\ell(x)}{\gcd(b(x),\ell(x))}$*. Then,*

1. $\bar{b}(x) = \frac{x^\alpha - 1}{(gcd(b(x),\ell(x)))^*} \in \mathbb{Z}_2[x]$,

2. $\bar{f}(x)\bar{h}(x)$ *is the Hensel lift of the polynomial* $\frac{(x^\beta - 1)\gcd(b(x),\ell(x)\tilde{g}(x))^*}{f^*(x)b^*(x)} \in \mathbb{Z}_2[x]$.

3. $\bar{f}(x)$ *is the Hensel lift of the polynomial* $\frac{(x^\beta - 1)\gcd(b(x),\ell(x))^*}{f^*(x)h^*(x)\gcd(b(x),\ell(x)\tilde{g}(x))^*} \in \mathbb{Z}_2[x]$.

4.

$$\bar{\ell}(x) = \frac{x^\alpha - 1}{b^*(x)} \left(\frac{\gcd(b(x), \ell(x)\tilde{g}(x))^*}{\gcd(b(x), \ell(x))^*} x^{\mathtt{m}-\deg(f(x))} \mu_1(x) \right.$$
$$\left. + \frac{b^*(x)}{\gcd(b(x), \ell(x)\tilde{g}(x))^*} x^{\mathtt{m}-\deg(f(x)h(x))} \mu_2(x) \right) \in \mathbb{Z}_2[x],$$

where

$$\begin{cases} \mu_1(x) = x^{\deg(\ell(x))}(\rho^*(x))^{-1} \mod \left(\frac{b^*(x)}{\gcd(b(x),\ell(x)\tilde{g}(x))^*} \right), \\ \mu_2(x) = x^{\deg(\ell(x))}(\rho^*(x))^{-1} \mod \left(\frac{b^*(x)}{\gcd(b(x),\ell(x))^*} \right). \end{cases}$$

Example 4.5. *Note that the code of Example 3.3 is in fact a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code generated $\mathcal{C} = \langle (x-1 \mid (x^2+x+1)+2) \rangle$ of type $(3,3;2,1;2)$. We have that $b(x) = x^3 - 1, \ell(x) = (x-1), f(x) = 1$ and $h(x) = x^2 + x + 1$.*

Then, applying the formulas of Theorem 4.4 we have $\bar{b}(x) = x^2 + x + 1, \bar{\ell}(x) = x, \bar{f}(x) = x - 1$, and $\bar{h}(x) = 1$. Therefore, $\mathcal{C}^\perp = \langle (x^2+x+1 \mid 0), (x \mid (x-1) + 2(x-1)) \rangle$.

Finally, we describe an infinite family of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, according to the type that was given in [BDF12, Theorem 4].

Proposition 4.6 ([BFT16a, Proposition 19])**.** *Let α be even and β odd. Let $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $b(x) = x^{\frac{\alpha}{2}} - 1$, $\ell(x) = 0$, $h(x) = x^\beta - 1$ and $f(x) = 1$. Then $\mathcal{C}$ is a self-dual code of type $(\alpha, \beta; \beta + \frac{\alpha}{2}, 0; \frac{\alpha}{2})$.*

4.2 $\mathbb{Z}_2$-double cyclic codes

A new topic of research, after the study of contributions in [BFT16a], was to study the binary images of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes which are linear. Motivated by the research done by J. Wolfmann in [Wol01], it looked like the linear images of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code had to maintain some kind of cyclic structure after an appropriate permutation of its coordinates. For this reason, we introduced the term *double cyclic code* and we studied the algebraic structures of $\mathbb{Z}_2$-double cyclic codes.

More recently, some other researchers have studied double cyclic codes over other particular finite chain rings. For example, in [GSWF16], Gao *et al.* showed double cyclic codes over $\mathbb{Z}_4$ and obtained some optimal or suboptimal non-linear binary codes, or in [YSS15], where Yao *et al.* presented the structure of double cyclic codes over $\mathbb{F}_q[u]/\langle u^3\rangle$. We have to say that, in fact, double cyclic codes over a finite field are generalised quasi-cyclic codes (GQC) with two different orbits introduced by Siap and Kulhan in [SK05].

At this point, it would be worthwhile to define the double cyclic property on binary codes described in [BFT17]. So, a binary linear code C is a $\mathbb{Z}_2$-double cyclic code if the set of coordinates can be partitioned into two subsets such that any cyclic shift of the coordinates of both subsets leaves invariant the code; i.e, the binary code C of length $r+s$ is called $\mathbb{Z}_2$*-double cyclic* if

$$(u_0, u_1, \dots, u_{r-2}, u_{r-1} \mid u'_0, u'_1, \dots, u'_{s-2}, u'_{s-1}) \in C$$

implies

$$(u_{r-1}, u_0, u_1, \dots, u_{r-2} \mid u'_{s-1}, u'_0, u'_1, \dots, u'_{s-2}) \in C.$$

These codes can be trivially identified as submodules of the $\mathbb{Z}_2[x]$-module $\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}$, where the vector $\mathbf{u} = (u \mid u')$ is identified with the polynomial tuple $\mathbf{u}(x) = (u(x) \mid u'(x))$. The following theorem describes the generators of such submodules.

Theorem 4.7 ([BFT17, Theorem 1 and Proposition 1])**.** *Let C be a $\mathbb{Z}_2$-double cyclic code of length $r+s$. Then C is generated by*

$$\langle (b(x) \mid 0), (\ell(x) \mid a(x))\rangle \subseteq \frac{\mathbb{Z}_2[x]}{\langle x^r - 1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s - 1\rangle},$$

where $a(x)|(x^s-1)$, $b(x)|(x^r-1)$ and we can assume that $\deg(\ell(x)) < \deg(b(x))$*.*

Once we obtained the generators of a $\mathbb{Z}_2$-double cyclic code C in terms of polynomials, we were able to describe a minimal generating set for the vector representation of C, see [BFT17, Proposition 3], and then we concluded that de dimension of the code C is $r+s-\deg(b(x))-\deg(a(x))$.

Let C be a $\mathbb{Z}_2$-double cyclic code and $C^\perp$ be its dual code. We proved that $C^\perp$ is also a $\mathbb{Z}_2$-double cyclic code, where $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x))\rangle$, for $\bar{b}(x), \bar{\ell}(x) \in \mathbb{Z}_2[x]/\langle x^r - 1\rangle$ with $\bar{b}(x) \mid (x^r-1)$ and $\bar{a}(x) \in \mathbb{Z}_2[x]/\langle x^s-1\rangle$ with $\bar{a}(x) \mid (x^s-1)$.

Let $\mathfrak{m}$ be the least common multiple of r and s. In [BFT17], we defined the following map, analogous to the map in Definition 4.2,

$$\circ : \left(\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}\right) \times \left(\frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}\right) \longrightarrow \mathbb{Z}_2[x]/\langle x^{\mathfrak{m}}-1\rangle,$$

such that for any $\mathbf{u}(x), \mathbf{v}(x) \in \frac{\mathbb{Z}_2[x]}{\langle x^r-1\rangle} \times \frac{\mathbb{Z}_2[x]}{\langle x^s-1\rangle}$, we have that $\mathbf{u}(x) \circ \mathbf{v}(x)$ is $u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) + u'(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))}v'^*(x) \in \frac{\mathbb{Z}_2[x]}{\langle x^{\mathfrak{m}}-1\rangle}$.

As soon as we defined the bilinear map $\circ$, and we had studied some structural properties of punctured codes obtained from a $\mathbb{Z}_2$-double cyclic code and their duals, we got the necessary tools to describe the generators of the dual code in terms of the generators of the code. We summarize the results in the next theorem.

Theorem 4.8 ([BFT17, Theorem 2]). *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x))\rangle$. Then,*

1. $\bar{b}(x) = \frac{x^r-1}{g^*_{b,l}(x)}$,
2. $\bar{a}(x) = \frac{(x^s-1)g^*_{b,l}(x)}{a^*(x)b^*(x)}$,
3. $\bar{\ell}(x) = \frac{x^r-1}{b^*(x)}\lambda(x)$, *where*

$$\lambda(x) = \begin{cases} 0, \text{ if } \ell(x) = 0, \\ x^{\mathfrak{m}-\deg(a(x))+\deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)}\right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)}\right), \text{ otherwise.} \end{cases}$$

After the description of the algebraic structure of $\mathbb{Z}_2$-double cyclic codes and their duals, we studied how $\mathbb{Z}_2$-double cyclic codes were related to other families of cyclic codes, say cyclic codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Recall the definition of the polynomial $(\tilde{g} \otimes \tilde{g})(x)$ in Definition 3.1.

Theorem 4.9 ([BFT17, Proposition 12 and Theorem 5]). *Let n be odd. Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$ be a cyclic code over $\mathbb{Z}_4$ of length n, where $f(x)h(x)g(x) = x^n - 1$ and $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$. Then, $\phi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$. Moreover,*

$$\phi(\mathcal{C}) = \langle (\tilde{f}(x)\tilde{h}(x) \mid 0), (\tilde{f}(x) \mid \tilde{f}(x))\rangle.$$

Therefore, we reached our goal to establish a relation between the generator polynomial of the cyclic code $\mathcal{C}$ over $\mathbb{Z}_4$ and its $\mathbb{Z}_2$-double cyclic image, $\phi(\mathcal{C})$. And we relate $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and $\mathbb{Z}_2$-double cyclic codes, by the following encouraging result.

Theorem 4.10 ([BFT17, Theorem 6]). *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. If $\Phi(\mathcal{C})$ is a linear binary code then $\Psi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code.*

Hence, if a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code has a linear image under the extended Gray map, then applying the appropriate permutation to the coordinates of its image we obtain an equivalent code with the double cyclic property. To conclude the paper [BFT17], we gave some examples of $\mathbb{Z}_2$-double cyclic codes which have the best known minimum distance, and some examples of $\mathbb{Z}_2$-double cyclic codes obtained from cyclic codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

4.3 On codes in a direct product of finite rings

Recently, some special type of mixed alphabet codes, that generalize single alphabet codes, has attracted much attention.

Aydogdu and Siap generalize $\mathbb{Z}_2\mathbb{Z}_4$-additive codes to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes and to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, see [AS13] and [AS15], respectively. With the study of mixed alphabet codes there have appeared new directions to be explored. For example, Aydogdu *et al.* introduce $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes in [AAS15], and recently the subfamilies of cyclic and constacyclic codes are discussed in [AAS16].

4.3.1 $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

In the contribution [BFT], we introduced $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. These codes can be seen as $\mathbb{Z}_{p^s}[x]$-submodules of $\frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha-1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta-1\rangle}$. We determined the generator polynomials of a code in the space $\frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha-1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta-1\rangle}$ and a minimal spanning set in $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ in terms of the generator polynomials. We used the techniques previously described to define a polynomial operation equivalent to the inner product of vectors, as in [BFT16a].

It became natural the study of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. On the one hand, as the study of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, presented in [AS15], with the cyclic property. And, on the other hand, as a generalization of the different types of cyclic codes studied in [ASA14], [BFT17], [BFT16a], [GSWF16], [CS95], and [KL97].

We want to remark that the definition of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code is well defined as long as $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ are different rings, since the elements on the first α coordinates and the ones in the last β coordinates belong to different rings, $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$, respectively. In the particular case that $r = s$, the cyclic code in $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^r}^\beta$ is a *double cyclic code.* In this case, it is also clear that the term double cyclic is given in order to distinguish the cyclic code in $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^r}^\beta$ from the cyclic code in $\mathbb{Z}_{p^r}^{\alpha+\beta}$.

4.3.2 $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes

In [AST], we generalized $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes to $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes. These codes are submodules of $\mathbb{Z}_2^\alpha \times (\mathbb{Z}_2[u]/\langle u^3\rangle)^\beta$. We also introduced cyclic codes and their duals over this class of codes. To study and determine the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive codes, we used similar approaches to the techniques employed in [BFP+10], [AS13] and [AAS15], and for $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes the ones described in [ASA14] and [BFT16a]

In [GO04], the authors describe the notion of a homogeneous weight for codes over Frobenius rings. Applying the conditions to the ring $\mathbb{Z}_2[u]/\langle u^3\rangle$, the ideal structure of the ring dictates an homogeneous weight of the form

$$\omega_{hom}(x) = \begin{cases} 0, \text{ if } x = 0, \\ 2\eta, \text{ if } x = u^2, \\ \eta, \ \text{ otherwise }, \end{cases}$$

where η is a non-negative real number. In order to define a distance preserving Gray map from codes over $\mathbb{Z}_2[u]/\langle u^3\rangle$ to binary codes, first, we took $\eta = 2$ and hence the homogeneous weight in our case is

$$\omega_{hom}(x) = \begin{cases} 0, \text{ if } x = 0, \\ 4, \text{ if } x = u^2, \\ 2, \ \text{ otherwise.} \end{cases}$$

Then we used the first order Reed-Muller code of degree 2, and we had the Gray isometry of this ring into $\mathbb{Z}_2^4$ defined in [AST] as $\phi : \mathbb{Z}_2[u]/\langle u^3\rangle \to \mathbb{Z}_2^4$ given by

$$\phi(0) = (0,0,0,0), \ \phi(1) = (0,1,0,1), \ \phi(u) = (0,0,1,1), \ \phi(u^2) = (1,1,1,1),$$

and then extend it linearly to all elements in $\mathbb{Z}_2[u]/\langle u^3\rangle$. Note that, by construction, ϕ is a linear map.

Finally, in [AST] we listed some optimal binary linear codes with respect to the minimum distance, according to [Gra07], which are actually images of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes under the Gray map ϕ.

4.4 Quasi-cyclic codes as cyclic codes over a family of local rings

During the study of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes, we realized that cyclic codes over $\mathbb{Z}_2[u]/\langle u^3\rangle$ maps to binary quasi-cyclic codes.

In [YK11], the authors study cyclic codes over the commutative ring $\mathbb{Z}_2[u,v]/\langle u^2, v^2\rangle$ which give rise to quasi-cyclic codes of index 4. In [DYK11], [DKY12] and [DYK13], a family of rings, $\mathbb{Z}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2\rangle$, is introduced. Cyclic codes are studied over this family of rings and these codes are used to produce quasi-cyclic binary codes whose index is a power of 2.

Another way to interpret the elements of $\mathbb{Z}_2[u]/\langle u^3\rangle$ as binary vectors is as elements of a vector space over $\mathbb{Z}_2$. So we can view the group structure of $\mathbb{Z}_2[u]/\langle u^3\rangle$ as the vector space $\mathbb{Z}_2^3$ with basis $\{1, u, u^2\}$. Then the Gray map of each element of the basis can be given and then extended it linearly to all of $\mathbb{Z}_2[u]/\langle u^3\rangle$. Under this map, cyclic codes become binary quasi-cyclic codes of index at most 3.

In contribution [DFT16], we constructed a family of commutative rings which generalize all the previous rings, and we described a canonical Gray map such that cyclic codes over this family of rings produce quasi-cyclic codes of arbitrary index in the Hamming space.

Let $p_1, p_2, \ldots, p_t$ be prime numbers with $t \geq 1$ and $p_i \neq p_j$ if $i \neq j$, and let $\Delta = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$. Let $\{u_{p_i,j}\}_{(1\leq j\leq k_i)}$ be a set of indeterminants. Define the following ring

$$R_\Delta = R_{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}} = \mathbb{F}_2[u_{p_1,1}, \ldots, u_{p_1,k_1}, u_{p_2,1} \ldots, u_{p_2,k_2}, \ldots, u_{p_t,k_t}]/\langle u_{p_i,j}^{p_i} = 0\rangle,$$

where the indeterminants $\{u_{p_i,j}\}_{(1\leq i\leq t, 1\leq j\leq k_i)}$ commute. Note that for each Δ there is a ring in this family.

Any indeterminant $u_{p_i,j}$ may have an exponent $\alpha_{p_i,j}$ in the set $J_i = \{0, 1, \ldots, p_i - 1\}$. For a monomial $u_{p_1,1}^{\alpha_{1,1}} \cdots u_{p_1,k_1}^{\alpha_{1,k_1}} \cdots u_{p_t,1}^{\alpha_{t,1}} \cdots u_{p_t,k_t}^{\alpha_{t,k_t}}$ in R_Δ we write u^α, where $\alpha \in J = J_1^{k_1} \times \cdots \times J_t^{k_t}$.

Any element c in R_Δ can be written as

$$c = \sum_{\alpha\in J} c_\alpha u^\alpha = \sum_{\alpha\in J} c_\alpha u_{p_1,1}^{\alpha_{1,1}} \cdots u_{p_1,k_1}^{\alpha_{1,k_1}} \cdots u_{p_t,1}^{\alpha_{t,1}} \cdots u_{p_t,k_t}^{\alpha_{t,k_t}}, \tag{4.1}$$

with $c_\alpha \in \mathbb{F}_2$.

Example 4.11. *Let $\Delta = 135 = 3^3 5$ and let $c = 1 + u_{3,2}^2 u_{3,3} + u_{3,2} u_{5,1}^3 + u_{5,1}^4$. Then,*

$$c_{(0,0,0,0)} = c_{(0,2,1,0)} = c_{(0,1,0,3)} = c_{(0,0,0,4)} = 1.$$

We have proven that R_Δ is in fact a Frobenius ring, and we give the MacWilliams relations explicitly, as showed in [Woo99]. We also studied some ideals in order to understand the ideal structure of R_Δ.

Let A_Δ be the set of all monomials of R_Δ and $\widehat{A}_\Delta$ be the subset of A_Δ of all monomials with one indeterminant.

Example 4.12. *Let* $\Delta = 6 = 2 \cdot 3$. *Then,*

$$A_\Delta = \{1, u_{2,1}, u_{2,1}u_{3,1}, u_{2,1}u_{3,1}^2, u_{3,1}, u_{3,1}^2\}$$

and $\widehat{A}_\Delta = \{u_{2,1}, u_{3,1}, u_{3,1}^2\}$.

We can view each element $a \in A_\Delta$, $a = u^\alpha$ for some $\alpha \in J$, as the subset $\{u_{p_i,j}^{\alpha_{i,j}} | \alpha_{i,j} \neq 0\}_{(1 \leq i \leq t, 1 \leq j \leq k_i)} \subseteq \widehat{A}_\Delta$. We denote by $\widehat{a}$ the corresponding subset of $\widehat{A}_\Delta$. Note that $1 \in A_\Delta$ and $\widehat{1} = \emptyset$, the empty set.

Example 4.13. *Let* $\Delta = 4050 = 2 \cdot 3^4 \cdot 5^2$. *Then,* $a = u_{2,1}u_{3,4}^2u_{5,2}^3$ *is identified with the set* $\widehat{a} = \{u_{2,1}, u_{3,4}^2, u_{5,2}^3\}$.

We consider the elements in R_Δ as binary vectors of Δ coordinates. Consider the set A_Δ, order the elements of A_Δ lexicographically, and use this ordering to label the coordinate positions of $\mathbb{F}_2^\Delta$.

Example 4.14. *Let* $\Delta = 6 = 2 \cdot 3$. *Then,*

$$A_\Delta = \{1, u_{2,1}, u_{3,1}, u_{3,1}^2, u_{2,1}u_{3,1}, u_{2,1}u_{3,1}^2\},$$

and we consider the following ordering of the monomials

$$[1, u_{2,1}, u_{2,1}u_{3,1}, u_{2,1}u_{3,1}^2, u_{3,1}, u_{3,1}^2].$$

Let $v = (100100) \in \mathbb{F}_2^6$. *Then,* $v_1 = v_{u_{2,1}u_{3,1}^2} = 1$ *and* $v_{u_{2,1}} = v_{u_{2,1}u_{3,1}} = v_{u_{3,1}} = v_{u_{3,1}^2} = 0$.

Define the Gray map $\Psi : R_\Delta \to \mathbb{F}_2^\Delta$ as follows:

$$\Psi(a)_b = \begin{cases} 1 & \text{if } \widehat{b} \subseteq \{\widehat{a} \cup 1\}, \\ 0 & \text{otherwise,} \end{cases}$$

where $a, b \in A_\Delta$ and $\Psi(a)_b$ indicates the coordinate of $\Psi(a)$ corresponding to the position of the element b with the defined ordering.

Example 4.15. *Let* $\Delta = 6 = 2 \cdot 3$. *Then, we have the following ordering of the monomials* $[1,\ u_{2,1},\ u_{2,1}u_{3,1},\ u_{2,1}u_{3,1}^2,\ u_{3,1},\ u_{3,1}^2]$. *Let* $a = u_{2,1}u_{3,1}^2$ *then* $\{\hat{a} \cup 1\} = \{1,\ u_{2,1},\ u_{3,1}^2\}$. *Then,*

$$\begin{array}{lll} \Psi(u_{2,1}u_{3,1}^2)_1 = 1, & \Psi(u_{2,1}u_{3,1}^2)_{u_{2,1}} = 1, & \Psi(u_{2,1}u_{3,1}^2)_{u_{2,1}u_{3,1}} = 0, \\ \Psi(u_{2,1}u_{3,1}^2)_{u_{2,1}u_{3,1}^2} = 1, & \Psi(u_{2,1}u_{3,1}^2)_{u_{3,1}} = 0, & \Psi(u_{2,1}u_{3,1}^2)_{u_{3,1}^2} = 1. \end{array}$$

So, $\Psi(u_{2,1}u_{3,1}^2) = (1,1,0,1,0,1)$. *More examples,*

$$\begin{array}{ll} \Psi(0) = (0,0,0,0,0,0), & \Psi(1) = (1,0,0,0,0,0), \\ \Psi(u_{2,1}) = (1,1,0,0,0,0), & \Psi(u_{2,1}u_{3,1}) = (1,1,1,0,1,0), \\ \Psi(u_{3,1}) = (1,0,0,0,1,0), & \Psi(u_{3,1}^2) = (1,0,0,0,0,1). \end{array}$$

The following theorem gives a construction of linear binary quasi-cyclic codes of arbitrary index from cyclic codes and quasi-cyclic codes over R_Δ.

Theorem 4.16 ([DFT16, Theorem 7.2]). *Let C be a linear cyclic code over R_Δ of length n. Then $\Psi(C)$ is a linear binary quasi-cyclic code of length Δn and index at most Δ.*

This theorem allows for a straightforward computational technique to find binary quasi-cyclic codes of index at most Δ from cyclic codes over R_Δ. As usual, the study of cyclic codes over R_Δ of length n is equivalent to the description of the ideals of $R_\Delta[x]/\langle x^n - 1\rangle$. The next theorem follows from the canonical decomposition of rings, noting that for odd n the factorization is unique.

Theorem 4.17 ([DFT16, Theorem 5.3]). *Let n be an odd integer and let $x^n - 1 = f_1 f_2 \dots f_r$ be a factorization on basic irreducible polynomials over R_Δ. Then, the ideals in $R_\Delta[x]/\langle x^n - 1\rangle$ can be written as $I \cong I_1 \oplus I_2 \oplus \cdots \oplus I_r$ where I_i is an ideal of the ring $R_\Delta[x]/\langle f_i\rangle$, for $i = 1, \dots, r$.*

Later, we have shown that if f is a basic monic irreducible polynomial over R_Δ then there is a one-to-one correspondence between ideals of $R_\Delta[x]/\langle f\rangle$ and ideals of R_Δ. Therefore, if I_Δ is the number of ideals on R_Δ and r is the number of distinct basic irreducible polynomials appearing in the factorization of $x^n - 1$, then the number of linear cyclic codes of length n over R_Δ is $(I_\Delta)^r$.

Finally, we examined codes that have a single generator using similar techniques that the ones in [DKY12], and we gave some examples of one generator cyclic codes over R_Δ whose binary image via Ψ gives optimal codes with respect to the minimum distance.

Chapter 5

Conclusions

5.1 Summary

The theme of the dissertation is the cyclic properties on codes developed on finite fields, on finite rings, and on mixed finite alphabets.

Codes defined over finite fields and finite rings are studied in Chapter 2. In Chapter 3, the Gray map is presented and $\mathbb{Z}_2\mathbb{Z}_4$-additive codes are introduced. These chapters provide a background and framework over which Chapter 4 is developed.

Since this thesis was developed as a compendium of publications, Chapter 4 contains most of results obtained in the work done while completing my PhD degree and describes the research evolution linking the publications of this compendium.

The first goal of my research was to establish a well concept of duality for the polynomial representation of cyclic codes over $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and gave formulas to describe the generator polynomials of the dual of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code in terms of the generators of the code. This goal was reached in [BFT16a] as it is shown in Proposition 4.3 and Theorem 4.4 using the inner product defined in Definition 4.2.

With the techniques and tools used in [ASA14] and [BFT16a], we introduced and described the generator polynomials of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes and their duals in [AST]. In [BFT], we also used these approaches to define the cyclic property of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, first introduced in [AS15], and to study their algebraic structure and the inner product of the polynomial representation of these cyclic codes.

In the study of Gray maps, we have introduced two new families of codes.

The first one as the images of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. This family is a subfamily of binary linear codes called $\mathbb{Z}_2$-double cyclic codes. We have studied their algebraic structure and completely described their duals in [BFT17].

The second one is a family of cyclic codes over local rings such that they are preimages of binary quasi-cyclic codes. These rings generalize the rings $\mathbb{Z}_2[u]/\langle u^t\rangle$ and $\mathbb{Z}_2[u_1, \dots, u_t]/\langle u_i^2\rangle$. The images of cyclic codes over these local rings produce quasi-cyclic codes of any index depending on the structure of the chosen ring, as it could be seen in [DFT16].

Finally, we want to remark that we developed a package in Magma software to work with $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. We implemented functions to construct $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes as well as to return the generator polynomials of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code in the case that it is cyclic. This last algorithm is described in [BFT16b].

It is important to mention that Magma, [BCP97], provides machinery to study cyclic codes over finite fields $\mathbb{F}_q$, over the integer residue classes $\mathbb{Z}_m$, and over Galois rings $GR(p^n, k)$. The ring $\mathbb{Z}_4$ receives a special attention and there are available specific functions to work with codes over $\mathbb{Z}_4$. Nevertheless, Magma provides functions to get the generator polynomials for cyclic codes only over finite fields, e.g., for binary cyclic codes. Therefore, our functionalities allow to compute the generators for cyclic codes over $\mathbb{Z}_4$ considering $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes with $\alpha = 0$ and β is odd.

Appendix F contains the manual describing all implemented functions for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. These functionalities will be soon available in the new version of the *Combinatorics, Coding and Security Group* (*CCSG*) package for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, [BFP$^+$12], and will be able to be downloaded from the *CCSG* web page `http://ccsg.uab.cat/`.

5.2 Future research

In this section, we indicate some open problems that derive from this dissertation which may be considered for future research on this topic.

In [Wol01], the author characterizes all linear cyclic codes over $\mathbb{Z}_4$ of odd length whose Gray map images are linear binary codes as it is shown in Theorem 3.2. So, an open problem is to give a classification of all $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes with odd β whose Gray images are linear binary codes.

Talking about binary images of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes it easily comes to mind the study of the rank and the dimension of the kernel. If $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, it could be proven that the related codes $\mathcal{K}(\mathcal{C})$ and

$\mathcal{R}(\mathcal{C})$ are also cyclic with an analogous proof of Theorems 4 and 22 in [DF16]. Therefore, it would be also interesting to complement the study of the families of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes by computing the rank and the dimension of the kernel of the obtained codes, as it was done in [DF16] for cyclic codes over $\mathbb{Z}_4$.

In this dissertation, we have presented some new families of cyclic codes and we have studied the duality of these codes. In Proposition 4.6, we give a large family of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. A future work could focus on the description of the self-duality of these families of codes.

As we have seen, with the techniques described in [ASA14] and [BFT16a], we have studied $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-additive cyclic codes and we generalized $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. In addition, we presented in *Computational and Mathematical Methods in Science and Engineering* (CMMSE 2016), [BFT16c], a generalization of these results to a direct product of two finite commutative chain rings $\mathcal{R}_1^\alpha \times \mathcal{R}_2^\beta$ where $\mathcal{R}_1$ can be viewed as an $\mathcal{R}_2$-module. A first study that considers codes with two alphabets is contributed by Brouwer *et al.* in [BHOS98] entitled *Bounds on Mixed Binary/Ternary Codes*. Most of the approaches and methods used in this dissertation are not valid to describe codes over this structure since $\mathbb{Z}_2$ is not a $\mathbb{Z}_3$-module, and vice versa. Thus, another line of study would be to investigate which are the largest families of rings that could be used to describe codes over mixed alphabets using these tools.

Another research area would focus on providing an effective lower bound for the minimum distance of $\mathbb{Z}_2$-double cyclic codes as the generalization of the BCH bound in the case of cyclic codes.

Bibliography

[AAS15] Ismail Aydogdu, Taher Abualrub, and Irfan Siap, *On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes*, Int. J. Comput. Math. **92** (2015), no. 9, 1806–1814.

[AAS16] ______, *$\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes*, IEEE Transactions on Information Theory **PP** (2016), no. 99, 1–1.

[AD16] N. Annamalai and Chinnappillai Durairajan, *The structure of $\mathbb{Z}_2[u]\mathbb{Z}_2[u,v]$-additive codes*, CoRR **abs/1601.04859** (2016).

[AM63] Edward F. Assmus, Jr. and Harold F. Mattson, *Error-correcting codes: An axiomatic approach*, Information and Control **6** (1963), 315–330.

[AS13] Ismail Aydogdu and Irfan Siap, *The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: bounds on the minimum distance*, Appl. Math. Inf. Sci. **7** (2013), no. 6, 2271–2278.

[AS15] ______, *On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes*, Linear Multilinear Algebra **63** (2015), no. 10, 2089–2102.

[ASA14] Taher Abualrub, Irfan Siap, and Nuh Aydin, *$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes*, IEEE Trans. Inform. Theory **60** (2014), no. 3, 1508–1514.

[AST] Ismail Aydogdu, Irfan Siap, and Roger Ten-Valls, *On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes*, Finite Fields Appl.

[BBDF11] Muhammad Bilal, Joaquim Borges, Steven T. Dougherty, and Cristina Fernández-Córdoba, *Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$*, Des. Codes Cryptogr. **61** (2011), no. 1, 31–40.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma Algebra System I: The User Language*, Journal of Symbolic Computation **24** (1997), no. 3-4, 235–265.

[BDF12] Joaquim Borges, Steven T. Dougherty, and Cristina Fernández-Córdoba, *Characterization and constructions of self-dual codes over* $\mathbb{Z}_2 \times \mathbb{Z}_4$, Adv. Math. Commun. **6** (2012), no. 3, 287–303.

[BFP$^+$10] Joaquim Borges, Cristina Fernández-Córdoba, Jaume Pujol, Josep Rifà, and Mercè Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes: generator matrices and duality*, Des. Codes Cryptogr. **54** (2010), no. 2, 167–179.

[BFP$^+$12] ______, $\mathbb{Z}_2\mathbb{Z}_4$*-linear codes: A* MAGMA *package, v. 3.5*, Universitat Autònoma de Barcelona, `http://ccsg.uab.cat/` (2012).

[BFT] Joaquim Borges, Cristina Fernández-Córdoba, and Roger Ten-Valls, *On* $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$*-additive cyclic codes*, Adv. Math. Commun.

[BFT16a] ______, $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic codes, generator polynomials, and dual codes*, IEEE Trans. Inform. Theory **62** (2016), no. 11, 6348–6354.

[BFT16b] ______, *Computing the generator polynomials of* $\mathbb{Z}_2\mathbb{Z}_4$*-additive cyclic codes*, CoRR **abs/1606.01745** (2016).

[BFT16c] ______, *Linear and cyclic codes over direct product of finite chain rings*, Proceedings of the 16th International Conference on Computational and Mathematical Methods in Science and Engineering CMMSE-2016 (Jesús Vigo-Aguiar, ed.), 2016, pp. 250–260.

[BFT17] ______, $\mathbb{Z}_2$*-double cyclic codes*, Designs, Codes and Cryptography (2017), 1–17.

[BHOS98] Andries E. Brouwer, Heikki O. Hämäläinen, Patric R. J. Östergård, and Neil J. A. Sloane, *Bounds on mixed binary/ternary codes*, IEEE Trans. Inform. Theory **44** (1998), no. 1, 140–161.

[Bla72] Ian F. Blake, *Codes over certain rings*, Information and Control **20** (1972), 396–404.

[Bla75] ______, *Codes over integer residue rings*, Information and Control **29** (1975), no. 4, 295–300.

[Bla83] Richard E. Blahut, *Theory and practice of error control codes*, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[Bla08] ______, *Algebraic codes on lines, planes, and curves*, Cambridge University Press, Cambridge, 2008, An engineering approach.

[BR99] Joaquim Borges and Josep Rifà, *A characterization of* 1*-perfect additive codes*, IEEE Trans. Inform. Theory **45** (1999), no. 5, 1688–1697.

[BRC60] Raj Chandra Bose and Dijen K. Ray-Chaudhuri, *On a class of error correcting binary group codes*, Information and Control **3** (1960), 68–79.

[BU99] Alexis Bonnecaze and Parampalli Udaya, *Cyclic codes and self-dual codes over* F_2+uF_2, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1250–1255.

[CMKH96] A. Robert Calderbank, Gary M. McGuire, P. Vijay Kumar, and Tor Helleseth, *Cyclic codes over* $\mathbb{Z}_4$*, locator polynomials, and Newton's identities*, IEEE Trans. Inform. Theory **42** (1996), no. 1, 217–226.

[CS95] A. Robert Calderbank and Neil J. A. Sloane, *Modular and* p*-adic cyclic codes*, Des. Codes Cryptogr. **6** (1995), no. 1, 21–35.

[Del73] Philippe Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. (1973), no. 10, vi+97.

[DF16] Steven T. Dougherty and Cristina Fernández-Córdoba, *Kernels and ranks of cyclic and negacyclic quaternary codes*, Des. Codes Cryptogr. **81** (2016), no. 2, 347–364.

[DFT16] Steven T. Dougherty, Cristina Fernández-Córdoba, and Roger Ten-Valls, *Quasi-cyclic codes as cyclic codes over a family of local rings*, Finite Fields Appl. **40** (2016), 138–149.

[DGPW07] Steven T. Dougherty, T. Aaron Gulliver, Young Ho Park, and John N. C. Wong, *Optimal linear codes over $\mathbb{Z}_m$*, J. Korean Math. Soc. **44** (2007), no. 5, 1139–1162.

[DKY12] Steven T. Dougherty, Suat Karadeniz, and Bahattin Yildiz, *Cyclic codes over R_k*, Des. Codes Cryptogr. **63** (2012), no. 1, 113–126.

[DL04] Hai Quang Dinh and Sergio R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744.

[DYK11] Steven T. Dougherty, Bahattin Yildiz, and Suat Karadeniz, *Codes over R_k, Gray maps and their binary images*, Finite Fields Appl. **17** (2011), no. 3, 205–219.

[DYK13] ______, *Self-dual codes over R_k and binary self-dual codes*, Eur. J. Pure Appl. Math. **6** (2013), no. 1, 89–106.

[FPV08] Cristina Fernández-Córdoba, Jaume Pujol, and Mercè Villanueva, *On rank and kernel of $\mathbb{Z}_4$-linear codes*, pp. 46–55, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[FPV10] Cristina Fernández-Córdoba, Jaume Pujol, and Mercè Villanueva, *$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel*, Des. Codes Cryptogr. **56** (2010), no. 1, 43–59.

[GO04] Marcus Greferath and Michael E. O'Sullivan, *On bounds for codes over Frobenius rings under homogeneous weights*, Discrete Math. **289** (2004), no. 1-3, 11–24.

[Gol49] Marcel J. E. Golay, *Notes on digital coding*, Proceedings of the IRE **37** (1949), 657.

[Gop70] Valery D. Goppa, *A new class of linear correcting codes*, Problemy Peredači Informacii **6** (1970), no. 3, 24–30.

[Gra07] Markus Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at `http://www.codetables.de` (2007).

[GSWF16] Jian Gao, Minjia Shi, Tingting Wu, and Fang-Wei Fu, *On double cyclic codes over $\mathbb{Z}_4$*, Finite Fields Appl. **39** (2016), 233–250.

[Hel74] Hermann J. Helgert, *Alternant codes*, Information and Control **26** (1974), no. 4, 369–380.

[HKC$^+$94] A. Roger Hammons, Jr., P. Vijay Kumar, A. Robert Calderbank, Neil J. A. Sloane, and Patrick Solé, *The* $\mathbf{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

[Hoc59] Alexis Hocquenghem, *Codes correcteurs d'erreurs*, Chiffres **2** (1959), 147–156.

[HP03] W. Cary Huffman and Vera S. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[KL97] Pramod Kanwar and Sergio R. López-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields Appl. **3** (1997), no. 4, 334–352.

[LF01] Kristine Lally and Patrick Fitzpatrick, *Algebraic structure of quasicyclic codes*, Discrete Appl. Math. **111** (2001), no. 1-2, 157–175.

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn.

[LNS06] San Ling, Harald Niederreiter, and Patrick Solé, *On the algebraic structure of quasi-cyclic codes. IV. Repeated roots*, Des. Codes Cryptogr. **38** (2006), no. 3, 337–361.

[LS01] San Ling and Patrick Solé, *On the algebraic structure of quasi-cyclic codes. I. Finite fields*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2751–2760.

[LS03] ______, *On the algebraic structure of quasi-cyclic codes. II. Chain rings*, Des. Codes Cryptogr. **30** (2003), no. 1, 113–130.

[LS05] ______, *On the algebraic structure of quasi-cyclic codes. III. Generator theory*, IEEE Trans. Inform. Theory **51** (2005), no. 7, 2692–2700.

[LZ15] Zhenliang Lu and Shixin Zhu, $\mathbb{Z}_p\mathbb{Z}_p[u]$*-additive codes*, CoRR **abs/1510.08636** (2015).

[Mac62] F. Jessie MacWilliams, *Combinatorial problems of elementary abelian groups*, ProQuest LLC, Ann Arbor, MI, 1962, Thesis (Ph.D.)–Radcliffe College.

[Mac63] ______, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–94.

[McD74] Bernard R. McDonald, *Finite rings with identity*, Marcel Dekker, Inc., New York, 1974, Pure and Applied Mathematics, Vol. 28.

[MS77] F. Jessie MacWilliams and Neil J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, North-Holland Mathematical Library, Vol. 16.

[Nec89] Aleksandr A. Nechaev, *Kerdock's code in cyclic form*, Diskret. Mat. **1** (1989), no. 4, 123–139.

[NS00a] Graham H. Norton and Ana Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory **46** (2000), no. 3, 1060–1067.

[NS00b] ______, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 6, 489–506.

[PQ96] Vera S. Pless and Zhongqiang Qian, *Cyclic codes and quadratic residue codes over Z_4*, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600.

[Pra57] Eugene Prange, *Cyclic error-correcting codes in two symbols*, AFCRC-TN-57-103, Air Force Cambridge Research Center, 1957.

[Pra58] ______, *Some cyclic error-correcting codes with simple decoding algorithms*, AFCRC-TN-58-156, Air Force Cambridge Research Center, 1958.

[Pre68] Franco P. Preparata, *A class of optimum nonlinear double-error-correcting codes*, Information and Control **13** (1968), 378–400.

[PRV06] Kevin T. Phelps, Josep Rifà, and Mercè Villanueva, *On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel*, IEEE Trans. Inform. Theory **52** (2006), no. 1, 316–319.

[RP97] Josep Rifà and Jaume Pujol, *Translation-invariant propelinear codes*, IEEE Trans. Inform. Theory **43** (1997), no. 2, 590–598.

[RS60] Irving S. Reed and Gustave Solomon, *Polynomial codes over certain finite fields*, J. Soc. Indust. Appl. Math. **8** (1960), 300–304.

[Sha48] Claude E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656.

[Sin64] Richard C. Singleton, *Maximum distance q-nary codes*, IEEE Trans. Information Theory **IT-10** (1964), 116–118.

[SK05] Irfan Siap and Nilgun Kulhan, *The structure of generalized quasi cyclic codes*, Appl. Math. E-Notes **5** (2005), 24–30.

[Wan97] Zhe-Xian Wan, *Quaternary codes*, Series on Applied Mathematics, vol. 8, World Scientific Publishing Co., Inc., River Edge, NJ, 1997.

[Wol99] Jacques Wolfmann, *Negacyclic and cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2527–2532.

[Wol01] ———, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 1773–1779.

[Woo99] Jay A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.

[YK11] Bahattin Yildiz and Suat Karadeniz, *Cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$*, Des. Codes Cryptogr. **58** (2011), no. 3, 221–234.

[YSS15] Ting Yao, Minjia Shi, and Patrick Solé, *Double cyclic codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$*, Int. J. Inf. Coding Theory **3** (2015), no. 2, 145–157.

Appendix A

Quasi-cyclic codes as cyclic codes over a family of local rings

Finite Fields and Their Applications 40 (2016) 138–149

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Quasi-cyclic codes as cyclic codes over a family of local rings[☆]

Steven T. Dougherty[a], Cristina Fernández-Córdoba[b,*], Roger Ten-Valls[b]

[a] Department of Mathematics, University of Scranton, Scranton, PA 18510, USA
[b] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

ARTICLE INFO

Article history:
Received 3 December 2015
Accepted 3 April 2016
Available online xxxx
Communicated by Gary L. Mullen

MSC:
94B60
94B25

Keywords:
Quasi-cyclic codes
Codes over rings

ABSTRACT

We give an algebraic structure for a large family of binary quasi-cyclic codes. We construct a family of commutative rings and a canonical Gray map such that cyclic codes over this family of rings produce quasi-cyclic codes of arbitrary index in the Hamming space via the Gray map. We use the Gray map to produce optimal linear codes that are quasi-cyclic.

1. Introduction

Cyclic codes have been a primary area of study for coding theory since its inception. In many ways, they were a natural object of study since they have a natural algebraic

[☆] This work has been partially supported by the Spanish MINECO grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-0691.

[*] Corresponding author.
E-mail addresses: prof.steven.dougherty@gmail.com (S.T. Dougherty), cristina.fernandez@uab.cat (C. Fernández-Córdoba), roger.ten@uab.cat (R. Ten-Valls).

http://dx.doi.org/10.1016/j.ffa.2016.04.002
1071-5797/© 2016 Elsevier Inc. All rights reserved.

description. Namely, cyclic codes can be described as ideals in a corresponding polynomial ring. A canonical algebraic description for quasi-cyclic codes has been more elusive. In this paper, we shall give an algebraic description of a large family of quasi-cyclic codes by viewing them as the image under a Gray map of cyclic codes over rings from a family which we describe. This allows for a construction of binary quasi-cyclic codes of arbitrary index.

In [6], cyclic codes were studied over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which gives rise to quasi-cyclic codes of index 2. In [1,2] and [3], a family of rings, $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0\rangle$, was introduced. Cyclic codes were studied over this family of rings. These codes were used to produce quasi-cyclic binary codes whose index was a power of 2. In this work, we shall describe a new family of rings which contains the family of rings R_k. With this new family, we can produce quasi-cyclic codes with arbitrary index as opposed to simply indices that are a power of 2.

A code of length n over a ring R is a subset of R^n. If the code is also a submodule then we say that the code is linear. Let π act on the elements of R^n by $\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. Then a code C is said to be cyclic if $\pi(C) = C$. If $\pi^s(C) = C$ then the code is said to be quasi-cyclic of index s.

2. A family of rings

In this section, we shall describe a family of rings which contains the family of rings described in [1,2] and [3].

Let $p_1, p_2, \ldots, p_t$ be prime numbers with $t \geq 1$ and $p_i \neq p_j$ if $i \neq j$, and let $\Delta = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$. Let $\{u_{p_i,j}\}_{(1\leq j\leq k_i)}$ be a set of indeterminants. Define the following ring

$$R_\Delta = R_{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}} = \mathbb{F}_2[u_{p_1,1}, \ldots, u_{p_1,k_1}, u_{p_2,1} \ldots, u_{p_2,k_2}, \ldots, u_{p_t,k_t}]/\langle u_{p_i,j}^{p_i} = 0\rangle,$$

where the indeterminants $\{u_{p_i,j}\}_{(1\leq i\leq t, 1\leq j\leq k_i)}$ commute. Note that for each Δ there is a ring in this family.

Any indeterminant $u_{p_i,j}$ may have an exponent in the set $J_i = \{0, 1, \ldots, p_i - 1\}$. For $\alpha_i \in J_i^{k_i}$ denote $u_{p_i,1}^{\alpha_i,1} \cdots u_{p_i,k_i}^{\alpha_i,k_i}$ by $u_i^{\alpha_i}$, and for a monomial $u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ in R_Δ we write u^α, where $\alpha = (\alpha_1, \ldots, \alpha_t) \in J_1^{k_1} \times \cdots \times J_t^{k_t}$. Let $J = J_1^{k_1} \times \cdots \times J_t^{k_t}$.

Any element c in R_Δ can be written as

$$c = \sum_{\alpha\in J} c_\alpha u^\alpha = \sum_{\alpha\in J} c_\alpha u_{p_1,1}^{\alpha_1,1} \cdots u_{p_1,k_1}^{\alpha_1,k_1} \cdots u_{p_t,1}^{\alpha_t,1} \cdots u_{p_t,k_t}^{\alpha_t,k_t}, \tag{1}$$

with $c_\alpha \in \mathbb{F}_2$.

Lemma 2.1. *The ring R_Δ is a commutative ring with $|R_\Delta| = 2^{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}}$.*

Proof. The fact that the ring is commutative follows from the fact that the indeterminants commute.

There are $p_1^{k_1} \cdots p_t^{k_t}$ different values for $\alpha \in J$. Moreover, for each fixed α, we have that $c_\alpha \in \mathbb{F}_2$ and hence there are $2^{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}}$ elements in R_Δ. □

We define the ideal $\mathfrak{m} = \langle u_{p_i,j} \rangle_{(1 \leq i \leq t, 1 \leq j \leq k_i)}$. We can write every element in R_Δ as $R_\Delta = \{a_0 + a_1 m \mid a_0, a_1 \in \mathbb{F}_2, m \in \mathfrak{m}\}$. We will prove that units of R_Δ are elements $a_0 + a_1 m$, with $m \in \mathfrak{m}$ and $a_0 \neq 0$. First, the following lemma is needed.

Lemma 2.2. *Let $m \in \mathfrak{m}$. There exists $\xi > 0$ such that $m^\xi \neq 0$ and $m^{\xi+1} = 0$.*

Proof. It is enough to prove that for $m \in \mathfrak{m}$ there exists ϵ such that $m^\epsilon = 0$; for example, it is true if $\epsilon = p_1 p_2 \cdots p_t$. Then it follows that there must be a minimal such exponent. □

Define the map $\mu : R_\Delta \to \mathbb{F}_2$, as $\mu(c) = c_{\mathbf{0}}$, where $c = \sum_{\alpha \in J} c_\alpha u^\alpha \in R_\Delta$ and $\mathbf{0}$ is the all-zero vector.

Lemma 2.3. *Let $c = \sum_{\alpha \in J} c_\alpha u^\alpha \in R_\Delta$. Then c is a unit if and only if $\mu(c) = 1$; that is, $c = 1 + m$, for $m \in \mathfrak{m}$.*

Proof. Consider $c = \sum_{\alpha \in J} c_\alpha u^\alpha \in R_\Delta$, and $A = \{\alpha \in J | c_\alpha = 1\}$.

If $c_{\mathbf{0}} = 0$, then define $\beta_{i,j} = p_i - \max_{\alpha \in A}(\alpha_{i,j})$, for $i = 1, \ldots, t$, $j = 1 \ldots, k_i$, and $\tilde{c} = u_1^{\beta_1} \cdots u_t^{\beta^t}$. We have that $c \cdot \tilde{c} = 0$ and therefore c is not a unit.

In the case when $c_{\mathbf{0}} = 1$, there exists $m \in \mathfrak{m}$ such that $c = 1 + m$. Consider the maximum ξ such that $m^\xi \neq 0$. We know such a ξ exists by Lemma 2.2. Then, $(1 + m)(1 + m + \cdots + m^\xi) = 1 + m^{\xi+1} = 1$. Therefore $c = 1 + m$ is a unit. □

As a natural consequence of the proof of the previous lemma, we have the following proposition.

Proposition 2.4. *For $m \in \mathfrak{m}$,*

$$(1 + m)^{-1} = 1 + m + \cdots + m^\xi,$$

where ξ is the maximum value such that $m^\xi \neq 0$.

Note that $\mu(m) = 0$ for $m \in \mathfrak{m}$. In fact, $\mathfrak{m} = Ker(\mu)$.

Lemma 2.5. *The ring R_Δ is a local ring, where the maximal ideal is $\mathfrak{m}$. Moreover $[R_\Delta : \mathfrak{m}] = 2$ and hence $R_\Delta / \mathfrak{m} \cong \mathbb{F}_2$.*

Proof. We have that $R_\Delta / Ker(\mu) \cong Im(\mu) = \mathbb{F}_2$. Therefore $[R_\Delta : \mathfrak{m}] = 2$ and $\mathfrak{m}$ is a maximal ideal.

If $\mathfrak{m}' \neq \mathfrak{m}$ is a maximal ideal, then there exits a unit $u \in \mathfrak{m}'$ which gives that $\mathfrak{m}' = R_\Delta$. Therefore $\mathfrak{m}$ is the unique maximal ideal. □

Now we will prove that R_Δ is in fact a Frobenius ring. To do that, first we shall determine the Jacobson radical and the socle of R_Δ. Recall that for a ring R, the Jacobson radical consists of all annihilators of simple left R-submodules. It can be characterized as the intersection of all maximal right ideals. Since R_Δ is a commutative local ring, we have that its Jacobson radical is:

$$Rad(R_\Delta) = \mathfrak{m} = \langle u_{p_i,j} \rangle_{(1 \le i \le t, 1 \le j \le k_i)}.$$

The socle of a ring R is defined as the sum of all the minimal one sided ideals of the ring. For the ring R_Δ there is a unique minimal ideal and hence the socle of the ring R_Δ is:

$$Soc(R_\Delta) = \{0, u_{p_1,1}^{p_1-1} \cdots u_{p_1,k_1}^{p_1-1} \cdots u_{p_t,1}^{p_t-1} \cdots u_{p_t,k_t}^{p_t-1}\}.$$

Note that the socle of R_Δ is, in fact, the annihilator of $\mathfrak{m}$, $Ann_{R_\Delta}(\mathfrak{m})$.

Theorem 2.6. *The local ring R_Δ is a Frobenius ring.*

Proof. With the definition of $Rad(R_\Delta)$ and $Soc(R_\Delta)$, we have that $R_\Delta/Rad(R_\Delta) = R_\Delta/\mathfrak{m} \cong \mathbb{F}_2 \cong Soc(R_\Delta)$ and hence R_Δ is a Frobenius ring. □

For a complete description of codes over Frobenius rings, see [7].

2.1. Codes over R_Δ and their orthogonals

Recall that a linear code of length n over R_Δ is a submodule of R_Δ^n. We define the usual inner-product, namely

$$[\mathbf{w}, \mathbf{v}] = \sum w_i v_i \text{ where } \mathbf{w}, \mathbf{v} \in \mathcal{R}_\Delta^n.$$

The orthogonal of a code C is defined in the usual way as

$$C^\perp = \{\mathbf{w} \in \mathcal{R}_\Delta^n \mid [\mathbf{w}, \mathbf{v}] = 0, \ \forall \mathbf{v} \in C\}.$$

By Theorem 2.6, we have that R_Δ is a Frobenius ring and hence we have that both MacWilliams relations hold, see [7] for a complete description. This implies that we have at our disposal the main tools of coding theory to study codes over this family of rings. In particular, we have that $|C||C^\perp| = |{R_\Delta}^n| = 2^{\Delta n}$.

2.2. Ideals of R_Δ

In this subsection, we shall study some ideals in the ring R_Δ. We will see later in Theorem 5.5 the importance of understanding the ideal structure of R_Δ.

Let A_Δ be the set of all monomials of R_Δ and let $\widehat{A}_\Delta$ be the subset of A_Δ of all monomials with one indeterminant. Clearly $|A_\Delta| = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} = \Delta$ and $|\widehat{A}_\Delta| = p_1^{k_1} + p_2^{k_2} + \cdots + p_t^{k_t}$. View each element $a \in A_\Delta$, $a = u^\alpha$ for some $\alpha \in J$, as the subset $\{u_{p_i,j}^{\alpha_{i,j}} | \alpha_{i,j} \neq 0\}_{(1\leq i\leq t, 1\leq j\leq k_i)} \subseteq \widehat{A}_\Delta$. We will denote by $\widehat{a}$ the corresponding subset of $\widehat{A}_\Delta$. For example, the element $a = u_{2,1}u_{3,4}^2 u_{5,2}^3$ is identified with the set $\widehat{a} = \{u_{2,1}, u_{3,4}^2, u_{5,2}^3\}$. Note that $1 \in A_\Delta$ and $\widehat{1} = \emptyset$, the empty set.

Consider the vector of exponents $\alpha = (\alpha_{1,1}, \ldots, \alpha_{1,k_1}, \ldots, \alpha_{t,1}, \ldots, \alpha_{t,k_t}) \in J$ and denote by $\bar{\alpha}$ the vector $(p_1 - \alpha_{1,1}, \ldots, p_1 - \alpha_{1,k_1}, \ldots, p_t - \alpha_{t,k_t})$, note that $\bar{\bar{\alpha}} = \alpha$.

Let I_α be the ideal $I_\alpha = \langle u^\alpha \rangle$, for $\alpha \in J$. Note that $I_{\mathbf{0}} = \langle 1 \rangle = R_\Delta$. We also define $I_{(p_1,\cdots,p_1,p_2\cdots,p_t,\cdots,p_t)} = \{0\}$. Now we define the ideal

$$\widehat{I}_\alpha = \langle \widehat{u^\alpha} \rangle = \langle u_{p_i,j}^{\alpha_{i,j}} \mid \alpha_{i,j} \neq 0 \rangle_{(1\leq i\leq t, 1\leq j\leq k_i)}.$$

Example 1. Consider $\Delta = 3^2 5$ and $\alpha = (2, 1, 2)$. Then with the previous definitions, $I_\alpha = \langle u_{3,1}^2 u_{3,2} u_{5,1}^2 \rangle$, $\widehat{I}_\alpha = \langle u_{3,1}^2, u_{3,2}, u_{5,1}^2 \rangle$, and $I_{\bar{\alpha}} = \langle u_{3,1} u_{3,2}^2 u_{5,1}^3 \rangle$. Note that $\langle u_{3,1}^2, u_{3,2}, u_{5,1}^2 \rangle^\perp = \langle u_{3,1} u_{3,2}^2 u_{5,1}^3 \rangle$. The following proposition will prove this fact in general.

Proposition 2.7. *Let $\alpha \in J$ be a vector of exponents. Then $\widehat{I}_\alpha^\perp = I_{\bar{\alpha}}$.*

Proof. It is clear that $I_{\bar{\alpha}} \subset \widehat{I}_\alpha^\perp$. Then we are going to see that $\widehat{I}_\alpha^\perp \subset I_{\bar{\alpha}}$. Suppose that it is not true, then there exists an element $b = \sum_{\beta\in J} c_\beta u^\beta \in \widehat{I}_\alpha^\perp$ that does not belong to $I_{\bar{\alpha}}$. Then there exists a particular β such that $c_\beta \neq 0$ and $\beta_{i,j} < \bar{\alpha}_{i,j}$ for some i and j. Then, $u_{p_i,j}^{\alpha_{i,j}} \cdot b \neq 0$ for $u_{p_i,j}^{\alpha_{i,j}} \in \widehat{I}_\alpha$. Therefore, $b \notin \widehat{I}_\alpha^\perp$ and $\widehat{I}_\alpha^\perp \subset I_{\bar{\alpha}}$. □

Here, we have $\widehat{I}_{\mathbf{0}}^\perp = R_\Delta^\perp = \{0\} = I_{(p_1,\cdots,p_1,p_2\cdots,p_t,\cdots,p_t)} = I_{\bar{\mathbf{0}}}$.

Proposition 2.8. *The number of elements of I_α is $2^{\prod_{i\in\bar{\alpha}} i}$ and the number of elements of $\widehat{I}_\alpha$ is $2^{\Delta - \prod_{i\in\alpha} i}$.*

Proof. Consider the set of all monomials of I_α. There are $p_1 - \alpha_{1,1}$ different monomials fixing all the indeterminates except the first one, $u_{p_1,1}$. There are $p_1 - \alpha_{1,2}$ different monomials fixing all the indeterminates except the second one, $u_{p_1,2}$. By induction and by the laws of counting, there are $\prod_{1\leq i\leq t, 1\leq j\leq k_i}(p_i - \alpha_{i,j})$ different monomials in I_α. Since $\bar{\alpha}$ is the vector $(p_1 - \alpha_{1,1}, \cdots, p_1 - \alpha_{1,k_1}, \cdots, p_t - \alpha_{t,k_t})$ and all elements in I_α are a linear combination of its monomials, we have that $|I_\alpha| = 2^{\prod_{i\in\bar{\alpha}} i}$. By Proposition 2.7, clearly we have that $|\widehat{I}_\alpha| = 2^{\Delta - \prod_{i\in\alpha} i}$. □

Example 2. We continue Example 1 by counting the size of the ideals given there. We note that $\Delta = 45$. Here $\alpha = (2, 1, 2)$ and so $\bar{\alpha} = (1, 2, 3)$. Then $|I_\alpha| = 2^6 = 64$ and $|\widehat{I}_\alpha| = 2^{45-4} = 2^{41} = 2{,}199{,}023{,}255{,}552$.

3. Gray map to the Hamming space

We will consider the elements in R_Δ as a binary vector of Δ coordinates and consider the set A_Δ. Order the elements of A_Δ lexicographically and use this ordering to label the coordinate positions of $\mathbb{F}_2^\Delta$. For $a \in A_\Delta$, define the Gray map $\Psi : R_\Delta \to \mathbb{F}_2^\Delta$ as follows:

For all $b \in A_\Delta$

$$\Psi(a)_b = \begin{cases} 1 & \text{if } \widehat{b} \subseteq \{\widehat{a} \cup 1\}, \\ 0 & \text{otherwise}, \end{cases}$$

where $\Psi(a)_b$ indicates the coordinate of $\Psi(a)$ corresponding to the position of the element $b \in A_\Delta$ with the defined ordering. We have that $\Psi(a)_b$ is 1 if each indeterminant $u_{p_i,j}$ in the monomial b with non-zero exponent is also in the monomial a with the same exponent; that is, $\bar{b}$ is a subset of $\bar{a}$. In order to consider all the subsets of $\bar{a}$, we also add the empty subset that is given when $b = 1$; that is we compare $\bar{b}$ to $\widehat{a} \cup 1$. Then extend Ψ linearly for all elements of R_Δ.

Example 3. Let $\Delta = 6 = 2 \cdot 3$, then we have the following ordering of the monomials $[1, u_{2,1}, u_{2,1}u_{3,1}, u_{2,1}u_{3,1}^2, u_{3,1}, u_{3,1}^2]$. As examples,

$$\Psi(1) = (1,0,0,0,0,0), \qquad \Psi(u_{3,1}^2) = (1,0,0,0,0,1),$$
$$\Psi(u_{2,1}u_{3,1}) = (1,1,1,0,1,0), \qquad \Psi(u_{2,1}u_{3,1}^2) = (1,1,0,1,0,1).$$

Proposition 3.1. *Let $a \in A_\Delta$ such that $a \neq 1$. Then $wt_H(\Psi(a))$ is even.*

Proof. Since $\widehat{a}$ is a non-empty set then $\widehat{a}$ has $2^{|\widehat{a}|}$ subsets. Thus, $\Psi(a)$ has an even number of non-zero coordinates. □

Notice that for $a, b \in A_\Delta$ such that $a, b \neq 1$, we have

$$wt_H(\Psi(a+b)) = wt_H(\Psi(a)) + wt_H(\Psi(b)) - 2wt_H(\Psi(a) \star \Psi(b))),$$

which is even, where $\star$ is the componentwise product. Therefore we have the following result.

Theorem 3.2. *Let m be an element of R_Δ. Then, $m \in \mathfrak{m}$ if and only if $wt_H(\Psi(m))$ is even.*

Proof. We showed that if $m \in \mathfrak{m}$ then $wt_H(\Psi(m))$ is even. Since $|\mathfrak{m}| = \frac{|R_\Delta|}{2}$ and there are precisely $|\mathfrak{m}| = \frac{|R_\Delta|}{2}$ binary vectors in $\mathbb{F}_2^\Delta$ of even weight, then the odd weight vectors correspond to the units in R_Δ. □

Each code C corresponds to a binary linear code, namely the code $\Psi(C)$ of length Δn. It is natural now to ask if orthogonality is preserved over the map Ψ. In the following case, as proven in [1], it is preserved as in the following proposition. Recall that the ring R_k was a special case of R_Δ when Δ was a power of 2.

Proposition 3.3. *Let $\Delta = 2^k$ and let C be a linear code over R_Δ of length n. Then,*

$$\Psi(C^\perp) = (\Psi(C))^\perp.$$

In general, orthogonality will not be preserved. In the next example we will see that if C is a code over R_Δ then, in general, $\Psi(C)^\perp \neq \Psi(C^\perp)$ and the following diagram does not commute:

$$\begin{tikzcd} C \arrow[r, "\Psi"] \arrow[d] & \Psi(C) \\ C^\perp \arrow[r, "\Psi"] & \Psi(C^\perp) \end{tikzcd}$$

Example 4. Let $\Delta = 6 = 2 \cdot 3$ and consider the length one code $\widehat{I}_{(1,2)} = \langle u_{2,1}, u_{3,1}^2 \rangle$. By Proposition 2.7, we have that the dual is $\widehat{I}^{\perp}_{(1,2)} = I_{(1,1)} = \langle u_{2,1}u_{3,1} \rangle$. Clearly, $[u_{3,1}^2, u_{2,1}u_{3,1}] = 0 \in R_\Delta$ but, by Example 3, we have that $[\Psi(u_{3,1}^2), \Psi(u_{2,1}u_{3,1})] \neq 0$.

Computing $\Psi(\widehat{I}_{(1,2)})^\perp$ and $\Psi(\widehat{I}^{\perp}_{(1,2)})$ one obtains binary linear codes with parameters $[6, 2, 2]$ and $[6, 2, 4]$, respectively. That is, they are not only different codes but they have different minimum weights and hence are not equivalent.

4. MacWilliams relations

Let C be a linear code over R_Δ of length n. Define the complete weight enumerator of C in the usual way, namely:

$$cwe_C(X) = \sum_{c \in C} \prod_{i=1}^{n} x_{c_i}.$$

We are using X to denote the set of variables (x_{c_i}) where the c_i are the elements of R_Δ in some order.

In order to relate the complete weight enumerator of C with the complete weight enumerator of its dual, first we shall define a generator character of the ring. It is well known, see [7], that a finite ring is Frobenius if and only if it admits a generating character. Hence, a generating character exits for the ring R_Δ. We shall find this character explicitly.

Define the character $\chi : R_\Delta \longrightarrow \mathbb{C}^\star$ as

$$\chi(\sum_{\alpha \in J} c_\alpha u^\alpha) = \prod_{\alpha \in J} (-1)^{c_\alpha}.$$

In other words, the character has a value of -1 if there are oddly many monomials and 1 if there are evenly many monomials in a given element.

Consider the minimal ideal of the ring

$$Soc(R_\Delta) = \{0, u_{p_1,1}^{p_1-1} \cdots u_{p_1,k_1}^{p_1-1} \cdots u_{p_t,1}^{p_t-1} \cdots u_{p_t,k_t}^{p_t-1}\}.$$

Note that $\chi(0) = 1$ and $\chi(u_{p_t,1}^{p_t-1} \cdots u_{p_t,k_t}^{p_t-1}) = -1$ since it is a single monomial. Therefore, χ is non-trivial on the minimal ideal. Note also that this minimal ideal is contained in all ideals of the ring R_Δ since it is the unique minimal ideal. This gives that $ker(\chi)$ contains no non-trivial ideal. Hence, by Lemma 4.1 in [7], we have that the character χ is a generating character of the ring R_Δ. This generating character allows us to give the MacWilliams relations explicitly.

Use the elements of R_Δ as coordinates for the rows and columns. Let T be the $|R_\Delta| \times |R_\Delta|$ matrix given by $T_{a,b} = \chi(ab)$, for $a, b \in R_\Delta$. By the results in [7], we have the following theorem.

Theorem 4.1. *Let C be a linear code over R_Δ. Then*

$$cwe_{C^\perp}(X) = \frac{1}{|C|} cwe_C(T \cdot X),$$

where $T \cdot X$ represents the action of T on the vector X given by matrix multiplication TX^t, where X^t is the transpose of X.

5. Cyclic codes over R_Δ

In this section, we shall give an algebraic description of cyclic codes over R_Δ. These codes will, in turn, give quasi-cyclic codes of index Δ over $\mathbb{F}_2$.

Recall that, for an element a in R_Δ, $\mu(a)$ is the reduction modulo $\{u_{p_i,j}\}$ for all $i \in \{1, \ldots, t\}$ and $j \in \{1, \ldots, k_i\}$. Now, we can define a polynomial reduction μ from $R_\Delta[x]$ to $\mathbb{F}_2[x]$ where $\mu(f) = \mu(\sum a_i x^i) = \sum \mu(a_i) x^i$.

A monic polynomial f over $R_\Delta[x]$ is said to be a basic irreducible polynomial if $\mu(f)$ is an irreducible polynomial over $\mathbb{F}_2[x]$. Since $\mathbb{F}_2$ is a subring of R_Δ then, any irreducible polynomial in $\mathbb{F}_2[x]$ is a basic irreducible polynomial viewed as a polynomial of $R_\Delta[x]$.

Lemma 5.1. *Let n be an odd integer. Then, $x^n - 1$ factors into a product of finitely many pairwise coprime basic irreducible polynomials over R_Δ, $x^n - 1 = f_1 f_2 \cdots f_r$. Moreover, $f_1, f_2, \ldots, f_r$ are uniquely determined up to a rearrangement.*

Proof. The field $\mathbb{F}_2$ is a subring of R_Δ and $x^n - 1$ factors uniquely as a product of pairwise coprime irreducible polynomials in $\mathbb{F}_2[x]$. Therefore, the polynomial factors in R_Δ since $\mathbb{F}_2$ is a subring of R_Δ. Then Hensel's Lemma gives that regular polynomials (namely, polynomials that are not zero divisors) over R_Δ have a unique factorization. □

The previous lemma is highly dependent upon the fact that $\mathbb{F}_2$ is a subring of the ambient ring. Were this not the case, the lemma would not hold.

As in any commutative ring we can identify cyclic codes with ideals in a corresponding polynomial ring. We give the standard definitions to assign notation. Let $R_{\Delta,n} = R_\Delta[x]/\langle x^n - 1\rangle$.

Theorem 5.2. *Cyclic codes over R_Δ of length n can be viewed as ideals in $R_{\Delta,n}$.*

Proof. We view each codeword $(c_0, c_1, \ldots, c_{n-1})$ as a polynomial $c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$ in $R_{\Delta,n}$ and multiplication by x as the cyclic shift and the standard proof applies. □

The next theorem follows from the canonical decomposition of rings, noting that for odd n the factorization is unique.

Theorem 5.3. *Let n be an odd integer and let $x^n - 1 = f_1f_2\cdots f_r$. Then, the ideals in $R_{\Delta,n}$ can be written as $I \cong I_1 \oplus I_2 \oplus \cdots \oplus I_r$ where I_i is an ideal of the ring $R_\Delta[x]/\langle f_i\rangle$, for $i = 1, \ldots, r$.*

Let f be an irreducible polynomial in $\mathbb{F}_2[x]$, then f is a basic monic irreducible polynomial over R_Δ. Our goal now is to show that there is a one-to-one correspondence between ideals of $R_\Delta[x]/\langle f\rangle$ and ideals of R_Δ. We have that $\mathbb{F}_2[x]/\langle f\rangle$ is a finite field of order $2^{\deg(f)}$. Let $L_{0,0} = \mathbb{F}_2[x]/\langle f\rangle$ and $L_{p_1,1} = L_{0,0}[u_{p_1,1}]/\langle u_{p_1,1}^{p_1}\rangle$. For $1 \le i \le t$, $1 \le j \le k_i$, define

$$L_{p_i,j} = \begin{cases} L_{p_{i-1},k_{i-1}}[u_{p_i,1}]/\langle u_{p_i,1}^{p_i}\rangle & \text{if } j = 1, \\ L_{p_i,j-1}[u_{p_i,j}]/\langle u_{p_i,j}^{p_i}\rangle & \text{otherwise.} \end{cases}$$

Then we have that any element $a \in L_{p_i,j}$ can be written as $a = a_0 + a_1u_{p_i,j} + a_2u_{p_i,j}^2 + \cdots + a_{p_i-1}u_{p_i,j}^{p_i-1}$ where $a_0, \ldots, a_{p_i-1}$ belong to $L_{p_i,j-1}$ if $j \ne 1$ or to $L_{p_{i-1},k_{i-1}}$ if $j = 1$.

Proposition 5.4. *Let $a = \sum_{d=0}^{p_i-1} a_d u_{p_i,j}^d$ be an element of $L_{p_i,j}$. Then, a is a unit in $L_{p_i,j}$ if and only if a_0 is a unit in $L_{p_i,j-1}$ if $j \ne 1$ or in $L_{p_{i-1},k_{i-1}}$ if $j = 1$.*

Proof. Suppose a_0 is a unit in $L_{p_i,j-1}$ if $j \ne 1$ or in $L_{p_{i-1},k_{i-1}}$ if $j = 1$. Define $b = a_0^{-1}(\sum_{d=1}^{p_i-1} a_d u_{p_i,j}^d)$. Clearly, b is a zero divisor and $1 + b$ is a unit since $(1 + b)(1 + b + b^2 + \cdots + b^{p_i-1}) = 1$. So $a_0(1 + b) = a$ is also a unit.

If a_0 is not a unit then there exists b in $L_{p_i,j-1}$ if $j \neq 1$ or in $L_{p_{i-1},k_{i-1}}$ if $j = 1$, such that $ba_0 = 0$. Therefore, $bu_{p_i,j}^{p_i-1}a = 0$. □

Denote by $\mathcal{U}(L_{p_i,j})$ the group of units of $L_{p_i,j}$. By the previous result we can see that

$$|\mathcal{U}(L_{p_i,j})| = \begin{cases} |\mathcal{U}(L_{p_{i-1},k_{i-1}})||L_{p_{i-1},k_{i-1}}| & \text{if } j = 1, \\ |\mathcal{U}(L_{p_i,j-1})||L_{p_i,j-1}| & \text{otherwise.} \end{cases}$$

Since $|\mathcal{U}(L_{0,0})| = 2^{\deg(f)}-1$, we get that $|\mathcal{U}(L_{p_1,1})| = 2^{\deg(f)}(2^{\deg(f)}-1)$. By induction, we obtain that

$$|L_{p_t,k_t}| = (2^{\deg(f)})^{\Delta} \text{ and } |\mathcal{U}(L_{p_t,k_t})| = (2^{\deg(f)})^{\Delta} - (2^{\deg(f)})^{\Delta-1}.$$

Moreover, the group $\mathcal{U}(L_{p_i,j})$ is the direct product of a cyclic group G of order $2^{\deg(f)-1}$ and an abelian group H of order $(2^{\deg(f)})^{\Delta-1}$.

Theorem 5.5. *The ideals of L_{p_t,k_t} are in bijective correspondence with the ideals of R_Δ.*

Proof. From Proposition 5.4, it is straightforward that the zero-divisors of L_{p_t,k_t} are of the form $\sum c_\alpha u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ with $c_\alpha \in L_{0,0}$ and $c_{\mathbf{0}} = 0$, furthermore there are $(2^{\deg(f)})^{\Delta-1}$ of them. This gives the result. □

Corollary 5.6. *Let n be an odd integer. Let $x^n - 1 = f_1 f_2 \cdots f_r$ be the factorization of $x^n - 1$ into basic irreducible polynomials over R_Δ and let I_Δ be the number of ideals in R_Δ. Then, the number of linear cyclic codes of length n over R_Δ is $(I_\Delta)^r$.*

6. One generator cyclic codes

We shall examine codes that have a single generator. We shall proceed in a similar way as was done in [2] for the case when Δ was a power of 2. If a polynomial $s \in R_{\Delta,n}$ generates an ideal, then the ideal is the entire space if and only if s is a unit. Hence we need to consider codes generated by a non-unit. For foundational results in this section, see [5].

Let $\mathfrak{C}_n$ denote the cyclic group of order n. Consider the group ring $R_\Delta\mathfrak{C}_n$. This ring is canonically isomorphic to $R_{\Delta,n}$. Any element in $R_\Delta\mathfrak{C}_n$ corresponds to a circulant matrix in the following form:

$$\sigma(a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_2 & \cdots & a_0 \end{pmatrix}.$$

Take the standard definition of the determinant function, $det : M_n(R_\Delta) \to R_\Delta$.

Proposition 6.1. *An element $\alpha = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in R_{\Delta,n}$ is a non-unit if and only if $det(\sigma(\alpha)) \in \mathfrak{m}$. Equivalently, we have that an element $\alpha = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in R_{\Delta,n}$ is a non-unit if and only if $\mu(det(\sigma(\alpha))) = 0$.*

This proposition allows for a straightforward computational technique to find generators for cyclic codes over R_Δ which give binary quasi-cyclic codes of index Δ via the Gray map.

7. Binary quasi-cyclic codes

In this section, we shall give an algebraic construction of binary quasi-cyclic codes from codes over R_Δ.

Lemma 7.1. *Let $\mathbf{v}$ be a vector in R_Δ^n. Then $\Psi(\pi(\mathbf{v})) = \pi^\Delta(\Psi(\mathbf{v}))$.*

Proof. The result is a direct consequence from the definition of Ψ. □

The following theorems give a construction of linear binary quasi-cyclic codes of arbitrary index from cyclic codes and quasi-cyclic codes over R_Δ.

Theorem 7.2. *Let C be a linear cyclic code over R_Δ of length n. Then $\Psi(C)$ is a linear binary quasi-cyclic code of length Δn and index Δ.*

Proof. Since C is a cyclic code, $\pi(C) = C$. Then by Lemma 7.1, $\Psi(C) = \Psi(\pi(C)) = \pi^\Delta(\Psi(C))$. Hence $\Psi(C)$ is a quasi-cyclic code of index Δ. □

Theorem 7.3. *Let C be a linear quasi-cyclic code over R_Δ of length n and index k. Then, $\Psi(C)$ is a linear binary quasi-cyclic code of length Δn and index Δk.*

Proof. We can apply the same argument as in Theorem 7.2, taking into account that $\Psi(C) = \Psi(\pi^k(C)) = \pi^{\Delta k}(\Psi(C))$. □

8. Examples R_Δ

Examples of R_Δ-cyclic codes of length n for the case $\Delta = 2^{k_1}$ can be found in [2].

Table 1 shows some examples of one generator R_Δ-cyclic codes, for $\Delta \neq 2^{k_1}$, whose binary image via the Ψ map gives optimal codes [4] with minimum distance at least 3. For each cyclic code $C \in \mathcal{R}_\Delta^n$, in the table there are the parameters $[\Delta, n]$, the generator polynomial, and the parameters $[N, k, d]$ of $\Psi(C)$, where N is the length, k is the dimension, and d is the minimum distance.

Table 1
Quasi-cyclic codes of index Δ.

$[\Delta, n]$	Generators	Binary image
$[6, 2]$	$(u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2 + u_{3,1})x + u_{2,1}u_{3,1} + u_{2,1} + u_{3,1}$	$[12, 6, 4]$
$[6, 3]$	$(u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1})x^2 + (u_{2,1}u_{3,1} + u_{2,1} + u_{3,1})x$	$[18, 11, 4]$
$[6, 3]$	$(u_{2,1}u_{3,1}^2 + u_{2,1} + u_{3,1}^2 + u_{3,1})x^2 + (u_{2,1}u_{3,1} + u_{2,1} + u_{3,1})x$	$[18, 10, 4]$
$[6, 3]$	$(u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2)x^2 + (u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2)x$	$[18, 4, 8]$
$[6, 3]$	$(u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2)x^2 + (u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2)x + u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2$	$[18, 2, 12]$
$[6, 4]$	$(u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{2,1} + u_{3,1})x^3 + (u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1})x^2 + (u_{2,1}u_{3,1} + u_{2,1} + u_{3,1})x$	$[24, 8, 8]$
$[6, 4]$	$(u_{2,1}u_{3,1}^2 + 1)x^3 + x^2 + (u_{2,1}u_{3,1} + u_{2,1} + 1)x + u_{2,1}u_{3,1} + u_{2,1} + 1$	$[24, 9, 8]$
$[6, 6]$	$(u_{2,1}u_{3,1}^2 + u_{2,1} + u_{3,1}^2 + 1)x^5 + (u_{3,1}^2 + 1)x^4 + (u_{2,1}u_{3,1}^2 + u_{2,1})x^3 + (u_{2,1} + u_{3,1}^2 + 1)x^2 + (u_{2,1}u_{3,1} + u_{2,1} + 1)x$	$[36, 17, 8]$
$[6, 6]$	$(u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1} + 1)x^5 + (u_{2,1}u_{3,1}^2 + u_{2,1}u_{3,1} + u_{3,1}^2)x^4 + (u_{2,1}u_{3,1} + u_{2,1} + u_{3,1}^2)x^3 + (u_{2,1}u_{3,1} + u_{2,1} + 1)x^2$	$[36, 18, 8]$
$[6, 7]$	$(u_{2,1}u_{3,1}^2 + u_{2,1} + u_{3,1} + 1)x^6 + (u_{2,1}u_{3,1} + u_{2,1} + u_{3,1} + 1)x^5 + (u_{2,1}u_{3,1} + u_{2,1} + 1)x^4 + (u_{2,1}u_{3,1} + u_{2,1} + 1)x^2$	$[42, 32, 4]$
$[6, 7]$	$(u_{2,1} + u_{3,1} + 1)x^6 + (u_{2,1} + u_{3,1}^2 + 1)x^5 + (u_{3,1}^2 + 1)x^4 + (u_{2,1}u_{3,1} + u_{3,1}^2 + u_{3,1})x^3 + (u_{2,1}u_{3,1} + u_{2,1} + 1)x^2$	$[42, 33, 4]$
$[9, 2]$	$(u_{3,1}^2u_{3,2} + u_{3,1}^2 + u_{3,1}u_{3,2})x + u_{3,1}^2u_{3,2}^2 + u_{3,1}^2u_{3,2} + u_{3,1}^2 + u_{3,1}u_{3,2}$	$[18, 4, 8]$
$[9, 2]$	$(u_{3,1}^2u_{3,2}^2+u_{3,1}^2+u_{3,1}u_{3,2}^2+u_{3,1}+1)x+u_{3,1}^2u_{3,2}+u_{3,1}u_{3,2}^2+u_{3,1}u_{3,2}+u_{3,1}+1$	$[18, 10, 4]$
$[9, 3]$	$(u_{3,1}^2u_{3,2} + u_{3,1}^2 + u_{3,1}u_{3,2}^2 + u_{3,1}u_{3,2} + u_{3,1} + u_{3,2}^2 + u_{3,2})x^2 + (u_{3,1}^2 + u_{3,1}u_{3,2}^2 + u_{3,1}u_{3,2} + u_{3,1})x + u_{3,2}^2$	$[27, 18, 4]$
$[9, 4]$	$(u_{3,1}^2u_{3,2}^2 + u_{3,1} + u_{3,2}^2)x^3 + (u_{3,1}^2 + u_{3,1} + 1)x^2 + (u_{3,1}^2 + u_{3,1}u_{3,2}^2 + u_{3,1}u_{3,2} + u_{3,2}^2 + 1)x$	$[36, 27, 4]$
$[12, 3]$	$(u_{2,1}u_{3,1}^2 + u_{2,1} + u_{2,2}u_{3,1}^2 + u_{2,2}u_{3,1} + u_{2,2} + u_{3,1}^2)x^2 + (u_{2,1}u_{2,2}u_{3,1}^2 + u_{2,1}u_{3,1}^2 + u_{2,2}u_{3,1} + u_{2,2})x + u_{2,1}u_{2,2}u_{3,1}^2 + u_{2,1}u_{2,2} + u_{2,1}u_{3,1} + u_{2,1} + u_{2,2}u_{3,1}^2 + u_{2,2}u_{3,1}$	$[36, 17, 8]$
$[12, 3]$	$u_{3,1}x^2 + (u_{2,1}u_{2,2}u_{3,1}^2 + u_{2,1}u_{3,1}^2 + u_{2,2}u_{3,1} + u_{2,2})x + u_{2,1}u_{2,2}u_{3,1}^2 + u_{2,1}u_{2,2} + u_{2,1}u_{3,1} + u_{2,1} + u_{2,2}u_{3,1}^2 + u_{2,2}u_{3,1}$	$[36, 18, 8]$

References

[1] S.T. Dougherty, B. Yildiz, S. Karadeniz, Codes over R_k, Gray maps and their binary images, Finite Fields Appl. 17 (3) (2011) 205–219.

[2] S.T. Dougherty, B. Yildiz, S. Karadeniz, Cyclic codes over R_k, Des. Codes Cryptogr. 63 (1) (2012) 113–126.

[3] S.T. Dougherty, B. Yildiz, S. Karadeniz, Self-dual codes over R_k and binary self-dual codes, Eur. J. Pure Appl. Math. 6 (1) (2013).

[4] M. Grassl, Table of bounds on linear codes, http://www.codestable.de.

[5] T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math. 31 (3) (2006) 319–335.

[6] B. Yildiz, S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr. 54 (2011) 61–81.

[7] Jay A. Wood, Duality for modules over finite rings and applications to coding theory, Am. J. Math. 121 (3) (1999) 555–575.

Appendix B

$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes

$\mathbb{Z}_2\mathbb{Z}_4$-Additive Cyclic Codes, Generator Polynomials, and Dual Codes

Joaquim Borges, Cristina Fernández-Córdoba, and Roger Ten-Valls

***Abstract*— A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called cyclic if the set of coordinates can be partitioned into two subsets, the set of $\mathbb{Z}_2$ and the set of $\mathbb{Z}_4$ coordinates, such that any cyclic shift of the coordinates of both subsets leaves the code invariant. These codes can be identified as submodules of the $\mathbb{Z}_4[x]$-module $\mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$. The parameters of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code are stated in terms of the degrees of the generator polynomials of the code. The generator polynomials of the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code are determined in terms of the generator polynomials of the code $\mathcal{C}$.**

***Index Terms*— Binary cyclic codes, cyclic codes over $\mathbb{Z}_4$, duality, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.**

I. Introduction

DENOTE by $\mathbb{Z}_2$ and $\mathbb{Z}_4$ the rings of integers modulo 2 and modulo 4, respectively. We denote the space of n-tuples over these rings as $\mathbb{Z}_2^n$ and $\mathbb{Z}_4^n$. A binary code is any non-empty subset C of $\mathbb{Z}_2^n$. If that subset is a vector space then we say that it is a linear code. A code over $\mathbb{Z}_4$ is a non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ and a submodule of $\mathbb{Z}_4^n$ is called a linear code over $\mathbb{Z}_4$.

In Delsarte's 1973 paper (see [5]), he defined additive codes as subgroups of the underlying abelian group in a translation association scheme. For the binary Hamming scheme, namely, when the underlying abelian group is of order 2^n, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. This means that the subgroups $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme. In [4], $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were studied.

For vectors $\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we write $\mathbf{u} = (u \mid u')$ where $u = (u_0, \dots, u_{\alpha-1}) \in \mathbb{Z}_2^\alpha$ and $u' = (u'_0, \dots, u'_{\beta-1}) \in \mathbb{Z}_4^\beta$.

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to a commutative structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and the number of order two codewords in $\mathcal{C}$ is $2^{\gamma+\delta}$.

Let X (respectively Y) be the set of $\mathbb{Z}_2$ (respectively $\mathbb{Z}_4$) coordinate positions, so $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set X corresponds to the first α coordinates and Y corresponds to the last β coordinates. Call $\mathcal{C}_X$ (respectively $\mathcal{C}_Y$) the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively Y). Let $\mathcal{C}_b$ be the subcode of $\mathcal{C}$ which contains all order two codewords and let κ be the dimension of $(\mathcal{C}_b)_X$, which is a binary linear code. For the case $\alpha = 0$, we will write $\kappa = 0$.

Considering all these parameters, we will say that $\mathcal{C}$ is of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Notice that $\mathcal{C}_Y$ is a linear code over $\mathbb{Z}_4$ of type $(0, \beta; \gamma_Y, \delta; 0)$, where $0 \leq \gamma_Y \leq \gamma$, and $\mathcal{C}_X$ is a binary linear code of type $(\alpha, 0; \gamma_X, 0; \gamma_X)$, where $\kappa \leq \gamma_X \leq \kappa + \delta$. A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is said to be separable if $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$.

Let κ_1 and δ_2 be the dimensions of the subcodes $\{(u \mid 0\dots0) \in \mathcal{C}\}$ and $\{(0\dots0 \mid u') \in \mathcal{C} :$ the order of u' is 4$\}$, respectively. Define $\kappa_2 = \kappa - \kappa_1$ and $\delta_1 = \delta - \delta_2$. By definition, it is clear that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code is separable if and only if κ_2 and δ_1 are zero; that is, $\kappa = \kappa_1$ and $\delta = \delta_2$.

We define a Gray Map as $\phi : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \to \mathbb{Z}_2^{\alpha+2\beta}$ such that $\phi(\mathbf{u}) = \phi(u \mid u') = (u, \phi_4(u'))$, where ϕ_4 is the usual quaternary Gray map defined by $\phi_4(0) = (0,0), \phi_4(1) = (0,1), \phi_4(2) = (1,1), \phi_4(3) = (1,0)$.

The *standard inner product*, defined in [4], can be written as

$$\mathbf{u} \cdot \mathbf{v} = 2\left(\sum_{i=0}^{\alpha-1} u_i v_i\right) + \sum_{j=0}^{\beta-1} u'_j v'_j \in \mathbb{Z}_4,$$

where the computations are made taking the zeros and ones in the α binary coordinates as zeros and ones in $\mathbb{Z}_4$, respectively. The *dual code* of $\mathcal{C}$, is defined in the standard way by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}.$$

If $\mathcal{C}$ is separable then $\mathcal{C}^\perp = (\mathcal{C}_X)^\perp \times (\mathcal{C}_Y)^\perp$. From [4], and the previous definition of κ_1 and δ_1 we obtain the number of codewords of $\mathcal{C}, \mathcal{C}_X, \mathcal{C}_Y$ and their duals.

Proposition 1: Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Let κ_1 and δ_1 be defined as before. Then,

$$\begin{aligned} |\mathcal{C}| &= 2^\gamma 4^\delta, \quad |\mathcal{C}^\perp| = 2^{\alpha+\gamma-2\kappa} 4^{\beta-\gamma-\delta+\kappa}, \\ |\mathcal{C}_X| &= 2^{\kappa+\delta_1}, \quad |(\mathcal{C}_X)^\perp| = 2^{\alpha-\kappa-\delta_1}, \\ |\mathcal{C}_Y| &= 2^{\gamma-\kappa_1} 4^\delta, \quad |(\mathcal{C}_Y)^\perp| = 2^{\gamma-\kappa_1} 4^{\beta-\gamma-\delta+\kappa_1}. \end{aligned}$$

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Then, $\mathcal{C}$ is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code with

Manuscript received March 3, 2015; revised April 1, 2016; accepted September 13, 2016. Date of publication September 20, 2016; date of current version October 18, 2016. This work was supported in part by Spanish MINECO under Grant TIN2016-77918P and in part by Catalan AGAUR under Grant 2014SGR-691. This paper was presented at Karatekin Mathematics Days 2014, International Mathematics Symposium, Çankırı, Turkey.

The authors are with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Barcelona, Spain (e-mail: joaquim.borges@uab.cat; cristina.fernandez@uab.cat; roger.ten@uab.cat).

Communicated by J. Lahtonen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2016.2611528

generator matrix of the form

$$\mathcal{G}_{\mathcal{C}} = \left(\begin{array}{cccc|ccccc} I_{\kappa_1} & T & T'_{b_1} & T_{b_1} & 0 & 0 & 0 & 0 & 0 \\ 0 & I_{\kappa_2} & T'_{b_2} & T_{b_2} & 2T_2 & 2T_{\kappa_2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2T_1 & 2T'_1 & 2I_{\gamma-\kappa} & 0 & 0 \\ \hline 0 & 0 & S_{\delta_1} & S_b & S_{11} & S_{12} & R_1 & I_{\delta_1} & 0 \\ 0 & 0 & 0 & 0 & S_{21} & S_{22} & R_2 & R_{\delta_1} & I_{\delta_2} \end{array}\right)$$

where I_r is the identity matrix of size $r \times r$; the matrices $T_{b_i}, T'_{b_i}, S_{\delta_1}, S_b$ are over $\mathbb{Z}_2$; the matrices $T_1, T_2, T_{\kappa_2}, T'_1, R_i$ are over $\mathbb{Z}_4$ with all entries in $\{0, 1\} \subset \mathbb{Z}_4$; and S_{ij} are matrices over $\mathbb{Z}_4$. The matrices S_{δ_1} and T_{κ_2} are square matrices of full rank δ_1 and κ_2 respectively, $\kappa = \kappa_1 + \kappa_2$ and $\delta = \delta_1 + \delta_2$.

This new generator matrix can be obtained by applying convenient column permutations and linear combinations of rows to the generator matrix given in [4]. This new form is going to help us to relate the parameters of the code and the degrees of the generator polynomials of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code.

II. $\mathbb{Z}_2\mathbb{Z}_4$-Additive Cyclic Codes

A. Parameters and Generators

Let $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and i be an integer. Then we denote by

$$\begin{aligned} \mathbf{u}^{(i)} &= (u^{(i)} \mid u'^{(i)}) \\ &= (u_{0+i}, u_{1+i}, \dots, u_{\alpha-1+i} \mid u'_{0+i}, u'_{1+i}, \dots, u'_{\beta-1+i}) \end{aligned}$$

the cyclic ith shift of $\mathbf{u}$, where the subscripts are read modulo α and β, respectively.

We say that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is *cyclic* if for any codeword $\mathbf{u} \in \mathcal{C}$ we have $\mathbf{u}^{(1)} \in \mathcal{C}$.

Let $R_{\alpha,\beta} = \mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$, for $\beta \geq 0$ odd, and define the operation $\star : \mathbb{Z}_4[x] \times R_{\alpha,\beta} \to R_{\alpha,\beta}$ as $\lambda(x) \star (p(x) \mid q(x)) = (\lambda(x)p(x) \bmod (2) \mid \lambda(x)q(x))$. From [1], we know that $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes are identified as $\mathbb{Z}_4[x]$-submodules of $R_{\alpha,\beta}$. Moreover, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then it is of the form

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle, \qquad (1)$$

where $f(x)h(x)g(x) = x^\beta - 1$ in $\mathbb{Z}_4[x]$, $b(x), \ell(x) \in \mathbb{Z}_2[x]/(x^\alpha - 1)$ with $b(x) | (x^\alpha - 1)$, $deg(\ell(x)) < deg(b(x))$, and $b(x)$ divides $\frac{x^\beta - 1}{f(x)}\ell(x) \pmod 2$.

Note that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle$, then the canonical projections $\mathcal{C}_X$ and $\mathcal{C}_Y$ are a cyclic code over $\mathbb{Z}_2$ and a cyclic code over $\mathbb{Z}_4$ generated by $gcd(b(x), \ell(x))$ and $(f(x)h(x) + 2f(x))$, respectively (see [6], [9]).

Since $b(x)$ divides $\frac{x^\beta - 1}{f(x)}\ell(x) \pmod 2$, we have the following result.

Corollary 2: Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with $\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle$. Then, $b(x)$ divides $\frac{x^\beta - 1}{f(x)} \gcd(b(x), \ell(x)) \pmod 2$ and $b(x)$ divides $h(x) \gcd(b(x), \ell(x)g(x)) \pmod 2$.

Note that if a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is separable, then $\ell(x) = 0$.

In the following, a polynomial $f(x) \in \mathbb{Z}_2[x]$ or $\mathbb{Z}_4[x]$ will be denoted simply by f and the parameter β will be an odd integer.

Lemma 3: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. Then,

$$\mathcal{C}_b = \langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh) \rangle.$$

Proof: $\mathcal{C}_b$ is the subcode of $\mathcal{C}$ which contains all codewords of order 2. Since $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$, then all codewords of order 2 are generated by $\langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh) \rangle$. ■

The following results show the close relation of the parameters of the type of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code and the degrees of the generator polynomials of the code.

First, the next theorem gives the spanning sets in terms of the generator polynomials.

Theorem 4 ([1, Th. 13]): Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fhg = x^\beta - 1$. Let

$$S_1 = \bigcup_{i=0}^{\alpha - \deg(b) - 1} \{x^i \star (b \mid 0)\},$$

$$S_2 = \bigcup_{i=0}^{\deg(g) - 1} \{x^i \star (\ell \mid fh + 2f)\}$$

and

$$S_3 = \bigcup_{i=0}^{\deg(h) - 1} \{x^i \star (\ell g \mid 2fg)\}.$$

Then, $S_1 \cup S_2 \cup S_3$ forms a minimal spanning set for $\mathcal{C}$ as a $\mathbb{Z}_4$-module. Moreover, $\mathcal{C}$ has $2^{\alpha - \deg(b)} 4^{\deg(g)} 2^{\deg(h)}$ codewords.

Note that S_2 generates all order 4 codewords and the subcode of codewords of order 2, $\mathcal{C}_b$, is generated by $\{S_1, 2S_2, S_3\}$. Hence, in the following theorem, by using these spanning sets, we can obtain the parameters $(\alpha, \beta; \gamma, \delta; \kappa)$ of the code.

Theorem 5: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fhg = x^\beta - 1$. Then

$$\begin{aligned} \gamma &= \alpha - \deg(b) + \deg(h), \\ \delta &= \deg(g), \\ \kappa &= \alpha - \deg(\gcd(\ell g, b)). \end{aligned}$$

Proof: The parameters γ and δ are known from Theorem 4 and the parameter κ is the dimension of $(\mathcal{C}_b)_X$. By Lemma 3, the space $(\mathcal{C}_b)_X$ is generated by the polynomials b and ℓg. Since the ring is a polynomial ring and thus a principal ideal ring, it is generated by the greatest common divisor of the two polynomials. Then, $\kappa = \alpha - deg(gcd(\ell g, b))$. ■

In this case we have that $|\mathcal{C}| = 2^{\alpha - deg(b)} 4^{deg(g)} 2^{deg(h)}$.

Proposition 6: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta = \delta_1 + \delta_2; \kappa = \kappa_1 + \kappa_2)$, where $fhg = x^\beta - 1$. Then,

$$\kappa_1 = \alpha - \deg(b), \quad \kappa_2 = \deg(b) - \deg(\gcd(b, \ell g)),$$
$$\delta_1 = \deg(\gcd(b, \ell g)) - \deg(\gcd(b, \ell)) \text{ and } \delta_2 = \deg(g) - \delta_1.$$

Proof: The result follows from Proposition 1 and knowing the generator polynomials of $\mathcal{C}_X$ and $(\mathcal{C}_b)_X$. They are $\gcd(b, \ell)$ and $\gcd(b, \ell g)$, respectively. ■

B. Dual $\mathbb{Z}_2\mathbb{Z}_4$-Additive Cyclic Codes

In [1], it is proven that the dual code of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is also a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code. So, we will denote

$$\mathcal{C}^{\perp} = \langle(\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle,$$

where $\bar{f}\bar{h}\bar{g} = x^{\beta} - 1$ in $\mathbb{Z}_4[x]$, $\bar{b}, \bar{\ell} \in \mathbb{Z}_2[x]/(x^{\alpha} - 1)$ with $\bar{b}|(x^{\alpha} - 1)$, $deg(\bar{\ell}) < deg(\bar{b})$ and $\bar{b}$ divides $\frac{x^{\beta}-1}{\bar{f}}\bar{\ell} \pmod 2$.

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. As in the theory of cyclic codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$ (see [6], [7]), reciprocal polynomials have an important role on duality.

We denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$. Using this notation we have the following proposition.

Proposition 7: Let $n, m \in \mathbb{N}$. Then,

$$x^{nm} - 1 = (x^n - 1)\theta_m(x^n).$$

Proof: It is well know that $y^m - 1 = (y - 1)\theta_m(y)$, replacing y by x^n the result follows. ■

From now on, $\mathfrak{m}$ denotes the least common multiple of α and β.

Definition 8: Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $R_{\alpha,\beta}$. We define the map

$$\circ : R_{\alpha,\beta} \times R_{\alpha,\beta} \longrightarrow \mathbb{Z}_4[x]/(x^{\mathfrak{m}} - 1),$$

such that

$$\begin{aligned}\circ(\mathbf{u}(x), \mathbf{v}(x)) = {} & 2u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^{\alpha})x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) \\ & + u'(x)\theta_{\frac{\mathfrak{m}}{\beta}}(x^{\beta})x^{\mathfrak{m}-1-\deg(v'(x))}v'^*(x) \\ & \bmod (x^{\mathfrak{m}} - 1),\end{aligned}$$

where the computations are made taking the binary zeros and ones in $u(x)$ and $v(x)$ as quaternary zeros and ones, respectively.

The map $\circ$ is linear in each of its arguments; i.e., if we fix the first entry of the map invariant, while letting the second entry vary, then the result is a linear map. Similarly, when fixing the second entry invariant. Then, the map $\circ$ is a bilinear map between $\mathbb{Z}_4[x]$-modules.

From now on, we denote $\circ(\mathbf{u}(x), \mathbf{v}(x))$ by $\mathbf{u}(x) \circ \mathbf{v}(x)$. Note that $\mathbf{u}(x) \circ \mathbf{v}(x)$ belongs to $\mathbb{Z}_4[x]/(x^{\mathfrak{m}} - 1)$.

Proposition 9: Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ with associated polynomials $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$. Then, $\mathbf{u}$ is orthogonal to $\mathbf{v}$ and all its shifts if and only if

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0.$$

Proof: The ith shift of $\mathbf{v}$ is $\mathbf{v}^{(i)} = (v_{0+i}v_{1+i}\dots v_{\alpha-1+i} \mid v'_{0+i}\dots v'_{\beta-1+i})$. Then,

$$\mathbf{u} \cdot \mathbf{v}^{(i)} = 0 \text{ if and only if } 2\sum_{j=0}^{\alpha-1} u_j v_{j+i} + \sum_{k=0}^{\beta-1} u'_k v'_{k+i} = 0.$$

Let $S_i = 2\sum_{j=0}^{\alpha-1} u_j v_{j+i} + \sum_{k=0}^{\beta-1} u'_k v'_{k+i}$. One can check that

$$\begin{aligned}\mathbf{u}(x) \circ \mathbf{v}(x) = {} & 2\theta_{\frac{\mathfrak{m}}{\alpha}}(x^{\alpha})\left[\sum_{n=0}^{\alpha-1}\sum_{j=n}^{\alpha-1} u_{j-n}v_j x^{\mathfrak{m}-1-n}\right. \\ & \left. + \sum_{n=1}^{\alpha-1}\sum_{j=n}^{\alpha-1} u_j v_{j-n} x^{\mathfrak{m}-1+n}\right] \\ & + \theta_{\frac{\mathfrak{m}}{\beta}}(x^{\beta})\left[\sum_{t=0}^{\beta-1}\sum_{k=t}^{\beta-1} u'_{k-t}v'_j x^{\mathfrak{m}-1-t}\right. \\ & \left. + \sum_{t=1}^{\beta-1}\sum_{k=t}^{\beta-1} u'_k v'_{k-t} x^{\mathfrak{m}-1+t}\right] \\ & \bmod (x^{\mathfrak{m}} - 1).\end{aligned}$$

Then, arranging the terms one obtains that

$$\mathbf{u}(x) \circ \mathbf{v}(x) = \sum_{i=0}^{\mathfrak{m}-1} S_i x^{\mathfrak{m}-1-i} \quad \bmod (x^{\mathfrak{m}} - 1).$$

Thus, $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$ if and only if $S_i = 0$ for $0 \leq i \leq \mathfrak{m} - 1$. ■

Lemma 10: Let $\mathbf{u} = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $R_{\alpha,\beta}$ such that $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$. If $u'(x)$ or $v'(x)$ equals 0, then $u(x)v^*(x) \equiv 0 \pmod{(x^{\alpha}-1)}$ over $\mathbb{Z}_2$. If $u(x)$ or $v(x)$ equals 0, then $u'(x)v'^*(x) \equiv 0 \pmod{(x^{\beta}-1)}$ over $\mathbb{Z}_4$.

Proof: Let $u'(x)$ or $v'(x)$ equals 0, then

$$\begin{aligned}0 &= \mathbf{u}(x) \circ \mathbf{v}(x) \\ &= 2u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^{\alpha})x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) + 0 \quad \bmod (x^{\mathfrak{m}} - 1).\end{aligned}$$

So,

$$2u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^{\alpha})x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) = 2\mu'(x)(x^{\mathfrak{m}} - 1),$$

for some $\mu'(x) \in \mathbb{Z}_4[x]$.

This is equivalent to

$$u(x)\theta_{\frac{\mathfrak{m}}{\alpha}}(x^{\alpha})x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) = \mu'(x)(x^{\mathfrak{m}} - 1) \in \mathbb{Z}_2[x].$$

By Proposition 7,

$$\begin{aligned}u(x)x^{\mathfrak{m}}v^*(x) &= \mu(x)(x^{\alpha} - 1), \\ u(x)v^*(x) &\equiv 0 \pmod{(x^{\alpha} - 1)}.\end{aligned}$$

A similar argument can be used to prove the other case. ■

The following proposition determines the degrees of the generator polynomials of the dual code in terms of the degrees of the generator polynomials of the code. These results will be helpful to determine the generator polynomials of the dual code.

Proposition 11: Let $\mathcal{C} = \langle(b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fgh = x^{\beta} - 1$, and with dual code $\mathcal{C}^{\perp} = \langle(\bar{b} \mid 0),$

$(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then,

$$\begin{aligned}
\deg(\bar{b}) &= \alpha - \deg(\gcd(b, \ell)),\\
\deg(\bar{f}) &= \deg(g) + \deg(\gcd(b, \ell)) - \deg(\gcd(b, \ell g)),\\
\deg(\bar{h}) &= \deg(h) - \deg(b) - \deg(\gcd(b, \ell))\\
&\quad + 2\deg(\gcd(b, \ell g)),\\
\deg(\bar{g}) &= \deg(f) + \deg(b) - \deg(\gcd(b, \ell g)).
\end{aligned}$$

Proof: Let $\mathcal{C}^\perp$ be a code of type $(\alpha, \beta; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$. It is easy to prove that $(\mathcal{C}_X)^\perp$ is a binary cyclic code generated by $\bar{b}$, so $|(\mathcal{C}_X)^\perp| = 2^{\alpha - \deg(\bar{b})}$. Moreover, by Proposition 1, $|(\mathcal{C}_X)^\perp| = 2^{\alpha-\kappa-\delta_1}$ and by Proposition 6, we obtain that $\deg(\bar{b}) = \alpha - \deg(\gcd(b, \ell))$. Finally, from [4] it is known that

$$\begin{aligned}
\bar{\gamma} &= \alpha + \gamma - 2\kappa,\\
\bar{\delta} &= \beta - \gamma - \delta + \kappa,\\
\bar{\kappa} &= \alpha - \kappa,
\end{aligned}$$

and applying Theorem 5 to the parameters of $\mathcal{C}$ and $\mathcal{C}^\perp$, we obtain the result. ■

We know that a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is separable if and only if $\mathcal{C}^\perp$ is separable. Moreover, if a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is separable, then it is easy to find the generator polynomials of the dual, that are given in the following proposition.

Proposition 12: Let $\mathcal{C} = \langle(b \mid 0), (0 \mid fh + 2f)\rangle$ be a separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fgh = x^\beta - 1$. Then,

$$\mathcal{C}^\perp = \langle(\frac{x^\alpha - 1}{b^*} \mid 0), (0 \mid g^*h^* + 2g^*)\rangle.$$

Proof: If $\mathcal{C}$ is separable, then $\mathcal{C}^\perp = (\mathcal{C}_X)^\perp \times (\mathcal{C}_Y)^\perp$, where $(\mathcal{C}_X)^\perp = \langle\frac{x^\alpha-1}{b^*}\rangle$ and $(\mathcal{C}_Y)^\perp = \langle g^*h^* + 2g^*\rangle$. ■

Proposition 13: Let $\mathcal{C} = \langle(b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with dual code $\mathcal{C}^\perp = \langle(\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle$. Then,

$$\bar{b} = \frac{x^\alpha - 1}{(gcd(b, \ell))^*} \in \mathbb{Z}_2[x].$$

Proof: We have that $(\bar{b} \mid 0)$ belongs to $\mathcal{C}^\perp$. Then,

$$\begin{aligned}
(b \mid 0) \circ (\bar{b} \mid 0) &= 0,\\
(\ell \mid fh + 2f) \circ (\bar{b} \mid 0) &= 0.
\end{aligned}$$

Therefore, by Lemma 10,

$$\begin{aligned}
b\bar{b}^* &\equiv 0 \pmod{(x^\alpha - 1)},\\
\ell\bar{b}^* &\equiv 0 \pmod{(x^\alpha - 1)},
\end{aligned}$$

over $\mathbb{Z}_2$. So, $\gcd(b, \ell)\bar{b}^* \equiv 0 \pmod{(x^\alpha - 1)}$, and there exist $\mu \in \mathbb{Z}_2[x]$ such that $\gcd(b, \ell)\bar{b}^* = \mu(x^\alpha - 1)$.
Moreover, since $\gcd(b, \ell)$ and $\bar{b}^*$ divides $(x^\alpha - 1)$ and, by Proposition 11, we have that $\deg(\bar{b}) = \alpha - \deg(\gcd(b, \ell))$. We conclude that

$$\bar{b}^* = \frac{x^\alpha - 1}{\gcd(b, \ell)} \in \mathbb{Z}_2[x].$$

■

Proposition 14: Let $\mathcal{C} = \langle(b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fgh = x^\beta - 1$, and with dual code $\mathcal{C}^\perp = \langle(\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then, $\bar{f}\bar{h}$ is the Hensel lift of the polynomial $\frac{(x^\beta-1)\gcd(b,\ell g)^*}{f^*b^*} \in \mathbb{Z}_2[x]$.

Proof: It is known that h and g are coprime, from which we deduce easily that $p_1fh + p_2fg = f$, for some p_1, $p_2 \in \mathbb{Z}_4[x]$. Since $(b \mid 0)$, $(0 \mid 2fh)$ and $(\ell g \mid 2fg)$ belong to $\mathcal{C}$, then

$$(0 \mid \frac{b}{\gcd(b, \ell g)}(2p_1fh + 2p_2fg)) = (0 \mid \frac{b}{\gcd(b, \ell g)}2f) \in \mathcal{C}.$$

Therefore,

$$(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (0 \mid \frac{b}{\gcd(b, \ell g)}2f) = 0.$$

Thus, by Lemma 10,

$$(\bar{f}\bar{h} + 2\bar{f})\left(\frac{b^*2f^*}{\gcd(b, \ell g)^*}\right) \equiv 0 \pmod{(x^\beta - 1)},$$

and

$$(2\bar{f}\bar{h})\left(\frac{b^*f^*}{\gcd(b, \ell g)^*}\right) = 2\mu(x^\beta - 1), \qquad (2)$$

for some $\mu \in \mathbb{Z}_4[x]$.

If (2) holds over $\mathbb{Z}_4$, then it is equivalent to

$$(\bar{f}\bar{h})\left(\frac{b^*f^*}{\gcd(b, \ell g)^*}\right) = \mu(x^\beta - 1) \in \mathbb{Z}_2[x].$$

It is known that $\bar{f}\bar{h}$ is a divisor of $x^\beta - 1$ and, by Corollary 2, we have that $\left(\frac{b^*f^*}{\gcd(b,\ell g)^*}\right)$ divides $(x^\beta - 1)$ over $\mathbb{Z}_2$. By Corollary 11, $\deg(\bar{f}\bar{h}) = \beta - \deg(f) - \deg(b) + \deg(\gcd(b, \ell g))$, so

$$\beta = \deg\left(\bar{f}\bar{h}\frac{b^*f^*}{\gcd(b, \ell g)^*}\right) = \deg(x^\beta - 1).$$

Hence, we obtain that $\mu = 1 \in \mathbb{Z}_2$ and

$$\bar{f}\bar{h} = \frac{(x^\beta - 1)\gcd(b, \ell g)^*}{f^*b^*} \in \mathbb{Z}_2[x]. \qquad (3)$$

Since β is odd and by the uniqueness of the Hensel lift [9, p.73], $\bar{f}\bar{h}$ is the unique monic polynomial in $\mathbb{Z}_4[x]$ dividing $(x^\beta - 1)$ and satisfying (3). ■

Proposition 15: Let $\mathcal{C} = \langle(b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, where $fgh = x^\beta - 1$, and with dual code $\mathcal{C}^\perp = \langle(\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h} = x^\beta - 1$. Then, $\bar{f}$ is the Hensel lift of the polynomial $\frac{(x^\beta-1)\gcd(b,\ell)^*}{f^*h^*\gcd(b,\ell g)^*} \in \mathbb{Z}_2[x]$.

Proof: One can factorize in $\mathbb{Z}_2[x]$ the polynomials $b, \ell, \ell g$ in the following way:

$$\begin{aligned}
\ell &= \gcd(b, \ell)\rho,\\
\ell g &= \gcd(b, \ell g)\rho\tau_1,\\
b &= \gcd(b, \ell g)\tau_2,
\end{aligned}$$

where τ_1 and τ_2 are coprime polynomials.

Hence, there exist $t_1, t_2 \in \mathbb{Z}_2[x]$ such that $t_1\tau_1 + t_2\tau_2 = 1$. Then,

$$\gcd(b, \ell g)\rho(t_1\tau_1 + t_2\tau_2) = \gcd(b, \ell g)\rho,$$

and

$$t_1\ell g + \rho t_2 b = \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}\ell.$$

Therefore,

$$\frac{\gcd(b,\ell g)}{\gcd(b,\ell)} \star (\ell \mid fh+2f) + t_1 \star (\ell g \mid 2fg) + \rho t_2 \star (b \mid 0) \\ = \left(0 \mid \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}(fh+2f) + t_1 2fg\right) \in \mathcal{C}.$$

Since $\bar h$ and $\bar g$ are coprime, there exist $\bar p_1, \bar p_2 \in \mathbb{Z}_4[x]$ such that $2\bar p_1 \bar f \bar h + 2\bar p_2 \bar f \bar g = 2\bar f$. So, $(2\bar p_1 + \bar p_2 \bar g) \star (\bar\ell \mid \bar f\bar h + 2\bar f) = (\bar p_2 \bar\ell \bar g \mid 2\bar f) \in \mathcal{C}^\perp$.

Therefore,

$$(\bar p_2 \bar\ell \bar g \mid 2\bar f) \circ \left(0 \mid \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}(fh+2f) + t_1 2fg\right) = 0.$$

By Lemma 10, arranging properly, we obtain that

$$2\bar f\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^*h^* \equiv 0 \pmod{(x^\beta - 1)}$$

and

$$2\bar f\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^*h^* = 2\mu(x^\beta - 1), \tag{4}$$

for some $\mu \in \mathbb{Z}_4[x]$.

If (4) holds over $\mathbb{Z}_4$, then it is equivalent to

$$\bar f\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^*h^* = \mu(x^\beta - 1) \in \mathbb{Z}_2[x].$$

It is easy to prove that $\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^*h^*$ divides $(x^\beta - 1)$ in $\mathbb{Z}_2[x]$. By Corollary 11, $\deg(\bar f) = \beta - \deg(f) - \deg(h) + \deg(\gcd(b,\ell)) - \deg(\gcd(b,\ell g))$, so

$$\beta = \deg\left(\bar f\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}\right) f^*h^*\right) = \deg(x^\beta - 1).$$

Hence, we obtain that $\mu = 1$ and

$$\bar f = \frac{(x^\beta - 1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^* f^*h^*} \in \mathbb{Z}_2[x]. \tag{5}$$

Since β is odd and by the uniqueness of the Hensel lift [9, p.73] then $\bar f$ is the unique monic polynomial in $\mathbb{Z}_4[x]$ dividing $(x^\beta - 1)$ and holding (5). ■

Lemma 16: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh = x^\beta - 1$. Then, the Hensel lift of $\frac{b}{\gcd(b,\ell g)}$ divides h.

Proof: In general, if $a \mid b \mid x^\beta - 1$ over $\mathbb{Z}_2[x]$ with β odd, then the Hensel lift of a divides the Hensel lift of b that divides $x^\beta - 1$ over $\mathbb{Z}_4[x]$. Then, by Corollary 2, the result follows. ■

In the family of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes there is a particular class when the polynomials b and $\gcd(b,\ell g)$ are the same. Applying Lemma 3 to this class we obtain that $\mathcal{C}_b$ has only two generators, $\langle (b \mid 0), (0 \mid 2f)\rangle$, instead of three, $\langle (b \mid 0), (\ell g \mid 2fg), (0 \mid 2fh)\rangle$. So, we have to take care of this class of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

Proposition 17: Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f)\rangle$ be a non-separable $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh = x^\beta - 1$, and with dual code $\mathcal{C}^\perp = \langle (\bar b \mid 0), (\bar\ell \mid \bar f\bar h + 2\bar f)\rangle$, where $\bar f\bar g\bar h = x^\beta - 1$. Let $\rho = \frac{\ell}{\gcd(b,\ell)}$. Then,

$$\bar\ell = \frac{x^\alpha - 1}{b^*}\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}x^{\mathfrak{m}-\deg(f)}\mu_1 \right.\\ \left. + \frac{b^*}{\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)}\mu_2\right),$$

where

$$\begin{cases} \mu_1 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell g)^*}\right), \\ \mu_2 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{b^*}{\gcd(b,\ell)^*}\right). \end{cases}$$

Proof: In order to calculate $\bar\ell$, by using $\circ$, we are going to operate $(\bar\ell \mid \bar f\bar h + 2\bar f)$ by three different codewords of $\mathcal{C}$. The result of these operations is 0 modulo $x^{\mathfrak{m}} - 1$.

First, consider $(\bar\ell \mid \bar f\bar h + 2\bar f) \circ (b \mid 0) = 0$. By Lemma 10, $\bar\ell b^* \equiv 0 \pmod{(x^\alpha - 1)}$ and, for some $\lambda \in \mathbb{Z}_2[x]$, we have that $\bar\ell = \frac{x^\alpha - 1}{b^*}\lambda$.

Second, consider $\tau = \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}$ and compute $(\bar\ell \mid \bar f\bar h + 2\bar f) \circ (\tau\ell \mid \tau fh + 2\tau f)$. Let $t = \deg(\tau)$ and note that $(fh + 2f)^* = f^*h^* + 2x^{\deg(h)}f^*$. We obtain that

$$\begin{aligned} 0 &= (\bar\ell \mid \bar f\bar h + 2\bar f) \circ (\tau\ell \mid \tau fh + 2\tau f) \\ &= 2\bar\ell\theta_{\frac{\mathfrak{m}}{\alpha}}(x^\alpha)x^{\mathfrak{m}-\deg(\ell)-1-t}\tau^*\ell^* \\ &\quad + \bar f\bar h\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-\deg(fh)-1-t}\tau^*f^*h^* \\ &\quad + 2\bar f\bar h\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-\deg(f)-1-t}\tau^*f^* \\ &\quad + 2\bar f\theta_{\frac{\mathfrak{m}}{\beta}}(x^\beta)x^{\mathfrak{m}-\deg(fh)-1-t}\tau^*f^*h^* \mod (x^{\mathfrak{m}} - 1). \end{aligned} \tag{6}$$

Apply Proposition 7 to each addend and $\bar\ell = \frac{x^\alpha - 1}{b^*}\lambda$. In the second addend, by Proposition 14, we may replace $\bar f\bar h$ by the Hensel lift of $\frac{(x^\beta - 1)\gcd(b,\ell g)^*}{f^*b^*}$. The Hensel lift of $(x^\beta - 1)$ and f^* (mod 2) are the same polynomials $(x^\beta - 1)$ and f^*. Moreover, by Lemma 16, the second addend is 0 modulo $(x^{\mathfrak{m}} - 1)$. Therefore, by Proposition 14 and Proposition 15, we get that

$$\begin{aligned} 0 &= (\bar\ell \mid \bar f\bar h + 2\bar f) \circ (\tau\ell \mid \tau fh + 2\tau f) \\ &= 2\frac{(x^{\mathfrak{m}} - 1)}{b^*}\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\tau^*\ell^* \\ &\quad + 2\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell)^*}{f^*h^*\gcd(b,\ell g)^*}x^{\mathfrak{m}-\deg(fh)-1-t}\tau^*f^*h^* \\ &\quad + 2\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell g)^*}{f^*b^*}x^{\mathfrak{m}-\deg(f)-1-t}\tau^*f^* \\ &\quad \mod (x^{\mathfrak{m}} - 1). \end{aligned} \tag{7}$$

Clearly, the second addend is 0 modulo $(x^{\mathfrak{m}} - 1)$. Since $\tau = \frac{\gcd(b,\ell g)}{\gcd(b,\ell)}$, we have that $(\bar\ell \mid \bar f\bar h + 2\bar f) \circ (\tau\ell \mid \tau fh + 2\tau f)$ is equal to

$$2\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell g)^*}{b^*}\left(\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\rho^* + x^{\mathfrak{m}-\deg(f)-1-t}\tau^*\right) \\ \equiv 0 \pmod{(x^{\mathfrak{m}} - 1)}. \tag{8}$$

This is equivalent, over $\mathbb{Z}_2$, to

$$\frac{(x^{\mathfrak{m}} - 1)\gcd(b,\ell g)^*}{b^*}\left(\lambda x^{\mathfrak{m}-\deg(\ell)-1-t}\rho^* + x^{\mathfrak{m}-\deg(f)-1-t}\tau^*\right) \\ \equiv 0 \pmod{(x^{\mathfrak{m}} - 1)}.$$

Then,

$$\begin{aligned}&\left(\lambda x^{\mathrm{m}-\deg(\ell)-1-t}\rho^* + x^{\mathrm{m}-\deg(f)-1-t}\tau^*\right)\\ &\qquad\equiv 0 \quad (\mathrm{mod}\ (x^{\mathrm{m}}-1)),\end{aligned} \tag{9}$$

or

$$\begin{aligned}&\left(\lambda x^{\mathrm{m}-\deg(\ell)-1-t}\rho^* + x^{\mathrm{m}-\deg(f)-1-t}\tau^*\right)\\ &\qquad\equiv 0 \quad \left(\mathrm{mod}\ \left(\frac{b^*}{\gcd(b,\ell g)^*}\right)\right).\end{aligned} \tag{10}$$

Since $(\frac{b^*}{\gcd(b,\ell g)^*})$ divides $(x^{\mathrm{m}}-1)$, then (9) implies (10).

The greatest common divisor between ρ and $\left(\frac{b}{\gcd(b,\ell g)}\right)$ is 1, then ρ^* is invertible modulo $\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$. Thus,

$$\lambda = \tau^* x^{\mathrm{m}-\deg(f)+\deg(\ell)}(\rho^*)^{-1} \quad \mathrm{mod}\ \left(\frac{b^*}{\gcd(b,\ell g)^*}\right).$$

Let $\lambda_1 = \tau^* x^{\mathrm{m}-\deg(f)+\deg(\ell)}(\rho^*)^{-1}$ mod $\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$. Then $\lambda = \lambda_1 + \lambda_2$ with $\lambda_2 \equiv 0$ (mod $\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$).

Finally, we compute $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh + 2f)$.

$$\begin{aligned}0 &= (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh + 2f)\\ &= 2\bar{\ell}\theta_{\frac{\mathrm{m}}{\alpha}}(x^{\alpha})x^{\mathrm{m}-\deg(\ell)-1}\ell^*\\ &\quad + \bar{f}\bar{h}\theta_{\frac{\mathrm{m}}{\beta}}(x^{\beta})x^{\mathrm{m}-\deg(fh)-1}f^*h^*\\ &\quad + 2\bar{f}\bar{h}\theta_{\frac{\mathrm{m}}{\beta}}(x^{\beta})x^{\mathrm{m}-\deg(f)-1}f^*\\ &\quad + 2\bar{f}\theta_{\frac{\mathrm{m}}{\beta}}(x^{\beta})x^{\mathrm{m}-\deg(fh)-1}f^*h^* \quad \mathrm{mod}\ (x^{\mathrm{m}}-1).\end{aligned} \tag{11}$$

Apply Proposition 7 to each addend. By Lemma 16 and replacing $\bar{f}\bar{h}$ by the Hensel lift of $\frac{(x^{\beta}-1)\gcd(b,\ell g)^*}{f^*b^*}$, then the second addend is 0 mod $(x^{\mathrm{m}}-1)$ and, by Proposition 14 and Proposition 15, $(\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \circ (\ell \mid fh+2f)$ is equal to

$$\begin{aligned}&2\frac{(x^{\mathrm{m}}-1)}{b^*}(\lambda_1+\lambda_2)x^{\mathrm{m}-\deg(\ell)-1}\ell^*\\ &\quad + 2\frac{(x^{\mathrm{m}}-1)\gcd(b,\ell g)^*}{b^*}x^{\mathrm{m}-\deg(f)-1}\\ &\quad + 2\frac{(x^{\mathrm{m}}-1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^*}x^{\mathrm{m}-\deg(fh)-1} \equiv 0 \ \ (\mathrm{mod}\ (x^{\mathrm{m}}-1)).\end{aligned}$$

Since $\lambda_1 = \tau^* x^{\mathrm{m}-\deg(f)+\deg(\ell)}(\rho^*)^{-1}$ mod $\left(\frac{b^*}{\gcd(b,\ell g)^*}\right)$, we have that

$$\begin{aligned}&2\frac{(x^{\mathrm{m}}-1)}{b^*}\lambda_1 x^{\mathrm{m}-\deg(\ell)-1}\ell^*\\ &\quad + 2\frac{(x^{\mathrm{m}}-1)\gcd(b,\ell g)^*}{b^*}x^{\mathrm{m}-\deg(f)-1} \equiv 0 \ \ (\mathrm{mod}\ (x^{\mathrm{m}}-1)).\end{aligned}$$

Therefore, we obtain that

$$\begin{aligned}&2\frac{(x^{\mathrm{m}}-1)}{b^*}\lambda_2 x^{\mathrm{m}-\deg(\ell)-1}\ell^*\\ &\quad + 2\frac{(x^{\mathrm{m}}-1)\gcd(b,\ell)^*}{\gcd(b,\ell g)^*}x^{\mathrm{m}-\deg(fh)-1} \equiv 0 \ \ (\mathrm{mod}\ (x^{\mathrm{m}}-1)),\end{aligned}$$

and then

$$\begin{aligned}&2\frac{(x^{\mathrm{m}}-1)\gcd(b,\ell)^*}{b^*}\\ &\times\left(\lambda_2 x^{\mathrm{m}-\deg(\ell)-1}\rho^*\frac{b^*}{\gcd(b,\ell g)^*}x^{\mathrm{m}-\deg(fh)-1}\right)\\ &\quad\equiv 0 \quad (\mathrm{mod}\ (x^{\mathrm{m}}-1)).\end{aligned}$$

Arguing similar to the calculation of λ in (8), we obtain that

$$\begin{aligned}\lambda_2 = {}&\frac{b^*}{\gcd(b,\ell g)^*}x^{\mathrm{m}-\deg(fh)+\deg(\ell)}(\rho^*)^{-1}\\ &\mathrm{mod}\ \left(\frac{b^*}{\gcd(b,\ell)^*}\right).\end{aligned}$$

Now, considering the values of λ_1 and λ_2 and defining properly μ_1 and μ_2 we obtain the expected result. ■

We summarize the previous results in the next theorem.

Theorem 18: Let $\mathcal{C} = \langle(b \mid 0), (\ell \mid fh+2f)\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha,\beta;\gamma,\delta;\kappa)$, where $fgh = x^{\beta}-1$, and with dual code $\mathcal{C}^{\perp} = \langle(\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h}+2\bar{f})\rangle$, where $\bar{f}\bar{g}\bar{h} = x^{\beta}-1$. Let $\rho = \frac{\ell}{\gcd(b,\ell)}$. Then,

1) $\bar{b} = \frac{x^{\alpha}-1}{(gcd(b,\ell))^*} \in \mathbb{Z}_2[x]$,

2) $\bar{f}\bar{h}$ is the Hensel lift of the polynomial $\frac{(x^{\beta}-1)\gcd(b,\ell g)^*}{f^*b^*} \in \mathbb{Z}_2[x]$.

3) $\bar{f}$ is the Hensel lift of the polynomial $\frac{(x^{\beta}-1)\gcd(b,\ell)^*}{f^*h^*\gcd(b,\ell g)^*} \in \mathbb{Z}_2[x]$.

4)
$$\begin{aligned}\bar{\ell} = \frac{x^{\alpha}-1}{b^*}&\left(\frac{\gcd(b,\ell g)^*}{\gcd(b,\ell)^*}x^{\mathrm{m}-\deg(f)}\mu_1\right.\\ &\left.+\frac{b^*}{\gcd(b,\ell g)^*}x^{\mathrm{m}-\deg(fh)}\mu_2\right) \in \mathbb{Z}_2[x],\end{aligned}$$

where

$$\begin{cases}\mu_1 = x^{\deg(\ell)}(\rho^*)^{-1} \quad \mathrm{mod}\ \left(\frac{b^*}{\gcd(b,\ell g)^*}\right),\\ \mu_2 = x^{\deg(\ell)}(\rho^*)^{-1} \quad \mathrm{mod}\ \left(\frac{b^*}{\gcd(b,\ell)^*}\right).\end{cases}$$

Note that from Theorem 18 and Theorem 4 one can easily compute the minimal spanning set of the dual code $\mathcal{C}^{\perp}$ as a $\mathbb{Z}_4$-module, and use the encoding method for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes described in [1].

III. Examples

As a simple example, consider the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code $\mathcal{C}_1 = \langle(x-1 \mid (x^2+x+1)+2)\rangle$ of type $(3,3;2,1;2)$. We have that $b = x^3-1$, $\ell = (x-1)$, $f = 1$ and $h = x^2+x+1$.

The generator matrix ([4]) is

$$G = \left(\begin{array}{c|c}101 & 200\\ 011 & 220\\ \hline 000 & 111\end{array}\right).$$

Then, applying the formulas of Theorem 18 we have $\bar{b} = x^2+x+1$, $\bar{\ell} = x$, $\bar{f}\bar{h} = x-1$, and $\bar{f} = x-1$. Therefore, $\mathcal{C}_1^{\perp} = \langle(x^2+x+1 \mid 0), (x \mid (x-1)+2(x-1))\rangle$, is of type $(3,3;1,2;1)$ and has generator matrix

$$H = \left(\begin{array}{c|c}111 & 000\\ \hline 100 & 310\\ 001 & 301\end{array}\right).$$

In order to determine some cyclic codes with good parameters, we will consider some optimal codes with respect to the minimum distance. Applying the classical Singleton bound [8] to a $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and minimum distance d, the following bound is obtained:

$$\frac{d-1}{2} \leq \frac{\alpha}{2} + \beta - \frac{\gamma}{2} - \delta. \qquad (12)$$

According to [2], a code meeting the bound (12) is called maximum distance separable with respect to the Singleton bound, briefly MDSS.

By [1, Th. 19] it is known that $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh + 2f) \rangle$ with $b = x-1$, $\ell = 1$ and $f = h = 1$ is an MDSS code of type $(\alpha, \beta; \alpha-1, \beta; \alpha-1)$. Applying Theorem 18 to compute the dual code of $\mathcal{C}$ one obtain that $\mathcal{C}^{\perp} = \langle (\bar{b} \mid 0), (\bar{\ell} \mid \bar{f}\bar{h} + 2\bar{f}) \rangle$ with $\bar{b} = x^{\alpha} - 1$, $\bar{\ell} = \theta_{\alpha}(x)$, $\bar{f} = \theta_{\beta}(x)$ and $\bar{h} = x - 1$, which is also an MDSS code. In fact, the binary image of $\mathcal{C}$ is the set of all even weight vectors and the binary image of $\mathcal{C}^{\perp}$ is the repetition code. Moreover, these are the only MDSS $\mathbb{Z}_2\mathbb{Z}_4$-additive codes with more than one codeword and minimum distance $d > 1$, as can be seen in [2].

Finally, we are going to see a pair of examples of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, giving the generators and type of these codes.

Generators	Type
$b = x^{10}+x^8+x^7+x^3+x+1, \ell = x^6+x^4+x+1, fh = y^4+2y^3+3y^2+y+1, f = 1$	(14, 7; 8, 3; 7)
$b = x^5+1, \ell = 0, fh = y^5-1, f = 1$	(10, 5; 10, 0; 5)

The second code in the table belongs to an infinite family of self-dual $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes that was given in [3, Th. 4].

Proposition 19: Let α be even and β odd. Let $\mathcal{C} = \langle (b \mid 0), (\ell \mid fh+2f) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $b = x^{\frac{\alpha}{2}} - 1$, $\ell = 0$, $h = x^{\beta} - 1$ and $f = 1$. Then $\mathcal{C}$ is a self-dual code of type $(\alpha, \beta; \beta + \frac{\alpha}{2}, 0; \frac{\alpha}{2})$.

Proof: By Theorem 18, one obtains that $\bar{b} = x^{\frac{\alpha}{2}} - 1$, $\bar{\ell} = 0$, $\bar{h} = x^{\beta} - 1$ and $\bar{f} = 1$. Hence $\mathcal{C}$ is self-dual and, by Theorem 5, it is of type $(\alpha, \beta; \beta + \frac{\alpha}{2}, 0; \frac{\alpha}{2})$. ■

References

[1] T. Abualrub, I. Siap, and N. Aydin, "$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 3, pp. 1508–1514, Mar. 2014.

[2] M. Bilal, J. Borges, S. T. Dougherty, and C. F. Córdoba, "Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$," *Designs Codes Cryptogr.*, vol. 61, no. 3, pp. 31–40, Oct. 2011.

[3] J. Borges, S. T. Dougherty, and C. F. Córdoba, "Characterization and constructions of self-dual codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$," *Adv. Math. Commun.*, vol. 6, no. 3, pp. 287–303, Aug. 2012.

[4] J. Borges, C. F. Córdoba, J. Pujol, J. Rifà, and M. Villanueva, "$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator matrices and duality," *Designs, Codes Cryptogr.*, vol. 54, no. 2, pp. 167–179, Feb. 2010.

[5] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Rep. Suppl.*, vol. 10, pp. 1–97 Jan. 1973.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory Error-Correcting Codes*. Amsterdam, The Netherlands: Oxford Univ. Press, 1975.

[7] V. S. Pless and Z. Qian, "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$," *IEEE Trans. Inf. Theory*, vol. 42, no. 5, pp. 1594–1600, Sep. 1996.

[8] R. C. R. C. Singleton, "Maximum distance q-nary codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 2, pp. 116–118, Apr. 1964.

[9] Z. Wan, *Quaternary Codes*. Singapore: World Scientific, 1997.

Joaquim Borges was born in Lleida, Catalonia, Spain, in October 1965. He received the graduate degree in Sciences (Computer Science Section) in 1988 from the Universitat Autònoma de Barcelona, Spain, and the Ph.D. degree in Computer Science Engineering in 1998 from the same university.

Since 1988, he has been with the Computer Science Department first, and from 2005 with the Information and Communications Engineering Department, at the Universitat Autònoma de Barcelona, where he is currently Associate Professor. His research interests include subjects related to Combinatorics, Coding Theory and Graph Theory.

Cristina Fernández-Córdoba was born in Sabadell, Catalonia (Spain) in December 1977. She received her Bachelor's degree in Mathematics in 2000 from the Universitat Autònoma de Barcelona and the Ph.D. degree in Science (Computer Science Section) in 2005 from the same university. In 2000 she joined the Department of Computer Science at the Universitat Autònoma de Barcelona, and in 2005 the Department of Information and Communications Engineering at the same university. In 2008, she joined the Fundación Española para la Ciencia y la Tecnología and she did a one year research stay at Auburn University under a Fulbright grant. From 2009, she is within the Department of Information and Communications Engineering at the Universitat Autònoma de Barcelona where currently is an Associate Professor. Her research interests include subjects related to combinatorics, coding theory and graph theory.

Roger Ten-Valls was born in Barcelona, Catalonia (Spain) in June 1987. He received the B.Sc. degree in mathematics in 2011 from the Universitat Autònoma de Barcelona and the M.Sc. in mathematics in 2013 from Universitat Politècnica de Catalunya. He is currenty working toward the Ph.D. at the Department of Information and Communications Engineering at the Universitat Autònoma de Barcelona. His research interests include coding theory, combinatorics and abstract algebra.

Appendix C

$\mathbb{Z}_2$-double cyclic codes

Des. Codes Cryptogr.
DOI 10.1007/s10623-017-0334-8

$\mathbb{Z}_2$-double cyclic codes

Joaquim Borges[1] · **Cristina Fernández-Córdoba**[1] · **Roger Ten-Valls**[1]

Received: 9 November 2015 / Revised: 13 January 2017 / Accepted: 19 January 2017

Abstract A binary linear code C is a $\mathbb{Z}_2$-double cyclic code if the set of coordinates can be partitioned into two subsets such that any cyclic shift of the coordinates of both subsets leaves invariant the code. These codes can be identified as submodules of the $\mathbb{Z}_2[x]$-module $\mathbb{Z}_2[x]/(x^r-1) \times \mathbb{Z}_2[x]/(x^s-1)$. We determine the structure of $\mathbb{Z}_2$-double cyclic codes giving the generator polynomials of these codes. We give the polynomial representation of $\mathbb{Z}_2$-double cyclic codes and its duals, and the relations between the generator polynomials of these codes. Finally, we study the relations between $\mathbb{Z}_2$-double cyclic and other families of cyclic codes, and show some examples of distance optimal $\mathbb{Z}_2$-double cyclic codes.

Keywords Binary linear codes · Duality · $\mathbb{Z}_2$-double cyclic codes

Mathematics Subject Classification 94B60 · 94B25

1 Introduction

Let $\mathbb{Z}_2$ be the ring of integers modulo 2. Let $\mathbb{Z}_2^n$ denote the set of all binary vectors of length n. A non-empty subset of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code*. In this paper we introduce a subfamily of binary linear codes, called $\mathbb{Z}_2$*-double cyclic codes*, with the property that the set of coordinates can be partitioned into two subsets, the

Communicated by J. Wolfmann.

✉ Roger Ten-Valls
rten@deic.uab.cat

Joaquim Borges
jborges@deic.uab.cat

Cristina Fernández-Córdoba
cfernandez@deic.uab.cat

[1] Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193 Cerdanyola del Vallès, Spain

Published online: 10 February 2017

first r coordinates and the last s coordinates, such that any cyclic shift of the coordinates of both subsets of a codeword is also a codeword.

Note that if one of these sets of coordinates is empty, for example $r = 0$, then we obtain a binary cyclic code of length s. Therefore, binary cyclic codes are a special class of $\mathbb{Z}_2$-double cyclic codes. Another special case is when $r = s$, where a $\mathbb{Z}_2$-double cyclic code is permutation equivalent to a quasi-cyclic code of index 2 and even length. Theory of binary cyclic codes and quasi-cyclic codes of index 2 can be found in [11].

Recently, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been studied (see [4,7]). For $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, the set of coordinates is partitioned into two subsets, the first one of binary coordinates and the second one of quaternary coordinates. The simultaneous cyclic shift of the subsets of coordinates of a codeword has been defined in [1], where the authors study $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and identify these codes as $\mathbb{Z}_4[x]$-modules of a certain ring. Furthermore $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes and $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive cyclic and constacylic codes have been studied in [2] and [3] respectively, where these codes are another special classes of mixed type codes.

Since [9], a lot of variants of linear and cyclic codes over different rings are studied. Obviously, these codes have a theoretical interest, from a mathematical point of view, since they are related to algebraic structures such as rings, ideals or modules. But the interest for such codes is not purely mathematical because some of them have binary images with better parameters than classical binary linear codes. Here, we present a new variant of cyclic codes, the $\mathbb{Z}_2$-double cyclic codes, closely related to generalized quasi-cyclic codes of index 2 [13]. We give examples of $\mathbb{Z}_2$-double cyclic codes that are optimal with respect to the minimum distance. The aim of this paper is to study the algebraic structure of $\mathbb{Z}_2$-double cyclic codes and their dual codes. The paper is organized as follows. In Sect. 2, we give the definition of $\mathbb{Z}_2$-double cyclic codes, we find the relation between some canonical projections of these codes and binary cyclic codes. Also we present the $\mathbb{Z}_2[x]$-module $\mathbb{Z}_2[x]/(x^r-1)\times\mathbb{Z}_2[x]/(x^s-1)$, denoted by $R_{r,s}$. In Sect. 3, we determine the algebraic structure of a $\mathbb{Z}_2$-double cyclic code and we state some relations between its generators. In Sect. 4, we study the concept of duality and, for a $\mathbb{Z}_2$-double cyclic code, we determine the generators of the dual code in terms of the generators of the code. In Sect. 5, we study the relations between $\mathbb{Z}_2$-double cyclic codes and other families of cyclic codes such as $\mathbb{Z}_4$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Finally, in Sect. 6 we give tables with the generator polynomials of some specific $\mathbb{Z}_2$-double cyclic codes and their dual codes. In some cases, the codes are optimal with respect to the minimum distance. We also give examples of $\mathbb{Z}_2$-double cyclic codes obtained from $\mathbb{Z}_4$-cyclic and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

2 $\mathbb{Z}_2$-double cyclic codes

Let C be a binary code of length n. Let r and s be non-negative integers such that $n = r + s$. We consider a partition of the set of the n coordinates into two subsets of r and s coordinates respectively, so that C is a subset of $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$.

Definition 1 Let C be a binary linear code of length $n = r + s$. The code C is called $\mathbb{Z}_2$*-double cyclic* if

$$(u_0, u_1, \dots, u_{r-2}, u_{r-1} \mid u'_0, u'_1, \dots, u'_{s-2}, u'_{s-1}) \in C$$

implies

$$(u_{r-1}, u_0, u_1, \dots, u_{r-2} \mid u'_{s-1}, u'_0, u'_1, \dots, u'_{s-2}) \in C.$$

Let $\mathbf{u} = (u_0, u_1, \dots, u_{r-1} \mid u'_0, \dots, u'_{s-1})$ be a codeword in C and let i be an integer. We denote by

$$\mathbf{u}^{(i)} = (u_{0-i}, u_{1-i}, \dots, u_{r-1-i} \mid u'_{0-i}, \dots, u'_{s-1-i}) \tag{1}$$

the ith shift of $\mathbf{u}$, where the subscripts are read modulo r and s, respectively. Note that $\mathbf{u}^{(-1)} = \mathbf{u}^{(lcm(r,s)-1)}$ and, in fact, $\mathbf{u}^{(i)} = \mathbf{u}^{(lcm(r,s)+i)}$, for $i \in \mathbb{Z}$.

Let $C \subseteq \mathbb{Z}_2^r \times \mathbb{Z}_2^s$ be a $\mathbb{Z}_2$-double cyclic code. Let C_r be the canonical projection of C on the first r coordinates and C_s on the last s coordinates. Note that C_r and C_s are binary cyclic codes of length r and s, respectively. The code C is called *separable* if it is the direct product of C_r and C_s.

There is a bijective map between $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ and $\mathbb{Z}_2[x]/(x^r - 1) \times \mathbb{Z}_2[x]/(x^s - 1)$ given by:

$$(u_0, u_1, \dots, u_{r-1} \mid u'_0, \dots, u'_{s-1}) \mapsto (u_0 + u_1 x + \cdots + u_{r-1}x^{r-1} \mid u'_0 + \cdots + u'_{s-1}x^{s-1}).$$

We denote the image of the vector $\mathbf{u}$ by $\mathbf{u}(x)$.

Definition 2 Denote the ring $\mathbb{Z}_2[x]/(x^r - 1) \times \mathbb{Z}_2[x]/(x^s - 1)$ by $R_{r,s}$. We define the operation

$$\star : \mathbb{Z}_2[x] \times R_{r,s} \to R_{r,s}$$

as

$$\lambda(x) \star (p(x) \mid q(x)) = (\lambda(x)p(x) \mid \lambda(x)q(x)),$$

where $\lambda(x) \in \mathbb{Z}_2[x]$ and $(p(x) \mid q(x)) \in R_{r,s}$.

The ring $R_{r,s}$ with the external operation $\star$ is a $\mathbb{Z}_2[x]$-module. Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ be an element of $R_{r,s}$. Note that if we operate $\mathbf{u}(x)$ by x we get

$$\begin{aligned}
x \star \mathbf{u}(x) &= x \star (u(x) \mid u'(x)) \\
&= x \star (u_0 + \cdots + u_{r-2}x^{r-2} + u_{r-1}x^{r-1} \mid u'_0 + \cdots + u'_{s-2}x^{s-2} + u'_{s-1}x^{s-1}) \\
&= (u_0 x + \cdots + u_{r-2}x^{r-1} + u_{r-1}x^{r} \mid u'_0 x + \cdots + u'_{s-2}x^{s-1} + u'_{s-1}x^{s}) \\
&= (u_{r-1} + u_0 x + \cdots + u_{r-2}x^{r-1} \mid u'_{s-1} + u'_0 x + \cdots + u'_{s-2}x^{s-1}).
\end{aligned}$$

Hence, $x \star \mathbf{u}(x)$ is the image of the vector $\mathbf{u}^{(1)}$. Thus, the operation of $\mathbf{u}(x)$ by x in $R_{r,s}$ corresponds to a shift of $\mathbf{u}$. In general, $x^i \star \mathbf{u}(x) = \mathbf{u}^{(i)}(x)$ for all i.

3 Algebraic structure and generators

In this section, we shall study submodules of $R_{r,s}$. We describe the generators of such submodules and state some properties. From now on, $\langle S \rangle$ will denote the submodule generated by a subset S of $R_{r,s}$. Let $\pi_r : R_{r,s} \to \mathbb{Z}_2[x]/(x^r - 1)$ and $\pi_s : R_{r,s} \to \mathbb{Z}_2[x]/(x^s - 1)$ be the canonical projections, and let N be a submodule of $R_{r,s}$. If $\pi_r(N) = \{0\}$ (resp. $\pi_s(N) = \{0\}$) then we may consider that the generator polynomial of $\pi_r(N)$ (resp. $\pi_s(N)$) is $x^r - 1$ (resp. $x^s - 1$). Define $N' = \{(p(x)|q(x)) \in N \mid q(x) = 0\}$. It is easy to check that $N' \cong \pi_r(N')$ by considering the map $(p(x) \mid 0) \mapsto p(x)$.

Theorem 1 *The $\mathbb{Z}_2[x]$-module $R_{r,s}$ is a noetherian $\mathbb{Z}_2[x]$-module, and every submodule N of $R_{r,s}$ can be written as*

$$N = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle,$$

where $b(x), \ell(x) \in \mathbb{Z}_2[x]/(x^r - 1)$ with $b(x) \mid (x^r - 1)$, and $a(x) \in \mathbb{Z}_2[x]/(x^s - 1)$ with $a(x) \mid (x^s - 1)$.

Proof By using the fact that $\mathbb{Z}_2[x]/(x^r - 1)$ and $\mathbb{Z}_2[x]/(x^s - 1)$ are principal ideal rings, we have that $N_s = \pi_s(N)$ and $\pi_r(N')$ are finitely generated. Moreover, since $N' \cong \pi_r(N')$, it follows that N' is finitely generated.

The generators of $\pi_r(N')$ may not be unique. Consider $b(x)$ the generator of $\pi_r(N')$ satisfying $b(x) \mid (x^r - 1)$. Then $(b(x) \mid 0)$ is a generator of N'. Similarly, consider $a(x) \in N_s$ such that $N_s = \langle a(x) \rangle$ and $a(x) \mid (x^s - 1)$. Then there exists $\ell(x) \in \mathbb{Z}_2[x]/(x^r - 1)$ such that $(\ell(x) \mid a(x)) \in N$.

We claim that

$$N = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle.$$

Let $(p(x) \mid q(x)) \in N$. We shall prove that $(p(x) \mid q(x))$ is generated by $(b(x) \mid 0)$ and $(\ell(x) \mid a(x))$. First, since $q(x) = \pi_s(p(x) \mid q(x)) \in N_s$ and $N_s = \langle a(x) \rangle$, there exists $\lambda(x) \in \mathbb{Z}_2[x]$ such that $q(x) = \lambda(x)a(x)$. Moreover,

$$(p(x) \mid q(x)) - \lambda(x) \star (\ell(x) \mid a(x)) = (p(x) - \lambda(x)\ell(x) \mid 0) \in N',$$

that is generated by $(b(x) \mid 0)$. Then, there exists $\mu(x) \in \mathbb{Z}_2[x]$ such that $(p(x) - \lambda(x)\ell(x) \mid 0) = \mu(x) \star (b(x) \mid 0)$. Thus,

$$(p(x) \mid q(x)) = \mu(x) \star (b(x) \mid 0) + \lambda(x) \star (\ell(x) \mid a(x)).$$

Therefore, N is finitely generated by $(b(x) \mid 0)$ and $(\ell(x) \mid a(x))$, and then $R_{r,s}$ is a noetherian $\mathbb{Z}_2[x]$-module. □

From the previous result, it is clear that we can identify $\mathbb{Z}_2$-double cyclic codes in $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ as submodules of $R_{r,s}$. Hence, any submodule of $R_{r,s}$ is a $\mathbb{Z}_2$-double cyclic code. From now on, we will denote by C indistinctly both the code and the corresponding submodule.

Note that if $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ is a $\mathbb{Z}_2$-double cyclic code, then the canonical projections C_r and C_s are binary cyclic codes generated by $\gcd(b(x), \ell(x))$ and $a(x)$, respectively. Moreover, the generator polynomials of C_r, C_s and C may not be unique. In the following proposition we give some conditions to the generator polynomials of a $\mathbb{Z}_2$-double cyclic code.

Proposition 1 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code. Then, we can assume that*

1. $C_s = \langle a(x) \rangle$, *with* $a(x) | (x^s - 1)$,
2. $\pi_r(C') = \langle b(x) \rangle$, *with* $b(x) | (x^r - 1)$,
3. $\deg(\ell(x)) < \deg(b(x))$.

Proof The conditions for $a(x)$ and $b(x)$ follow from the proof of Theorem 1. Now, suppose that $\deg(\ell(x)) \geq \deg(b(x))$. Let $i = \deg(\ell(x)) - \deg(b(x))$ and let $C_1 = \langle (b(x) \mid 0), (\ell(x) + x^i \star b(x) \mid a(x)) \rangle$.

On the one hand, $\deg(\ell(x) + x^i \star b(x)) < \deg(\ell(x))$ and since the generators of C_1 belong to C, we have that $C_1 \subseteq C$. On the other hand,

$$(\ell(x) \mid a(x)) = (\ell(x) + x^i \star b(x) \mid a(x)) + x^i \star (b(x) \mid 0).$$

Then, $\langle(\ell(x) \mid a(x))\rangle \subseteq C_1$ and hence $C \subseteq C_1$. It follows that $C = C_1$, which implies that we may consider $\deg(\ell(x)) < \deg(b(x))$. □

Example 1 Consider the code C_1 generated by $\langle(x^2 + x + 1 \mid 0), (x + 1 \mid x^4 + x^3 + x^2 + x + 1)\rangle \subseteq R_{3,5}$. Since $(x + 1) \star (x + 1 \mid x^4 + x^3 + x^2 + x + 1) = (x^2 + 1 \mid 0)$ and $(x^2 + x + 1 \mid 0)$ belong to C_1, it is easy to see that $\pi_r(C_1) = \langle 1\rangle$. Clearly, the generators of C_1 are not as in Proposition 1 since $\langle x^2 + x + 1\rangle \neq \pi_r(C_1)$. Thus, we may consider $C_1 = \langle(1 \mid 0), (0 \mid x^4 + x^3 + x^2 + x + 1)\rangle$, and these polynomials satisfy the conditions of Proposition 1.

Proposition 2 *Let $C = \langle(b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, $b(x) \mid \frac{x^s-1}{a(x)}\ell(x)$.*

Proof By Proposition 1, $N' = \langle(b(x) \mid 0)\rangle$. We have that $\frac{x^s-1}{a(x)} \star (\ell(x) \mid a(x)) \in N'$ and, therefore, $\frac{x^s-1}{a(x)}\ell(x) \in \langle b(x)\rangle$ and $b(x) \mid \frac{x^s-1}{a(x)}\ell(x)$. □

Corollary 1 *Let $C = \langle(b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, $b(x) \mid \frac{x^s-1}{a(x)} \gcd(b(x), \ell(x))$.*

We have seen that $R_{r,s}$ is a $\mathbb{Z}_2[x]$-module, and the product by $x \in \mathbb{Z}_2[x]$ is equivalent to the double right shift on the vector space $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$. Moreover, we have that $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ is a $\mathbb{Z}_2$-module, where the operations are addition and multiplication by elements of $\mathbb{Z}_2$. Our goal now is to find a set of generators for C as a $\mathbb{Z}_2$-module.

Proposition 3 *Let $C = \langle(b(x) \mid 0), (\ell(x) \mid a(x))\rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Define the sets*

$$S_1 = \{(b(x) \mid 0), x \star (b(x) \mid 0), \ldots, x^{r-\deg(b(x))-1} \star (b(x) \mid 0)\},$$
$$S_2 = \{(\ell(x) \mid a(x)), x \star (\ell(x) \mid a(x)), \ldots, x^{s-\deg(a(x))-1} \star (\ell(x) \mid a(x))\}.$$

Then, $S_1 \cup S_2$ forms a minimal generating set for C as a $\mathbb{Z}_2$-module.

Proof It is easy to check that the codewords of $S_1 \cup S_2$ are linearly independent.

Let $c(x) = p_1(x) \star (b(x) \mid 0) + p_2(x) \star (\ell(x) \mid a(x)) \in C$. We have to check that $c(x) \in \langle S_1 \cup S_2\rangle$.

If $\deg(p_1(x)) \leq r - \deg(b(x)) - 1$, then $p_1(x) \star (b(x) \mid 0) \in \langle S_1\rangle$. Otherwise, using the division algorithm, we compute $p_1(x) = q_1(x)\frac{x^r-1}{b(x)} + r_1(x)$ with $\deg(r_1(x)) \leq r - \deg(b(x)) - 1$, hence

$$p_1(x) \star (b(x) \mid 0) = \left(q_1(x)\frac{x^r - 1}{b(x)} + r_1(x)\right) \star (b(x) \mid 0) = r_1(x) \star (b(x) \mid 0) \in \langle S_1\rangle.$$

It follows that $c(x) \in \langle S_1 \cup S_2\rangle$ if $p_2(x) \star (\ell(x) \mid a(x)) \in \langle S_1 \cup S_2\rangle$.

If $\deg(p_2(x)) \leq s - \deg(a(x)) - 1$, then $p_2(x) \star (\ell(x) \mid a(x)) \in \langle S_2\rangle$. If not, using the division algorithm, consider $p_2(x) = q_2(x)\frac{x^s-1}{a(x)} + r_2(x)$, where $\deg(r_2(x)) \leq s - \deg(a(x)) - 1$. Then,

$$
\begin{aligned}
p_2(x) \star (\ell(x) \mid a(x)) &= \left(q_2(x)\frac{x^s-1}{a(x)} + r_2(x) \right) \star (\ell(x) \mid a(x)) \\
&= \left(q_2(x)\frac{x^s-1}{a(x)} \right) \star (\ell(x) \mid a(x)) + r_2(x) \star (\ell(x) \mid a(x)) \\
&= (q_2(x)\frac{x^s-1}{a(x)}\ell(x) \mid 0) + r_2(x) \star (\ell(x) \mid a(x)).
\end{aligned}
$$

To prove that $p_2(x) \star (\ell(x) \mid a(x)) \in \langle S_1 \cup S_2 \rangle$ first note that $r_2(x) \star (\ell(x) \mid a(x)) \in \langle S_2 \rangle$. Finally, by Proposition 2, $b(x)$ divides $\frac{x^s-1}{a(x)}\ell(x)$ and it follows that $(q_2(x)\frac{x^s-1}{a(x)}\ell(x) \mid 0) \in \langle S_1 \rangle$. Thus, $c(x) \in \langle S_1 \cup S_2 \rangle$. □

Corollary 2 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, C is a binary linear code of dimension $r + s - \deg(b(x)) - \deg(a(x))$.*

4 Duality

Let C be a $\mathbb{Z}_2$-double cyclic code and $C^\perp$ be its dual code (see [10]). Taking a vector $\mathbf{v}$ of $C^\perp$, $\mathbf{u} \cdot \mathbf{v} = 0$ for all $\mathbf{u}$ in C. Since $\mathbf{u}$ belongs to C, we know that $\mathbf{u}^{(-1)}$ is also a codeword. So, $\mathbf{u}^{(-1)} \cdot \mathbf{v} = \mathbf{u} \cdot \mathbf{v}^{(1)} = 0$ for all $\mathbf{u} \in C$, therefore $\mathbf{v}^{(1)}$ is in $C^\perp$ and $C^\perp$ is also a $\mathbb{Z}_2$-double cyclic code. Consequently, we obtain the following proposition.

Proposition 4 *Let C be a $\mathbb{Z}_2$-double cyclic code. Then the dual code of C is also a $\mathbb{Z}_2$-double cyclic code.*

We denote $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$, where $\bar{b}(x), \bar{\ell}(x) \in \mathbb{Z}_2[x]/(x^r - 1)$ with $\bar{b}(x) \mid (x^r - 1)$ and $\bar{a}(x) \in \mathbb{Z}_2[x]/(x^s - 1)$ with $\bar{a}(x) \mid (x^s - 1)$.

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. As in the theory of binary cyclic codes, reciprocal polynomials have an important role in duality (see [11]).

We denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$. Using this notation we have the following proposition.

Proposition 5 *Let $n, m \in \mathbb{N}$. Then, $x^{nm} - 1 = (x^n - 1)\theta_m(x^n)$.*

Proof It is well known that $y^m - 1 = (y - 1)\theta_m(y)$. Replacing y by x^n, the result follows. □

From now on, $\mathfrak{m}$ denotes the least common multiple of r and s.

Definition 3 Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be elements in $R_{r,s}$. We define the map

$$\circ : R_{r,s} \times R_{r,s} \longrightarrow \mathbb{Z}_2[x]/(x^{\mathfrak{m}} - 1),$$

such that

$$
\begin{aligned}
\circ(\mathbf{u}(x), \mathbf{v}(x)) =& u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x) + \\
&+ u'(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))}v'^*(x) \mod (x^{\mathfrak{m}} - 1).
\end{aligned}
$$

The map $\circ$ is linear in each of its arguments. That is, $\circ$ is a bilinear map between $\mathbb{Z}_2[x]$-modules.

From now on, we denote $\circ(\mathbf{u}(x), \mathbf{v}(x))$ by $\mathbf{u}(x) \circ \mathbf{v}(x)$. Note that $\mathbf{u}(x) \circ \mathbf{v}(x)$ belongs to $\mathbb{Z}_2[x]/(x^{\mathfrak{m}} - 1)$.

Proposition 6 *Let* $\mathbf{u}$ *and* $\mathbf{v}$ *be vectors in* $\mathbb{Z}_2^r \times \mathbb{Z}_2^s$ *with associated polynomials* $\mathbf{u}(x) = (u(x) \mid u'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$*, respectively. Then,* $\mathbf{v}$ *is orthogonal to* $\mathbf{u}$ *and all its shifts if and only if*

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0.$$

Proof Let $\mathbf{u}^{(i)} = (u_{0-i}, u_{1-i}, \ldots, u_{r-1-i} \mid u'_{0-i}, \ldots, u'_{s-1-i})$ be the ith shift of $\mathbf{u}$. Then,

$$\mathbf{u}^{(i)} \cdot \mathbf{v} = 0 \text{ if and only if } \sum_{j=0}^{r-1} u_{j-i} v_j + \sum_{k=0}^{s-1} u'_{k-i} v'_k = 0.$$

Let $S_i = \sum_{j=0}^{r-1} u_{j-i} v_j + \sum_{k=0}^{s-1} u'_{k-i} v'_k$. Computing $\mathbf{u}(x) \circ \mathbf{v}(x)$ we obtain

$$\begin{aligned}\mathbf{u}(x) \circ \mathbf{v}(x) = \theta_{\frac{\mathfrak{m}}{r}}(x^r) &\left[\sum_{n=0}^{r-1} \sum_{j=n}^{r-1} u_{j-n} v_j x^{\mathfrak{m}-1-n} + \sum_{n=1}^{r-1} \sum_{j=n}^{r-1} u_j v_{j-n} x^{\mathfrak{m}-1+n} \right] \\ + \theta_{\frac{\mathfrak{m}}{s}}(x^s) &\left[\sum_{t=0}^{s-1} \sum_{k=t}^{s-1} u'_{k-t} v'_j x^{\mathfrak{m}-1-t} + \sum_{t=1}^{s-1} \sum_{k=t}^{s-1} u'_k v'_{k-t} x^{\mathfrak{m}-1+t} \right].\end{aligned}$$

Then, arranging the terms, we have that

$$\mathbf{u}(x) \circ \mathbf{v}(x) = \sum_{i=0}^{\mathfrak{m}-1} S_i x^{\mathfrak{m}-1-i} \mod (x^{\mathfrak{m}} - 1).$$

This implies that $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$ if and only if $S_i = 0$ for $0 \le i \le \mathfrak{m} - 1$. □

Lemma 1 *Let* $\mathbf{u}(x) = (u(x) \mid u'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$ *be elements in* $R_{r,s}$ *such that* $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$*. If* $u'(x)$ *or* $v'(x)$ *equals* 0*, then* $u(x)v^*(x) \equiv 0 \pmod{(x^r - 1)}$*. Respectively, if* $u(x)$ *or* $v(x)$ *equals* 0*, then* $u'(x)v'^*(x) \equiv 0 \pmod{(x^s - 1)}$*.*

Proof Let $u'(x)$ or $v'(x)$ equals 0. Then

$$0 = \mathbf{u}(x) \circ \mathbf{v}(x) = u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r) x^{\mathfrak{m}-1-\deg(v(x))} v^*(x) + 0 \mod (x^{\mathfrak{m}} - 1).$$

Therefore, $u(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r) x^{\mathfrak{m}-1-\deg(v(x))} v^*(x) = \mu'(x)(x^{\mathfrak{m}} - 1)$, for some $\mu'(x) \in \mathbb{Z}_2[x]$. Let $\mu(x) = \mu'(x) x^{\deg(v(x))+1}$. By Proposition 5, $u(x) x^{\mathfrak{m}} v^*(x) = \mu(x)(x^r - 1)$, and hence $u(x)v^*(x) \equiv 0 \pmod{(x^r - 1)}$. The same argument can be used to prove the other case. □

The following proposition shows that the dual of a separable $\mathbb{Z}_2$-double cyclic code is also separable.

Proposition 7 *Let* $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ *be a separable* $\mathbb{Z}_2$*-double cyclic code. Assume the generator polynomials of* C *satisfy the conditions in Proposition 1. Then* $\ell(x) = 0$*. Moreover,* $C^\perp$ *is a separable* $\mathbb{Z}_2$*-double cyclic code such that* $C^\perp = \langle (\frac{x^r - 1}{b^*(x)} \mid 0), (0 \mid \frac{x^s - 1}{a^*(x)}) \rangle$*.*

Proof If C is separable, then $C = C_r \times C_s$ and clearly $\ell(x) = 0$. Hence, it is easy to see that $C^\perp = C_r^\perp \times C_s^\perp$. By [11], we have that $C_r^\perp = \langle \frac{x^r - 1}{b^*(x)} \rangle$ and $C_s^\perp = \langle \frac{x^s - 1}{a^*(x)} \rangle$. Therefore, the statement follows. □

In view of Proposition 7, we shall focus on non-separable $\mathbb{Z}_2$-double cyclic codes for the rest of the section. From now on, we will denote $\gcd(b(x), l(x))$ by $g_{b,l}(x)$.

Proposition 8 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code. Assume the generator polynomials of C satisfy the conditions in Proposition 1. Then,*

$$\begin{aligned} |C_r| = 2^{r-\deg(b(x))+\kappa}, \, |C_s| = 2^{s-\deg(a(x))}, \\ |(C_r)^\perp| = 2^{\deg(b(x))-\kappa}, \, |(C_s)^\perp| = 2^{\deg(a(x))}, \\ |(C^\perp)_r| = 2^{\deg(b(x))}, \, |(C^\perp)_s| = 2^{\deg(a(x))+\kappa}, \end{aligned}$$

where $\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$.

Proof Let C be a $\mathbb{Z}_2$-double cyclic code with $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$, and assume the generator polynomials of C satisfy the conditions in Proposition 1. Then, by Proposition 3, C is generated by the matrix whose rows are the elements of the set $S_1 \cup S_2$. The subcode of C generated by the elements of S_1 and the subcode generated by the elements of S_2 have generator matrices of the form

$$\begin{aligned} G_1 &= \left(I_{r-\deg(b(x))} \;\; A \middle| \, 0 \right), \\ G_2 &= \left(B \middle| \, D \;\; I_{s-\deg(a(x))} \right), \end{aligned}$$

respectively.

Consider the subcode C_0 of C with 0 in the first r coodinates. Clearly C_0 is generated by elements in S_2 and therefore the dimension of C_0 is $s - \deg(a(x)) - \kappa$, for some $\kappa \geq 0$. Taking into account κ and the matrices G_1 and G_2, we have that C is permutation equivalent to a binary linear code with generator matrix of the form

$$G = \left(\begin{array}{ccc|ccc} I_{r-\deg(b(x))} & A_1 & A_2 & 0 & 0 & 0 \\ 0 & B_\kappa & B_1 & D_1 & I_\kappa & 0 \\ 0 & 0 & 0 & D_2 & R & I_{s-\deg(a(x))-\kappa} \end{array} \right),$$

where B_κ is a square matrix of full rank. Note that $\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$. The cardinalities of C_r, $(C_r)^\perp$, C_s and $(C_s)^\perp$ follow easily from G. The values of $|(C^\perp)_r|$ and $|(C^\perp)_s|$ can be obtained from the projections on the first r and on the last s coordinates of the following parity check matrix of C

$$H = \left(\begin{array}{ccc|ccc} A_1^t & I_\kappa & 0 & 0 & B_\kappa^t & B_\kappa^t R^t \\ A_2^t & 0 & I_{\deg(b(x))-\kappa} & 0 & B_1^t & B_1^t R^t \\ 0 & 0 & 0 & I_{\deg(a(x))} & D_1^t & D_2^t + D_1^t R^t \end{array} \right).$$

□

Corollary 3 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

$$\begin{aligned} \deg(\bar{b}(x)) &= r - \deg(g_{b,l}(x)), \\ \deg(\bar{a}(x)) &= s - \deg(a(x)) - \deg(b(x)) + \deg(g_{b,l}(x)). \end{aligned}$$

Proof It is easy to prove that $(C_r)^\perp$ is a cyclic code generated by $\bar{b}(x)$. Therefore, $|(C_r)^\perp| = 2^{r-\deg(\bar{b}(x))}$. Moreover, by Proposition 8, $|(C_r)^\perp| = 2^{\deg(b(x))-\kappa}$ with $\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$. Thus, $\deg(\bar{b}(x)) = r - \deg(g_{b,l}(x))$.

Since $C^\perp$ is a $\mathbb{Z}_2$-double cyclic code, $(C^\perp)_s$ is a cyclic code generated by $\bar{a}(x)$, and hence $|(C^\perp)_s| = 2^{s-\deg(\bar{a}(x))}$. By Proposition 8, we have that $|(C^\perp)_s| = 2^{\deg(a(x))+\kappa}$ with

$\kappa = \deg(b(x)) - \deg(g_{b,l}(x))$ and consequently $\deg(\bar{a}(x)) = s - \deg(a(x)) - \deg(b(x)) + \deg(g_{b,l}(x))$. □

The previous propositions and corollaries will be helpful to determine the relations between the generator polynomials of a $\mathbb{Z}_2$-double cyclic code and the generator polynomials of its dual code.

Proposition 9 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^{\perp} = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^{\perp}$ satisfy the conditions in Proposition 1. Then,*

$$\bar{b}(x) = \frac{x^r - 1}{g^*_{b,l}(x)}.$$

Proof We have that $(\bar{b}(x) \mid 0)$ belongs to $C^{\perp}$. Then,

$$(b(x) \mid 0) \circ (\bar{b}(x) \mid 0) = 0,$$
$$(\ell(x) \mid a(x)) \circ (\bar{b}(x) \mid 0) = 0.$$

Applying Lemma 1 to the previous equations, we obtain

$$b(x)\bar{b}^*(x) \equiv 0 \pmod{(x^r - 1)},$$
$$\ell(x)\bar{b}^*(x) \equiv 0 \pmod{(x^r - 1)}.$$

Therefore, $g_{b,l}(x)\bar{b}^*(x) \equiv 0 \pmod{(x^r - 1)}$, and there exists $\mu(x) \in \mathbb{Z}_2[x]$ such that $g_{b,l}(x)\bar{b}^*(x) = \mu(x)(x^r - 1)$. Moreover, $g_{b,l}(x)$ and $\bar{b}^*(x)$ divide $(x^r - 1)$, and by Corollary 3 we have that $\deg(\bar{b}(x)) = r - \deg(g_{b,l}(x))$ and then $\bar{b}^*(x) = \frac{x^r - 1}{g_{b,l}(x)}$. □

Proposition 10 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^{\perp} = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^{\perp}$ satisfy the conditions in Proposition 1. Then,*

$$\bar{a}(x) = \frac{(x^s - 1)g^*_{b,l}(x)}{a^*(x)b^*(x)}.$$

Proof Consider the codeword

$$\frac{b(x)}{g_{b,l}(x)} \star (\ell(x) \mid a(x)) - \frac{\ell(x)}{g_{b,l}(x)} \star (b(x) \mid 0) = \left(0 \mid \frac{b(x)}{g_{b,l}(x)} a(x)\right).$$

Then, since $(\bar{\ell}(x) \mid \bar{a}(x)) \in C^{\perp}$, we have that $(\bar{\ell}(x) \mid \bar{a}(x)) \circ (0 \mid \frac{b(x)}{g_{b,l}(x)} a(x)) = 0$. Thus, by Lemma 1, $\bar{a}(x)\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} \equiv 0 \pmod{(x^s - 1)}$, and hence $\bar{a}(x)\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} = (x^s - 1)\mu(x)$, for some $\mu(x) \in \mathbb{Z}_2[x]$. By Corollary 1, it follows that $\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)}$ divides $(x^s - 1)$. Therefore, if $\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} \equiv 0 \pmod{(x^s - 1)}$ we may consider that $\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)} = (x^s - 1)$. By Corollary 3, $\deg(\bar{a}(x)) = s - \deg(a(x)) - \deg(b(x)) + \deg(g_{b,l}(x))$, thus

$$\deg(x^s - 1) = s = \deg\left(\bar{a}(x)\frac{a^*(x)b^*(x)}{g^*_{b,l}(x)}\right) = \deg((x^s - 1)\mu(x)).$$

Hence, we obtain that $\mu(x) = 1$ and $\bar{a}(x) = \frac{(x^s - 1)g^*_{b,l}(x)}{a^*(x)b^*(x)}$. □

Proposition 11 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a non-separable $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

$$\bar{\ell}(x) = \frac{x^r - 1}{b^*(x)} \lambda(x),$$

where $\lambda(x) = x^{\mathrm{m}-\deg(a(x))+\deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)}\right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)}\right)$.

Proof Let $\bar{c}(x) = (\bar{b}(x) \mid 0) + (\bar{\ell}(x) \mid \bar{a}(x)) \in C^\perp$. Then

$$\begin{aligned}\bar{c}(x) \circ (b(x) \mid 0) &= (\bar{b}(x) \mid 0) \circ (b(x) \mid 0) + (\bar{\ell}(x) \mid \bar{a}(x)) \circ (b(x) \mid 0) \\ &= 0 + (\bar{\ell}(x) \mid \bar{a}(x)) \circ (b(x) \mid 0) = 0.\end{aligned}$$

By Lemma 1, we have that $\bar{\ell}(x) b^*(x) \equiv 0 \pmod{(x^r - 1)}$ and therefore

$$\bar{\ell}(x) = \frac{x^r - 1}{b^*(x)} \lambda(x).$$

Computing $(\bar{\ell}(x) \mid \bar{a}(x)) \circ (\ell(x) \mid a(x))$ and arranging properly we obtain

$$\frac{(x^{\mathrm{m}} - 1) g^*_{b,l}(x)}{b^*(x)} \left(\lambda(x) x^{\mathrm{m}-\deg(\ell(x))-1} \frac{\ell^*(x)}{g^*_{b,l}(x)} + x^{\mathrm{m}-\deg(a(x))-1} \right),$$

that is congruent to $0 \pmod{(x^{\mathrm{m}} - 1)}$. Then, either

$$\left(\lambda(x) x^{\mathrm{m}-\deg(\ell(x))-1} \frac{\ell^*(x)}{g^*_{b,l}(x)} + x^{\mathrm{m}-\deg(a(x))-1} \right) \equiv 0 \pmod{(x^{\mathrm{m}} - 1)}, \tag{2}$$

or

$$\left(\lambda(x) x^{\mathrm{m}-\deg(\ell(x))-1} \frac{\ell^*(x)}{g^*_{b,l}(x)} + x^{\mathrm{m}-\deg(a(x))-1} \right) \equiv 0 \left(\mathrm{mod} \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right) \right). \tag{3}$$

Since $\frac{b^*(x)}{g^*_{b,l}(x)}$ divides $x^{\mathrm{m}} - 1$, clearly (2) implies (3). Hence,

$$\lambda(x) x^{\mathrm{m}} \frac{\ell^*(x)}{g^*_{b,l}(x)} = x^{\mathrm{m}-\deg(a(x))+\deg(\ell(x))} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right).$$

We have that $x^{\mathrm{m}} \equiv 1 \ (\mathrm{mod} \left(\frac{b^*(x)}{g^*_{b,l}(x)}\right))$. Moreover, the greatest common divisor between $\frac{\ell(x)}{g_{b,l}(x)}$ and $\frac{b(x)}{g_{b,l}(x)}$ is 1, and then $\frac{\ell^*(x)}{g^*_{b,l}(x)}$ is an invertible element modulo $\left(\frac{b^*(x)}{g^*_{b,l}(x)}\right)$. Therefore,

$$\lambda(x) = x^{\mathrm{m}-\deg(a(x))+\deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)} \right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)} \right).$$

□

We summarize the previous results in the next theorem.

Theorem 2 *Let $C = \langle (b(x) \mid 0), (\ell(x) \mid a(x)) \rangle$ be a $\mathbb{Z}_2$-double cyclic code with dual code $C^\perp = \langle (\bar{b}(x) \mid 0), (\bar{\ell}(x) \mid \bar{a}(x)) \rangle$. Assume the generator polynomials of C and $C^\perp$ satisfy the conditions in Proposition 1. Then,*

1. $\bar{b}(x) = \frac{x^r-1}{g^*_{b,l}(x)}$,
2. $\bar{a}(x) = \frac{(x^s-1)g^*_{b,l}(x)}{a^*(x)b^*(x)}$,
3. $\bar{\ell}(x) = \frac{x^r-1}{b^*(x)}\lambda(x)$, *where*

$$\lambda(x) = \begin{cases} 0, \text{ if } C \text{ is separable}, \\ x^{\mathrm{m}-\deg(a(x))+\deg(\ell(x))} \left(\frac{\ell^*(x)}{g^*_{b,l}(x)}\right)^{-1} \mod \left(\frac{b^*(x)}{g^*_{b,l}(x)}\right), \textit{otherwise}. \end{cases}$$

5 Relations between $\mathbb{Z}_2$-double cyclic codes and other codes

In this section, we study how $\mathbb{Z}_2$-double cyclic codes are related to other families of cyclic codes, say $\mathbb{Z}_4$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Since these families of codes have part or all the coordinates over $\mathbb{Z}_4$, their generator polynomials also have coefficients over the ring $\mathbb{Z}_4$. From now on, the binary reduction of a polynomial $p(x) \in \mathbb{Z}_4[x]$ will be denoted by $\tilde{p}(x)$.

Let $p(x)$ be a divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$ with n odd and let ξ be a primitive nth root of unity over $\mathbb{Z}_2$. The polynomial $(p \otimes p)(x)$ is defined as the divisor of $x^n - 1$ in $\mathbb{Z}_2[x]$ whose roots are the products $\xi^i\xi^j$ such that ξ^i and ξ^j are roots of $p(x)$.

From [12] and [10], it is known that a $\mathbb{Z}_4$-cyclic code $\mathcal{C}$ of length n is generated by a single element $f(x)h(x) + 2f(x) \in \mathbb{Z}_4[x]/(x^n - 1)$, where $f(x)h(x)g(x) = x^n - 1$ in $\mathbb{Z}_4[x]$, and $|\mathcal{C}| = 4^{\deg(g(x))}2^{\deg(h(x))}$.

Let $\mathbf{u} = (u_0, \dots, u_{n-1})$ be an element of $\mathbb{Z}_4^n$ such that $u_i = \tilde{u}_i + 2u'_i$ with $\tilde{u}_i, u'_i \in \{0, 1\}$. As in [9], the *Gray map* ϕ from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ is defined by

$$\phi(\mathbf{u}) = (u'_0, \dots, u'_{n-1} \mid \tilde{u}_0 + u'_0, \dots, \tilde{u}_{n-1} + u'_{n-1}).$$

Let $\mathbf{u}(x) = \tilde{\mathbf{u}}(x) + 2\mathbf{u}'(x)$ be the polynomial representation of $\mathbf{u} \in \mathbb{Z}_4^n$. Then, the polynomial version of the Gray map is $\phi(\mathbf{u}(x)) = (\mathbf{u}'(x) \mid \tilde{\mathbf{u}}(x) + \mathbf{u}'(x))$. The *Nechaev permutation* is the permutation π on $\mathbb{Z}_2^{2n}$ with n odd defined by

$$\pi(v_0, v_1, \dots, v_{2n-1}) = (v_{\tau(0)}, v_{\tau(1)}, \dots, v_{\tau(2n-1)}),$$

where τ is the permutation on $\{0, 1, \dots, 2n - 1\}$ given by

$$(1, n + 1)(3, n + 3)\dots(2i + 1, n + 2i + 1)\dots(n - 2, 2n - 2).$$

Let ψ be the map from $\mathbb{Z}_4^n$ into $\mathbb{Z}_2^{2n}$ defined by $\psi = \pi\phi$, with n odd. The map ψ is called the *Nechaev–Gray map*, [15]. Therefore we give the following theorem.

Theorem 3 ([15, Theorem 20]) *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$ be a $\mathbb{Z}_4$-cyclic code of odd length n and where $f(x)h(x)g(x) = x^n - 1$. Let ϕ be the Gray map and let ψ be the Nechaev–Gray map. The following properties are equivalent.*

1. $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ *in* $\mathbb{Z}_2[x]$*;*
2. $\phi(\mathcal{C})$ *is a binary linear code of length* $2n$*;*
3. $\psi(\mathcal{C})$ *is a binary linear cyclic code of length* $2n$ *generated by* $\tilde{f}(x)^2\tilde{h}(x)$.

Using the last theorem, we can relate $\mathbb{Z}_2$-double cyclic codes to $\mathbb{Z}_4$-cyclic codes.

5.1 $\mathbb{Z}_2$-double cyclic codes versus $\mathbb{Z}_4$-cyclic codes

Let $\mathcal{C}$ be a $\mathbb{Z}_4$-cyclic code of length n, and $\mathbf{w} \in \phi(\mathcal{C})$. The codeword $\mathbf{w}$ can be written as $(u'_0, \dots, u'_{n-1} \mid \tilde{u}_0 + u'_0, \dots, \tilde{u}_{n-1} + u'_{n-1})$, for $(u_0, \dots, u_{n-1}) = \mathbf{u} = \phi^{-1}(\mathbf{w}) \in \mathcal{C}$. By definition of the Gray map, we have that $\mathbf{w}^{(1)}$ is $(u'_{n-1}, u'_0, \ldots, u'_{n-2} \,|\, \tilde{u}_{n-1} + u'_{n-1}, \tilde{u}_0 + u'_0, \ldots, \tilde{u}_{n-2} + u'_{n-2}) = \phi(u_{n-1}, u_0, \ldots, u_{n-2})$. Therefore, since $\mathcal{C}$ is $\mathbb{Z}_4$-cyclic, we have that $\mathbf{w}^{(i)} \in \phi(\mathcal{C})$.

In general, the Gray image of a linear code over $\mathbb{Z}_4$ is not linear. Hence, we shall consider $\mathbb{Z}_2$-double cyclic codes as images of $\mathbb{Z}_4$-cyclic codes, $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$, in the case that such a code $\mathcal{C}$ has linear image under the Gray map; that is, when $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ in $\mathbb{Z}_2[x]$, by Theorem 3. Consequently, we obtain the following proposition.

Proposition 12 *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle$ be a $\mathbb{Z}_4$-cyclic code of odd length n, where $f(x)h(x)g(x) = x^n - 1$, and $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$. Then, $\phi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$.*

Our goal is to establish a relation between the generator polynomial of the $\mathbb{Z}_4$-cyclic code $\mathcal{C}$ and its $\mathbb{Z}_2$-double cyclic image, $\phi(\mathcal{C})$.

Let $i \in \{2, 4\}$. If $\mathcal{C}$ is a $\mathbb{Z}_i[x]$-module and $g_1, \ldots, g_t \in \mathcal{C}$. Then $\langle g_1, \ldots, g_t\rangle_i$ will denote the $\mathbb{Z}_i[x]$-submodule of $\mathcal{C}$ generated by $g_1, \ldots, g_t$.

The following theorem is proved in [14, Theorem 8].

Theorem 4 *Let n be odd and let $f(x), h(x), g(x)$ be in $\mathbb{Z}_4[x]$ such that $f(x)h(x)g(x) = x^n - 1$. Then $\langle f(x)h(x) + 2f(x)\rangle_4 = \langle \tilde{f}(x)\tilde{h}(x)\rangle_2 + 2\langle \tilde{f}(x)\rangle_2$ if and only if $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$ in $\mathbb{Z}_2[x]$.*

Lemma 2 *Let $\mathcal{C}$ be a linear code over $\mathbb{Z}_4$ of type $2^\gamma 4^\delta$ such that $\phi(\mathcal{C})$ is a linear code. Let $\{\mathbf{u}_i\}_{i=1}^{\gamma}$ be codewords of order two and $\{\mathbf{v}_j\}_{j=1}^{\delta}$ codewords of order four such that $\mathcal{C} = \langle \{\mathbf{u}_i\}_{i=1}^{\gamma}, \{\mathbf{v}_j\}_{j=1}^{\delta}\rangle_4$. Then,*

$$\phi(\mathcal{C}) = \langle \{\phi(\mathbf{u}_i)\}_{i=1}^{\gamma}, \{\phi(\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j)\}_{j=1}^{\delta}\rangle_2.$$

Proof From [6, Lemma 3], it is known that if $\mathcal{C}$ is a linear code over $\mathbb{Z}_4$ of type $2^\gamma 4^\delta$ such that $\mathcal{C} = \langle \{\mathbf{u}_i\}_{i=1}^{\gamma}, \{\mathbf{v}_j\}_{j=1}^{\delta}\rangle_4$, then

$$\langle \phi(\mathcal{C})\rangle_2 = \langle \{\phi(\mathbf{u}_i)\}_{i=1}^{\gamma}, \{\phi(\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j * \mathbf{v}_t)\}_{1 \le j < t \le \delta}\rangle_2,$$

where $\mathbf{u} * \mathbf{v}$ denote the component-wise product for any $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_4^n$. We know that $\phi(\mathcal{C})$ is linear if and only if $2\mathbf{u} * \mathbf{v} \in \mathcal{C}$ for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, [9]. Since $\phi(\mathcal{C})$ is a binary linear code, then $\{2\mathbf{v}_j * \mathbf{v}_t\}_{1 \le j < t \le \delta} \in \mathcal{C}$. Therefore, $\langle \{\phi(2\mathbf{v}_j * \mathbf{v}_t)\}_{1 \le j < t \le \delta}\rangle_2 \subseteq \langle \{\phi(\mathbf{u}_i)\}_{i=1}^{\gamma}, \{\phi(\mathbf{v}_j)\}_{j=1}^{\delta}, \{\phi(2\mathbf{v}_j)\}_{j=1}^{\delta}\rangle_2$. □

Theorem 5 *Let $\mathcal{C} = \langle f(x)h(x) + 2f(x)\rangle_4$ be a $\mathbb{Z}_4$-cyclic code of odd length n, where $f(x)h(x)g(x) = x^n - 1$ and $\gcd(\tilde{f}(x), (\tilde{g} \otimes \tilde{g})(x)) = 1$. Then,*

$$\phi(\mathcal{C}) = \langle (\tilde{f}(x)\tilde{h}(x) \mid 0), (\tilde{f}(x) \mid \tilde{f}(x))\rangle_2.$$

Proof By Theorem 4, the generators of $\mathcal{C}$ are $\langle \tilde{f}(x)\tilde{h}(x)\rangle_2$ and $2\langle \tilde{f}(x)\rangle_2$. By Proposition 12, we have that $\phi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code. Then, by Lemma 2, it is easy to see that the generator polynomials of $\phi(\mathcal{C})$ are $\phi(\tilde{f}(x)\tilde{h}(x))$ and $\phi(2\tilde{f}(x))$. The corresponding images of the Gray map are $\phi(\tilde{f}(x)\tilde{h}(x)) = (0 \mid \tilde{f}(x)\tilde{h}(x))$ and $\phi(2\tilde{f}(x)) = (\tilde{f}(x) \mid \tilde{f}(x))$, hence $\phi(\mathcal{C}) = \langle (0 \mid \tilde{f}(x)\tilde{h}(x)), (\tilde{f}(x) \mid \tilde{f}(x))\rangle_2$. Therefore,

$$\phi(\mathcal{C}) = \langle (\tilde{f}(x)\tilde{h}(x) \mid 0), (\tilde{f}(x) \mid \tilde{f}(x))\rangle_2.$$

□

5.2 $\mathbb{Z}_2$-double cyclic codes versus $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ (see [4]). Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to a commutative structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ and it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords.

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called cyclic if the set of coordinates can be partitioned into two subsets, the set of $\mathbb{Z}_2$ and the set of $\mathbb{Z}_4$ coordinates, denoted by X and Y, such that any cyclic shift of the coordinates of both subsets leaves invariant the code. As it was done in (1), for $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we also denote by $(\mathbf{u}, \mathbf{v})^{(1)}$ such shift. These codes can be identified as submodules of the $\mathbb{Z}_4[x]$-module $\mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$. From [1] and [5], we know that if $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where β is an odd integer, then it is of the form

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle_4,$$

where $f(x)h(x)g(x) = x^\beta - 1$ in $\mathbb{Z}_4[x]$, $b(x), \ell(x) \in \mathbb{Z}_2[x]/(x^\alpha - 1)$ with $b(x) | (x^\alpha - 1)$, $deg(\ell(x)) < deg(b(x))$, and $b(x)$ divides $\frac{x^\beta - 1}{f(x)} \ell(x) \pmod 2$.

The *extended Gray map* Φ and the *extended Nechaev–Gray map* Ψ are the maps from $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ into $\mathbb{Z}_2^{\alpha+2\beta}$ given by

$$\Phi(\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \phi(\mathbf{v})), \quad \Psi(\mathbf{u}, \mathbf{v}) = (\mathbf{u}, \psi(\mathbf{v})),$$

where $\mathbf{u} \in \mathbb{Z}_2^\alpha$, $\mathbf{v} \in \mathbb{Z}_4^\beta$, ϕ is the Gray map and ψ is the Nechaev–Gray map.

Table 1 Optimal $\mathbb{Z}_2$-double cyclic codes

Code	Generators	[r, s]	Parameters
C_1	$b(x) = x^2 + x + 1, \ell(x) = x, a(x) = x + 1$	[3,3]	$[\,6, 3, 3\,]^*$
C_2	$b(x) = x^2 + 1, \ell(x) = 1, a(x) = x^2 + x + 1$	[2,6]	$[\,8, 4, 4\,]_s^*$
C_3	$b(x) = x^3 + x^2 + x + 1, \ell(x) = x^2 + x, a(x) = x + 1$	[4,4]	$[\,8, 4, 4\,]_s^*$
C_4	$b(x) = x^4+x^3+x+1, \ell(x) = x^2+x+1, a(x) = x^2+x+1$	[6,6]	$[\,12, 6, 4\,]_s^*$
C_5	$b(x) = x^7+1, \ell(x) = x^4+x^2+x+1, a(x) = x^4+x^2+x+1$	[7,7]	$[\,14, 3, 8\,]^*$
C_6	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x^2 + 1, a(x) = x^4 + x^2 + x + 1$	[7,7]	$[\,14, 4, 7\,]^*$
C_7	$b(x) = x^4 + x^3 + x^2 + 1, \ell(x) = x^3 + x + 1, a(x) = x^3 + x^2 + 1$	[7,7]	$[\,14, 7, 4\,]_s^*$
C_8	$b(x) = x^7 + 1, \ell(x) = x^3 + x + 1, a(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$	[7,14]	$[\,21, 5, 10\,]^*$
C_9	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^4 + x^3 + 1, a(x) = x^5 + x^2 + x + 1$	[7,14]	$[\,21, 10, 7\,]^*$
C_{10}	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) s = x + 1, a(x) = x^3 + x^2 + 1$	[7,14]	$[\,21, 12, 5\,]^*$
C_{11}	$b(x) = x^3 + x^2 + 1, \ell(x) = 1, a(x) = x^2 + 1$	[7,14]	$[\,21, 16, 3\,]^*$
C_{12}	$b(x) = x^2 + 1, \ell(x) = x + 1, a(x) = x^{16} + x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x + 1$	[2,30]	$[\,32, 14, 8\,]$
C_{13}	$b(x) = x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^5 + x^3 + x^2 + x + 1, \ell(x) = x^{15} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^5 + 1, a(x) = x^6 + x^4 + x^3 + 1$	[31,31]	$[\,62, 36, 10\,]$

Call $\mathcal{C}_X$ (respectively $\mathcal{C}_Y$) the punctured code of $\mathcal{C}$ by deleting the coordinates outside X (respectively Y). Notice that if $\phi(\mathcal{C}_Y)$ and $\psi(\mathcal{C}_Y)$ are binary linear codes, then $\Phi(\mathcal{C})$ and $\Psi(\mathcal{C})$ are not necessary binary linear codes.

Example 2 Let $\mathcal{C} = \langle(x-1 \mid x+1)\rangle_4 \subset \mathbb{Z}_2^2 \times \mathbb{Z}_4^3$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code with $b(x) = 0$, $\ell(x) = x-1$, $f(x) = 1$, $h(x) = x-1$ and $g(x) = x^2+x+1$. Since $f(x) = 1$, by Theorem 3, we have that $\phi(\mathcal{C}_Y)$ is linear. By [5], a generator matrix for $\mathcal{C}$ is

$$\left(\begin{array}{cc|ccc} 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 0 & 1 \end{array}\right).$$

We know that $\Phi(\mathcal{C})$ is linear if and only if $2(\mathbf{u},\mathbf{v}) * (\mathbf{w},\mathbf{z}) \in \mathcal{C}$ for all $(\mathbf{u},\mathbf{v}), (\mathbf{w},\mathbf{z}) \in \mathcal{C}$, [7]. Clearly, $2(0,0,3,1,0) * (0,0,3,0,1) = (0,0,2,0,0) \notin \mathcal{C}$. Therefore, $\Phi(\mathcal{C})$ is not a binary linear code.

Theorem 6 *Let $\mathcal{C} = \langle(b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x))\rangle_4 \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ be a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code, where β is an odd integer and $f(x)h(x)g(x) = x^\beta - 1$. Let Ψ be the extended Nechaev–Gray map. If $\Psi(\mathcal{C})$ is a binary linear code, then $\Psi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code of length $\alpha + 2\beta$ and dimension $\alpha - \deg(b(x)) + \deg(h(x)) + 2\deg(g(x))$.*

Proof By the definition of Ψ, the length of $\Psi(\mathcal{C})$ is $\alpha+2\beta$ and, since $\Psi(\mathcal{C})$ is a linear code, we need to prove that $\Psi((\mathbf{u},\mathbf{v}))^{(1)} \in \Psi(\mathcal{C})$ for all $(\mathbf{u},\mathbf{v}) \in \mathcal{C}$. By [15], we can easily deduce that $\Psi((\mathbf{u},\mathbf{v}))^{(1)} = \Psi((\mathbf{u},-\mathbf{v})^{(1)})$. We have that $(\mathbf{u},-\mathbf{v})^{(1)} \in \mathcal{C}$ and consequently $\Psi((\mathbf{u},\mathbf{v}))^{(1)}$ belongs to $\Psi(\mathcal{C})$. Hence, $\Psi(\mathcal{C})$ is a $\mathbb{Z}_2$-double cyclic code. Finally, since $|\Psi(\mathcal{C})| = |\mathcal{C}|$, we have that $|\mathcal{C}| = 2^{\alpha-\deg(b(x))+\deg(h(x))}4^{\deg(g(x))}$ by [1]. □

Table 2 Dual $\mathbb{Z}_2$-double cyclic codes

Code	Generators of the dual codes	[r, s]	Parameters
C_1	$\bar{b}(x) = x^3+1, \bar{\ell}(x) = x+1, \bar{a}(x) = 1$	[3,3]	[6, 3, 3]
C_2	$\bar{b}(x) = x^2+1, \bar{\ell}(x) = 1, \bar{a}(x) = x^2+x+1$	[2,6]	[8, 4, 4]^s
C_3	$\bar{b}(x) = x^3+x^2+x+1, \bar{\ell}(x) = x^2+x, \bar{a}(x) = x+1$	[4,4]	[8, 4, 4]^s
C_4	$\bar{b}(x) = x^4+x^3+x+1, \bar{\ell}(x) = x^2+x+1, \bar{a}(x) = x^2+x+1$	[6,6]	[12, 6, 4]^s
C_5	$\bar{b}(x) = x^3+x^2+1, \bar{\ell}(x) = 1, \bar{a}(x) = 1$	[7,7]	[14, 11, 2]
C_6	$\bar{b}(x) = x^4+x^2+x+1, \bar{\ell}(x) = x^3+x, \bar{a}(x) = 1$	[7,7]	[14, 10, 3]
C_7	$\bar{b}(x) = x^4+x^3+x^2+1, \bar{\ell}(x) = x^3+x+1, \bar{a}(x)$ $= x^3+x^2+1$	[7,7]	[14, 7, 4]^s
C_8	$\bar{b}(x) = x^4+x^3+x^2+1, \bar{\ell}(x) = x, \bar{a}(x) = x+1$	[7,14]	[21, 16, 3]
C_9	$\bar{b}(x) = x^7+1, \bar{\ell}(x) = x^4+x^3+x^2+x, \bar{a}(x) = x^3+x+1$	[7,14]	[21, 11, 6]
C_{10}	$\bar{b}(x) = x^7+1, \bar{\ell}(x) = x^6+x^4+x^3+x^2+x+1, \bar{a}(x)$ $= x^5+x^4+x^3+1$	[7,14]	[21, 9, 6]
C_{11}	$\bar{b}(x) = x^7+1, \bar{\ell}(x) = x^6+x^5+x^2+1, \bar{a}(x)$ $= x^9+x^6+x^5+x^4+x^3+x+1$	[7,14]	[21, 5, 7]
C_{12}	$\bar{b}(x) = x+1, \bar{\ell}(x) = 1, \bar{a}(x)$ $= x^{13}+x^{11}+x^9+x^8+x^7+x^2+x+1$	[2,30]	[32, 18, 2]
C_{13}	$\bar{b}(x) = x^{26}+x^{23}+x^{21}+x^{20}+x^{17}+x^{16}+x^{15}+x^{14}$ $+x^{13}+x^9+x^8+x^6+x^5+x^4+x^2+1, \bar{\ell}(x)$ $= x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{13}$ $+x^{11}+x^{10}+x^8+x^5+x^3+x, \bar{a}(x) = x^{10}+x^9+x^3+x+1$	[31,31]	[62, 26, 15]

Table 3 $\mathbb{Z}_2$-double cyclic codes from $\mathbb{Z}_4$-cyclic codes

n	$\mathbb{Z}_4$-cyclic generators	$\mathbb{Z}_2$-double cyclic generators	Binary parameters
3	$f(x)h(x) = x^3 + 3,\ f(x) = x + 3$	$b(x) = x^3 + 1, \ell(x) = x + 1, a(x) = x + 1$	[6, 2, 4]
7	$f(x)h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\ f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x^2 + 1, a(x) = x^3 + x^2 + 1$	[14, 5, 6]
7	$f(x)h(x) = x^4 + 2x^3 + 3x^2 + x + 1,\ f(x) = x + 3$	$b(x) = x^4 + x^2 + x + 1, \ell(x) = x + 1, a(x) = x + 1$	[14, 9, 4]
9	$f(x)h(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\ f(x) = x^2 + x + 1$	$b(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^2 + x + 1, a(x) = x^2 + x + 1$	[18, 8, 4]
9	$f(x)h(x) = x^7 + 3x^6 + x^4 + 3x^3 + x + 3,\ f(x) = x^6 + x^3 + 1$	$b(x) = x^7 + x^6 + x^4 + x^3 + x + 1, \ell(x) = x^6 + x^3 + 1, a(x) = x^6 + x^3 + 1$	[18, 5, 6]
15	$f(x)h(x) = x^{11} + 3x^{10} + x^6 + 3x^5 + x + 3,\ f(x) = x^4 + 3x^3 + 2x^2 + 1$	$b(x) = x^{11} + x^{10} + x^6 + x^5 + x + 1, \ell(x) = x^4 + x^3 + 1, a(x) = x^4 + x^3 + 1$	[30, 15, 6]
15	$f(x)h(x) = x^{13} + 3x^{12} + x^{10} + 3x^9 + x^7 + 3x^6 + x^4 + 3x^3 + x + 3,\ f(x) = x^4 + 3x^3 + 2x^2 + 1$	$b(x) = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1, \ell(x) = x^4 + x^3 + 1, a(x) = x^4 + x^3 + 1$	[30, 13, 6]

Table 4 $\mathbb{Z}_2$-double cyclic codes from $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes

$[\alpha, \beta]$	$\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic generators	$\mathbb{Z}_2$-double cyclic generators	Binary parameters
[2,3]	$b(x) = x^2 + 1, \ell(x) = x + 1, f(x)h(x) = x^3 + 3, f(x) = 1$	$b(x) = x^2 + 1, \ell(x) = x + 1, a(x) = x^3 + 1$	[8, 3, 4]
[3,3]	$b(x) = x^2 + x + 1, \ell(x) = x, f(x)h(x) = x^2 + x + 1, f(x) = 1$	$b(x) = x^2 + x + 1, \ell(x) = x + 1, a(x) = x^2 + x + 1$	[9, 5, 3]
[9,3]	$b(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^6 + x^3 + 1, f(x)h(x) = x^3 + 3, f(x) = x + 3$	$b(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^6 + x^3 + 1, a(x) = x^4 + x^3 + x + 1$	[15, 3, 7]
[4,7]	$b(x) = x^3 + x^2 + x + 1, \ell(x) = x^2 + 1, f(x)h(x) = x^4 + 2x^3 + 3x^2 + x + 1, f(x) = 1$	$b(x) = x^3 + x^2 + x + 1, \ell(x) = x^2 + 1, a(x) = x^4 + x^2 + x + 1$	[18, 11, 4]
[4,7]	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, f(x)h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, a(x) = x^9 + x^6 + x^5 + x^4 + x^3 + x + 1$	[18, 5, 6]
[4,7]	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, f(x)h(x) = x^7 + 3, f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^4 + 1, \ell(x) = x^3 + x^2 + x + 1, a(x) = x^{10} + x^9 + x^7 + x^3 + x^2 + 1$	[18, 4, 8]
[7,7]	$b(x) = x^7 + 1, \ell(x) = x^6 + x^5 + x^3, f(x)h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, f(x) = x^3 + 3x^2 + 2x + 3$	$b(x) = x^7 + 1, \ell(x) = x^3 + x^2 + 1, a(x) = x^9 + x^6 + x^5 + x^4 + x^3 + x + 1$	[21, 5, 10]
[7,7]	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x + 1, f(x)h(x) = x^7 + 1, f(x) = x + 3$	$b(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \ell(x) = x^3 + x + 1, a(x) = x^8 + x^7 + x + 1$	[21, 7, 7]
[7,7]	$b(x) = x^3 + x + 1, \ell(x) = x, f(x)h(x) = x^4 + 2x^3 + 3x^2 + x + 1, f(x) = x + 3$	$b(x) = x^3+x+1, \ell(x) = x^2+x, a(x) = x^5+x^4+x^3+1$	[21, 13, 3]

6 Examples

Table 1 gives some examples of $\mathbb{Z}_2$-double cyclic codes which have the best known minimum distance. In the table, the parameters are $[n, k, d]$, where $n = r + s$ is the length, k is the dimension, and d is the minimum distance of the code. It is denoted by $[.]^*$ when the code is optimal according to [8]. It is denoted by $[.]_s$ when the code is self-dual. Table 2 shows the generators and the parameters of the dual codes of the codes in Table 1.

In Sect. 5, we have studied how $\mathbb{Z}_2$-double cyclic codes are related to other families of cyclic codes. By Theorem 5, we know how to construct the generators of $\mathbb{Z}_2$-double cyclic codes starting from the generators of $\mathbb{Z}_4$-cyclic codes. Also, by Theorem 6 we know that the image of a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code under the Nechaev–Gray map, whenever it is linear, is also a $\mathbb{Z}_2$-double cyclic code. In Tables 3, 4, we present some examples of $\mathbb{Z}_2$-double cyclic codes obtained from $\mathbb{Z}_4$-cyclic codes and $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

Acknowledgements This work has been partially supported by the Spanish MINECO Grants TIN2016-77918-P and MTM2015-69138-REDT, and by the Catalan AGAUR Grant 2014SGR-691.

References

1. Abualrub T., Siap I., Aydin N.: $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. IEEE Trans. Inf. Theory **60**, 1508–1514 (2014).
2. Aydogdu I., Abualrub T., Siap I.: On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. Int. J. Comput. Math. **92**(9), 1806–1814 (2015).
3. Aydogdu I., Abualrub T., Siap I.: $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. IEEE Trans. Inf. Theory. doi:10.1109/TIT.2016.2632163.
4. Borges J., Fernández-Córdoba C., Pujol J., Rifà J., Villanueva M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality. Des. Codes Cryptogr. **54**, 167–179 (2010).
5. Borges J., Fernández-Córdoba C., Ten-Valls R.: $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inf. Theory **62**, 6348–6354 (2016).
6. Fernández-Córdoba C., Pujol J., Villanueva M.: On Rank and Kernel of $\mathbb{Z}_4$-Linear Codes. Lecture Notes in Computer Science, vol. 5228, pp. 46–55. Springer, Berlin (2008).
7. Fernández-Córdoba C., Pujol J., Villanueva M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: rank and kernel. Des. Codes Cryptogr. **56**, 43–59 (2010).
8. Grassl M.: Table of bounds on linear codes. [Online]. Available: http://www.codestable.de (1995).
9. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.: The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes. IEEE Trans. Inf. Theory **40**, 301–319 (1994).
10. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
11. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, New York (1977).
12. Pless V.S., Qian Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory **42**, 1594–1600 (1996).
13. Siap I., Kulhan N.: The structure of generalized quasi cyclic codes. Appl. Math. E-Notes **5**, 24–30 (2005).
14. Vega G., Wolfmann J.: Some families of $\mathbb{Z}_4$-cyclic codes. Finite Fields Appl. **10**, 530–539 (2004).
15. Wolfmann J.: Binary images of cyclic codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory **47**, 1773–1779 (2001).

Appendix D

On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

Advances in Mathematics of Communications
Volume X, No. 0X, 200X, X–XX

doi:10.3934/xx.xx.xx.xx

ON $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-ADDITIVE CYCLIC CODES

Joaquim Borges, Cristina Fernández-Córdoba, and Roger Ten-Valls

Department of Information and Communications Engineering
Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

(Communicated by the associate editor name)

Abstract. A $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code, $r \leq s$, is a $\mathbb{Z}_{p^s}$-submodule of $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$. We introduce $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. These codes can be seen as $\mathbb{Z}_{p^s}[x]$-submodules of $\mathcal{R}_{r,s}^{\alpha,\beta} = \frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha - 1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta - 1\rangle}$. We determine the generator polynomials of a code over $\mathcal{R}_{r,s}^{\alpha,\beta}$ and a minimal spanning set over $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ in terms of the generator polynomials. We also study the duality in the module $\mathcal{R}_{r,s}^{\alpha,\beta}$. Our results generalise those for $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes.

1. Introduction

$\mathbb{Z}_2\mathbb{Z}_4$-additive codes have been introduced in [4] and intensely studied during last years. The set of coordinates of a $\mathbb{Z}_2\mathbb{Z}_4$-additive code can be partitioned into two subsets, the set of coordinates over $\mathbb{Z}_2$ and the set of coordinates over $\mathbb{Z}_4$. In recent times, $\mathbb{Z}_2\mathbb{Z}_4$-additive codes were generalized to $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes in [2], and later to $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, in [3]. In [2] and [3], the authors determine, in particular, the standard forms of generator and parity-check matrices and present some bounds on the minimum distance.

One of the most studied class of codes is the class of cyclic codes. For example, the algebraic structure and the generators of cyclic codes over $\mathbb{Z}_{p^m}$ have been studied in [7] and [10]. Newly, the concept of double cyclic codes over rings appeared in the literature. A double cyclic code is a code such that the set of coordinates can be partitioned into two subsets such that any cyclic shift of the coordinates of both subsets leaves invariant the code. Notice that if one of these sets of coordinates is empty then we obtain a cyclic code. We can find examples of double cyclic codes over the rings $\mathbb{Z}_2$ and $\mathbb{Z}_4$ in [5] and [9], respectively. Also, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes have been defined in [1]. These codes have the property that a simultaneous cyclic shift of the coordinates over $\mathbb{Z}_2$ and the coordinates over $\mathbb{Z}_4$ of a codeword is also a codeword. A $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code is identified as a $\mathbb{Z}_4[x]$-module of a certain ring. The duality of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes has been studied in [6].

After all these papers, it becomes natural the study of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. On the one hand, as the study of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, presented in [3], with the cyclic property. And, on the other hand, as a generalization of the different types of cyclic codes studied in [1, 5, 6, 9, 7, 10].

The aim of this paper is the study of the algebraic structure of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes. We will assume that $r \leq s$. As $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes can be

2010 *Mathematics Subject Classification:* 94B05, 94B15, 94B60.

Key words and phrases: Additive codes, codes over rings, cyclic codes, duality.

This work has been partially supported by the Spanish MINECO grants TIN2016-77918-P and MTM2015-69138-REDT, and by the Catalan AGAUR grant 2014SGR-691.

identified as $\mathbb{Z}_{p^s}[x]$-submodules of $\frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha-1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta-1\rangle}$ then, Section 2 reviews cyclic codes over $\mathbb{Z}_{p^m}$ and details a minimal generating set of a cyclic code over $\mathbb{Z}_{p^m}$ as a $\mathbb{Z}_{p^m}$-module. In Section 3, we recall definitions and basic results of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, defined in [3]. In Section 4, we give the definition of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code, we discuss the algebraic structure of these codes, we determine the generator polynomials of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code, and we describe a minimal generating set for the code as a $\mathbb{Z}_{p^s}$-module in terms of the generator polynomials. Finally, in Section 5, we study the duality of these codes over the $\mathbb{Z}_{p^s}[x]$-module $\frac{\mathbb{Z}_{p^r}[x]}{\langle x^\alpha-1\rangle} \times \frac{\mathbb{Z}_{p^s}[x]}{\langle x^\beta-1\rangle}$.

2. Cyclic codes over $\mathbb{Z}_{p^m}$

Let p be a prime number and let $\mathbb{Z}_{p^m}$ be the ring of integers modulo p^m. A linear code of length n over $\mathbb{Z}_{p^m}$ is a submodule of $\mathbb{Z}_{p^m}^n$, and a cyclic code of length n over $\mathbb{Z}_{p^m}$ is a linear code with the property that if $(c_0,\cdots,c_{n-2},c_{n-1})$ is a codeword then $(c_{n-1},c_0,\cdots,c_{n-2})$ is also a codeword.

Let $g_1,\dots,g_r$ be polynomials in a $\mathbb{Z}_{p^m}[x]$-module. We denote by $\langle g_1,\dots,g_r\rangle$ the $\mathbb{Z}_{p^m}[x]$-submodule, resp. $\langle g_1,\dots,g_r\rangle_{\mathbb{Z}_{p^m}}$ the $\mathbb{Z}_{p^m}$-submodule, generated by $g_1,\dots,g_r$.

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. We can identify $\mathcal{C}$ as an ideal of $\mathbb{Z}_{p^m}[x]/\langle x^n-1\rangle$. We assume that n is a positive integer such that it is coprime with p. Therefore, the polynomial x^n-1 has a unique decomposition as a product of basic irreducible polynomials that are pairwise coprime over $\mathbb{Z}_{p^m}[x]$.

Theorem 2.1 ([8, Theorem 3.5])**.** *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. Then, there exist polynomials $g_0,g_1,\dots,g_{m-1}$ in $\mathbb{Z}_{p^m}[x]$ such that $\mathcal{C}$ is generated by $\{g_0,pg_1,\dots,p^{m-1}g_{m-1}\}$ and $g_{m-1}\mid g_{m-2}\mid\cdots\mid g_1\mid g_0\mid(x^n-1)$.*

Let $\mathcal{C}=\langle g_0,pg_1,\dots,p^{m-1}g_{m-1}\rangle$ be a cyclic code of length n and let $g=g_0+pg_1+\cdots+p^{m-1}g_{m-1}$. Since g_0 is a factor of x^n-1 and, for $i=1\dots m-1$, the polynomial g_i is a factor of g_{i-1}, we may define the polynomials $\hat{g}_0=\frac{x^n-1}{g_0}$ and $\hat{g}_i=\frac{g_{i-1}}{g_i}$ for $i=1\dots m-1$. Define $G=\prod_{i=0}^{m-1}\hat{g}_i$. It is clear that $Gg=\left(\prod_{i=0}^{m-1}\hat{g}_i\right)g=0$ over $\mathbb{Z}_{p^m}[x]/\langle x^n-1\rangle$.

Lemma 2.2. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. Let $g_0,g_1,\dots,g_{m-1}$ in $\mathbb{Z}_{p^m}[x]$ such that $\mathcal{C}=\langle g_0,pg_1,\dots,p^{m-1}g_{m-1}\rangle$ and $g_{m-1}\mid g_{m-2}\mid\cdots\mid g_1\mid g_0\mid(x^n-1)$, and let $g=g_0+pg_1+\cdots+p^{m-1}g_{m-1}$. Then,*

1. *$p^{m-1}g=p^{m-1}g_{m-1}\frac{G}{\hat{g}_0}$,*
2. *$p^{m-1-i}(\prod_{j=0}^{i-1}\hat{g}_j)g=p^{m-1}g_{m-1}\frac{G}{\hat{g}_i}$, for $i=1,\dots,m-1$.*

Proof. We have

$$\begin{aligned} p^{m-1}g &= p^{m-1}g_0\frac{1}{g_1}\frac{g_1}{g_2}\cdots\frac{g_{m-3}}{g_{m-2}}\frac{g_{m-2}}{g_{m-1}}g_{m-1}\\ &= p^{m-1}g_{m-1}\hat{g}_1\hat{g}_2\cdots\hat{g}_{m-2}\hat{g}_{m-1}\\ &= p^{m-1}g_{m-1}\frac{G}{\hat{g}_0}, \end{aligned}$$

and 1 holds. For $i=1,\dots,m-1$ we have

$$\begin{aligned} p^{m-1-i}(\textstyle\prod_{j=0}^{i-1}\hat{g}_j)g &= p^{m-1-i}(\textstyle\prod_{j=0}^{i-1}\hat{g}_j)p^ig_i\\ &= p^{m-1-i}(\textstyle\prod_{j=0}^{i-1}\hat{g}_j)p^ig_i\frac{1}{g_{i+1}}\frac{g_{i+1}}{g_{i+2}}\cdots\frac{g_{m-2}}{g_{m-1}}g_{m-1}\\ &= p^{m-1}g_{m-1}\hat{g}_0\hat{g}_1\cdots\hat{g}_{i-1}\hat{g}_{i+1}\cdots\hat{g}_{m-1}\\ &= p^{m-1}g_{m-1}\frac{G}{\hat{g}_i}, \end{aligned}$$

and statement 2 is proved.

□

From Theorem 2.1, we get the following result.

Corollary 2.3. *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$ such that $\mathcal{C}$ is generated by $\{g_0, pg_1, \dots, p^{m-1}g_{m-1}\}$ with $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. Then,*

$$|\mathcal{C}| = p^{\sum_{i=0}^{m-1}(m-i)\deg(\hat{g}_i)}.$$

Proof. From the previous definition of $\hat{g}_i$, these polynomials are the same polynomials described in [8, Theorem 3.4]. □

In [7], it is proved that $\mathbb{Z}_{p^m}[x]/\langle x^n-1\rangle$ is a principal ideal ring. Furthermore, they showed how are the generator polynomials of the ideals. Joining these results we obtain the following.

Theorem 2.4 ([7])**.** *Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$. Let $g_0, g_1, \dots, g_{m-1}$ polynomials in $\mathbb{Z}_{p^m}[x]$ such that $\mathcal{C} = \langle g_0, pg_1, \dots, p^{m-1}g_{m-1}\rangle$ and $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. Then, the polynomial $g = g_0 + pg_1 + \cdots + p^{m-1}g_{m-1}$ is a generator polynomial of $\mathcal{C}$, i.e., $\mathcal{C} = \langle g\rangle$.*

Theorem 2.5. *Let $\mathcal{C} = \langle g\rangle = \langle g_0 + pg_1 + \cdots + p^{m-2}g_{m-2} + p^{m-1}g_{m-1}\rangle$ be a cyclic code of length n over $\mathbb{Z}_{p^m}$ with $g_{m-1} \mid g_{m-2} \mid \cdots \mid g_1 \mid g_0 \mid (x^n-1)$. We define the following sets*

$$S_0 = \{x^i g\}_{i=0}^{\deg(\hat{g}_0)} = \{x^i(g_0 + pg_1 + \cdots + p^{m-2}g_{m-2} + p^{m-1}g_{m-1})\}_{i=0}^{\deg(\hat{g}_0)},$$

$$S_1 = \{x^i \hat{g}_0 g\}_{i=0}^{\deg(\hat{g}_1)} = \{x^i(pg_1\hat{g}_0 + \cdots + p^{m-2}g_{m-2}\hat{g}_0 + p^{m-1}g_{m-1}\hat{g}_0)\}_{i=0}^{\deg(\hat{g}_1)},$$

$$\vdots$$

$$S_j = \left\{x^i(\prod_{t=0}^{j-1}\hat{g}_t)g\right\}_{i=0}^{\deg(\hat{g}_j)},$$

$$\vdots$$

$$S_{m-1} = \left\{x^i(\prod_{t=0}^{m-2}\hat{g}_t)g\right\}_{i=0}^{\deg(\hat{g}_{m-1})} = \left\{x^i(\prod_{t=0}^{m-2}\hat{g}_t)p^{m-1}g_{m-1}\right\}_{i=0}^{\deg(\hat{g}_{m-1})}.$$

Then,

$$S = \bigcup_{j=0}^{m-1} S_j$$

forms a minimal generating set for $\mathcal{C}$ as a $\mathbb{Z}_{p^m}$-module.

Proof. Let $c \in \mathcal{C}$. We have $c = dg$, with $d \in \mathbb{Z}_{p^m}[x]$. If $\deg(d) < \deg(\hat{g}_0)$ then $dg \in \langle S_0\rangle_{\mathbb{Z}_{p^m}}$ and $c \in \langle S\rangle_{\mathbb{Z}_{p^m}}$. Otherwise, compute $d = d_0\hat{g}_0 + r_0$ with $\deg(r_0) < \deg(\hat{g}_0)$, so $dg = d_0\hat{g}_0 g + r_0 g$ and $r_0 g \in \langle S_0\rangle_{\mathbb{Z}_{p^m}}$.

If $\deg(d_0) < \deg(\hat{g}_1)$, then $d_0\hat{g}_0 g \in \langle S_1\rangle_{\mathbb{Z}_{p^m}}$ and $c \in \langle S\rangle_{\mathbb{Z}_{p^m}}$. Otherwise, compute $d_0 = d_1\hat{g}_1 + r_1$ with $\deg(r_1) < \deg(\hat{g}_1)$, so $d_0\hat{g}_0 g = d_1\hat{g}_1\hat{g}_0 g + r_1\hat{g}_0 g$ and $r_1\hat{g}_0 g \in \langle S_1\rangle_{\mathbb{Z}_{p^m}}$.

In the worst-case scenario, and reasoning similarly, one obtains $c \in \langle S\rangle_{\mathbb{Z}_{p^m}}$ if $d_{m-2}(\prod_{t=0}^{m-2} \hat{g}_t)g \in \langle S\rangle_{\mathbb{Z}_{p^m}}$. It is obvious that if $\deg(d_{m-2}) < \deg(\hat{g}_{m-1})$ then $d_{m-2}(\prod_{t=0}^{m-2} \hat{g}_t)g \in \langle S_{m-1}\rangle_{\mathbb{Z}_{p^m}}$. If not, $d_{m-2} = d_{m-1}\hat{g}_{m-1} + r_{m-1}$. Therefore,

$$d_{m-2}(\prod_{t=0}^{m-2} \hat{g}_t)g = d_{m-1}(\prod_{t=0}^{m-1} \hat{g}_t)g + r_{m-1}(\prod_{t=0}^{m-2} \hat{g}_t)g = r_{m-1}(\prod_{t=0}^{m-2} \hat{g}_t)g \in \langle S_{m-1}\rangle_{\mathbb{Z}_{p^m}}.$$

Since $r_{m-1}(\prod_{t=0}^{m-2} \hat{g}_t)g \in \langle S_{m-1}\rangle_{\mathbb{Z}_{p^m}}$, we have $c \in \langle S\rangle_{\mathbb{Z}_{p^m}}$, hence S is a generating set. If one compute $|S|$ clearly

$$|S| = \sum_{i=0}^{m-1}(m-i)\deg(\hat{g}_i).$$

By Corollary 2.3, $|\mathcal{C}| = |\langle S\rangle|$ and S is a minimal generating set. □

3. $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes

Let $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ be the rings of integers modulo p^r and p^s, respectively, with p prime and $r \leq s$. Since the residue field of both $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ is $\mathbb{Z}_p$, an element b of $\mathbb{Z}_{p^r}$ could be written uniquely as $b = b_0 + pb_1 + p^2b_2 + \cdots + p^{r-1}b_{r-1}$, and any element $a \in \mathbb{Z}_{p^s}$ as $a = a_0 + pa_1 + p^2a_2 + \cdots + p^{s-1}a_{s-1}$, where $b_i, a_j \in \mathbb{Z}_p$.

Then we can consider the surjective ring homomorphism

$$\begin{array}{rccl} \pi: & \mathbb{Z}_{p^s} & \to & \mathbb{Z}_{p^r} \\ & a & \mapsto & a \mod p^r. \end{array}$$

Note that $\pi(p^i) = 0$ if $i \geq r$. Let a be an element of $\mathbb{Z}_{p^s}$ and b be an element of $\mathbb{Z}_{p^r}$. We define a multiplication $*$ as follows: $a * b = \pi(a)b$. Then, $\mathbb{Z}_{p^r}$ is a $\mathbb{Z}_{p^s}$-module with the external multiplication $*$ given by π. Since $\mathbb{Z}_{p^r}$ is commutative, $*$ has the commutative property. Then, we can generalize this multiplication over the ring $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ as follows. Let a be an element of $\mathbb{Z}_{p^s}$ and $\mathbf{u} = (u \mid u') = (u_0, u_1, \ldots, u_{\alpha-1} \mid u'_0, u'_1, \ldots, u'_{\beta-1}) \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$. Then,

$$a * \mathbf{u} = (\pi(a)u_0, \pi(a)u_1, \ldots, \pi(a)u_{\alpha-1} \mid au'_0, au'_1, \ldots, au'_{\beta-1}).$$

With this external operation, the ring $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is also a $\mathbb{Z}_{p^s}$-module.

Definition 3.1. A $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ is a $\mathbb{Z}_{p^s}$-submodule of $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$.

The structure of the generator matrix in standard form and the type of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes are defined and determined in [3].

Let $\mathcal{C}_X$ be the canonical projection of $\mathcal{C}$ on the first α coordinates and $\mathcal{C}_Y$ on the last β coordinates. Then, $\mathcal{C}_X$ and $\mathcal{C}_Y$ are $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ linear codes of length α and β, respectively. A code $\mathcal{C}$ is called *separable* if $\mathcal{C}$ is the direct product of $\mathcal{C}_X$ and $\mathcal{C}_Y$, i.e., $\mathcal{C} = \mathcal{C}_X \times \mathcal{C}_Y$.

Since $r \leq s$, we consider the inclusion map

$$\begin{array}{rccl} \iota: & \mathbb{Z}_{p^r} & \hookrightarrow & \mathbb{Z}_{p^s} \\ & b & \mapsto & b \end{array}.$$

Let $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$, then the inner product is defined in [3] as

$$\mathbf{u} \cdot \mathbf{v} = p^{s-r}\sum_{i=0}^{\alpha-1}\iota(u_iv_i) + \sum_{j=0}^{\beta-1}u'_jv'_j \in \mathbb{Z}_{p^s},$$

and the dual code of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code $\mathcal{C}$ is defined in a natural way as

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta \mid \mathbf{u}\cdot\mathbf{v} = 0,\ \forall \mathbf{u} \in \mathcal{C}\}.$$

Let $\mathcal{C}$ be a separable code in $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$, then $\mathcal{C}^\perp$ is also separable and $\mathcal{C}^\perp = \mathcal{C}_X^\perp \times \mathcal{C}_Y^\perp$.

4. $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes

Definition 4.1. Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code. The code $\mathcal{C}$ is called *cyclic* if

$$(u_0, u_1, \dots, u_{\alpha-2}, u_{\alpha-1} \mid u'_0, u'_1, \dots, u'_{\beta-2}, u'_{\beta-1}) \in \mathcal{C}$$

implies

$$(u_{\alpha-1}, u_0, u_1, \dots, u_{\alpha-2} \mid u'_{\beta-1}, u'_0, u'_1, \dots, u'_{\beta-2}) \in \mathcal{C}.$$

Let $\mathbf{u} = (u_0, u_1, \dots, u_{\alpha-1} \mid u'_0, \dots, u'_{\beta-1})$ be a codeword in $\mathcal{C}$ and i be an integer. We then denote by $\mathbf{u}^{(i)} = (u_{0-i}, u_{1-i}, \dots, u_{\alpha-1-i} \mid u'_{0-i}, \dots, u'_{\beta-1-i})$ the ith shift of $\mathbf{u}$, where the subscripts are read modulo α and β, respectively. Note that if $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ is cyclic, then $\mathcal{C}_X$ (resp. $\mathcal{C}_Y$) is a cyclic code over $\mathbb{Z}_{p^r}^\alpha$ (resp. $\mathbb{Z}_{p^s}^\beta$).

We remark that in this paper the definition of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code is well defined as long as $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$ are different rings, since the elements on the first α coordinates and the ones in the last β coordinates belong to different rings, $\mathbb{Z}_{p^r}$ and $\mathbb{Z}_{p^s}$, respectively. In the particular case that $r = s$, the cyclic code in $\subseteq \mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^r}^\beta$ is known in the literature as *double cyclic code*, see [5], [9]. The term double cyclic is given in order to distinguish the cyclic code in $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^r}^\beta$ from the cyclic code in $\mathbb{Z}_{p^r}^{\alpha+\beta}$.

Denote by $\mathcal{R}_{r,s}^{\alpha,\beta}$ the ring $\mathbb{Z}_{p^s}[x]/\langle x^\alpha - 1\rangle \times \mathbb{Z}_{p^s}[x]/\langle x^\beta - 1\rangle$. There is a bijective map between $\mathbb{Z}_{p^r}^\alpha \times \mathbb{Z}_{p^s}^\beta$ and $\mathcal{R}_{r,s}^{\alpha,\beta}$ given by:

$$(u_0, u_1, \dots, u_{\alpha-1} \mid u'_0, \dots, u'_{\beta-1}) \mapsto (u_0 + u_1x + \cdots + u_{\alpha-1}x^{\alpha-1} \mid u'_0 + \cdots + u'_{\beta-1}x^{\beta-1}).$$

We denote the image of the vector $\mathbf{u}$ by $\mathbf{u}(x)$. Note that we can extend the maps ι and π to the polynomial rings $\mathbb{Z}_{p^r}[x]$ and $\mathbb{Z}_{p^s}[x]$ applying these maps to each of the coefficients of a given polynomial.

Definition 4.2. Define the operation $* : \mathbb{Z}_{p^s}[x] \times \mathcal{R}_{r,s}^{\alpha,\beta} \to \mathcal{R}_{r,s}^{\alpha,\beta}$ as

$$\lambda(x) * (t(x) \mid q(x)) = (\pi(\lambda(x))t(x) \mid \lambda(x)q(x)),$$

where $\lambda(x) \in \mathbb{Z}_{p^s}[x]$ and $(t(x) \mid q(x)) \in \mathcal{R}_{r,s}^{\alpha,\beta}$.

The ring $\mathcal{R}_{r,s}^{\alpha,\beta}$ with the external operation $*$ is a $\mathbb{Z}_{p^s}[x]$-module. Let $\mathbf{u}(x) = (u(x) \mid u'(x))$ be an element of $\mathcal{R}_{r,s}^{\alpha,\beta}$. Note that if we operate $\mathbf{u}(x)$ by x we get

$$\begin{aligned} x * \mathbf{u}(x) &= x * (u(x) \mid u'(x)) \\ &= (u_0x + \cdots + u_{\alpha-2}x^{\alpha-1} + u_{\alpha-1}x^\alpha \mid u'_0x + \cdots + u'_{\beta-2}x^{\beta-1} + u'_{\beta-1}x^\beta) \\ &= (u_{\alpha-1} + u_0x + \cdots + u_{\alpha-2}x^{\alpha-1} \mid u'_{\beta-1} + u'_0x + \cdots + u'_{\beta-2}x^{\beta-1}). \end{aligned}$$

Hence, $x * \mathbf{u}(x)$ is the image of the vector $\mathbf{u}^{(1)}$. Thus, the operation of $\mathbf{u}(x)$ by x in $R_{\alpha,\beta}$ corresponds to a shift of $\mathbf{u}$. In general, $x^i * \mathbf{u}(x) = \mathbf{u}^{(i)}(x)$ for all i.

4.1. Algebraic structure and generators of cyclic codes. In this section, we study submodules of $\mathcal{R}_{r,s}^{\alpha,\beta}$. We describe the generators of such submodules and state some properties. From now on, $\langle S\rangle$ will denote the $\mathbb{Z}_{p^s}[x]$-submodule generated by a subset S of $\mathcal{R}_{r,s}^{\alpha,\beta}$.

For the rest of the discussion we will consider that α and β are coprime integers with p. From this assumption, we know that $\mathbb{Z}_{p^r}[x]/(x^\alpha-1)$ and $\mathbb{Z}_{p^s}[x]/(x^\beta-1)$ are principal ideal rings, see [7], [8].

Theorem 4.3. *Every submodule $\mathcal{C}$ of the $\mathbb{Z}_{p^s}[x]$-module $\mathcal{R}_{r,s}^{\alpha,\beta}$ can be written as*

$$\mathcal{C}=\langle(b(x)\mid 0),(\ell(x)\mid a(x))\rangle,$$

where $b(x),a(x)$ are generator polynomials in $\mathbb{Z}_{p^r}[x]/(x^\alpha-1)$ and $\mathbb{Z}_{p^s}[x]/(x^\beta-1)$ resp., and $\ell(x)\in\mathbb{Z}_{p^r}[x]/(x^\alpha-1)$.

Proof. Let $\psi_X:\mathcal{R}_{r,s}^{\alpha,\beta}\to\mathbb{Z}_{p^r}[x]/\langle x^\alpha-1\rangle$ and $\psi_Y:\mathcal{R}_{r,s}^{\alpha,\beta}\to\mathbb{Z}_{p^s}[x]/\langle x^\beta-1\rangle$ be the canonical projections, let $\mathcal{C}$ be a submodule of $\mathcal{R}_{r,s}^{\alpha,\beta}$. Define $\mathcal{C}'=\{(p(x)|q(x))\in\mathcal{C}\mid q(x)=0\}$. It is easy to check that $\mathcal{C}'\cong\psi_X(\mathcal{C}')$ by $(p(x)\mid 0)\mapsto p(x)$. Hence, by Theorem 2.4, $\psi_X(\mathcal{C}')$ is finitely generated and so is $\mathcal{C}'$. Let $b(x)$ be a generator of $\psi_X(\mathcal{C}')$, then $(b(x)\mid 0)$ is a generator of $\mathcal{C}'$.
As $\mathbb{Z}_{p^s}[x]/\langle x^\beta-1\rangle$ is also a principal ideal ring, then $\mathcal{C}_Y=\psi_Y(\mathcal{C})$ is generated by one element. Let $a(x)\in\mathcal{C}_Y$ such that $\mathcal{C}_Y=\langle a(x)\rangle$, then there exists $\ell(x)\in\mathbb{Z}_{p^r}[x]/\langle x^\alpha-1\rangle$ such that $(\ell(x)\mid a(x))\in\mathcal{C}$.
We claim that

$$\mathcal{C}=\langle(b(x)\mid 0),(\ell(x)\mid a(x))\rangle.$$

Let $(p(x)\mid q(x))\in\mathcal{C}$, then $q(x)=\psi_Y(p(x)\mid q(x))\in\mathcal{C}_Y$. So, there exists $\lambda(x)\in\mathbb{Z}_{p^s}[x]$ such that $q(x)=\lambda(x)a(x)$. Now,

$$(p(x)\mid q(x))-\lambda(x)*(\ell(x)\mid a(x))=(p(x)-\pi(\lambda(x))\ell(x)\mid 0)\in\mathcal{C}'.$$

Then, there exists $\mu(x)\in\mathbb{Z}_{p^s}[x]$ such that $(p(x)-\pi(\lambda(x))\ell(x)\mid 0)=\mu(x)*(b(x)\mid 0)$. Thus,

$$(p(x)\mid q(x))=\mu(x)*(b(x)\mid 0)+\lambda(x)*(\ell(x)\mid a(x)).$$

So, $\mathcal{C}$ is finitely generated by $\langle(b(x)\mid 0),(\ell(x)\mid a(x))\rangle$.

□

From the previous results, it is clear that we can identify codes in $\mathbb{Z}_{p^r}^\alpha\times\mathbb{Z}_{p^s}^\beta$ that are cyclic as submodules of $\mathcal{R}_{r,s}^{\alpha,\beta}$. So, any submodule of $\mathcal{R}_{r,s}^{\alpha,\beta}$ is a cyclic code. From now on, we will denote by $\mathcal{C}$ indistinctly both the code and the corresponding submodule.

In the following, a polynomial $f(x)\in\mathbb{Z}_{p^r}[x]$ or $\mathbb{Z}_{p^s}[x]$ will be denoted simply by f.

Proposition 4.4. *Let $\mathcal{C}\subseteq\mathbb{Z}_{p^r}^\alpha\times\mathbb{Z}_{p^s}^\beta$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then, there exist polynomials ℓ and $b_0\mid b_1\mid\cdots\mid b_{r-1}\mid(x^\alpha-1)$ over $\mathbb{Z}_{p^r}[x]$, and polynomials $a_0\mid a_1\mid\cdots\mid a_{s-1}\mid(x^\beta-1)$ over $\mathbb{Z}_{p^s}[x]$ such that*

$$\mathcal{C}=\langle(b_0+pb_1+\cdots+p^{r-1}b_{r-1}\mid 0),(\ell\mid a_0+pa_1+\cdots+p^{s-1}a_{s-1})\rangle.$$

Proof. Let $\mathcal{C}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. By Theorem 4.3, there exist polynomials $b,\ell\in\mathbb{Z}_{p^s}[x]/\langle x^\alpha-1\rangle$ and $a\in\mathbb{Z}_{p^s}[x]/\langle x^\beta-1\rangle$ such that $\mathcal{C}=\langle(b\mid 0),(\ell\mid a)\rangle$. By Theorem 2.4, one can consider $b=b_0+pb_1+\cdots+p^{r-1}b_{r-1}$ and $a=a_0+pa_1+\cdots+p^{s-1}a_{s-1}$ such that $b_{r-1}|b_{r-2}|\dots|b_1|b_0|(x^\alpha-1)$ and $a_{s-1}|a_{s-2}|\dots|a_1|a_0|(x^\beta-1)$. □

For the rest of the discussion any cyclic code $\mathcal{C}$ over $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ is of the form $\mathcal{C} = \langle (b \mid 0), (\ell \mid a) \rangle$, where $b = b_0 + pb_1 + \cdots + p^{r-1}b_{r-1}$ and $a(x) = a_0 + pa_1 + \cdots + p^{s-1}a_{s-1}$, for polynomials b_i and a_j as in Proposition 4.4. Since b_0 is a factor of $x^{\alpha} - 1$ and for $i = 1 \dots r-1$ the polynomial b_i is a factor of b_{i-1}, we will denote $\hat{b}_0 = \frac{x^{\alpha}-1}{b_0}$, $\hat{b}_i = \frac{b_{i-1}}{b_i}$ for $i = 1 \dots r-1$, and $\hat{b}_r = b_{r-1}$. In the same way, we define $\hat{a}_0 = \frac{x^{\beta}-1}{a_0}$, $\hat{a}_j = \frac{a_{j-1}}{a_j}$ for $j = 1 \dots s-1$, and $\hat{a}_s = a_{s-1}$.

Proposition 4.5. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

$$\prod_{t=0}^{s-1} \hat{a}_t * (\ell \mid a) \in \langle (b \mid 0) \rangle.$$

Proof. $\prod_{t=0}^{s-1} \hat{a}_t * (\ell \mid a) = \frac{x^{\beta}-1}{a_{s-1}} * (\ell \mid a) = (\pi(\frac{x^{\beta}-1}{a_{s-1}})\ell \mid \frac{x^{\beta}-1}{a_{s-1}}a) = (\pi(\frac{x^{\beta}-1}{a_{s-1}})\ell \mid 0)$. □

Theorem 4.6. *Let $\mathcal{C} \subseteq \mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Define*

$$B_j = \left\{ x^i (\prod_{t=0}^{j-1} \hat{b}_t) * (b \mid 0) \right\}_{i=0}^{\deg(\hat{b}_j)-1},$$

for $0 \le j \le r-1$, and

$$A_k = \left\{ x^i (\prod_{t=0}^{k-1} \hat{a}_t) * (\ell \mid a) \right\}_{i=0}^{\deg(\hat{a}_k)-1},$$

for $0 \le k \le s-1$. Then,

$$S = \left(\bigcup_{j=0}^{r-1} B_j \right) \bigcup \left(\bigcup_{t=0}^{s-1} A_t \right)$$

forms a minimal generating set for $\mathcal{C}$ as a $\mathbb{Z}_{p^s}$-module. Moreover,

$$|\mathcal{C}| = p^{\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i) + \sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)}.$$

Proof. By Theorem 2.5, it is clear that the elements in S are $\mathbb{Z}_{p^s}$-linearly independent since $\left(\bigcup_{j=0}^{r-1} B_j\right)_X$ and $\left(\bigcup_{t=0}^{s-1} A_t\right)_Y$ are minimal generating sets for the codes $\mathcal{C}_X$ and $\mathcal{C}_Y$, respectively. Let c be a codeword of $\mathcal{C}$, then $c = q * (b \mid 0) + d * (\ell \mid a)$. Reasoning similarly as in Theorem 2.5, $q * (b \mid 0) \in \langle \bigcup_{j=0}^{r-1} B_j \rangle_{\mathbb{Z}_{p^s}}$. So we have to prove that $d * (\ell \mid a) \in \langle S \rangle_{\mathbb{Z}_{p^s}}$.

If $\deg(d) < \deg(\hat{a}_0)$ then $d*(\ell \mid a) \in \langle A_0 \rangle_{\mathbb{Z}_{p^s}}$ and $c \in \langle S \rangle_{\mathbb{Z}_{p^s}}$. Otherwise, compute $d = d_0\hat{a}_0 + r_0$ with $\deg(r_0) < \deg(\hat{a}_0)$. Then, $d * (\ell \mid a) = d_0\hat{a}_0 * (\ell \mid a) + r_0 * (\ell \mid a)$ and $r_0 * (\ell \mid a) \in \langle A_0 \rangle_{\mathbb{Z}_{p^s}}$.

In the worst-case scenario and reasoning similarly, one obtains that c belongs to $\langle S \rangle_{\mathbb{Z}_{p^s}}$ if $d_{s-2}(\prod_{t=0}^{s-2} \hat{a}_t)*(\ell \mid a) \in \langle S \rangle_{\mathbb{Z}_{p^s}}$. It is obvious that if $\deg(d_{s-2}) < \deg(\hat{a}_{s-1})$ then $d_{s-2}(\prod_{t=0}^{s-2} \hat{a}_t)*(\ell \mid a) \in \langle A_{s-1} \rangle_{\mathbb{Z}_{p^s}}$, if not, $d_{s-2} = d_{s-1}\hat{a}_{s-1} + r_{s-1}$. Therefore,

$$d_{s-2}\left(\prod_{t=0}^{s-2} \hat{a}_t\right) * (\ell \mid a) = d_{s-1}\left(\prod_{t=0}^{s-1} \hat{a}_t\right) * (\ell \mid a) + r_{s-1}\left(\prod_{t=0}^{s-2} \hat{a}_t\right) * (\ell \mid a).$$

On the one hand, $r_{s-1}(\prod_{t=0}^{s-2}\hat{a}_t)*(\ell \mid a) \in \langle A_{s-1}\rangle_{\mathbb{Z}_{p^s}}$. On the other hand, $d_{s-1}(\prod_{t=0}^{s-1}\hat{a}_t)*(\ell \mid a) = d_{s-1}(\prod_{t=0}^{s-1}\hat{a}_t)*(\ell \mid 0)$ and then

$$d_{s-1}(\prod_{t=0}^{s-1}\hat{a}_t)*(\ell \mid a) = f*(b \mid 0) \in \langle \bigcup_{j=0}^{r-1} B_j\rangle_{\mathbb{Z}_{p^s}}.$$

Thus, $c \in \langle S\rangle_{\mathbb{Z}_{p^s}}$ and S is a minimal generating set for $\mathcal{C}$. $\square$

The *order* of an element $\mathbf{v}$ of an abelian group, $ord(\mathbf{v})$, is the smallest positive integer m such that $m\cdot\mathbf{v}=0$. Let $\mathcal{C}$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code. Define

$$\mathcal{C}_{p^i} = \{\mathbf{v} = (v \mid v') \in \mathcal{C} \mid ord(\mathbf{v}) = p^i \text{ and } ord(v') = p^i\}.$$

Let k_0 be the dimension of $\mathcal{C}_{p^r}$ restricted in the first α coordinates, i.e., $k_0 = \dim((\mathcal{C}_{p^r})_X)$. Define $k_i = \dim((\mathcal{C}_{p^{r-i}})_X) - \sum_{j=0}^{i-1} k_j$, for $i = 1,\dots,r-1$. The code $\mathcal{C}$ is of type $(\alpha,\beta;k_0,k_1,\dots,k_{r-1};l_0,\dots,l_{s-1})$ if it is group isomorphic to $\mathbb{Z}_{p^r}^{k_0}\times\mathbb{Z}_{p^{r-1}}^{k_1}\times\cdots\times\mathbb{Z}_p^{k_{r-1}}\times\mathbb{Z}_{p^s}^{l_0}\times\cdots\times\mathbb{Z}_p^{l_{s-1}}$. With this definition, it is clear that $|\mathcal{C}| = p^{\sum_{i=0}^{r-1}(r-i)k_i+\sum_{j=0}^{s-1}(s-j)l_j}$. The type and the generator matrices of $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes were given in [3].

Example 4.7. *In this example, we show the standard form of the generator matrix, according to [3], of a $\mathbb{Z}_4\mathbb{Z}_8$-additive code of type $(\alpha,\beta;k_0,k_1;l_0,l_1,l_2)$.*

$$\left(\begin{array}{ccc|cccc}
I_{k_0} & B_{0,1} & B_{0,2} & 0 & 0 & 2T_{0,1} & 2T_{0,2}\\
0 & 2I_{k_1} & 2B_{1,2} & 0 & 0 & 0 & 4T_{1,2}\\
\hline
0 & S_{0,1} & S_{0,2} & I_{l_0} & A_{0,1} & A_{0,2} & A_{0,3}\\
0 & 0 & 2S_{1,2} & 0 & 2I_{l_1} & 2A_{1,2} & 2A_{1,3}\\
0 & 0 & 0 & 0 & 0 & 4I_{l_2} & 4A_{2,3}
\end{array}\right).$$

In this example, $\mathcal{C}_{2^2}$ is generated by

$$\left(\begin{array}{ccc|cccc}
I_{k_0} & B_{0,1} & B_{0,2} & 0 & 0 & 2T_{0,1} & 2T_{0,2}\\
0 & 2S_{0,1} & 2S_{0,2} & 2I_{l_0} & 2A_{0,1} & 2A_{0,2} & 2A_{0,3}\\
0 & 0 & 2S_{1,2} & 0 & 2I_{l_1} & 2A_{1,2} & 2A_{1,3}
\end{array}\right),$$

and $\mathcal{C}_2$ is generated by

$$\left(\begin{array}{ccc|cccc}
2I_{k_0} & 2B_{0,1} & 2B_{0,2} & 0 & 0 & 4T_{0,1} & 4T_{0,2}\\
0 & 2I_{k_1} & 2B_{1,2} & 0 & 0 & 0 & 4T_{1,2}\\
0 & 0 & 0 & 4I_{l_0} & 4A_{0,1} & 4A_{0,2} & 4A_{0,3}\\
0 & 0 & 0 & 0 & 4I_{l_1} & 4A_{1,2} & 4A_{1,3}\\
0 & 0 & 0 & 0 & 0 & 4I_{l_2} & 4A_{2,3}
\end{array}\right).$$

The following result relates the type and the generator polynomials of a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive code when $r=1$.

Proposition 4.8. *Let $\mathcal{C}$ be a $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic code of type $(\alpha,\beta;k_0;l_0,\dots,l_{s-1})$. Then*

- $k_0 = \alpha - \deg(\gcd(b, \frac{x^\beta-1}{a_{s-2}}l))$,
- $l_j = \deg(\hat{a}_j)$ *for* $j \in \{0,\dots,s-2\}$,
- $l_{s-1} = \deg(\hat{a}_{s-1}) + \deg(\gcd(b, \frac{x^\beta-1}{a_{s-2}}l)) - \deg(b)$.

Proof. By Theorem 4.6, it follows from the sets $A_0,\dots,A_{s-2}$ that $l_j = \deg(\hat{a}_j)$ for $j\in\{0,\dots,s-2\}$. By the definition, k_0 is the dimension of the space generated by the firsts α coordinates of B_0 and A_{s-1} that it is generated by the greatest common divisor of b and $\frac{x^\beta-1}{a_{s-2}}l$. Therefore, $k_0=\alpha-\deg(\gcd(b,\frac{x^\beta-1}{a_{s-2}}l))$. Finally, by Theorem 4.6, since $|\mathcal{C}|=p^{\deg(\hat{b})+\sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)}=p^{k_0+\sum_{j=0}^{s-1}(s-j)l_j}$ and $\deg(\hat{b})=\alpha-\deg(b)$, the following equality is straightforward

$$l_{s-1}=\deg(\hat{a}_{s-1})+\deg(\gcd(b,\frac{x^\beta-1}{a_{s-2}}l))-\deg(b).$$

□

For the general case, it is easy to prove that, for $i\in\{0,\dots,s-r-1\}$, $l_i=\deg(\hat{a}_i)$. But the computation of the remaining parameters become a really meticulous and tedious work. This is because one has to obtain the generator matrix in standard form, described in [3], as the proper linear combination of the sets B_j and A_k from Theorem 4.6.

5. Duality for cyclic codes

Let $\mathcal{C}$ be a $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic code and let $\mathcal{C}^\perp$ be the dual code of $\mathcal{C}$. Taking a vector $\mathbf{v}$ of $\mathcal{C}^\perp$, $\mathbf{u}\cdot\mathbf{v}=0$, for all $\mathbf{u}$ in $\mathcal{C}$. Since $\mathbf{u}$ belongs to $\mathcal{C}$, we know that $\mathbf{u}^{(-1)}$ is also a codeword. So, $\mathbf{u}^{(-1)}\cdot\mathbf{v}=\mathbf{u}\cdot\mathbf{v}^{(1)}=0$ for all $\mathbf{u}$ from $\mathcal{C}$, therefore $\mathbf{v}^{(1)}$ is in $\mathcal{C}^\perp$ and $\mathcal{C}^\perp$ is also a cyclic code. Consequently, we obtain the following proposition.

Proposition 5.1. *Let $\mathcal{C}\subseteq\mathbb{Z}_{p^r}^\alpha\times\mathbb{Z}_{p^s}^\beta$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then, the dual code of $\mathcal{C}$ is also a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code.*

Proposition 5.2. *Let $\mathcal{C}\subseteq\mathbb{Z}_{p^r}^\alpha\times\mathbb{Z}_{p^s}^\beta$ be a $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic code. Then,*

$$|\mathcal{C}^\perp|=p^{\sum_{i=1}^{r}i\deg(\hat{b}_i)+\sum_{j=1}^{s}j\deg(\hat{a}_j)},$$

Proof. It is well known that $|\mathbb{Z}_{p^r}^\alpha\times\mathbb{Z}_{p^s}^\beta|=|\mathcal{C}||\mathcal{C}^\perp|=p^{\alpha r+\beta s}$ and that $|\mathcal{C}^\perp|=p^l$, for some l. By Theorem 4.6, $|\mathcal{C}|=p^{\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i)+\sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)}$. Therefore,

$$\begin{aligned} l= &\ \alpha r+\beta s-\textstyle\sum_{i=0}^{r-1}(r-i)\deg(\hat{b}_i)+\sum_{j=0}^{s-1}(s-j)\deg(\hat{a}_j)\\ = &\ \textstyle\sum_{i=1}^{r}i\deg(\hat{b}_i)+\sum_{j=1}^{s}j\deg(\hat{a}_j).\end{aligned}$$

□

Finally, we exhibit a polynomial operation equivalent to the inner product of vectors, as in [6].

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. We denote the polynomial $\sum_{i=0}^{m-1}x^i$ by $\theta_m(x)$, and the least common multiple of α and β by $\mathfrak{m}$.

Definition 5.3. Let $\mathbf{u}(x)=(u(x)\mid u'(x))$ and $\mathbf{v}(x)=(v(x)\mid v'(x))$ be elements in $\mathcal{R}_{r,s}^{\alpha,\beta}$. We define the map

$$\circ:\mathcal{R}_{r,s}^{\alpha,\beta}\times\mathcal{R}_{r,s}^{\alpha,\beta}\longrightarrow\mathbb{Z}_{p^s}[x]/\langle x^{\mathfrak{m}}-1\rangle,$$

such that

$$\begin{aligned}\circ(\mathbf{u}(x),\mathbf{v}(x))=&p^{s-r}\iota(u(x)v^*(x))\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))}+\\ &+u'(x)v'^*(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))}\mod(x^{\mathfrak{m}}-1).\end{aligned}$$

The map $\circ$ is linear in each of its arguments; i.e., if we fix the first entry of the map invariant, while letting the second entry vary, then the result is a linear map. Similarly, when fixing the second entry invariant. Then, the map $\circ$ is a bilinear map between $\mathbb{Z}_{p^s}[x]$-modules.

From now on, we denote $\circ(\mathbf{u}(x), \mathbf{v}(x))$ by $\mathbf{u}(x) \circ \mathbf{v}(x)$. Note that $\mathbf{u}(x) \circ \mathbf{v}(x)$ belongs to $\mathbb{Z}_{p^s}[x]/\langle x^{\mathfrak{m}} - 1\rangle$.

Theorem 5.4. *Let $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{Z}_{p^r}^{\alpha} \times \mathbb{Z}_{p^s}^{\beta}$ with associated polynomials $\mathbf{u}(x) = (u(x) \mid u'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$, respectively. Then, $\mathbf{v}$ is orthogonal to $\mathbf{u}$ and all its shifts if and only if*

$$\mathbf{u}(x) \circ \mathbf{v}(x) = 0.$$

Proof. Let $\mathbf{u}^{(i)} = (u_{0-i}u_{1-i} \dots u_{\alpha-1-i} \mid u'_{0-i} \dots u'_{\beta-1-i})$ be the ith shift of $\mathbf{u}$. Then,

$$\mathbf{u}^{(i)} \cdot \mathbf{v} = 0 \text{ if and only if } p^{s-r} \sum_{j=0}^{\alpha-1} \iota(u_{j-i}v_j) + \sum_{k=0}^{\beta-1} u'_{k-i}v'_k = 0 \mod p^s.$$

Let $S_i = p^{s-r} \sum_{j=0}^{\alpha-1} \iota(u_{j-i}v_j) + \sum_{k=0}^{\beta-1} u'_{k-i}v'_k$. One can check the equality

$$\mathbf{u}(x) \circ \mathbf{v}(x) = p^{s-r}\theta_{\frac{\mathfrak{m}}{\alpha}}(x^{\alpha}) \left(\sum_{n=0}^{\alpha-1}\sum_{j=n}^{\alpha-1} \iota(u_{j-n}v_j)x^{\mathfrak{m}-1-n} + \sum_{n=1}^{\alpha-1}\sum_{j=n}^{\alpha-1} \iota(u_j v_{j-n})x^{\mathfrak{m}-1+n} \right)$$
$$+ \theta_{\frac{\mathfrak{m}}{\beta}}(x^{\beta}) \left(\sum_{t=0}^{\beta-1}\sum_{k=t}^{\beta-1} u'_{k-t}v'_j x^{\mathfrak{m}-1-t} + \sum_{t=1}^{\beta-1}\sum_{k=t}^{\beta-1} u'_k v'_{k-t} x^{\mathfrak{m}-1+t} \right) \mod (x^{\mathfrak{m}} - 1).$$

Then, arranging the terms one obtains

$$\mathbf{u}(x) \circ \mathbf{v}(x) = \sum_{i=0}^{\mathfrak{m}-1} S_i x^{\mathfrak{m}-1-i} \mod (x^{\mathfrak{m}} - 1).$$

Thus, $\mathbf{u}(x) \circ \mathbf{v}(x) = 0$ if and only if $S_i = 0$, for $0 \leq i \leq \mathfrak{m} - 1$. □

Theorem 5.4 shows that $\circ$ is the corresponding polynomial operation to the inner product of vectors. Finally, the following example illustrates this correspondence.

Example 5.5. *Let $\mathcal{R}_{3,9}^{4,5} = \mathbb{Z}_3^4 \times \mathbb{Z}_9^5$, then the inner product is*

$$\mathbf{u} \cdot \mathbf{v} = 3^{2-1} \sum_{i=0}^{4-1} \iota(u_i v_i) + \sum_{j=0}^{5-1} u'_j v'_j \in \mathbb{Z}_9.$$

Let $\mathbf{u} = (1,1,1,1 \mid 1,1,1,1,1)$ *and* $\mathbf{v} = (1,0,1,0 \mid 2,0,1,0,0)$. *Clearly, all the shifts of* $\mathbf{v}$ *are orthogonal to* $\mathbf{u}$. *Then,*

$$\begin{aligned}
\mathbf{u}(x) \circ \mathbf{v}(x) &= (x^3+x^2+x+1 \mid x^4+x^3+x^2+x+1) \circ (x^2+1 \mid x^3+2) \\
&= 3^{2-1}\iota\left((x^3+x^2+x+1)(x^2+1)^*\right)\theta_{\frac{20}{4}}(x^4)x^{20-1-2} \\
&+ (x^4+x^3+x^2+x+1)(x^3+2)^*\theta_{\frac{20}{5}}(x^5)x^{20-1-3} \mod (x^{20}-1) \\
&= 3(x^3+x^2+x+1)(x^2+1)\theta_5(x^4)x^{17} \\
&+ (x^4+x^3+x^2+x+1)(2x^3+1)\theta_4(x^5)x^{16} \mod (x^{20}-1) \\
&= 5x^{38}+5x^{37}+8x^{36}+4x^{18}+4x^{17}+x^{16} \mod (x^{20}-1) \\
&= 0.
\end{aligned}$$

References

[1] T. Abualrub, I. Siap and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, *IEEE Transactions on Information Theory*, **60** (2014), 1508–1514.

[2] I. Aydogdu and I. Siap, The Structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-Additive Codes: Bounds on the Minimum Distance, *Applied Mathematics & Information Sciences*, **7** (2013), 2271–2278.

[3] I. Aydogdu and I. Siap, On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, *Linear and Multilinear Algebra*,**63** (2014), 2089–2102.

[4] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, *Designs, Codes and Cryptography*, **54** (2010), 167–179.

[5] J. Borges, C. Fernández-Córdoba, and R. Ten-Valls. $\mathbb{Z}_2$-double cyclic codes. *Designs, Codes and Cryptography*, (2017), doi:10.1007/s10623-017-0334-8

[6] J. Borges, C. Fernández-Córdoba and R. Ten-Valls, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes, *IEEE Transactions on Information Theory*, **62** (2016), 6348–6354.

[7] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes and Cryptography*, **6** (1995), 21–35.

[8] H.Q. Dinh and S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, *Lecture Notes in Computer Science*, **5228** (2008), 46–55.

[9] J. Gao, M. Shi, T. Wu and F. Fu, On double cyclic codes over $\mathbb{Z}_4$, *Finite Fields and Their Applications*, **39** (2016), 233–250.

[10] P. Kanwar and S.R. López-Permouth, Cyclic Codes over the Integers Modulo p^m, *Finite Fields and their Applications*, **3** (1997), 334–352.

Received xxxx 20xx; revised xxxx 20xx.

Appendix E

On the structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes

On the Structure of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-Linear and Cyclic Codes*

Ismail Aydogdu[a]†,
Department of Mathematics
Yildiz Technical University
Istanbul, Turkey
Irfan Siap[a]‡
Istanbul, Turkey
and
Roger Ten-Valls[a]§
Department of Information and Communication Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain

February 12, 2017

Abstract

Recently some special type of mixed alphabet codes that generalize the standard codes has attracted much attention. Besides $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes are introduced as a new member of such families. In this paper, we are interested in a new family of such mixed alphabet codes, i.e., codes over $\mathbb{Z}_2\mathbb{Z}_2[u^3]$ where $\mathbb{Z}_2[u^3] = \{0, 1, u, 1+u, u^2, 1+u^2, u+u^2, 1+u+u^2\}$ is an 8-element ring with $u^3 = 0$. We study and determine the algebraic structures of linear and cyclic codes defined over this family. First, we introduce $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes and give standard forms of generator and parity-check matrices and later we present generators of both cyclic codes and their duals over $\mathbb{Z}_2\mathbb{Z}_2[u^3]$. Further, we present some examples of optimal binary codes which are obtained through Gray images of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes.

Keywords: Linear Codes, Cyclic Codes, $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-Linear Cyclic Codes, Duality.

2000 Mathematics Subject Classification: 94B05, 94B60.

*This work has been partially supported by the Spanish MEC grant TIN2013-40524-P and by the Catalan grant 2014SGR691.

†iaydogdu@yildiz.edu.tr (Ismail Aydogdu)

‡irfan.siap@gmail.com (Irfan Siap)

§roger10valls@gmail.com (Roger Ten-Valls)

1 Introduction

Linear codes over finite rings have attracted a great attention after the famous paper written by Hammons et al. in 1994 ([11]) where algebraic structures are presented for some well-known nonlinear binary codes via a Gray map. After this paper, there have been and are still many studies on codes over rings. Recently, codes over mixed alphabet rings viewed as submodules have been studied. The first of these studies is an interesting paper authored by Borges et al. (2010) presenting $\mathbb{Z}_2\mathbb{Z}_4$-additive codes as $\mathbb{Z}_4$ submodules (additive groups) of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ where α and β are positive integers [7]. Later, Aydogdu and Siap generalized these additive codes to codes over $\mathbb{Z}_2 \times \mathbb{Z}_{2^s}$ ([3]) and $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ ([4]) where r and s $(1 \leq r < s)$ are positive integers and p is prime. The mixed alphabet approach has brought other possible choices and also new directions to be explored. In one of the such studies, Aydogdu et al. have introduced $\mathbb{Z}_2\mathbb{Z}_2[u]$ codes where $\mathbb{Z}_2[u] = \{0, 1, u, 1+u\}$ and $u^2 = 0$ as submodules in [5] recently. Although, the structure of these codes is similar to the structure of codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$, these codes have some advantages compared to $\mathbb{Z}_2\mathbb{Z}_4$-additive codes. For example, the Gray images of linear codes over $\mathbb{Z}_2\mathbb{Z}_2[u]$ are also binary linear codes, however, this is not always the case for codes over $\mathbb{Z}_2\mathbb{Z}_4$. Another advantage of working over such submodules is that, the factorization of polynomials in $\mathbb{Z}_2[x]$ is also valid since $\mathbb{Z}_2$ is a subring of $\mathbb{Z}_2[u]$ and Hensel's lift is not necessary.

Recently, Abualrub et al. defined cyclic codes for $\mathbb{Z}_2\mathbb{Z}_4$-additive codes [2]. Inspired by this paper, Aydogdu et al. presented the structure of cyclic and constacyclic codes and their duals in [6].

In this paper we generalize the results of the papers [5] and [6] as $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear and cyclic codes and determine the spanning sets of both cyclic codes and their duals. We also give some examples of optimal binary codes derived from the $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes.

2 $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes

Consider the finite binary field $\mathbb{Z}_2 = \{0, 1\}$ and the finite ring $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 = \mathcal{R}_3 = \left\{0, 1, u, 1+u, u^2, 1+u^2, u+u^2, 1+u+u^2\right\}$ where $u^3 = 0$. It is clear that the ring $\mathbb{Z}_2$ is a subring of $\mathcal{R}_3$. We construct the set

$$\mathbb{Z}_2\mathcal{R}_3 = \{(v, v') \,|v \in \mathbb{Z}_2 \text{ and } v' \in \mathcal{R}_3\}.$$

This set can not be made an $\mathcal{R}_3$-submodule with respect to scalar multiplication directly. We need to define an auxiliary map

$$\begin{aligned} \eta : \mathcal{R}_3 &\to \mathbb{Z}_2 \\ \eta\left(a + ub + u^2c\right) &= a, \end{aligned} \tag{1}$$

where $\eta(0) = 0,\ \eta(1) = 1,\ \eta(u) = 0,\ \eta(1+u) = 1,\ \eta(u^2) = 0,\ \eta(1+u^2) = 1,\ \eta(u+u^2) = 0$ and $\eta(1+u+u^2) = 1$. Now, it is not difficult to show that η is a ring homomorphism. For an element $d \in \mathcal{R}_3$, define the following multiplication

$$d \cdot (v, v') = (\eta(d)v, dv').$$

This is a well-defined scalar multiplication. In fact this multiplication can be generalized over the set $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ in the following way. For any $d \in \mathcal{R}_3$ and $\mathbf{v} = (v_0, v_1, ..., v_{r-1}, v'_0, v'_1, ..., v'_{s-1}) \in \mathbb{Z}_2^r \times \mathcal{R}_3^s$ define

$$d \cdot \mathbf{v} = \left(\eta(d)v_0, \eta(d)v_1, ..., \eta(d)v_{r-1}, dv'_0, dv'_1, ..., dv'_{s-1}\right).$$

This definition leads to the following result.

Lemma 2.1. *The set $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ is an $\mathcal{R}_3$-module with respect to the scalar multiplication defined above.*

Definition 2.2. *A non-empty subset $\mathcal{C}$ of $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code if $\mathcal{C}$ is an $\mathcal{R}_3$-submodule of $\mathbb{Z}_2^r \times \mathcal{R}_3^s$.*

Definition 2.3. *We define a Gray map $\phi : \mathcal{R}_3 \to \mathbb{Z}_2^4$ as $\phi(0) = 0000$, $\phi(1) = 0101$, $\phi(u) = 0011$, $\phi(1+u) = 0110$, $\phi(u^2) = 1111$, $\phi(1+u^2) = 1010$, $\phi(u+u^2) = 1100$, and $\phi(1+u+u^2) = 1001$. It is easy to see that ϕ is a linear map. We can also generalize this Gray map for all $v = (v_0, v_1, ..., v_{r-1}) \in \mathbb{Z}_2^r$ and $v' = (v'_0, v'_1, ..., v'_{s-1}) \in \mathcal{R}_3^s$ as follows*

$$\begin{aligned} \Phi &: \mathbb{Z}_2^r \times \mathcal{R}_3^s \to \mathbb{Z}_2^n \\ \Phi(v, v') &= \left(v_0, v_1, ..., v_{r-1}, \phi(v'_0), \phi(v'_1), ..., \phi(v'_{s-1})\right). \end{aligned}$$

Hence, the binary image $\Phi(\mathcal{C}) = C$ of a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code $\mathcal{C}$ is also a linear code of length $n = r + 4s$.

2.1 Generator matrices of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes

In this subsection, we determine standard forms of generator matrices of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes whose rows consist of minimal spanning sets. First, we define the type of a code. For $v' \in \mathcal{R}_3$, v' can be written uniquely as $v' = a + ub + u^2c$ where $a, b, c \in \mathbb{Z}_2$. And also, the ring $\mathcal{R}_3$ is isomorphic to $\mathbb{Z}_2^3$ as an additive group. Therefore, if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code then it is additively isomorphic to a group of the form $\mathbb{Z}_2^{k_0} \times \mathbb{Z}_2^{3k_1} \times \mathbb{Z}_2^{2k_2} \times \mathbb{Z}_2^{k_3}$. So, under these parameters, we say that the $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code $\mathcal{C}$ is of type $(r, s; k_0; k_1, k_2, k_3)$ and hence $\mathcal{C}$ has $2^{k_0}2^{3k_1}2^{2k_2}2^{k_3}$ codewords.

Theorem 2.4. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code of type $(r, s; k_0; k_1, k_2, k_3)$. Then $\mathcal{C}$ is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code with the following standard form generator matrix*

$$G_S = \left(\begin{array}{cc|cccc} I_{k_0} & \bar{A}_{01} & 0 & 0 & 0 & u^2T_{01} \\ 0 & S_{01} & I_{k_1} & A_{01} & A_{02} + uB_{02} & A_{03} + uB_{03} + u^2C_{03} \\ 0 & S_{11} & 0 & uI_{k_2} & uA_{12} & uA_{13} + u^2B_{13} \\ 0 & 0 & 0 & 0 & u^2I_{k_3} & u^2A_{23} \end{array}\right) \quad (2)$$

where $\bar{A}_{01}, A_{01}, A_{02}, A_{03}, A_{12}, A_{13}, A_{23}, B_{02}, B_{03}, B_{13}$ and C_{03} and further S_{01}, S_{11} and T_{01} are matrices over $\mathbb{Z}_2$.

Proof. Let $\mathcal{C}_s$ be the shortened code obtained by restricting $\mathcal{C}$ to its last s coordinates. Since $\mathcal{C}_s$ is a linear code over $\mathcal{R}_3$, we can put the generator matrix of $\mathcal{C}_s$ into the following form

$$\left(\begin{array}{c|cccc} & I_{k_1} & A'_{01} & A'_{02}+uB'_{02} & A'_{03}+uB'_{03}+u^2C'_{03} \\ & 0 & uI_{k_2} & uA'_{12} & uA'_{13}+u^2B'_{13} \\ & 0 & 0 & u^2I_k & u^2A'_{23} \end{array}\right).$$

Now getting back to the original generator matrix, we have

$$\left(\begin{array}{cc|cccc} S_1 & S_2 & I_{k_1} & A'_{01} & A'_{02}+uB'_{02} & A'_{03}+uB'_{03}+u^2C'_{03} \\ S_3 & S_4 & 0 & uI_{k_2} & uA'_{12} & uA'_{13}+u^2B'_{13} \\ S_5 & S_6 & 0 & 0 & u^2I_k & u^2A'_{23} \end{array}\right)$$

where for $i \in \{1,2,3,4,5,6\}$, S_i's are matrices with entries from $\mathbb{Z}_2$. Next, by applying necessary row operations to last k_3 rows and row and column operations to the first r coordinates we can rearrange the former matrix as

$$\left(\begin{array}{cc|cccc} S'_1 & S'_2 & I_{k_1} & A''_{01} & A''_{02}+uB''_{02} & A''_{03}+uB''_{03}+u^2C''_{03} \\ S'_3 & S'_4 & 0 & uI_{k_2} & uA''_{12} & uA''_{13}+u^2B''_{13} \\ 0 & 0 & 0 & 0 & u^2I_{k_3} & u^2A''_{23} \\ I_{k_0} & S'_6 & 0 & 0 & u^2I_{k'_3} & u^2A_{24} \end{array}\right).$$

Finally, by applying the necessary row and column operations to the above matrix, we can easily obtain the standard form generator matrix in (2). □

Example 1. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code generated by the matrix*

$$G = \left(\begin{array}{ccc|cccc} 1 & 1 & 0 & u & u+u^2 & 1+u & 1+u^2 \\ 0 & 1 & 0 & 1 & u & u^2 & 0 \\ 0 & 1 & 1 & 0 & u^2 & 0 & u^2 \\ 1 & 1 & 1 & u^2 & u & u+u^2 & 0 \end{array}\right).$$

Hence, we can write the standard form of this matrix easily as follows.

$$G_S = \left(\begin{array}{ccc|cccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & u \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & u & u+u^2 \end{array}\right) \tag{3}$$

Therefore, $\mathcal{C}$ is of type $(3,4;1;2,1,0)$ and $\mathcal{C}$ has $2^1 \cdot 2^{3\cdot 2} \cdot 2^2 \cdot 2^0 = 512$ codewords.

2.2 Parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear codes

In this subsection, we give standard form of generator matrices of the dual code $\mathcal{C}^\perp$ of a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code $\mathcal{C}$. We define a new inner product for $\mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^r \times \mathcal{R}_3^s$ as

$$\mathbf{v} \cdot \mathbf{w} = u^2 \left(\sum_{i=1}^{r} v_i w_i\right) + \sum_{j=r+1}^{r+s} v_j w_j.$$

Next, with respect to this inner product, we can also define the dual code $\mathcal{C}^\perp$ in the usual way

$$\mathcal{C}^\perp = \{\mathbf{w} \in \mathbb{Z}_2^r \times \mathcal{R}_3^s \mid \mathbf{v} \cdot \mathbf{w} = 0 \; for \; all \; \mathbf{v} \in \mathcal{C}\}.$$

It is easy to prove that $\mathcal{C}^\perp$ is also a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code.

Theorem 2.5. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code with the standard form generator matrix as in (2). Then,*

$$H = \left(\begin{array}{cc|cccc} \bar{A}_{01}^t & I_{r-k_0} & & uS_{11}^t & 0 & 0 \\ T_{01}^t & 0 & P & \bar{A}_{13}^t + A_{23}^t A_{12}^t & A_{23}^t & I_{s-k_1-k_2-k_3} \\ 0 & 0 & & uA_{12}^t & uI_{k_3} & 0 \\ 0 & 0 & & u^2 I_{k_2} & 0 & 0 \end{array}\right) \tag{4}$$

is the generator matrix of the dual code $\mathcal{C}^\perp$ (the parity-check matrix of $\mathcal{C}$) where

$$P = \begin{pmatrix} u^2 S_{01}^t + uS_{11}^t A_{01}^t \\ \bar{A}_{03}^t + \bar{A}_{13}^t A_{01}^t + A_{23}^t \bar{A}_{02}^t + A_{23}^t A_{12}^t A_{01}^t \\ u\bar{A}_{02}^t + uA_{12}^t A_{01}^t \\ u^2 A_{01}^t \end{pmatrix}$$

and

$$\bar{A}_{02} = A_{02} + uB_{02},\ \bar{A}_{03} = A_{03} + uB_{03} + u^2 C_{03}, \textit{and } \bar{A}_{13} = A_{13} + uB_{13}.$$

Proof. It can be easily checked that $G_S \cdot H^T = 0$. Therefore, every row of H is orthogonal to the rows of G_S. In other words, the submodule spanned by the rows of H is a submodule of $\mathcal{C}^\perp$. The first $r - k_0$ rows of (4) are linearly independent with the others and contribute $2^{(r-k_0)}$ codewords. The other rows contribute $2^{3(s-k_1-k_2-k_3)} 2^{2k_3} 2^{k_2}$ many codewords. Since all rows are linearly independent, the subspace generated by H has cardinality $2^{(r-k_0)} 2^{3(s-k_1-k_2-k_3)} 2^{2k_3} 2^{k_2}$. Hence, $|\mathcal{C}||\mathcal{C}^\perp| = \left(2^{k_0} 2^{3k_1} 2^{2k_2} 2^{k_3}\right)\left(2^{(r-k_0)} 2^{3(s-k_1-k_2-k_3)} 2^{2k_3} 2^{k_2}\right) = 2^{r+3s}$. Consequently, the rows of the matrix H generate all dual space and hence H is in the desired matrix. □

Corollary 2.6. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code of type $(r, s; k_0; k_1, k_2, k_3)$ with generator matrix in the standard form as in (2) and let $\delta = rank(S_{11})$. Then, the dual code $\mathcal{C}^\perp$ is of type $(r, s; r - k_0 - \delta; s - k_1 - k_2 - k_3, k_3 + \delta, k_2 - \delta)$.*

Example 2. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code of type $(3, 4; 1; 2, 1, 0)$ with the generator matrix (3). Then the parity-check matrix of $\mathcal{C}$ is*

$$H_S = \left(\begin{array}{ccc|cccc} 1 & 1 & 0 & 0 & u^2 & u & 0 \\ 1 & 0 & 1 & u^2 & 0 & u & 0 \\ 0 & 0 & 0 & u & 1 & 1+u & 1 \\ 0 & 0 & 0 & 0 & 0 & u^2 & 0 \end{array}\right)$$

and therefore $\mathcal{C}^\perp$ is of type $(3, 4; 1; 1, 1, 0)$.

3 $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes

Recently, new generalizations of cyclic codes over mixed alphabet codes have been introduced. For the codes over mixed alphabet, the set of coordinates are partitioned into two subsets, such that any simultaneous cyclic shift of the coordinates of both subsets leaves the code invariant. The generators of both codes and their duals have been studied by several authors ([2, 6, 8] and [9]). Here, we introduce $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes and study their properties.

Definition 3.1. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-linear code of length $n = r + s$. $\mathcal{C}$ is called* cyclic *if*

$$(v_0, v_1, \dots, v_{r-2}, v_{r-1} \mid v'_0, v'_1, \dots, v'_{s-2}, v'_{s-1}) \in \mathcal{C}$$

implies

$$(v_{r-1}, v_0, v_1, \dots, v_{r-2} \mid v'_{s-1}, v'_0, v'_1, \dots, v'_{s-2}) \in \mathcal{C}.$$

Let $\mathbf{v} = (v_0, v_1, \dots, v_{r-2}, v_{r-1} \mid v'_0, v'_1, \dots, v'_{s-2}, v'_{s-1})$ be a codeword in $\mathcal{C}$ and i be an integer, then the ith shift of $\mathbf{v}$ is denoted by

$$\mathbf{v}^{(i)} = (v_{0-i}, v_{1-i}, \dots, v_{r-1-i} \mid v'_{0-i}, \dots, v'_{s-1-i})$$

where the subscripts are taken modulo r and s, respectively.

Let $\mathcal{C}_r$ be the canonical projection of $\mathcal{C}$ on the first r coordinates and $\mathcal{C}_s$ on the last s coordinates. Since the canonical projection is a linear map, $\mathcal{C}_r$ is a binary cyclic code of length r and $\mathcal{C}_s$ is an $\mathcal{R}_3$ cyclic code of length s. If $\mathcal{C} = \mathcal{C}_r \times \mathcal{C}_s$, then $\mathcal{C}$ is called *separable.*

There is a bijective map between $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ and $\mathbb{Z}_2[x]/(x^r - 1) \times \mathcal{R}_3[x]/(x^s - 1)$ given by

$$(v_0, v_1, \dots, v_{r-1} \mid v'_0, \dots, v'_{s-1}) \mapsto (v_0 + v_1 x + \cdots + v_{r-1}x^{r-1} \mid v'_0 + \cdots + v'_{s-1}x^{s-1}).$$

We denote the image of the vector $\mathbf{v}$ by $\mathbf{v}(x)$.

Definition 3.2. *Let $\lambda(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_t x^t \in \mathcal{R}_3[x]$ and $(p(x) \mid q(x)) \in R_{r,s} = \mathbb{Z}_2[x]/(x^r - 1) \times \mathcal{R}_3[x]/(x^s - 1)$.*

We define a scalar multiplication

$$* : \mathcal{R}_3[x] \times R_{r,s} \to R_{r,s}$$

by

$$\lambda(x) * (p(x) \mid q(x)) = \big(\eta(\lambda(x))p(x) \mid \lambda(x)q(x)\big)$$

where η is the map defined in (1) and $\eta(\lambda(x)) = \eta(\lambda_0) + \eta(\lambda_1)x + \cdots + \eta(\lambda_t)x^t$.

Therefore, $R_{r,s}$ with the scalar multiplication $*$ is an $\mathcal{R}_3[x]$-module. Let $\mathbf{v}(x) = (v(x) \mid v'(x))$ be an element of $R_{r,s}$. Note that if we multiply $\mathbf{v}(x)$ by x we get

$$\begin{aligned} x * \mathbf{v}(x) &= x * (v(x) \mid v'(x)) \\ &= (v_0 x + \cdots + v_{r-2}x^{r-1} + v_{r-1}x^r \mid v'_0 x + \cdots + v'_{s-2}x^{s-1} + v'_{s-1}x^s) \\ &= (v_{r-1} + v_0 x + \cdots + v_{r-2}x^{r-1} \mid v'_{s-1} + v'_0 x + \cdots + v'_{s-2}x^{s-1}). \end{aligned}$$

Hence, $x * \mathbf{v}(x)$ is the image of the vector $\mathbf{v}^{(1)}$. Thus, the multiplication of $\mathbf{v}(x)$ by x in $R_{r,s}$ corresponds to a shift of $\mathbf{v}$. In general, $x^i * \mathbf{v}(x) = \mathbf{v}^{(i)}(x)$ for all i.

3.1 Generator polynomials over $R_{r,s}$

In this subsection, we study submodules of $R_{r,s}$ and describe their generators and state some related results. We focus on studying a particular case where the rings $\mathbb{Z}_2[x]/(x^r - 1)$ and $\mathcal{R}_3[x]/(x^s - 1)$ are both principal ideal rings. In the sequel, we assume that s is an odd integer [1].

Also note that $\langle S \rangle$ denotes the submodule generated by a subset S of $R_{r,s}$. The following theorem plays an important role in the study of cyclic codes over $R_{r,s}$.

Theorem 3.3. *Let s be an odd integer. The $\mathcal{R}_3[x]$-module $R_{r,s}$ is a Noetherian $\mathcal{R}_3[x]$-module, and every submodule $\mathcal{C}$ of $R_{r,s}$ can be expressed by*

$$\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle,$$

where $f(x), \ell(x), g(x), a(x), a_2(x) \in \mathbb{Z}_2[x]$ with $f(x) \mid (x^r - 1)$ and $a_2(x) \mid a(x) \mid g(x) \mid (x^s - 1)$.

Proof. Let $\pi_r : R_{r,s} \to \mathbb{Z}_2[x]/(x^r - 1)$ and $\pi_s : R_{r,s} \to \mathcal{R}_3[x]/(x^s - 1)$ be the canonical projections and $\mathcal{C}$ be a submodule of $R_{r,s}$. As $\mathcal{R}_3[x]/(x^s - 1)$ is Noetherian, $\mathcal{C}_s = \pi_s(\mathcal{C})$ is finitely generated.
Define $\mathcal{C}' = \{(p(x)|q(x)) \in \mathcal{C} \mid q(x) = 0\}$. It is easy to check that $\mathcal{C}' \cong \pi_r(\mathcal{C}')$ by $(p(x) \mid 0) \mapsto p(x)$. Hence $\mathbb{Z}_2[x]/(x^r - 1)$ is Noetherian, and $\pi_r(\mathcal{C}')$ is finitely generated and so is $\mathcal{C}'$.
Let $f(x)$ be a generator of $\pi_r(\mathcal{C}')$. Then $f(x) \mid (x^r - 1)$ and $(f(x) \mid 0)$ is a generator of $\mathcal{C}'$. Let $g(x), a(x), a_2(x) \in \mathbb{Z}_2[x]$ such that $\mathcal{C}_s = \langle g(x) + ua(x) + u^2a_2(x) \rangle$. Then, $a_2(x) \mid a(x) \mid g(x) \mid (x^s - 1)$ and there exists $\ell(x) \in \mathbb{Z}_2[x]/(x^r - 1)$ such that $(\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \in \mathcal{C}$.
We claim that

$$\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle.$$

Let $(p(x) \mid q(x)) \in \mathcal{C}$. Then, $q(x) = \pi_s(p(x) \mid q(x)) \in \mathcal{C}_s$. So, there exists $\lambda(x) \in \mathcal{R}_3[x]$ such that $q(x) = \lambda(x)(g(x) + ua(x) + u^2a_2(x))$. Now,

$$(p(x) \mid q(x)) - \lambda(x) * (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) = (p(x) - \lambda(x)\ell(x) \mid 0) \in \mathcal{C}'.$$

Hence, there exists $\mu(x) \in \mathcal{R}_3[x]$ such that $(p(x) - \lambda(x)\ell(x) \mid 0) = \mu(x) * (f(x) \mid 0)$. Thus,

$$(p(x) \mid q(x)) = \mu(x) * (f(x) \mid 0) + \lambda(x) * (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)).$$

So, $\mathcal{C}$ is finitely generated by $\{f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\}$ and $R_{r,s}$ is a Noetherian $\mathcal{R}_3[x]$-module. □

From the previous results, it is clear that we can identify $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes in $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ as submodules of $R_{r,s}$. So, any submodule of $R_{r,s}$ is a cyclic code. From now on, we denote by $\mathcal{C}$ indistinctly both the code and the corresponding submodule.

Note that if $\mathcal{C}$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code with $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle$, then the canonical projection $\mathcal{C}_r$ is a binary cyclic code generated by $\gcd(f(x), \ell(x))$ and the canonical projection $\mathcal{C}_s$ is an $\mathcal{R}_3$ cyclic code generated by $g(x) + ua(x) + u^2a_2(x)$.

Proposition 3.4. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code. Then, we can assume that $\deg(\ell(x)) < \deg(f(x))$.*

Proof. Suppose that $\deg(\ell(x)) \geq \deg(f(x))$. Let $i = \deg(\ell(x)) - \deg(f(x))$ and $\mathcal{C}'$ be a code generated by

$$\mathcal{C}' = \langle (f(x) \mid 0), (\ell(x) + x^i * f(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle.$$

On one hand, $\deg(\ell(x) + x^i * f(x)) < \deg(\ell(x))$ and since the generators of $\mathcal{C}'$ belong to $\mathcal{C}$, we have $\mathcal{C}' \subseteq \mathcal{C}$. On the other hand,

$$(\ell(x) \mid g(x)+ua(x)+u^2a_2(x)) = (\ell(x)+x^i*f(x) \mid g(x)+ua(x)+u^2a_2(x))+x^i*(f(x) \mid 0).$$

Then, $\langle (\ell(x) \mid g(x)+ua(x)+u^2a_2(x)) \rangle \subseteq \mathcal{C}'$ and hence $\mathcal{C} \subseteq \mathcal{C}'$. Thus, $\mathcal{C} = \mathcal{C}'$. □

Proposition 3.5. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code. Then, $f(x) \mid \frac{x^s-1}{a_2(x)}\ell(x)$.*

Proof. Let π be the projective homomorphism of $\mathcal{R}_3[x]$-modules defined by

$$\begin{array}{rcc} \pi : \mathcal{C} & \longrightarrow & \mathcal{R}_3[x]/(x^s-1) \\ (p_1(x) \mid p_2(x)) & \longrightarrow & p_2(x). \end{array}$$

It can be easily checked that $\ker(\pi) = \langle (f(x) \mid 0) \rangle$.
Now, consider $\frac{x^s-1}{a_2(x)} * (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) = (\frac{x^s-1}{a_2(x)}\ell(x) \mid 0)$. So,

$$\frac{x^s-1}{a_2(x)} * (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \in \ker(\pi) = \langle (f(x) \mid 0) \rangle.$$

Thus, $f(x) \mid \frac{x^s-1}{a_2(x)}\ell(x)$. □

Corollary 3.6. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code. Then, $f(x) \mid \frac{x^s-1}{a_2(x)} \gcd(\ell(x), f(x))$.*

We have seen that $R_{r,s}$ is an $\mathcal{R}_3[x]$-module, and also multiplication by $x \in \mathcal{R}_3[x]$ corresponds to the right shift on $\mathbb{Z}_2^r \times \mathcal{R}_3^s$. Moreover, we know that $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ is an $\mathcal{R}_3$-module, where the operations are addition and scalar multiplication by elements of $\mathcal{R}_3$.

So, our goal is to find a set of generators for $\mathcal{C}$ as an $\mathcal{R}_3$-module. We denote $\mathcal{R}_3$-linear combinations of elements of a subset $S \subseteq R_{r,s}$ by $\langle S \rangle_{\mathcal{R}_3} = \{\sum_i \lambda_i s_i \mid \lambda_i \in \mathcal{R}_3, s_i \in S\}$, and we call a set S an $\mathcal{R}_3$-*linear independent* set if the relation $\sum_i \lambda_i s_i = \mathbf{0}$ implies that $\lambda_i s_i = 0$ for all i.

Proposition 3.7. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code such that $g(x)h(x) = x^s - 1$, $g(x) = a_0(x)a(x)$ and $a(x) = a_1(x)a_2(x)$. Define the sets*

$$\begin{aligned} S_1 = & \ \{x^i * (f(x) \mid 0)\}_{i=0}^{r-\deg(f(x))-1}, \\ S_2 = & \ \{x^i * (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\}_{i=0}^{\deg(h(x))-1}, \\ S_3 = & \ \{x^i * (\ell(x)h(x) \mid ua(x)h(x) + u^2a_2(x)h(x))\}_{i=0}^{\deg(a_0(x))-1}, \ \textit{and} \\ S_4 = & \ \{x^i * (\ell(x)h(x)a_0(x) \mid u^2a_2(x)h(x)a_0(x))\}_{i=0}^{\deg(a_1(x))-1}. \end{aligned}$$

Then, $S = S_1 \cup S_2 \cup S_3 \cup S_4$ forms a minimal generating set for $\mathcal{C}$ as an $\mathcal{R}_3$-module.

Proof. If c is a codeword of $\mathcal{C}$, then $c = q * (f \mid 0) + d * (\ell \mid g + ua + u^2a_2)$. Reasoning similarly as in [2, Theorem 13], we have $q * (f \mid 0) \in \langle S_1 \rangle_{\mathcal{R}_3}$. Now, we need to show that $d * (\ell \mid g + ua + u^2a_2) \in \langle S \rangle_{\mathcal{R}_3}$.

If $\deg(d) < \deg(h)$, then $d * (\ell \mid g + ua + u^2a_2) \in \langle S_2 \rangle_{\mathcal{R}_3}$ and $c \in \langle S \rangle_{\mathcal{R}_3}$. Otherwise, compute $d = d_0h + r_0$ with $\deg(r_0) < \deg(h)$, so $d * (\ell \mid g + ua + u^2a_2) = d_0h*(\ell \mid g+ua+u^2a_2)+r_0*(\ell \mid g+ua+u^2a_2)$ and $r_0*(\ell \mid g+ua+u^2a_2) \in \langle S_2 \rangle_{\mathcal{R}_3}$.

If $\deg(d_0) < \deg(a_0)$, then $d_0h * (\ell \mid g + ua + u^2a_2) \in \langle S_3 \rangle_{\mathcal{R}_3}$ and $c \in \langle S \rangle_{\mathcal{R}_3}$. Otherwise, compute $d_0 = d_1a_0 + r_1$ with $\deg(r_1) < \deg(a_0)$, so $d_0 * (h\ell \mid uha + u^2ha_2) = d_1a_0 * (h\ell \mid uha + u^2ha_2) + r_1 * (\ell h \mid uha + u^2ha_2)$ and $r_1 * (\ell h \mid uha + u^2ha_2) \in \langle S_3 \rangle_{\mathcal{R}_3}$.

If $\deg(d_1) < \deg(a_1)$, then $d_1ha_0 * (\ell \mid g+ua+u^2a_2) \in \langle S_4\rangle_{\mathcal{R}_3}$ and $c \in \langle S\rangle_{\mathcal{R}_3}$. Otherwise, compute $d_1 = d_2a_1 + r_2$ with $\deg(r_2) < \deg(a_1)$, so $d_1 * (ha_0\ell \mid u^2ha_0a_2) = d_2a_1 * (ha_0\ell \mid u^2ha_0a_2) + r_2 * (ha_0\ell \mid u^2ha_0a_2)$. Therefore, $r_2 * (ha_0\ell \mid u^2ha_0a_2) \in \langle S_4\rangle_{\mathcal{R}_3}$. Also, $d_2a_1 * (ha_0\ell \mid u^2ha_0a_2) = (d_2ha_0a_1\ell \mid 0)$ and by Proposition 3.5 it belongs to $\langle S_1\rangle_{\mathcal{R}_3}$. Thus, $c \in \langle S\rangle_{\mathcal{R}_3}$. □

Remark: Note that if $f = \gcd(f,\ell)$, then the code $\mathcal{C}$ is separable and hence $\ell(x) = 0$. ▮

Corollary 3.8. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code such that $g(x)h(x) = x^s - 1$, $g(x) = a_0(x)a(x)$ and $a(x) = a_1(x)a_2(x)$. Then, $|\mathcal{C}| = 2^{r-\deg(f)}8^{\deg(h)}4^{\deg(a_0)}2^{\deg(a_1)}$.*

Proposition 3.9. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code of type $(r, s; k_0; k_1, k_2, k_3)$ such that $g(x)h(x) = x^s - 1$, $g(x) = a_0(x)a(x)$ and $a(x) = a_1(x)a_2(x)$. Then, $k_0 = r - \deg(\gcd(f, a_0h\ell))$, $k_1 = \deg(h)$, $k_2 = \deg(a_0)$ and $k_3 = \deg(a_1) + \deg(\gcd(f, a_0h\ell)) - \deg(f)$.*

Proof. The parameters k_1 and k_2 are clear from Proposition 3.7. The parameter k_0 is the dimension of the space that generates the codewords of order two in the first r coordinates. Again by Proposition 3.7, it is clear that this space is generated by the polynomials f and $a_0h\ell$. Since the ring of the projection on the first r coordinates is a polynomial ring and thus a principal ideal ring, we can conclude that it is generated by the greatest common divisor of the two polynomials. Then, $k_0 = r - \deg(\gcd(f, a_0h\ell))$. Finally, since $|\mathcal{C}| = 2^{k_0}8^{k_2}4^{k_2}2^{k_3}$ and by Corollary 3.8, we have $k_3 = \deg(a_1) + \deg(\gcd(f, a_0h\ell)) - \deg(f)$. □

3.2 Duality on $R_{r,s}$

Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code and $\mathcal{C}^\perp$ be the dual code of $\mathcal{C}$. If we take an element $\mathbf{v}$ of $\mathcal{C}^\perp$, then clearly we have $\mathbf{w}\cdot\mathbf{v} = 0$ for all $\mathbf{w}$ in $\mathcal{C}$. Since $\mathbf{w}$ belongs to $\mathcal{C}$, we know that $\mathbf{w}^{(-1)}$ (the left cyclic shift by one position) is also a codeword. So, $\mathbf{w}^{(-1)} \cdot \mathbf{v} = \mathbf{w} \cdot \mathbf{v}^{(1)} = 0$ for all $\mathbf{w}$ from $\mathcal{C}$, therefore $\mathbf{v}^{(1)}$ is in $\mathcal{C}^\perp$ and $\mathcal{C}^\perp$ is also a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code. Consequently, we obtain the following proposition.

Proposition 3.10. *Let $\mathcal{C}$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code. Then, the dual code of $\mathcal{C}$ is also a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code. Furthermore*

$$\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2\bar{a}_2(x))\rangle,$$

where $\bar{f}(x), \bar{\ell}(x), \bar{g}(x), \bar{a}(x), \bar{a}_2(x) \in \mathbb{Z}_2[x]$ with $\bar{f}(x) \mid (x^r - 1)$ and $\bar{a}_2(x) \mid \bar{a}(x) \mid \bar{g}(x) \mid (x^s - 1)$.

Proposition 3.11. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code with $g = a_0a$ and $a = a_1a_2$. Then,*

$$|\mathcal{C}^\perp| = 2^{\deg(f)}8^{\deg(a_2)}4^{\deg(a_1)}2^{\deg(a_0)}.$$

Proof. Since $|\mathcal{C}||\mathcal{C}^\perp| = 2^r8^s$ and $|\mathcal{C}| = 2^{r-\deg(f)}8^{\deg(h)}4^{\deg(a_0)}2^{\deg(a_1)}$, by Corollary 3.8, the result follows immediately. □

The *reciprocal polynomial* of a polynomial $p(x)$ is $x^{\deg(p(x))}p(x^{-1})$ and is denoted by $p^*(x)$. As in the theory of binary cyclic codes, reciprocal polynomials have an important role in the duality (see [12]).

We denote the polynomial $\sum_{i=0}^{m-1} x^i$ by $\theta_m(x)$. Using this notation we give the following proposition.

Proposition 3.12. *Let $n, m \in \mathbb{N}$. Then, $x^{nm} - 1 = (x^n - 1)\theta_m(x^n)$.*

Proof. It is well known that $y^m - 1 = (y-1)\theta_m(y)$. So, we have the result by replacing y with x^n. □

From now on, $\mathfrak{m}$ denotes the least common multiple of r and s.

Definition 3.13. *Let $\mathbf{w}(x) = (w(x) \mid w'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$ be any two elements in $R_{r,s}$. Define the map*

$$\circ : R_{r,s} \times R_{r,s} \longrightarrow \mathcal{R}_3[x]/(x^{\mathfrak{m}} - 1),$$

such that

$$\begin{aligned}\circ(\mathbf{w}(x), \mathbf{v}(x)) =& u^2(w(x)\theta_{\frac{\mathfrak{m}}{r}}(x^r)x^{\mathfrak{m}-1-\deg(v(x))}v^*(x)) + \\ &+ w'(x)\theta_{\frac{\mathfrak{m}}{s}}(x^s)x^{\mathfrak{m}-1-\deg(v'(x))}v'^*(x) \mod (x^{\mathfrak{m}} - 1).\end{aligned}$$

The map $\circ$ is bilinear, i.e., if we fix the first entry of the map, while letting the second entry vary, then the result is a linear map. Similarly we have the linearity for the second component.

From now on, we denote $\circ(\mathbf{w}(x), \mathbf{v}(x))$ by $\mathbf{w}(x) \circ \mathbf{v}(x)$. Note that $\mathbf{w}(x) \circ \mathbf{v}(x) \in \mathcal{R}_3[x]/(x^{\mathfrak{m}} - 1)$.

Proposition 3.14. *Let $\mathbf{w}$ and $\mathbf{v}$ be elements in $\mathbb{Z}_2^r \times \mathcal{R}_3^s$ with associated polynomials $\mathbf{w}(x) = (w(x) \mid w'(x))$ and $\mathbf{v}(x) = (v(x) \mid v'(x))$, respectively. Then, $\mathbf{w}$ is orthogonal to $\mathbf{v}$ and all of its shifts if and only if*

$$\mathbf{w}(x) \circ \mathbf{v}(x) = 0 \mod (x^{\mathfrak{m}} - 1).$$

Proof. Let $\mathbf{v}^{(i)} = (v_{0-i}v_{1-i}\dots v_{r-1-i} \mid v'_{0-i}\dots v'_{s-1-i})$ be the ith shift of $\mathbf{v}$. Then,

$$\mathbf{w} \cdot \mathbf{v}^{(i)} = 0 \text{ if and only if } u^2 \sum_{j=0}^{r-1} w_j v_{j-i} + \sum_{k=0}^{s-1} w'_k v'_{k-i} = 0.$$

Let $S_i = u^2 \sum_{j=0}^{r-1} w_j v_{j-i} + \sum_{k=0}^{s-1} w'_k v'_{k-i}$. We see that

$$\begin{aligned}\mathbf{w}(x) \circ \mathbf{v}(x) &= u^2 \sum_{n=0}^{r-1} \left[\theta_{\frac{\mathfrak{m}}{r}}(x^r) \sum_{j=0}^{r-1} w_j v_{j-n} x^{\mathfrak{m}-1-n}\right] + \sum_{t=0}^{s-1} \left[\theta_{\frac{\mathfrak{m}}{s}}(x^s) \sum_{k=0}^{s-1} w'_k v'_{k-t} x^{\mathfrak{m}-1-t}\right] \\ &= \theta_{\frac{\mathfrak{m}}{r}}(x^r) \left[u^2 \sum_{n=0}^{r-1}\sum_{j=0}^{r-1} w_j v_{j-n} x^{\mathfrak{m}-1-n}\right] + \theta_{\frac{\mathfrak{m}}{s}}(x^s) \left[\sum_{t=0}^{s-1}\sum_{k=0}^{s-1} w'_k v'_{k-t} x^{\mathfrak{m}-1-t}\right].\end{aligned}$$

Then, by rearranging the terms we obtain

$$\mathbf{w}(x) \circ \mathbf{v}(x) = \sum_{i=0}^{\mathfrak{m}-1} S_i x^{\mathfrak{m}-1-i} \mod (x^{\mathfrak{m}} - 1).$$

Thus, $\mathbf{w}(x) \circ \mathbf{v}(x) = 0$ if and only if $S_i = 0$ for $0 \leq i \leq \mathfrak{m} - 1$. □

Now, we determine the generator polynomials of the dual in terms of the generator polynomials of the code. First we introduce two auxiliary lemmas that will be helpful to achieve our goal.

Lemma 3.15. *Let* $\mathbf{w}(x) = (w(x) \mid w'(x))$ *and* $\mathbf{v}(x) = (v(x) \mid v'(x))$ *be elements in* $R_{r,s}$ *such that* $\mathbf{w}(x) \circ \mathbf{v}(x) = 0 \mod (x^{\mathtt{m}} - 1)$*. If* $w'(x)$ *or* $v'(x)$ *equal* 0*, then* $w(x)v^*(x) = 0 \mod (x^r - 1)$*. Respectively, if* $w(x)$ *or* $v(x)$ *equal to* 0*, then* $w'(x)v'^*(x) = 0 \mod (x^s - 1)$*.*

Proof. Suppose that $w'(x)$ or $v'(x)$ equals to 0. Then,

$$\mathbf{w}(x) \circ \mathbf{v}(x) = u^2(w(x)\theta_{\frac{\mathtt{m}}{r}}(x^r)x^{\mathtt{m}-1-\deg(v(x))}v^*(x)) + 0 = 0 \mod (x^{\mathtt{m}} - 1).$$

So,

$$w(x)\theta_{\frac{\mathtt{m}}{r}}(x^r)x^{\mathtt{m}-1-\deg(v(x))}v^*(x) = \mu'(x)(x^{\mathtt{m}} - 1),$$

over $\mathbb{Z}_2[x]$ for some $\mu'(x) \in \mathbb{Z}_2[x]$. Let $\mu(x) = \mu'(x)x^{\deg(v(x))+1}$. Since $\theta_{\frac{\mathtt{m}}{r}}(x^r) = \frac{x^{\mathtt{m}}-1}{x^r-1}$ by Proposition 3.12,

$$w(x)x^{\mathtt{m}}v^*(x) = \mu(x)(x^r - 1),$$

$$w(x)v^*(x) = 0 \mod (x^r - 1).$$

The same argument can be used to prove the other case. □

Lemma 3.16. *Let* $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x)+ua(x)+u^2a_2(x))\rangle$ *be a* $\mathbb{Z}_2\mathbb{Z}_2[u^3]$*-cyclic code. Then,* $\frac{\gcd(f,a_0h\ell)}{\gcd(f,h\ell)}h\ell$ *belongs to* $\langle f, a_0h\ell\rangle$ *and* $\frac{\gcd(f,h\ell)}{\gcd(f,\ell)}\ell$ *belongs to* $\langle f, h\ell\rangle$*.*

Proof. Let $h\ell = \gcd(f, h\ell)t_1$ and $f = \gcd(f, a_0h\ell)t_2$. Then, we can write $a_0h\ell = \gcd(f, a_0h\ell)t_1t_3$ with $\gcd(t_2, t_3) = 1$. Therefore, there exist polynomials p and q such that $pt_2 + qt_3 = 1$. Thus, $\frac{\gcd(f,a_0h\ell)}{\gcd(f,h\ell)}h\ell = pt_1f + qa_0h\ell$. Similarly, it is easy to see that $\frac{\gcd(f,a_0h\ell)}{\gcd(f,h\ell)}h\ell \in \langle f, a_0h\ell\rangle$. □

Proposition 3.17. *Let* $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ *be a* $\mathbb{Z}_2\mathbb{Z}_2[u^3]$*-cyclic code and* $\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2\bar{a}_2(x))\rangle$*. Then,*

$$\bar{f}(x) = \frac{x^r - 1}{\gcd(f(x), \ell(x))^*}.$$

Proof. For all $(v \mid v') \in \mathcal{C}$, we have $(\bar{f} \mid 0) \circ (v \mid v') = 0 \mod (x^{\mathtt{m}} - 1)$. By Lemma 3.15, $(\bar{f} \mid 0) \circ (v \mid v') = 0 \mod (x^{\mathtt{m}} - 1)$ is equivalent to $\bar{f}v^* = 0 \mod (x^r - 1)$. So, clearly the generator polynomial of $(\mathcal{C}_r)^\perp$ is $\bar{f}$. Since $\mathcal{C}_r = \langle\gcd(f, \ell)\rangle$, we have

$$\bar{f} = \frac{x^r - 1}{\gcd(f, \ell)^*}.$$

□

Proposition 3.18. *Let* $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ *be a* $\mathbb{Z}_2\mathbb{Z}_2[u^3]$*-cyclic code and* $\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2\bar{a}_2(x))\rangle$*. Then,*

$$\bar{g}(x) = \frac{(x^s - 1)\gcd(f(x), \ell(x)h(x)a_0(x))^*}{f^*(x)a_2^*(x)}.$$

Proof. Since $(\ell h a_0 \mid u^2 a_2 h a_0), (0 \mid u^2 a_1 a_2^2) \in \mathcal{C}$ and $\gcd(a_1 a_2, h a_0) = 1$, there exists $p \in \mathcal{R}_3[x]$ such that $(\ell h a_0 p \mid u^2 a_2) \in \mathcal{C}$ and hence $(0 \mid \frac{f}{\gcd(f,\ell h a_0)} u^2 a_2) \in \mathcal{C}$.

We are going to compute $(\bar{\ell} \mid \bar{g} + u\bar{a} + u^2 \bar{a}_2) \circ (0 \mid \frac{f}{\gcd(f,\ell h a_0)} u^2 a_2)$. From Lemma 3.15, we have $(\bar{\ell} \mid \bar{g} + u\bar{a} + u^2 \bar{a}_2) \circ (0 \mid \frac{f}{\gcd(f,\ell h a_0)} u^2 a_2) = 0 \in \mathcal{R}_3[x]/(x^{\mathfrak{m}} - 1)$, which is equivalent to

$$\bar{g} \frac{f^* a_2^*}{\gcd(f, \ell h a_0)^*} = 0 \quad \text{over } \mathbb{Z}_2[x]/(x^s - 1).$$

Then,

$$\bar{g} = \frac{(x^s - 1)\gcd(f, \ell h a_0)^*}{f^* a_2^*}.$$

□

Proposition 3.19. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2 a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code and $\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2 \bar{a}_2(x)) \rangle$. Then,*

$$\bar{a}(x) = \frac{(x^s - 1)\gcd(f(x), \ell(x)h(x))^*}{a^*(x)\gcd(f(x), \ell(x)h(x)a_0(x))^*}.$$

Proof. It is clear that $(f \mid 0), (h\ell \mid uha + u^2 h a_2), (a_0 h \ell \mid u^2 a_0 h a_2) \in \mathcal{C}$. By Lemma 3.16, we get $(0 \mid \frac{\gcd(f, a_0 h \ell)}{\gcd(f, h\ell)}(uha + u^2 h a_2) + q u^2 a_0 h a_2) \in \mathcal{C}$, for some polynomial $q \in \mathcal{R}_3[x]$. Since $(0 \mid ug + u^2 a) \in \mathcal{C}$ and $\gcd(g, h) = 1$, we have $(0 \mid \frac{\gcd(f, a_0 h \ell)}{\gcd(f, h\ell)} ua + u^2 Q)$ for some polynomial $Q \in \mathcal{R}_3[x]$. The code $\mathcal{C}_s^\perp$ is a cyclic code over $\mathcal{R}_3$ generated by $\bar{g} + u\bar{a} + u^2 \bar{a}_2$. Then by [1, Theorem 2], there exists $\gamma \in \mathcal{R}_3[x]$ such that $\gamma(\bar{g} + u\bar{a} + u^2 \bar{a}_2) = u\bar{a}$. Hence $(\eta(\gamma)\bar{\ell} \mid u\bar{a}) \in \mathcal{C}^\perp$.

Now, we consider $(\eta(\gamma)\bar{\ell} \mid u\bar{a}) \circ (0 \mid \frac{\gcd(f, a_0 h \ell)}{\gcd(f, h\ell)} ua + u^2 Q)$. By Lemma 3.15, we obtained that $(\eta(\gamma)\bar{\ell} \mid u\bar{a}) \circ (0 \mid \frac{\gcd(f, a_0 h \ell)}{\gcd(f, h\ell)} ua + u^2 Q) = 0 \in \mathcal{R}_3[x]/(x^{\mathfrak{m}} - 1)$, which is equivalent to

$$\bar{a} \frac{\gcd(f, a_0 h \ell)^*}{\gcd(f, h\ell)^*} a^* = 0 \text{ over } \mathbb{Z}_2[x]/(x^s - 1).$$

Hence,

$$\bar{a} = \frac{(x^s - 1)\gcd(f, h\ell)^*}{\gcd(f, a_0 h \ell)^* a^*}.$$

□

Proposition 3.20. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2 a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code and $\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2 \bar{a}_2(x)) \rangle$. Then,*

$$\bar{a}_2(x) = \frac{(x^s - 1)\gcd(f(x), \ell(x))^*}{g^*(x)\gcd(f(x), \ell(x)h(x))^*}.$$

Proof. Since $(f \mid 0), (h\ell \mid uha + u^2 h a_2), (\ell \mid g + ua + u^2 a_2) \in \mathcal{C}$, by Lemma 3.16, we have $(0 \mid \frac{\gcd(f, h\ell)}{\gcd(f, \ell)} g + uQ) \in \mathcal{C}$ for some polynomial $Q \in \mathcal{R}_3[x]$. The code $\mathcal{C}_s^\perp$ is a cyclic code over $\mathcal{R}_3$ generated by $\bar{g} + u\bar{a} + u^2 \bar{a}_2$. Then by [1, Theorem 2], there exists $\gamma \in \mathcal{R}_3[x]$ such that $\gamma(\bar{g} + u\bar{a} + u^2 \bar{a}_2) = u^2 \bar{a}_2$. Then, $(\eta(\gamma)\bar{\ell} \mid u^2 \bar{a}_2) \in \mathcal{C}^\perp$.

By Lemma 3.15, we know that $(\eta(\gamma)\bar{\ell} \mid u^2\bar{a}_2) \circ (0 \mid \frac{\gcd(f,h\ell)}{\gcd(f,\ell)}g + uQ) = 0 \in \mathcal{R}_3[x]/(x^{\mathfrak{m}} - 1)$ which is equivalent to

$$\bar{a}_2 \frac{\gcd(f,h\ell)^*}{\gcd(f,\ell)^*} g^* = 0 \text{ over } \mathbb{Z}_2[x]/(x^s - 1).$$

Hence,

$$\bar{a}_2 = \frac{(x^s-1)\gcd(f,\ell)^*}{\gcd(f,h\ell)^* g^*}.$$

□

In the family of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes, there are some particular classes. For example, if the polynomials f and $\gcd(f,\ell)$ are the same, then the code is separable. Now, we consider all the cases separately and finally present the most general case for $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes.

Proposition 3.21. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x)) \rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code and $\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2\bar{a}_2(x)) \rangle$. Let $\rho = \frac{\ell}{\gcd(f,\ell)}$. Then,*

$$\begin{aligned}\bar{\ell}(x) =& \frac{x^r-1}{f^*(x)}\left(\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a_2)}\lambda_1\right.\\ &+ \frac{f^*\gcd(f,\ell h)^*}{\gcd(f,\ell h a_0)^*\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a)}\lambda_2\\ &+ \left.\frac{f^*}{\gcd(f,\ell h)^*}x^{\mathfrak{m}-\deg(g)}\lambda_3\right),\end{aligned}$$

where

$$\lambda_1 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{f^*}{\gcd(f,\ell h a_0)^*}\right).$$

$$\lambda_2 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{f^*}{\gcd(f,\ell h)^*}\right).$$

$$\lambda_3 = x^{\deg(\ell)}(\rho^*)^{-1} \mod \left(\frac{f^*}{\gcd(f,\ell)^*}\right).$$

Proof. Let $\bar{c} \in \mathcal{C}^\perp$ with $\bar{c} = (\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2)$. Then

$$\begin{aligned}\bar{c}\circ(f \mid 0) =& ((\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2))\circ(f \mid 0)\\ =& 0 + ((\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2))\circ(f \mid 0)\\ =& 0 \mod (x^{\mathfrak{m}} - 1).\end{aligned}$$

So, by Lemma 3.15,

$$\bar{\ell}f^* = 0 \mod (x^r - 1)$$

and

$$\bar{\ell} = \frac{x^r-1}{f^*}\lambda.$$

Now, we consider $(\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2) \circ \left(\frac{\gcd(f,\ell h a_0)}{\gcd(f,\ell)} * (\ell \mid g + ua + u^2a_2)\right)$. Let $t = \deg(\frac{\gcd(f,\ell h a_0)}{\gcd(f,\ell)})$. By Propositions 3.18, 3.19 and 3.20, we obtain

$$(\bar{\ell} \mid \bar{g}+u\bar{a}+u^2\bar{a}_2) \circ \left(\frac{\gcd(f,\ell h a_0)}{\gcd(f,\ell)} * (\ell \mid g+ua+u^2a_2)\right) =$$

$$u^2\frac{(x^{\mathtt{m}}-1)}{f^*}\lambda x^{\mathtt{m}-\deg(\ell)-t-1}\ell^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}$$

$$+\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h a_0)^*}{f^*a_2^*}x^{\mathtt{m}-\deg(g)-t-1}g^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*} \tag{5}$$

$$+u\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h)^*}{\gcd(f,\ell h a_0)^*a^*}x^{\mathtt{m}-\deg(g)-t-1}g^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*} \tag{6}$$

$$+u\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h a_0)^*}{f^*a_2^*}x^{\mathtt{m}-\deg(a)-t-1}a^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*} \tag{7}$$

$$+u^2\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell)^*}{\gcd(f,\ell h)^*g^*}x^{\mathtt{m}-\deg(g)-t-1}g^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*} \tag{8}$$

$$+u^2\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h)^*}{\gcd(f,\ell h a_0)^*a^*}x^{\mathtt{m}-\deg(a)-t-1}a^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*} \tag{9}$$

$$+u^2\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h a_0)^*}{f^*a_2^*}x^{\mathtt{m}-\deg(a_2)-t-1}a_2^*\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}.$$

By Corollary 3.5, we know that $f|a_1\gcd(f,\ell h a_0)$. Clearly the summands (5), (6), (7), (8), (9) are 0 modulo $x^{\mathtt{m}}-1$. Since they are orthogonal codewords we have that

$$u^2\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h a_0)^*}{f^*}\left(\lambda x^{\mathtt{m}-\deg(\ell)-1-t}\rho^* + \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathtt{m}-\deg(a_2)-1-t}\right) = 0.$$

This is equivalent, over $\mathbb{Z}_2$, to

$$\frac{(x^{\mathtt{m}}-1)\gcd(f,\ell h a_0)^*}{f^*}\left(\lambda x^{\mathtt{m}-\deg(\ell)-1-t}\rho^* + \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathtt{m}-\deg(a_2)-1-t}\right) = 0.$$

Then,

$$\left(\lambda x^{\mathtt{m}-\deg(\ell)-1-t}\rho^* + \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathtt{m}-\deg(a_2)-1-t}\right) = 0 \mod (x^{\mathtt{m}}-1), \tag{10}$$

or

$$\left(\lambda x^{\mathtt{m}-\deg(\ell)-1-t}\rho^* + \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathtt{m}-\deg(a_2)-1-t}\right) = 0 \mod \left(\frac{f^*}{\gcd(f,\ell h a_0)^*}\right). \tag{11}$$

Since $(\frac{f^*}{\gcd(f,\ell h a_0)^*})$ divides $(x^{\mathtt{m}}-1)$, we have (10) implies (11).

The greatest common divisor of $\rho = \left(\frac{(\ell)}{\gcd(f,\ell)}\right)$ and $\left(\frac{f}{\gcd(f,\ell h a_0)}\right)$ is 1, hence ρ^* has an inverse modulo $\left(\frac{f^*}{\gcd(f,\ell h a_0)^*}\right)$. Thus,

$$\lambda = \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathtt{m}-\deg(a_2)+\deg(\ell)}\left(\rho^*\right)^{-1} \mod \left(\frac{f^*}{\gcd(f,\ell h a_0)^*}\right).$$

Let $\lambda_1 = x^{\deg(\ell)}\left(\rho^*\right)^{-1} \mod \left(\frac{f^*}{\gcd(f,\ell h a_0)^*}\right)$. Then $\lambda = \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a_2)}\lambda_1 +$ λ' with $\lambda' = 0 \mod \left(\frac{f^*}{\gcd(f,\ell h a_0)^*}\right)$.

Now, we compute $(\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2) \circ \left(\frac{\gcd(f,\ell h)}{\gcd(f,\ell)} * (\ell \mid g + u\bar{a} + u^2\bar{a}_2)\right)$. Let $t = \deg\left(\frac{\gcd(f,\ell h)}{\gcd(f,\ell)}\right)$. Then,

$$\begin{aligned}
&(\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2) \circ \left(\frac{\gcd(f,\ell h)}{\gcd(f,\ell)} * (\ell \mid g + u\bar{a} + u^2\bar{a}_2)\right) = \\
&\qquad u^2\frac{(x^{\mathfrak{m}}-1)}{f^*}\left(\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a_2)}\lambda_1 + \lambda'\right)x^{\mathfrak{m}-\deg(\ell)-1-t}\ell^*\frac{\gcd(f,\ell h)^*}{\gcd(f,\ell)^*} \\
&\qquad + u^2\frac{(x^{\mathfrak{m}}-1)\gcd(f,\ell h a_0)^*}{a_2^* f^*}x^{\mathfrak{m}-\deg(a_2)-1-t}a_2^*\frac{\gcd(f,\ell h)^*}{\gcd(f,\ell)^*}
\end{aligned}$$

$$+u^2\frac{(x^{\mathfrak{m}}-1)\gcd(f,\ell h)^*}{a^*\gcd(f,\ell h a_0)^*}x^{\mathfrak{m}-\deg(a)-1-t}a^*\frac{\gcd(f,\ell h)^*}{\gcd(f,\ell)^*}. \tag{12}$$

Clearly, $u^2\frac{(x^{\mathfrak{m}}-1)}{f^*}\left(\frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a_2)}\lambda_1\right)x^{\mathfrak{m}-\deg(\ell)-1-t}\ell^*\frac{\gcd(f,\ell h)^*}{\gcd(f,\ell)^*} + (12) =$ 0. Thus, we obtain

$$u^2\frac{(x^{\mathfrak{m}}-1)\gcd(f,\ell h)^*}{f^*}\left(\lambda' x^{\mathfrak{m}-\deg(\ell)-1-t}\rho^* + \frac{f^*\gcd(f,\ell h)^*}{\gcd(f,\ell h a_0)^*\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a)-1-t}\right) = 0$$

modulo $(x^{\mathfrak{m}}-1)$. Furthermore, arguing similarly we obtain

$$\lambda' = \frac{f^*\gcd(f,\ell h)^*}{\gcd(f,\ell h a_0)^*\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a)}\lambda_2$$

where $\lambda_2 = x^{\deg(\ell)}\left(\rho^*\right)^{-1} \mod \left(\frac{f^*}{\gcd(f,\ell h)^*}\right)$. Then, $\lambda = \frac{\gcd(f,\ell h a_0)^*}{\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a_2)}\lambda_1 +$ $\frac{f^*\gcd(f,\ell h)^*}{\gcd(f,\ell h a_0)^*\gcd(f,\ell)^*}x^{\mathfrak{m}-\deg(a)}\lambda_2 + \lambda'$ with $\lambda' = 0 \mod \left(\frac{f^*}{\gcd(f,\ell h)^*}\right)$.

Finally, we consider $(\bar{\ell} \mid \bar{g} + u\bar{a} + u^2\bar{a}_2) \circ (\ell \mid g + ua + u^2a_2)$. And using a similar argument, we can get the desired results for both for λ and λ_3.

□

Proposition 3.22. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code such that $g(x)h(x) = x^s - 1$, $g(x) = a_0(x)a(x)$ and $a(x) = a_1(x)a_2(x)$. Let $(r, s; \bar{k}_0; \bar{k}_1, \bar{k}_2, \bar{k}_3)$ be the type of $\mathcal{C}^\perp$. Then, $\bar{k}_0 = \deg(\gcd(f, h\ell))$, $\bar{k}_1 = \deg(a_2) - \deg(\gcd(f, a_0h\ell)) - \deg(f)$, $\bar{k}_2 = \deg(a_1) + 2\deg(\gcd(f, a_0h\ell)) - \deg(f) - \deg(\gcd(f, h\ell))$ and $\bar{k}_3 = \deg(a_0) - \deg(\gcd(f, a_0h\ell)) + \deg(\gcd(f, h\ell))$.*

Proof. On one hand, since $\mathcal{C}^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code we know that $\bar{k}_2 = \deg(\bar{a}_0)$, by Proposition 3.9. On the other hand, by Propositions 2.6 and 3.9, we get $\bar{k}_2 = \deg(a_1) + \deg(\gcd(f, a_0h\ell)) - \deg(f) + \delta$. Computing $\bar{a}_0 = \frac{\bar{g}}{\bar{a}}$, we get $\bar{a}_0 = \left(\frac{\gcd(f,a_0h\ell)^2a_1}{\gcd(f,h\ell)f}\right)^*$. Equalizing $\bar{k}_2$'s and isolating δ, we obtain $\delta = \deg(\gcd(f, a_0h\ell)) - \deg(\gcd(f, h\ell))$. Now, the result follows from Propositions 2.6 and 3.9. □

We summarize the previous results in the next theorem.

Theorem 3.23. *Let $\mathcal{C} = \langle (f(x) \mid 0), (\ell(x) \mid g(x) + ua(x) + u^2a_2(x))\rangle$ be a $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic code and $\mathcal{C}^\perp = \langle (\bar{f}(x) \mid 0), (\bar{\ell}(x) \mid \bar{g}(x) + u\bar{a}(x) + u^2\bar{a}_2(x))\rangle$. Then,*

1. $\bar{f}(x) = \frac{x^r-1}{\gcd(f(x),\ell(x))^*}$,
2. $\bar{g}(x) = \frac{(x^s-1)\gcd(f(x),\ell(x)h(x)a_0(x))^*}{a_2^*(x)f^*(x)}$,
3. $\bar{a}(x) = \frac{(x^s-1)\gcd(f(x),\ell(x)h(x))^*}{a^*(x)\gcd(f(x),\ell(x)h(x)a_0(x))^*}$,
4. $\bar{a}_2(x) = \frac{(x^s-1)\gcd(f(x),\ell(x))^*}{g^*(x)\gcd(f(x),\ell(x)h(x))^*}$,
5. $\bar{\ell}(x) = \frac{x^r-1}{f^*(x)}\lambda(x)$, *where $\lambda(x)$ is as in Proposition 3.21.*

Moreover, $|\mathcal{C}^\perp| = 2^{\deg(f)}8^{\deg(a_2)}4^{\deg(a_1)}2^{\deg(a_0)}$.

3.3 Examples

In this subsection, we present some good examples that are obtained within this family of codes. The following table presents these examples of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes, giving the generators and the parameters r and s, whose binary images via the Gray map give optimal codes [10].

Generators	[r, s]	Binary Image
$f = x^3 - 1, \ell = x^2 + x, g = x^9 - 1, a = x^9 - 1, a_2 = x^7 + x^6 + x^4 + x^3 + x + 1$	[3, 9]	[39, 2, 26]
$f = x^3 - 1, \ell = x^2 + x + 1, g = x - 1, a = 1, a_2 = 1$	[3, 3]	[15, 8, 4]
$f = x^4 + x^3 + x^2 + 1, \ell = x^3 + x + 1, g = x - 1, a = 1, a_2 = 1$	[7, 1]	[11, 5, 4]
$f = x - 1, \ell = 0, g = x^4 + x^2 + x + 1, a = x^4 + x^2 + x + 1, a_2 = x - 1$	[1, 7]	[29, 12, 8]
$f = x^5 - 1, \ell = x^4 + x^3 + x^2 + x + 1, g = x^7 - 1, a = x^7 - 1, a_2 = x^3 + x + 1$	[5, 7]	[33, 4, 16]
$f = x^7 - 1, \ell = x^4 + x^3 + x, g = x^7 - 1, a = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, a_2 = x^3 + x^2 + 1$	[7, 7]	[35, 5, 16]
$f = x^5 - 1, \ell = x^4 + x^3 + x^2 + x + 1, g = x^{31} - 1, a = x^{31} - 1, a_2 = x^{25} + x^{22} + x^{21} + x^{17} + x^{16} + x^{15} + x^{14} + x^{11} + x^9 + x^7 + x^6 + x^4 + x^3 + x^2 + 1$	[5, 31]	[129, 6, 64]
$f = x^7 - 1, \ell = x^4 + x^3 + x^2 + 1, g = x^{21} - 1, a = x^{21} - 1, a_2 = x^{18} + x^{17} + x^{16} + x^{14} + x^{11} + x^{10} + x^9 + x^7 + x^4 + x^3 + x^2 + 1$	[7, 21]	[91, 3, 52]
$f = x^{15} - 1, \ell = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1, g = x^{15} - 1, a = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, a_2 = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$	[15, 15]	[75, 6, 36]
$f = x^{15} - 1, \ell = x^{12} + x^8 + x^7 + x^6 + x^5 + x^3 + x + 1, g = x^{15} - 1, a = x^{15} - 1, a_2 = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$	[15, 15]	[75, 4, 40]
$f = x^{15} - 1, \ell = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1, g = x^{15} - 1, a = x^{15} - 1, a_2 = x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x + 1$	[15, 15]	[75, 2, 50]

4 Conclusion

In this paper, we generalize $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes to codes over $\mathbb{Z}_2\mathbb{Z}_2[u^3]$, where $\mathbb{Z}_2[u^3] = \left\{0, 1, u, 1 + u, u^2, 1 + u^2, u + u^2, 1 + u + u^2\right\}$ is the 8-element ring with $u^3 = 0$ which are viewed as submodules. We also introduce cyclic codes and their duals over this class of codes. Furthermore, we list some optimal binary linear codes which are actually Gray images of $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes. For future research, self-dual codes over $\mathbb{Z}_2\mathbb{Z}_2[u^3]$-cyclic codes can be investigated. In this paper, the results are restricted to the parts of odd lengths. So, the general case is an open problem. And also, it will be interesting to generalize these codes to $\mathbb{Z}_2[u^r]\mathbb{Z}_2[u^s]$-cyclic codes where r and s are positive integers such that $1 \leq r \leq s$ together with a suitable Gray image.

Acknowledgement: The authors wish to thank the anonymous reviewers for their valuable remarks that led to an improved version of our paper.

References

[1] T. Abualrub and I. Siap, Cyclic codes over the rings $\mathbb{Z}_2+u\mathbb{Z}_2$ and $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2$. *Designs, Codes and Cryptography*, vol. 42(3), pp. 273-287, (2007).

[2] T. Abualrub, I. Siap and N. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. *IEEE Trans. Info. Theory*, vol. 60(3), pp. 1508-1514, (2014).

[3] I. Aydogdu and I. Siap, The Structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-Additive Codes: Bounds on the minimum distance, *Applied Mathematics and Information Sciences(AMIS)*,vol. 7(6), pp. 2271-2278, (2013).

[4] I. Aydogdu and I. Siap, On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive codes, *Linear and Multilinear Algebra*, vol. 63(10), pp. 2089-2102, (2015).

[5] I. Aydogdu, T. Abualrub, and I. Siap, On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes, *International Journal of Computer Mathematics*, Vol.92 (9), pp.1806-1814, (2015).

[6] I. Aydogdu, T. Abualrub and I. Siap, $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes, *IEEE Trans. Info. Theory*, vol.PP, no.99, pp.1-1, doi: 10.1109/TIT.2016.2632163.

[7] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator Matrices and Duality, *Designs, Codes and Cryptography*, vol. 54(2), pp. 167-179, (2010).

[8] J. Borges, C. Fernández-Córdoba and R. Ten-Valls, $\mathbb{Z}_2$-double cyclic codes, arXiv:1406.4425.

[9] J. Borges, C. Fernández-Córdoba and R. Ten-Valls, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, generator polynomials and dual codes, *IEEE Trans. Info. Theory*, vol. 62, no. 11, pp. 6348-6354, Nov. 2016.

[10] M. Grassl, Table of bounds on linear codes, http://www.codestable.de

[11] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Sole, The Z4-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, vol. 40(2), 301-319 (1994).

[12] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland Publishing Company, Amsterdam, New York, Oxford, (1975).

Appendix F

Magma package implementation

A $\mathbb{Z}_2\mathbb{Z}_4$-additive code C is cyclic if for any codeword

$$c = (a_0, \dots, a_{\alpha-1} \mid b_0, \dots, b_{\beta-1}) \in C \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta,$$

its double right cyclic shift $(a_{\alpha-1}, a_0, \dots, a_{\alpha-2} \mid b_{\beta-1}, b_0, \dots, b_{\beta-2})$ is also a codeword in C. An element $c = (a_0, \dots, a_{\alpha-1} \mid b_0, \dots, b_{\beta-1}) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ can be identified with a module element consisting of two polynomials $c(x) = (a_0 + a_1x + \cdots + a_{\alpha-1}x^{\alpha-1} \mid b_0 + b_1x + \cdots + b_{\beta-1}x^{\beta-1}) = (a(x) \mid b(x)) \in R_{\alpha,\beta}$, where $R_{\alpha,\beta} = \mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$. This identification gives a one-to-one correspondence between the elements of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and $R_{\alpha,\beta}$. Let $C(x)$ be the set of all polynomials associated to the $\mathbb{Z}_2\mathbb{Z}_4$-additive code C. A subset $C \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code if and only if the subset $C(x) \subseteq R_{\alpha,\beta}$ is a $\mathbb{Z}_4[x]$-submodule of $R_{\alpha,\beta}$. Moreover, if C is a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with β odd, then

$$C(x) = \langle (p(x) \mid 0), (l(x) \mid f(x)h(x) + 2f(x)) \rangle, \tag{F.1}$$

where $p(x), l(x) \in \mathbb{Z}_2[x]/(x^\alpha - 1)$, $\deg(l(x)) < \deg(p(x))$, $p(x) | (x^\alpha - 1)$, $f(x), h(x) \in \mathbb{Z}_4[x]/(x^\beta - 1)$ with $f(x)h(x) | (x^\beta - 1)$, and $p(x)$ divides $\frac{x^\beta - 1}{f(x)} l(x)$ a $\mathbb{Z}_2[x]$. Note that if β is even, then $x^\beta - 1$ does not factorize uniquely over $\mathbb{Z}_4[x]$.

For more information about $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, the reader is referred to [ASA14] and [BFT16a], where these codes were introduced and have been studied deeply.

Z2Z4CyclicCode(α, β, p, l, f, h)

Given two non-negative integers α and β, and four polynomials $p(x)$, $l(x)$, $f(x)$ and $h(x)$, such that $p(x)$, $l(x) \in \mathbb{Z}_2[x]$ and $f(x)$, $h(x) \in \mathbb{Z}_4[x]$, construct the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ generated by $(p(x) \mid 0)$ and $(l(x) \mid f(x)h(x) + 2f(x))$.

Z2Z4CyclicCode(α, β, a, b)

Given two non-negative integers α and β, and two polynomials $a(x) \in \mathbb{Z}_2[x]$ and $b(x) \in \mathbb{Z}_4[x]$, construct the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ generated by $(a(x) \mid b(x))$.

Z2Z4CyclicCode(α, β, G)

Given two non-negative integers α and β, and a non-empty sequence G containing r tuples of polynomials, that is $G = [< a_1(x), b_1(x) >, \dots, < a_r(x), b_r(x) >]$, where $a_i(x) \in \mathbb{Z}_2[x]$ and $b_i(x) \in \mathbb{Z}_4[x]$, for $1 \leq i \leq r$, construct the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ generated by $(a_1(x) \mid b_1(x)), \dots, (a_r(x) \mid b_r(x))$.

Z2Z4CyclicCode(α, u)

Given a non-negative integer α and a vector $u = (u_\alpha | u_\beta) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, represented as an element in $V = \mathbb{Z}_4^{\alpha+\beta}$ by changing the ones in the first α coordinates by twos, construct the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ generated by the double right cyclic shifts of the vector u. It is checked whether the elements in the first α coordinates are in $\{0, 2\}$.

Z2Z4CyclicCode(α, G)

Given a non-negative integer α and a non-empty sequence of r vectors $G = [u_1, u_2, \dots, u_r]$, where, for $1 \leq i \leq r$, $u_i \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is represented as an element in $V = \mathbb{Z}_4^{\alpha+\beta}$ by changing the ones in the first α coordinates by twos, construct the $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ generated by the double right cyclic shifts of the vectors $u_1, u_2, \dots, u_r$. It is checked whether the elements in the first α coordinates are in $\{0, 2\}$.

Example F.1.
```
> PR2<x> := PolynomialRing(Integers(2));
> PR4<y> := PolynomialRing(Integers(4));

> p := x^5+x^3+x+1;
> l := x^4+x^3+1;
> f := PR4!1;
> h := y^4+y^3+3*y^2+2*y+1;
> alpha := 15;
> beta := 7;
> C1 := Z2Z4CyclicCode(alpha, beta, p, l, f, h);
> C2 := Z2Z4CyclicCode(alpha, beta, [<p, PR4!0>, <l, f*h + 2*f>]);
> Z2Z4Equal(C1, C2);
true

> IsZ2Z4Cyclic(C1);
true

> V := RSpace(Integers(4), alpha + beta);

> g1 := V!([2*(Coefficient(PR4!p, i)) : i in [0 .. alpha - 1]]
           cat [Integers(4)!0 : j in [0 .. beta - 1]]);
> g1;
(2 2 0 2 0 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
> g2 := V!([2*(Coefficient(PR4!l, i)) : i in [0 .. alpha - 1]]
           cat [Coefficient(f*h + 2*f, j) : j in [0 .. beta - 1]]);
> g2;
(2 0 0 2 2 0 0 0 0 0 0 0 0 0 0 3 2 3 1 1 0 0)
> C3 := Z2Z4CyclicCode(alpha, [g1, g2]);
> Z2Z4Equal(C1, C3);
true

> C4 := Z2Z4CyclicCode(alpha, g1);
> C5 := Z2Z4CyclicCode(alpha, g2);
> Z2Z4Subset(C4, C3) and Z2Z4Subset(C5, C3);
true

> G := Z2Z4MinRowsGeneratorMatrix(C1);
> v := Eltseq(G[1]);
> v;
[ 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 2 ]
> u := Rotate(v[1..alpha],3) cat Rotate(v[alpha+1..alpha+beta],3);
> u;
[ 2, 2, 2, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 2, 0, 0, 0, 0 ]
> V ! u in C1‘Code;
true
```

`IsZ2Z4Cyclic(C)`

Return `true` if and only if the $\mathbb{Z}_2\mathbb{Z}_4$-additive code C is cyclic.

`Z2Z4GeneratorPolynomials(C)`

Given a $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with β odd, return a tuple containing the generator polynomials $< p(x), l(x), f(x), h(x) >$, where $p(x)$, $l(x) \in \mathbb{Z}_2[x]$ and $f(x)$, $h(x) \in \mathbb{Z}_4[x]$, described in F.1.

Example F.2.

```
> PR2<x> := PolynomialRing(Integers(2));
> PR4<y> := PolynomialRing(Integers(4));

> alpha := 15;
> beta := 7;
> U := Z2Z4AdditiveUniverseCode(alpha, beta);
> Z := Z2Z4AdditiveZeroCode(alpha, beta);
> IsZ2Z4Cyclic(U);
true
> IsZ2Z4Cyclic(Z);
true
> Z2Z4GeneratorPolynomials(U);
<1, 0, 1, 1>
> Z2Z4GeneratorPolynomials(Z);
<x^15 + 1, 0, y^7 + 3, 1>

> a1 := x^6+x^4+x^2+x;
> a2 := x^5+x^4+x;
> b1 := PR4!0;
> b2 := y^5+y^4+3*y^3+2*y^2+3*y;

> C1 := Z2Z4CyclicCode(alpha, beta, [<a1, b1>, <a2, b2>]);
> Z2Z4GeneratorPolynomials(C1);
<x^5 + x^3 + x + 1, x^4 + x^3 + 1, 1, y^4 + y^3 + 3*y^2 + 2*y + 1>

> p := x^5+x^3+x+1;
> l := x^4+x^3+1;
> f := PR4!1;
> h := y^4+y^3+3*y^2+2*y+1;
> C2 := Z2Z4CyclicCode(alpha, beta, [<p, PR4!0>, <l, f*h + 2*f>]);
> Z2Z4Equal(C1, C2);
true
```

Roger Ten Valls
Cerdanyola del Vallès, May 2017