N° d'ordre: 55/2022-C/MT

République Algérienne démocratique et populaire
Ministère de l'enseignement superieur et de la recherche scientifique
Université des sciences et de la technologie Houari Boumediene
Faculté de Mathématiques

Thèse de doctorat

Présentée pour l'obtention du grade de **Docteur**
En: Mathématiques

Spécialité: Mathématiques Fondamentales et Cryptographie

Par: Sarra TALBI

Titre

Hulls of codes over chain rings

Soutenue publiquement, le 05 /05 /2022, devant le jury composé de:

Mme. Kenza Guenda	Professeure	à l'USTHB	Présidente.
Mme. Aicha Batoul	Professeure	à l'USTHB	Directrice de thèse.
M. Edgar Martinez-Moro	Maître de conférence /A	à l'Univ. de Valladolid	Co-Directeur de thèse.
M. Bouchair Abderrahmane	Professeur	à l'Univ. de Jijel	Examinateur.
Mme. Fatiha Mamache	Maître de conférence /A	à l'USTHB	Examinatrice.
M. FOTUE TABUE Alexandre	Maître de conférence /B	à l'Univ. de Bertoua	Invité.

Hulls of codes over chain rings

Algebraic Coding theory

Sarra TALBI

Supervised by Prof. *Aicha* BATOUL

Co-supervised by Prof.*Edgar* MARTINEZ-MORO

Department of Algebra and Number Theory

Faculty of Mathematics

Houari Boumediene University of Science and Technology

2022

A Thesis submitted in partial fulfilment of the requirements for the degree of Doctorate in Mathematics.

To my parents

For inspiring me to pursue my higher studies.

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Pr. Aicha Batoul, for her consistent guidance, immense encouragement and endless support in every step throughout the process. In fact, without her effective guidance and dedicated involvement, this work would have never been carried out.

I would like to thank my co-supervisor, Dr. Edgar Martinez-Moro for his constructive and valuable advice, proper guidance, and opportunities he had provided me during my PhD program.

I wish also to extend my gratitude and appreciation to Dr. Alexandre Fotue Tabue for his help, advice, support and encouragement.

I am extremely grateful to my doctoral committee members, Pr. Kenza Guenda, Dr. Fatiha Mamache, Pr. Bouchair Abderrahmane and Dr.Fotue Tabue Alexandre for their valuable time, effort and observation.

I am very grateful for the endless and priceless support that I received from my family. Specifically, my parents, my sisters , my brothers, my nephews and my nieces.

Finally, I could not have completed this dissertation without the support of my friends, Ranya Djihad Boulanouar, Amel, Sabira and Anfal, who provided stimulating discussions as well as happy distractions to rest my mind outside of my research.

Abstract

In this thesis, we recalled some basic consents and key results on cyclic codes over finite fields and rings, we gave the characterization of the hull of cyclic codes in terms of their generator polynomials with respect to the Euclidean inner product over finite fields and rings. We discussed respectively about the type of the hulls of cyclic codes over $\mathbb{F}_q$ and $\mathbb{Z}_{p^2}$ and we gave a formula of the average q-dimensions of the hull of cyclic codes over a finite chain ring of parameters (p,r,a,e,r) where $q = p^r$. We generalized the notion of the hull of cyclic code over over $\mathbb{F}_q$ and $\mathbb{Z}_{p^2}$ to a finite chain ring R. Moreover, we explored some properties of hulls of cyclic serial codes over a finite chain ring. As special cases, we gave some results about LCD and self orthogonal codes. We provided an algorithm for computing all the possible parameters of the Euclidean hulls of those codes and we gave an expression of the set $\aleph(n,s,q)$ of q-dimensions of the Euclidean hulls of cyclic serial codes of length n over R. We determined the number $\wp(n,\tau;R)$ of cyclic serial codes of length R over finite chain rings having hulls of a given q-dimension. Finally, we established an alternative simpler expression of $\mathbb{E}_R(n)$, the average q-dimensions of the Euclidean hulls of cyclic serial codes over finite chain rings with its upper and lower bounds. We showed that $\mathbb{E}_R(n)$, grows at the same rate with ns as s and n is coprime with p.

Keywords: Finite chain rings; Cyclotomic cosets; Cyclic codes; Hull of a code; Parameters of the hull of a code; The average q-dimension.

Résumé

Dans cette thèse, nous avons rappelé quelques notions de base et résultats clés sur les codes cycliques sur les corps finis et les anneaux, nous avons donné la caractérisation du hull des codes cycliques en fonction de leur polynôme générateur par rapport au produit scalaire euclidien. Nous avons discuté respectivement sur le type du hull des codes cycliques sur $\mathbb{F}_q$ et $\mathbb{Z}_{p^2}$ et nous avons donné une formule de la dimensions moyennes du hull des codes cycliques sur les anneaux de chaîne finie de paramètres (p,r,a,e,r) ou $q = p^r$. Nous avons généralisé la notion du hull des codes cycliques sur $\mathbb{F}_q$ et $\mathbb{Z}_{p^2}$ aux anneaux de chaîne finie R. De plus, nous avons exploré certaines propriétés du hull des codes cycliques sériels sur les anneaux de chaîne finie. Comme cas particuliers, nous avons donné quelques résultats sur les codes LCD et auto orthogonaux. Nous avons fourni un algorithme pour calculer tous les paramètres possibles du hull euclidien de ces codes et nous avons donné une expression de l'ensemble des q-dimensions du hull euclidien des codes cycliques sériels de longueur n sur R. . Nous avons déterminé le nombre $\wp(n,\tau;R)$ des codes cycliques sériels de longueur n sur des anneaux de chaîne finis ayant des dimensions du hull donnée. Enfin, nous avons établi une expression alternative plus simple de $\mathbb{E}_R(n)$, the q-dimensions moyennes du hull euclidien des codes cycliques sériels les anneaux de chaîne finis avec ses bornes supérieure et inférieure. Nous avons montré que $\mathbb{E}_R(n)$ croît au même rythme avec ns, n et s sont premiers avec p .

Mots clés: Anneaux finis de chaîne, Classes cyclotomiques, Codes cycliques, Hull d'un code, Paramètres du hull d'un code, La dimension moyenne.

Contents

List of Figures

List of Algorithms

*

1

Introduction

Error correction is an important aspect of classical information processing that protects the classical bits against errors, similarly.

1.1 | Toward codes over finite rings

The theory of error-correcting codes has historically been most useful in the context of linear codes. Such codes may be viewed as vector spaces over finite fields carrying with them many familiar and well-studied properties. A generalization of finite fields is the concept of finite rings. It is therefore natural to consider codes over finite rings to study which properties such codes maintain in the move to a more general setting. Codes over rings started being of interest to many researchers since the appearance of [15; 25], where it was shown that the binary non-linear codes known as Kerdock and Preparata codes are actually dual codes when viewed as codes over $\mathbb{Z}_4$, via the Gray map. So the most natural class of ring that is suitable for coding theory is given by finite chain rings as it allow to formulate the dual code similar to finite fields. So it is worth to delve into codes over finite chain rings.

1.2 | Review of litterature

The class of cyclic codes is one of the most studied class of linear codes. The algebraic structure of cyclic codes makes easier their implementation, for this reason

many practically important codes are cyclic. The theory of cyclic codes over rings have been studied in a series of papers (see [10; 11; 13; 24; 27]). In particular, Dinh and Permouth [10] gave the algebraic structure of simple root cyclic codes over finite chain rings R. Martínez and Rúa [24] generalized these results to multivariable cyclic codes. Free cyclic serial codes have been determined by using cyclotomic cosets and trace map over finite chain rings by Fotue and Mouaha in [11].

The Euclidean hull is defined to be the intersection of a code and its Euclidean dual. It was originally introduced by Assume and Key [1] to classify finite projective planes. Knowing the hull of a linear code is a key point to determine the complexity of some algorithms for investigating permutations of two linear codes and computing the automorphism group of the code, see [21; 28; 31]. In general, those algorithms have been proved to be very effective if the size of the Euclidean hull is small. In the case of codes over finite fields, Sendrier [32] established the number of linear codes of length n with a fix dimension Euclidean hull, also Skersys [34] discussed the average dimension of the Euclidean hull of cyclic codes. Later, Sangwisut et al. [33] determined the dimension of the Euclidean hull of cyclic and negacyclic codes of length n over a finite field. Furthermore, Jitman and Sangwisut [16] gave the average Euclidean hull dimension of negacyclic codes over a finite field. Recently, the concept of the Euclidean hulls has been generalized to cyclic codes of odd length over $\mathbb{Z}_4$ by Jitman et al. [17] where the authors provided an algorithm to determine the type of the Euclidean hull of cyclic codes over $\mathbb{Z}_4$.

1.3 | Motivation and problem

Based on the above survey, one must be agreed that these works motivate us to study the Galois hulls of cyclic codes over finite chain rings.

The main goal of this thesis is to study the Galois hulls of cyclic codes of length n over a finite chain ring R, such that n and p are coprime. This is the serial case stated in [24], i.e. The cyclic codes over R whose length n is coprime with p are serial modules over R. We will generalize the techniques used in [17] to obtain the parameters and the average q-dimensions of the Euclidean hull of cyclic serial codes over finite chain rings.

- Problem 1 : Generalize the notion of the hull of cyclic code over $\mathbb{F}_q$ and $\mathbb{Z}_4$ to a finite chain ring R.
- Problem 2 : Find a formula of the average q-dimensions of the Euclidean hulls of cyclic serial codes over finite chain rings R with its upper and lower bounds.

1.4 | Outline of thesis

A brief outline of the structure of this thesis is given below.

Chapter 1 is introduction.

In **Chapter 2**, we include basic concepts and definitions of classical coding theory over finite field and over a more general algebraic structure, finite rings.

In **Chapter 3**, We includes some basic definitions of cyclic codes and the dual of cyclic codes over finite field. We review some known results on the hulls of cyclic codes over finite fields.

In **Chapter 4**, We discuss about the characterization of the hull of cyclic codes over the finite ring $\mathbb{Z}_{p^2}$, the ring of integers modulo p^2 where $p$is a prime. We derive The average p-dimension of the hull of cyclic codes of length n over $\mathbb{Z}_{p^2}$.

Chapter 5, is the core of this thesis, we characterize Galois hulls of cyclic serial code over finite chain rings. We show the parameters and the q-dimensions of the Euclidean hull of cyclic serial codes. Finally, the average dimension of the Euclidean hull of cyclic serial codes is derived with its upper and lower bound.

Finally, **Chapter 6** concludes the thesis and proposes a few doable open directions for future investigation.

2

Preliminaries

2.1 | Error correcting codes

The theory of error-correcting codes and more broadly, information theory, originated in Claude Shannon monumental work " A mathematical theory of communication ", published in 1948 [36], he showed that the goal of finding error correcting codes that allowed for a high probability of successful transmission was attainable. Shannon defined of each channel a constant associated with it, called the channel capacity and he showed that reliable transmission at a rate bellow capacity is possible. More precisely, his channel coding theorem asserts that there exist error correcting codes that achieve successful transmission with probability arbitrarily close to 1, with the rate of the code arbitrarily close and below the channel capacity. Since then, with the development of new technologies for data communications and data storage, coding theory has become an active subject of research in different areas of knowledge such as mathematics, computer science, electrical engineering and others. Coding theory is used in order to improve the trustworthiness of the transmission of information over noisy channels. A representation of the transmission of information using coding theory is described in Figure 2.1. Suppose a source wants to send a message to a receiver. The message, which we usually assume to be a sequence of elements of a field or a ring, is encoded by adding redundancy. We call the encoded message a codeword and the set of codewords form the code. The codeword is transmitted over a channel that is subject to noise. This means, that it is possible that the symbols of the codeword are changed, and we call the changed

symbols errors. The decoder receives the possibly altered codeword and uses the redundancy to detect and correct errors. If possible, the decoder then determines which codeword has most likely been sent. If the decoder detects an error but is unable to correct it, then the decoder lets the source know that the message had been altered. An encoder can be described using an injective map, so if there is a codeword that is closest to the received word, the message can be retrieved and given to the receiver.

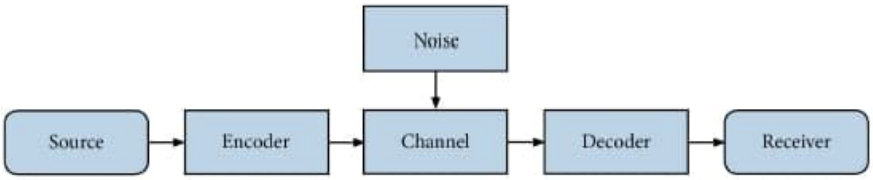

Figure 2.1: Block diagram of a communication system.

We give a small example of a well-known encoding map: Assume the symbols of our message are in $\mathbb{F}_2$, the finite field of two elements 0 and 1; the source wants to send the message 101. Assume further that in this encoding scheme the redundancy is given by adding a 0 or a 1 to our message, depending on whether we have an odd or an even number of 1's in the word. This way our code consists of words with an even number of 1's. So 101 will be encoded as 1010. Suppose the codeword is transmitted over a noisy channel and is changed to 1000. Then the decoder knows that an error has occurred, because a word with an odd number of 1's was received. The decoder detects the error and lets the transmitter know that received message was altered.

Given an alphabet $\mathscr{A}$ with q symbols, a block code C of length n over the alphabet $\mathscr{A}$ is simply a subset of $\mathscr{A}^n$. The q-ary ro-tuples from C are called the codewords of the code C. It is known that good codes are those who have the power to eliminate maximum errors. Towards this, an important notion is a minimum distance of the code which can correctly point out the maximum error-correcting capability. The minimum distance of a code C or equivalently the least Hamming distance between any two distinct codewords (number of places where they differ). A code having minimum distance d can detect up to $d-1$ places and correct

up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ places of errors. Thus the minimum distance determines the error-correcting capability, therefore, to find out good codes we need to search codes of larger minimum distance.

2.2 | Linear codes

In coding theory, a linear code is an error-correcting code for which any linear combination of codewords is also a codeword. In this section, we give some basics on linear block codes (see [14] and [25] for more information on linear block codes).

2.2.1 | Linear codes over finite fields

Let $\mathbb{F}_q$ be the finite field with q elements.

Definition 2.2.1. *A q-ary linear block code C is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. If the dimension of C as a vector space over $\mathbb{F}_q$ is k, we say C is of length n and of dimension k and we denote C an $[n,k]_q$-linear code. The elements of C are called codewords.*

Definition 2.2.2. *Let $\boldsymbol{x} = (x_1, \cdots, x_n)$ and $\boldsymbol{y} = (y_1, \cdots, y_n)$ be vectors in $\mathbb{F}_q^n$. The Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined as*

$$d_H(\boldsymbol{x}, \boldsymbol{y}) = |\{i \in 1, \cdots, n \,:\, x_i \neq y_i\}|.$$

Definition 2.2.3. *The minimum distance of an $[n,k]_q$-linear code, denoted by $d(C)$, is the minimum among all the Hamming distances between any two distinct codewords, i.e.*

$$d(C) = \min\{d_H(\boldsymbol{x}, \boldsymbol{y}) \,:\, (\boldsymbol{x}, \boldsymbol{y}) \in C^2, \boldsymbol{x} \neq \boldsymbol{y}\}.$$

If C has minimum distance d, then we refer to the code as an $[n,k,d]$ linear code over $\mathbb{F}_q$.

Definition 2.2.4. *The weight of a vector $\boldsymbol{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$ is defined to be the number of non-zero positions of x, i.e.*

$$wt(x) = |\{i \in 1, \cdots, n | x_i \neq 0\}|.$$

A natural upper bound on the minimum distance is given by the following:

Lemma 2.2.1. *Let C be an $[n,k]_q$-linear code of minimum distance $d(C)$. Then the distance is the minimum possible weight of the non-zero codewords, i.e.*

$$d(C) = \min\{wt(\boldsymbol{x}) : \boldsymbol{x} \in C, \boldsymbol{x} \neq 0\}.$$

Theorem 1. *If C is an $[n,k,d]$-code then $d \leq n-k+1$, moreover, codes which meet the Singleton bound are called maximum distance separable (MDS).*

For an $[n,k]_q$-linear code C, we define a generator matrix G of the code C to be a $k \times n$ matrix of rank k over $\mathbb{F}_q$ whose rows form a basis of C. Another way to describe this linear subspace is through a kernel representation. Indeed, an $(n-k) \times n$ matrix H over $\mathbb{F}_q$, such that $c \in C$ if and only if $H.x^\top = 0$, is called a parity-check matrix of C. In general, G and H are not unique due to the fact that one can write many different bases for a subspace.
We can describe an $[n,k]_q$-linear code C with generator matrix G and parity-check matrix H in the following two ways.

$$C = \{\mathbf{c} \in \mathbb{F}_q^n : H\mathbf{x}^\top = 0\} = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\}$$

Since the code is defined as the kernel of H and also as the image of G we have

$$HG^\top = 0 \text{ and } GH^\top = 0.$$

Proposition 2.2.1. *Let C be an $[n,k]_q$-linear code with parity-check matrix H. Then C has minimum distance $d(C) = d$ if and only if every set of $d-1$ columns of H are linearly independent and there exist d columns of H which are linearly dependent.*

Theorem 2. *If $G = [I_k|A]$ is a generator matrix for the $[n,k]_q$ code C in standard form, then $H = [-A^\top|I_{n-k}]$ is a parity check matrix for C.*

Definition 2.2.5. *Let C be a linear code of length n over $\mathbb{F}_q$. The dual code of C, denoted $C^\perp$, is the code*

$$C^\perp = \{\boldsymbol{x} \in \mathbb{F}_q^n : \boldsymbol{x} \cdot \boldsymbol{c} = 0 \quad \text{for all} \quad \boldsymbol{c} \in C\}$$

where, the usual inner product is denoted by $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_n y_n$ for $(\boldsymbol{x}, \boldsymbol{y}) \in \left(\mathbb{F}_q^n\right)^2$.

Lemma 2.2.2. *If C is an $[n,k]$ linear code, then its dual $C^\perp$ is an $[n,n-k]$ linear code and $(C^\perp)^\perp = C$. Moreover, a parity check matrix of C is a generator matrix for the dual code $C^\perp$.*

If $C \cap C^\perp$ then C is called self orthogonal and, if $C = C^\perp$, then C is called self dual.

Definition 2.2.6. *The hull of a linear code C is defined to be the intersection of the code with its dual. We will denote by $\mathscr{H}(C) = C \cap C^\perp$ the hull of a code C.*

2.2.2 | Finite chain rings

For an account on the results on finite rings in this section check [23]. Throughout this thesis, p is a prime number, a, e, r, s are positive integers and $\mathbb{Z}_{p^a}$ is the residue ring of integers modulo p^a. R will denote a finite commutative chain ring of characteristic p^a, of nilpotency index s, and of residue field $\mathbb{F}_q$ (where $q = p^r$). We will denote its maximal ideal by $\mathtt{J}(R)$ and $R^\times$ will denote its multiplicative group. Note that since R is a chain ring it is a principal ideal ring, thus we will denote as θ a generator of $\mathtt{J}(R)$ and the ideals of R form a chain under inclusion $\{0\} = \mathtt{J}(R)^s \subsetneq \mathtt{J}(R)^{s-1} \subsetneq \cdots \subsetneq \mathtt{J}(R) \subsetneq R$ and $\mathtt{J}(R) = \theta^t R$ for $0 \leq t < s$.

The ring epimorphism $\pi : R \to R/\mathtt{J}(R) \simeq \mathbb{F}_q$ naturally extends a ring epimorphism from $R[X]$ to $\mathbb{F}_{p^r}[X]$ and on the other hand it naturally induces an R-module epimorphism from R^n to $(\mathbb{F}_{p^r})^n$. As an abuse of notation we will denote both mappings by π.

A monic polynomial f is *basic-irreducible* over R if $\pi(f)$ is irreducible over $\mathbb{F}_{p^r}$. We will denote by $\mathtt{GR}(p^a, r)$ the *Galois ring* of characteristic p^a and cardinality p^{ra}. It is well known that, for a given finite chain ring R there is a 5-tuple (p, a, r, e, s) of positive integers, the so-called parameters of R, such that $R = \mathtt{GR}(p^a, r)[\theta]$, and $\langle\theta\rangle = \mathtt{J}(R)$, $\theta^e \in p(\mathbb{Z}_{p^a}[\theta])^\times$ and $\theta^{s-1} \neq \theta^s = 0_R$. From now on, we will denote as S_d the subring of R such that $S_d := \mathtt{GR}(p^a, d)[\theta]$ and d is a divisor of r. The *Teichmller set* of R will be denoted as $\Gamma(R)$ and it is defined as $\Gamma(R) = \{0\} \cup \{a \in R : a^{p^r-2} \neq a^{p^r-1} = 1\}$. It is the only cyclic subgroup of $R^\times$ isomorphic to the multiplicative group of $\mathbb{F}_{p^r}$. For each element a in R, there is a unique $(a_0, a_1, \cdots, a_{s-1})$ in $\Gamma(R)^s$ such that $a = a_0 + a_1\theta + \cdots + a_{s-1}\theta^{s-1}$.

Let R and S be two finite commutative chain rings, we say that R is an extension of S and we denote it by $S|R$ if $S \subset R$ and $1_R = 1_S$. We say that the extension is separable if $\mathtt{J}(S)R = \mathtt{J}(R)$. The Galois group of the extension $S|R$, denoted $\mathtt{Aut}_S(R)$, is the group of all the automorphisms γ of R whose restriction $\gamma_{|S}$ of γ to S, is the identity map of R. A separable extension is called Galois if $\{r \in R : (\forall \gamma \in \mathtt{Aut}_S(R))(\gamma(r) = r)\} = S$. This condition is equivalent to the condition R is ring-isomorphic to $S[X]/\langle f \rangle$, where f is a monic basic irreducible polynomial in $S[X]$, see [40, Section 4][23, Theorem XIV.8].

Let d be positive divisor of r, and let us consider $S = \mathbb{Z}_{p^a}[\theta]$, $R = \mathtt{GR}(p^a, r)[\theta]$, $S_d = \mathtt{GR}(p^a, d)[\theta]$, and

$$\mathtt{GSub}(S|R) := \{S_d : d \text{ is a divisor of } r \text{ and } \mathbb{Z}_{p^a}[\theta] \subseteq S_d\}.$$

It is well known that $\mathtt{Aut}_S(R)$ is a cyclic group generated by the *Frobenius automorphism* $\sigma : R \to R$ given by : $\sigma\left(\sum_{t=0}^{s-1} a_t \theta^t\right) = \sum_{t=0}^{s-1} a_t^p \theta^t$, and therefore, the set $\mathtt{Sub}(\mathtt{Aut}_S(R))$ of subgroups of $\mathtt{Aut}_S(R)$ is given by

$$\mathtt{Sub}(\mathtt{Aut}_S(R)) = \{\langle \sigma^d \rangle : d \text{ is a divisor of } r\}.$$

In [11], $\mathtt{GSub}(R)$, the authors established the Galois correspondence $(\mathtt{Stab};\mathtt{Fix})$ between $\mathtt{GSub}(S|R)$ and $\mathtt{Sub}(\mathtt{Aut}_S(R))$ as follows $\mathtt{Stab} : \mathtt{GSub}(S|R) \to \mathtt{Sub}(\mathtt{Aut}_S(R))$ and $\mathtt{Fix} : \mathtt{Sub}(\mathtt{Aut}_S(R)) \to \mathtt{GSub}(S|R)$ where $\mathtt{Stab}(S_d) = \langle \sigma^d \rangle$ and $\mathtt{Fix}(\langle \sigma^d \rangle) = S_d$, where d is a divisor of r (recall that $q = p^r$).

Given a divisor d of r, from [23, Theorem XV.2], σ^d is the only automorphism in $\mathtt{Aut}_S(R)$ such that $\overline{\sigma}^d \circ \pi = \pi \circ \sigma^d$, where $\overline{\sigma}$ is a generator of $\mathtt{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^r})$. The trace map $\mathtt{T}_d : S \to S_d$ of the ring extension $R|S_d$ is defined by $\mathtt{T}_d := \sum_{i=0}^{\frac{r}{d}-1} \sigma^{id}$, and the the trace map $\overline{\mathtt{T}}_d : \mathbb{F}_{p^r} \to \mathbb{F}_{p^d}$ of the field extension $\mathbb{F}_{p^r}|\mathbb{F}_{p^d}$ is defined by $\overline{\mathtt{T}}_d := \sum_{i=0}^{\frac{r}{d}-1} \overline{\sigma}^{id}$. It is well known that $\mathtt{T}_d : R \to S_q$ is an epimorphism of S_d-modules and $\overline{\mathtt{T}}_d : \mathbb{F}_{p^d} \to \mathbb{F}_{p^r}$ is an epimorphism of vector spaces over $\mathbb{F}_{p^d}$. Hence, for any divisor d of r, the following diagram commutes.

$$\begin{array}{ccccc} R & \xrightarrow{\sigma^d} & R & \xrightarrow{\mathtt{T}_d} & S_d \\ \pi\downarrow & & \pi\downarrow & & \downarrow\pi \\ \mathbb{F}_{p^r} & \xrightarrow{\overline{\sigma}^d} & \mathbb{F}_{p^r} & \xrightarrow{\overline{\mathtt{T}}_d} & \mathbb{F}_{p^d} \end{array}$$

2.2.3 | Codes over finite chain ring

A *linear code* C of length n over a ring R, is a submodule of the R-module R^n. We will denote by $\{\mathbf{0}\}$, the zero-submodule where $\mathbf{0} = (0,0,\ldots,0) \in R^n$. A linear code C over R is free if, $C \cong R^k$ as R-modules for some positive integer k. The residue code of a linear code C over R is the linear code $\pi(C)$ over $\mathbb{F}_q$, where

$$\pi(C) = \{(\pi(c_0), \pi(c_1), \cdots, \pi(c_{n-1}) : (c_0, c_1, \cdots, c_{n-1}) \in C\}.$$

In [11], the authors introduced the Galois closure of a linear code C over R of length n as follows, $\mathtt{Cl}_d(C) = \mathtt{Ext}(\mathtt{T}_d(C))$, where $\mathtt{Ext}(\mathtt{T}_d(C))$ is the linear code over R of all R-combinations of codewords in the linear code $\mathtt{T}_d(C)$ over S_d. A linear code C over R is $\langle\sigma^d\rangle$-invariant, if $\sigma^d(C) = C$, where d is a divisor of r. Recall that for any linear code C over R of length n, its subring subcode is given by $\mathtt{Res}_d(C) = C \cap (S_d)^n$. In [11], it is shown that any linear code C over R is $\langle\sigma^d\rangle$-invariant, if and only if, $\mathtt{T}_d(C) = \mathtt{Res}_d(C)$ if and only if, $C = \mathtt{Ext}(\mathtt{Res}_d(C))$. For $\ell \in \{0,1,\ldots,r-1\}$ we equip R^n with the ℓ-Galois inner-product defined as follows:

$$\langle \mathbf{u}, \mathbf{v} \rangle_\ell = \sum_{j=0}^{n-1} u_j \sigma^\ell(v_j), \quad \text{for all } \mathbf{u}, \mathbf{v} \in R^n.$$

When $\ell = 0$ it is just the usual Euclidean inner-product and if r is even and $r = 2\ell$ it is the Hermitian inner-product. The ℓ-Galois dual of a linear code C over R of length n, denoted $C^{\perp_\ell}$, is defined to be the linear code

$$C^{\perp_\ell} = \{\mathbf{u} \in R^n \ : \ \langle \mathbf{u}, \mathbf{c} \rangle_\ell = 0_R \text{ for all } \mathbf{c} \in C\}.$$

If $C \subseteq C^{\perp_\ell}$, then C is ℓ-Galois *self-orthogonal*. Moreover, C is ℓ-Galois self-dual if, $C = C^{\perp_\ell}$. The two statements in Proposition 2.2.3 below follow immediately from the identity

$$\langle \mathbf{u}, \mathbf{v} \rangle_\ell = \langle \mathbf{u}, \sigma^h(\mathbf{v}) \rangle_{\ell-h} = \sigma^h\big(\langle \sigma^{\ell-h}(\mathbf{v}), \mathbf{u} \rangle_{r-h}\big), \text{ for all } 0 \le h \le \ell, \mathbf{u}, \mathbf{v} \in R^n$$

where the action is taken componentwise $\sigma^\ell(\mathbf{v}) = (\sigma^\ell(v_0), \cdots, \sigma^\ell(v_{n-1}))$. The following proposition is a generalized Delsarte's Theorem.

Proposition 2.2.2. *[11, Theorem 3.3] Let C be a linear code over R of length n. Then for any $\ell \in \{0,1,\ldots,r-1\}$, $\mathtt{T}_d(C^{\perp_\ell}) = (\mathtt{Res}_d(C))^{\perp_\ell}$.*

Also [20, Proposition 2.2] has a natural generalization to finite chain rings.

Proposition 2.2.3. *Let C be a linear code over R of length n. Then*

1. $\left(\sigma^h(C)\right)^{\perp_\ell} = \sigma^h(C^{\perp_\ell})$, *and* $C^{\perp_\ell} = \sigma^h(C^{\perp_{\ell-h}})$, *for any* $0 \le h \le \ell$;
2. $(C^{\perp_\ell})^{\perp_h} = \sigma^{2r-\ell-h}(C)$, *for all* $0 \le \ell, h \le r-1$.

From Proposition 2.2.3 and [13, Theorem 3.1], we obtain the following result.

Corollary 1. *Let C and C' be linear codes over R of length n. Then*

1. $(C + C')^{\perp_\ell} = C^{\perp_\ell} \cap C'^{\perp_\ell}$;
2. $(C \cap C')^{\perp_\ell} = C^{\perp_\ell} + C'^{\perp_\ell}$.

Definition 2.2.7. *Let C be a linear code over R. The* ℓ-Galois hull *of C will be denoted as $\mathscr{H}_\ell(C)$, is the intersection of C and its ℓ-Galois dual, that is,*

$$\mathscr{H}_\ell(C) = C \cap C^{\perp_\ell}.$$

A linear code C over R is *ℓ-Galois Linear Complementary Dual* (Shortly, Galois LCD) if $\mathscr{H}_\ell(C) = \{\mathbf{0}\}$, and C is *ℓ-Galois self-orthogonal* if $\mathscr{H}_\ell(C) = C$. If we denote that for all $0 \le \ell; h \le r-1$, we have $\sigma^h(\mathscr{H}_\ell(C)) = \mathscr{H}_\ell(\sigma^h(C))$, and $\mathscr{H}_\ell(C) = \mathscr{H}_{r-\ell}(C^{\perp_\ell})$. From the generalized Delsarte's Theorem in Proposition 2.2.2, it follows that $\mathtt{T}_d(\mathscr{H}_\ell(C)) = (\mathtt{Res}_d(\mathscr{H}_{r-\ell}(C)))^{\perp_\ell}$. Note that if C is $\langle\sigma^\ell\rangle$-invariant, then $\mathscr{H}_\ell(C) = \mathscr{H}_0(C)$.

From [27, Proposition 3.2 and Theorem 3.5], for any linear code C over R of length n, there is a unique s-tuple $(k_0, k_1, \cdots, k_{s-1})$ of positive integers, such that C has a generator matrix in standard form

$$\begin{pmatrix} \mathrm{I}_{k_0} & \mathrm{G}_{0,1} & \mathrm{G}_{0,2} & \cdots & \mathrm{G}_{0,s-2} & \mathrm{G}_{0,s-1} & \mathrm{G}_{0,s} \\ \mathrm{O} & \theta\mathrm{I}_{k_1} & \theta\mathrm{G}_{1,2} & \cdots & \theta\mathrm{G}_{1,s-2} & \theta\mathrm{G}_{1,s-1} & \theta\mathrm{G}_{1,s} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \mathrm{O} & \mathrm{O} & \mathrm{O} & \cdots & \mathrm{O} & \theta^{s-1}\mathrm{I}_{k_{s-1}} & \theta^{s-1}\mathrm{G}_{s-1,s} \end{pmatrix} \mathrm{U},$$

where U is a suitable permutation matrix and O the all zeros matrix of suitable size. The elements in the s-tuple $(k_0, k_1, \cdots, k_{s-1})$ are called parameters of C and the

rank of C is $k_0 + k_1 + \cdots + k_{s-1}$. From [27, Theorem 3.10], the parameters of $C^{\perp_\ell}$ are $(n-k, k_{s-1}, \cdots, k_2, k_1)$, where $k = \mathtt{rank}_R(C)$. Note that C is free if and only if $\mathtt{rank}_R(C) = k_0$ and $k_1 = \cdots = k_{s-1} = 0$. The q-dimension of a linear code C over R, denoted $\mathtt{dim}_q(C)$, is defined to be $\mathtt{log}_q(|C|)$. Thus the q-dimension of a linear code C over R of parameters $(k_0, k_1, \cdots, k_{s-1})$ is $\sum_{t=0}^{s-1}(s-t)k_t$. Since R is also a Frobenius ring, it follows that $\mathtt{dim}_q(C) + \mathtt{dim}_q(C^{\perp_\ell}) = sn$.

Proposition 2.2.4. *Let C and C' be two codes over R of the same length. Then*

$$dim_q(C + C') = dim_q(C) + dim_q(C') - dim_q(C \cap C').$$

Moreover $dim_q(\mathscr{H}_\ell(C)) = dim_q(\mathscr{H}_{r-\ell}(C))$.

Proof. The map $\eta : C \times C' \to C + C'$ defined as follows: $\eta(x; x') = x + x'$, is an R-module epimorphism. From the first isomorphism theorem, it follows that the R-modules $C \times C'/\mathtt{Ker}(\eta)$ and $C + C'$ are isomorphic. Since $\mathtt{Ker}(\eta) = \{(x; -x) : x \in C \cap C'\}$, it is easy to see that $\mathtt{Ker}(\eta)$ and $C \cap C'$ are isomorphic R-modules. Thus $|C + C'| = \frac{|C|}{|C \cap C'|} \times |C'|$. Therefore $\log_q(|C + C'|) = \log_q(|C|) - \log_q(|C \cap C'|) + \log_q(|C'|)$. From the definition of q-dimension of a linear code we have that $\mathtt{dim}_q(C + C') = \mathtt{dim}_q(C) + \mathtt{dim}_q(C') - \mathtt{dim}_q(C \cap C')$. Moreover,

$$\begin{aligned}
\mathtt{dim}_q(\mathscr{H}_\ell(C)) &= \mathtt{dim}_q((C + C^{\perp_{r-\ell}})^{\perp_\ell}), \text{ from Corollary 1 ;} \\
&= sn - \mathtt{dim}_q(C + C^{\perp_{r-\ell}}), \text{ since } \mathtt{dim}_q(C + C^{\perp_{r-\ell}}) + \mathtt{dim}_q((C + \\
&\quad C^{\perp_{r-\ell}})^{\perp_\ell}) = sn; \\
&= sn - \big(\mathtt{dim}_q(C) + \mathtt{dim}_q(C^{\perp_{r-\ell}}) - \mathtt{dim}_q(\mathscr{H}_{r-\ell}(C))\big); \\
&= \mathtt{dim}_q(\mathscr{H}_{r-\ell}(C)), \text{ since } \mathtt{dim}_q(C) + \mathtt{dim}_q(C^{\perp_{r-\ell}}) = sn.
\end{aligned}$$

□

Proposition 2.2.5. *Let C be a free code over R of length n and ℓ be a positive integer. Then*

1. $dim_q(\sigma^\ell(C)) = s \times rank(\sigma^\ell(C)) = s \times dim_q(\pi(\sigma^\ell(C)))$;
2. $\pi(C)^{\perp_\ell} = \pi(C^{\perp_\ell})$;
3. $\pi(\mathscr{H}_\ell(C)) = \mathscr{H}_\ell(\pi(C))$.

Proof. Since C is free, a generator matrix for $\sigma^\ell(C)$ is $\left(\begin{array}{c|c} \mathrm{I}_k & \sigma^\ell(\mathrm{A}) \end{array} \right)\mathrm{U}$, where A is a $k \times (n-k)$-matrix over R and U is a permutation matrix. Thus $\left(\begin{array}{c|c} \mathrm{I}_k & \pi(\sigma^\ell(\mathrm{A})) \end{array} \right)\mathrm{U}$ is a generator matrix for $\pi(C)$. It follows that $|\sigma^\ell(C)| = q^{sk}$ and $\mathtt{rank}(\sigma^\ell(C)) = \mathtt{dim}_q(\pi(\sigma^\ell(C))) = k$. This proves Item 1. Now to prove Item 2. The codes $\pi(C)^{\perp_\ell}$ and $\pi(C^{\perp_\ell})$ have the same parity matrix, which is $\left(\begin{array}{c|c} \mathrm{I}_k & \pi(\sigma^\ell(\mathrm{A})) \end{array} \right)\mathrm{U}$. Hence $\pi(C)^{\perp_\ell} = \pi(C^{\perp_\ell})$. Item 3. is a consequence of the fact that the diagram 2.2.2 commutes, $\pi(\mathscr{H}_\ell(C)) \subseteq \mathscr{H}_\ell(\pi(C))$ and $\mathtt{dim}_q(\pi(\mathscr{H}_\ell(C))) = \mathtt{dim}_q(\mathscr{H}_\ell(\pi(C)))$. □

3

Hull of cyclic codes over finite fields

In this chapter, we introduce some preliminary concepts on both finite fields and cyclic codes. All results of this chapter can be found in [14; 33].

3.1 | Basics on finite fields

Finite fields form an essential part of the study of error-correcting codes. The purpose of this section is to assume some results without proof, upon which we base the rest of our study .

Let us introduce finite fields. A field $\mathbb{F}$ is a commutative ring with identity in which each nonzero element has an inverse. This means the ring must also satisfy the following condition:

$$(\forall a \neq 0 \in \mathbb{F})(\exists a^{-1} \in \mathbb{F})(a \cdot a^{-1} = 1).$$

In other words, a ring with identity $1 \neq 0$ is a field if $\mathbb{F}\backslash\{0\}$ is an abelian group under multiplication. Of course a finite field is a field with a finite number of elements.

- The order of a finite field is the number of elements in the field. It is always of the form p^m, where p is a prime number called the characteristic of the field and the arithmetic in a finite field is performed modulo p.
- For every prime p, the integers modulo p form a field, which denoted $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}_p$.

- For every prime p, there is a unique finite field of size p that is isomorphic to $\mathbb{F}_p$ which is the set $\{0,1,\cdots,p-1\}$ with addition and multiplication modulo p.
- Every finite field is isomorphic to such a field, and therefore must have p^r elements for some prime p and positive integer r.
- Additively, a finite field with p^r elements has the structure of a vector space of dimension r over $\mathbb{F}_p$.
- An element α in a finite field $\mathbb{F}_q$ is called a primitive element (or generator) of $\mathbb{F}_q$ if $\mathbb{F}_q = \{0,\alpha,\alpha^2,\cdots,\alpha^{q-1}\}$.
- Let $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ the multiplicative group of $\mathbb{F}_q$. Then the following are true:
  1) The group $\mathbb{F}_q^*$ is cyclic with order $q-1$.
  2) If α is a generator of of this cyclic group, then $\mathbb{F}_q = \{0,1 = \alpha^0,\alpha^1,\alpha^2,\cdots,\alpha^{q-2}\}$, and $\alpha^i = 1$ if and only if $(q-1)|i$.

3.2 | Irreducible factorization of X^n-1

3.2.1 | Minimal Polynomials and Cyclotomic Cosets

We now introduce the idea of minimal polynomials which leads us to cyclotomic polynomials. These polynomials will play a central not only in factoring X^n-1 but also in generators of cyclic codes.

Definition 3.2.1. *An irreducible polynomial is a nonconstant polynomial $f(X) \in \mathbb{F}_q[X]$, such that whenever $f(X) = p(X)q(X)$, then either $p(X)$ or $q(X)$ must be a constant in $\mathbb{F}_q$. A reducible polynomial is a polynomial that can be factored into two polynomials of a lesser degree. Mathematically, $f(X) \in \mathbb{F}_q[X]$ such that $f(X) = a(X)b(X)$ where $\deg(a(X)) < \deg(f(X))$, $\deg(b(X)) < deg(f(X))$.*

Theorem 3. *Let $f(X)$ be an irreducible polynomial, $f(X)|p(X)q(X) \Rightarrow f(X)|p(X)$ or $f(X)|q(X)$.*

Definition 3.2.2. *An element $\xi \in \mathbb{F}_p$ is an n-th root of unity if $\xi^n = 1$. If $\xi \neq 1$ for $0 < s < n$, then ξ is called a primitive n-th root of unity.*

Definition 3.2.3. *A minimal polynomial of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is a nonzero monic polynomial $f(X)$ of the least degree in $\mathbb{F}_q[X]$ such that $f(\alpha) = 0$.*

Next we note some basic facts about minimal polynomials.

Theorem 4. *Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$ and let α be an element of $\mathbb{F}_{q^m}$ with minimal polynomial $M_\alpha(X)$ in $\mathbb{F}_q[X]$. The following are true:*

- *$M_\alpha(X)$ is irreducible over $\mathbb{F}_q$.*
- *If $g(X)$ is any polynomial in $\mathbb{F}_q[X]$ satisfying $g(\alpha) = 0$, then $M_\alpha(X) | g(X)$.*
- *$M_\alpha(X)$ is unique.*

Theorem 5. *Let $h(X)$ be a monic irreducible polynomial over $\mathbb{F}_q$ of degree r. Then the following hold:*

- *All the roots of $h(X)$ are in $\mathbb{F}_{q^r}$ and in any field containing $\mathbb{F}_q$ along with a root of $h(X)$,*
- *$h(X) = \Pi_{i=1}^{r}(X-\alpha_i)$, where $\alpha_i \in \mathbb{F}_{q^r}$ for $1 \leq i \leq r$, and*
- *$h(X) | (X^{q^r} - X)$.*

In particular this theorem holds for minimal polynomials $M_\alpha(X)$ over $\mathbb{F}_q$ as such polynomials are monic irreducible.

Theorem 6. *Let $\mathbb{F}_{q^m}$ be a field extension over $\mathbb{F}_q$ and α an element in $\mathbb{F}_{q^m}$ with minimal polynomial $M_\alpha(X)$ in $\mathbb{F}_q[X]$. Then the following are true :*

- *$M_\alpha(X) | (X^{q^m} - X)$.*
- *$M_\alpha(X)$ has distinct roots all lying in $\mathbb{F}_{q^m}$.*
- *The degree of $M_\alpha(X)$ divides t.*
- *$(X^{q^m} - X) = \Pi_\alpha M_\alpha(X)$, where α runs through some subset of $\mathbb{F}_{q^m}$ which enumerates the minimal polynomials once.*

- $(X^{q^m}-1) = \Pi_h h(X)$, *where* h *runs through all monic irreducible polynomials whose degree divides* m.

Remark 3.2.1. *Two elements of* $\mathbb{F}_{q^m}$ *having the same minimal polynomial in* $\mathbb{F}_q[x]$ *are said to be conjugate over* $\mathbb{F}_q$.

We can find all the conjugates of α in $\mathbb{F}_q$, that is, all the roots of $M_\alpha(X)$. We know by Theorem 6 that the roots of $M_\alpha(X)$ are distinct and lie in $\mathbb{F}_{q^m}$. We can find these roots with the following theorem :

Theorem 7. *Let* $h(X)$ *be a polynomial in* $\mathbb{F}_q[X]$ *and let* α *be a root of* $h(X)$ *in a field extension* $\mathbb{F}_{q^m}$. *Then the following assertions are hold*

1. $h(X^q) = h(X)^q$, *and*
2. α^q *is also a root of* $h(X)$ *in* $\mathbb{F}_q$.

Every factorization of the polynomial X^q-X partitions the elements in a finite field of order q. If we let $X^q-X = g(X)f(X)$ then every element in the field is either a root of $g(X)$ or $f(X)$. We know that $X^q-X = X(X^{q-1}-1)$ so that we can separate the zero elements from the nonzero elements. We now have left to separate the nonzero elements according to their orders by factoring $X^{q-1}-1$. This is a special case of X^n-1.

If we are given the minimal polynomial of a primitive element $\alpha \in \mathbb{F}_{q^m}$, we would like to find the minimal polynomial of α^i, for any i. In order to do so, we have to start with cyclotomic cosets.

Definition 3.2.4. *For all* $j \in \mathbb{Z}_n$, *we define the* q*-cyclotomic coset of* j *modulo* n *over* $\mathbb{F}_q$ *by the set*

$$C_j = \{j, jq, \cdots, jq^{d-1}\}(\mod n),$$

where d *is the smallest positive integer such that* $jq^d \equiv j(\mod n)$.

Example 3.2.1. *We wish to compute the* 2*-cyclotomic cosets m o d u l o* 21. *We get:*

- *For* $j=1:\{1,2,4,8,16,32\equiv 11,64\equiv 1\}$ *which gives us* $C_1=\{1,2,4,8,11,16\}$. *Since* 2 *is in* C_1, *we need not compute a coset for* $j=2$.
- *For* $j=3:\{3,6,12,24\equiv 3\}$, *which gives us* $C_3=\{3,6,12\}$.
- *For* $j=5:\{5,10,20,40\equiv 19,80\equiv 17,160\equiv 13,320\equiv 5\}$, *which gives us* $C_5=\{5,10,13,17,19,20\}$.
- *For* $j=7: C_7=\{7,14\}$.
- *For* $j=9:\{9,18,36\equiv 15,72\equiv 9\}$, *which gives us* $C_9=\{9,15,18\}$.

The 2*-cyclotomic coset for* 0 *is always* $\{0\}$.

We are now ready to determine the minimal polynomials for all the elements in a finite field.

Theorem 8. *Let* n *be a positive integer relatively prime to* q. *Let* α *be a primitive* $n-$*th root of unity in* $\mathbb{F}_{q^m}$. *Then the minimal polynomial of* α^j *with respect to* $\mathbb{F}_q$ *is*

$$M_{\alpha^j}(x)=\prod_{i\in C_j}(X-\alpha^i)$$

Example 3.2.2. *Let* $n=7$ *et* $q=2$. *The* 2*-cyclotomic cosets modulo* 7 *are:*

$$C_0=\{0\},\ C_1=\{1,2,4\},\ C_3=\{3,5,6\}$$

since $X^7-1=M_{\alpha^0}(X).M_{\alpha^1}(X).M_{\alpha^3}(X)$, *where* $M_{\alpha^j}(X)$ *are its minimal polynomial, we have:*

- $M_{\alpha^0}(X)=X-1$ *corresponds to the cyclotomic coset* C_0.
- $M_{\alpha^1}(X)=X^3+X+1$ *corresponds to the cyclotomic coset* C_1.
- $M_{\alpha^3}(X)=X^3+X^2+1$ *corresponds to the cyclotomic coset* C_3.

Then the factorization of X^7-1 *is* $X^7-1=(X-1)(X^3+X+1)(X^3+X^2+1)$, *where* α *is a primitive* $7-$*th root of unity in* $\mathbb{F}_{2^3}$.

3.2.2 | Cyclotomic Polynomials

Let $\mathbb{F}_q$ be a finite field of characteristic p, n a positive integer not divisible by p, and ε a primitive j—th root of unity over $\mathbb{F}_q$, then the polynomial

$$\varphi_j = \prod_{\substack{s=1 \\ \gcd(s,j)=1}}^{j} (X-\varepsilon^s),$$

is called the j—th cyclotomic polynomial over $\mathbb{F}_q$.

Theorem 9. *Let $\mathbb{F}_q$ and n defined as above. Then*

$$X^n-1 = \prod_{d|n} \varphi_d(X). \tag{3.1}$$

Proof. Each n-th root of unity over $\mathbb{F}_q$ is a primitive d-th root of unity over $\mathbb{F}_q$ for exactly one divisor d of n. In detail, if ε is a primitive n-th root of unity over $\mathbb{F}_q$ and ε^s is an arbitrary n-th root of unity over $\mathbb{F}_q$, then $d = \frac{n}{\gcd(s,n)}$. That is d is the order of ε. Since

$$X^n-1 = \prod_{s=1}^{n} (X-\varepsilon^s),$$

the formula in 3.1 is obtained by collecting those factors $(X-\varepsilon^s)$ for which $\varepsilon^s$is a primitive d-th root of unity over $\mathbb{F}_q$. □

Let j and i be positive integers such that $\gcd(i,j)=1$ and let $\mathbb{Z}_j^\times$ be the unit group of $\mathbb{Z}_j$. The order of i in $\mathbb{Z}_j^\times$ is the smallest integer e such that $j|(i^e-1)$, denoted by $\mathtt{ord}_j(i)$

Let i and j be positive integers. We say the pair (i,j) is good if i divides j^k+1 for some non-negative integer k and bad otherwise.

Lemma 3.2.1. *Let j be a positive integer and let $\mathbb{F}_q$ be a finite field with $\gcd(j,q)=1$. The j-th cyclotomic polynomial $\varphi_j(x)$ factors into $\frac{\phi(j)}{e}$ distinct monic irreducible polynomials over $\mathbb{F}_q$ of the same degree e, where ϕ is Euler' s totient function and $e=\mathtt{ord}_j(q)$. Moreover, if (j,q) is good, then all irreducible polynomials in the factorization of $\varphi_j(X)$ are self-reciprocal. Otherwise, all of them form reciprocal polynomial pairs.*

Remark 3.2.2. *Let* $N_q = \{k \geq 1, k \text{ divides } q^i + 1\}$, *then the pair* (j,q) *is good if* $j \in N_q$ *and it is bad if* $j \notin N_q$.

By lemma 3.2.1 and theorem 9, the factorization of $X^n - 1 \in \mathbb{F}_q[X]$ can be viewed as

$$\begin{aligned} X^n - 1 &= \prod_{j \mid n} \varphi_j(X) = \prod_{\substack{j \mid n \\ j \in \mathcal{N}_q}} \varphi_j(X) \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_q}} \varphi_j(X) \\ &= \prod_{\substack{j \mid n \\ j \in \mathcal{N}_q}} \left(\prod_{i=1}^{\gamma(j;q)} h_{ij}(X) \right) \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_q}} \left(\prod_{i=1}^{\beta(j;q)} k_{ij}(X) k_{ij}^*(X) \right) \end{aligned}$$

Where

$$\gamma(j;q) = \frac{\phi(j)}{\mathtt{ord}_j(q)}, \quad \text{and } \beta(j;q) = \frac{\phi(j)}{2\mathtt{ord}_j(q)}.$$

- $h_{ij}(X)$ is a monic irreducible self-reciprocal polynomial of degree $\mathtt{ordj}_(q)$,
- $k_{ij}(X)$ and $k_{ij}^*(X)$ form a monic irreducible reciprocal polynomial pair of degree $\mathtt{ord}_j(q)$.

3.3 | Cyclic codes over finite fields

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 $X^n - 1$.

Definition 3.3.1. *A linear code* C *of length* n *over a finite field* $\mathbb{F}_q$ *is called a cyclic code if for every codeword* $c \in C$ *the codeword obtained by a cyclic shift is also a codeword in* C. *That is,*

$$c = (c_0, \cdots, c_{n-1}) \in C \Rightarrow c' = (c_{n-1}, c_0, \cdots, c_{n-2}) \in C.$$

Example 3.3.1. *The linear code* $C_1 := \{102, 210, 021, 201, 120, 012, 222, 111, 000\}$ *over* $\mathbb{Z}_3$ *is cyclic, but this linear code* $C_2 := \{000, 221, 212, 200, 121, 112, 100, 021, 012\}$ *over* $\mathbb{Z}_3$ *is not cyclic, since* $c_1 := (112) \in C$ *but* $c' := (211)$ *is not in* C_2.

Remark 3.3.1. *Let C_1 and C_2 be two linear codes of length n over $\mathbb{F}_q$. If C_1 and C_2 are cyclic, then C_1+C_2 and $C_1\cap C_2$ are cyclic, where $C_1+C_2=\{c_1+c_2 : c_1\in C_1, c_2\in C_2\}$.*

We remember that since $\mathbb{F}_q[x]$ is principle ideal domain also the ring $R_n = \mathbb{F}_q[x]/\langle X^n-1\rangle$ is a principle ideal hence the cyclic codes are principle ideals of R_n when writing a code word of a cyclic code as $c(X)$ we mean the coset $c(X)+\langle X^n-1\rangle$ in R_n.

Corollary 2. *The number of cyclic codes in R_n equal 2^m, where m is the number of q-cyclotomic cosets modulo n. Moreover, the dimensions of cyclic codes in R_n are all possible sums of the sizes of the q-cyclotomic cosets modulo n.*

3.3.1 | Generating polynomial of a cyclic code

Theorem 10. *A linear code C in $\mathbb{F}_q$ is cyclic if and only if C is an ideal in $R_n = \mathbb{F}_q[X]/\langle X^n-1\rangle$.*

Proof. If C is an ideal in $\mathbb{F}_q[X]/\langle X^n-1\rangle$ and $c(X) = c_0+c_1X+\cdots+c_{n-1}X^{n-1}$ is any codeword, then $Xc(X)$ is also a codeword, i.e. $(c_{n-1},c_0,c_1,\cdots,c_{n-2})\in C$. Conversely, if C is cyclic, then $c(X)\in C$ we have $Xc(X)\in C$. Therefore $X^ic(X)\in C$, and since C is linear, then $a(X)c(X)\in C$ for each polynomial $a(X)$. Hence C is an ideal of $\mathbb{F}_q[X]/\langle X^n-1\rangle$. □

The dimension of C, denoted by $\mathtt{dim}(C)$, is the dimension of C considered as linear space over $\mathbb{F}_q$.

Theorem 11. *Let C be an ideal in R_n. Then*

1) *There is a unique monic polynomial $g(X)$ of minimum degree in $C=\langle g(X)\rangle$, and it is called the generating polynomial for C.*

2) *The generating polynomial $g(X)$ divides X^n-1.*

3) *If $\deg(g(X)) = k$, then C has dimension $n-k$ and $C = \langle g(X)\rangle = \{s(X)g(X) : \deg(s(X)) < n-k\}$.*

4) If $g(X) = g_0 + g_1X + \cdots + g_kX^k$*, then* $g_0 \neq 0$ *and a generator matrix is:*

$$\begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_k & 0 & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_k \end{pmatrix}.$$

Proof.

1) Suppose that C contains two distinct monic polynomial $g_1$and g_2 of minimum degree k. Then their difference $g_1 - g_2$ would be a nonzero polynomial in C of degree less than k, which is not possible. Hence, there is a unique monic polynomial $g(X)$ of degree k in C. Since $g(X) \in C$ and C is an ideal, we have $\langle g(X)\rangle \subset C$. On the other hand, Suppose that $p(X) \in C$, and let

$$p(X) = q(X)g(X) + r(X), \text{ where } r(X) \neq 0 \text{ and } \deg(r(X)) < k.$$

Then $r(X) = p(X) - q(X)g(X) \in C$ has degree less than k, which possible only if $r(X) = 0$. Hence $p(X) = q(X)g(X) \in \langle g(X)\rangle$, and so $C \subset \langle g(X)\rangle$. Thu $C = \langle g(X)\rangle$.

2) Dividing $x^n - 1$ by $g(X)$ gives $X^n - 1 = q(X)g(X) + r(X)$, where $\deg(r(X)) < k$. Since in R_n, we see that $r(X) \in C$, and so $r(X) = 0$, which shows that $g(X)|(X^n - 1)$.

3) The ideal generated by $g(X)$ is

$$\langle g(X)\rangle = \{f(X)g(X) : f(X) \in R_n\}$$

with the usual reduction $mod\ (X^n - 1)$. Now $h(X)$ divides $X^n - 1$, and so $X^n - 1 = h(X)g(X)$ for some $h(X)$ of degree $n - k$. Divide $f(X)$ by $h(X)$, we get $f(X) = q(X)h(X) + s(X)$, where $\deg(s(X)) < n - k$, then

$$f(X)g(X) = q(X)g(X)h(X) + s(X)g(X) = q(X)(X^n - 1) + s(X)g(X).$$

So $f(X)g(X) = s(X)g(X) \in C$. Now let $c(X)$ be in C, then

$$\begin{aligned} c(X) &= s(X)g(X) = (a_0 + a_1X + a_2X^2 + \cdots + a_{n-k-1}X^{n-k-1})g(X) \\ &= (a_0g(X) + a_1Xg(X) + \cdots + a_{n-k-1}X^{n-k-1}g(X). \end{aligned}$$

So $c(X) \in \langle\{g(X), Xg(X), \cdots, X^{n-k-1}g(X)\}\rangle$, which shows that the set $\{g(X), Xg(X), \cdots, X^{n-k-1}g(x)\}$ spans C. Also $\{g(X), Xg(X), \cdots, X^{n-k-1}g(X)\}$ is linearly independent, since if

$$a_0 g(X) + a_1 Xg(X) + \cdots + a_{n-k-1}X^{n-k-1}g(X) = 0,$$

then $(a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-k-1}X^{n-k-1})g(X)) = 0$ which implies that

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-k-1}X^{n-k-1}$$

and since $1, X, X^2, \cdots, X^{n-k-1}$ are linearly independent, then $a_0 = a_1 = \cdots = a_{n-k-1} = 0$ and hence $\{g(X), Xg(X), \cdots, X^{n-k-1}g(X)\}$ forms a basis for C. Hence $\dim(C) = n-k$.

4) If $g_0 = 0$ and $g(X) = Xg_1(X)$, where $\deg(g_1(X)) < k$ and $g_1(X) = 1.g_1(X) = X^{n-1}g(X)$, so $g_1(X) \in C$ which contradict the fact that no nonzero polynomial in C has degree less than k. Thus $g_0 \neq 0$. Finally, G is a generator matrix of C since $\{g(X), Xg(X), \cdots, X^{n-k-1}g(X)\}$ is a basis for C.

□

3.3.2 | Check Polynomial

Let C be a cyclic code, its generator polynomial $g(X)$ must divide $X^n - 1$ and thus $X^n - 1 = g(X)h(X)$ where $h(X)$ is a monic polynomial of degree $n-k$. $h(X)$ is called the check polynomial of C.

Theorem 12. *Let C be a code in $\mathbb{F}_q[X]/(X^n-1)$ and $h(X) = h_0 + h_1 X + \cdots + h_{n-k}X^{n-k}$ be its check polynomial.*

1) $C = \{c(X) \in \mathbb{F}_q[X]/(X^n-1) | c(X)h(X) = 0\}$.

2) $C^\perp$ is the cyclic code of dimension k generated by the polynomial $h^* = h_0^{-1}(h_{n-k} + h_{n-k-1}X + \cdots + h_0 X^{n-k})$.

2) A parity check matrix for C is the following:

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}$$

Example 3.3.2. *Let C be a cyclic code of length $n = 9$. Since the factorisation of X^9-1 over $\mathbb{F}_2$ is*

$$X^9-1 = (X^3-1)(X^6+X^3+1) = (X-1)(X^2+X+1)(X^6+X^3+1).$$

Hence, there are $2^3 = 8$ cyclic codes in $R_9 = \mathbb{F}_2/\langle X^9-1\rangle$. Take $C = \langle X^6+X^3+1\rangle$ with generating polynomial $g(X) = X^6+X^3+1$. Then C has dimension $9-6 = 3$ and generating matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Also C has check polynomial $h(X) = \dfrac{X^9-1}{g(X)} = (X-1)(X^2+X+1) = (X^3-1)$. Then C has the parity check matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

3.4 | Hulls of cyclic codes over finite fields

In this section, the dimensions of the hulls of cyclic codes of length n over $\mathbb{F}_q$ are determined. Furthermore, we determine the number of cyclic codes of length n over $\mathbb{F}_q$ whose hulls have a given dimension. The average hull dimension of cyclic codes is given.

The generator of the hull of a cyclic code is determined as follows.

Theorem 13. *[33] Let C be a cyclic code of length n over $\mathbb{F}_q$ generated by $\langle g(X)\rangle$, where $g(X)$ is monic divisor of X^n-1 over $\mathbb{F}_q$. Then $\mathscr{H}(C))$ is generated by*

$$\langle lcm(g(X),h^*(X))\rangle,$$

where $h(X)=\dfrac{X^n-1}{g(X)}$.

Proof. Let $F(X)$ be the generator polynomial of $\mathscr{H}(C)$, since $F(X)\in C\cap C^{\perp}$, we have

$$F(X)\in C \quad \text{and } F(X)\in C^{\perp}.$$

Then

$$g(X)\mid F(X) \quad \text{and } h^*(X)\mid F(X) \quad \text{dans } \mathbb{F}_q[X],$$

which imply that

$$\mathtt{lcm}(g(X),h^*(X))\mid F(X).$$

On the other side

$$g(X)\mid \mathtt{lcm}(g(X),h^*(X)) \quad \text{and } h^*(X)\mid \mathtt{lcm}(g(X),h^*(X)).$$

Hence, $\mathtt{lcm}(g(X),h^*(X))$ is in C and $C^{\perp}$, consequently $\mathtt{lcm}(g(X),h^*(X))$ is in $C\cap C^{\perp}$. Then

$$F(X) \mid \mathtt{lcm}(g(X),h^*(X)).$$

Therefore, $F(x)=\mathtt{lcm}(g(X),h^*(X))$ i s desired.

□

Example 3.4.1. *In $\mathbb{F}_q[X]$, $X^7-1=(X+1)(X^3+X^2+1)(X^3+X+1)$ is the factorization of X^7-1 into a product of irreducible polynomials. Let C be the cyclic code of length 7 over $\mathbb{F}_q$ generated by*

$$\langle g(X)\rangle, \quad \text{where } g(X)=(X^3+X+1).$$

Then $C^{\perp}$ is of the form

$$\langle h^*(X)\rangle, \quad \text{where } h^*(X)=(X+1)^*(X^3+X^2+1)^*=(X+1)g(X).$$

$\mathscr{H}(C)$ is generated by

$$\langle lcm(g(X),\, h^*(X))\rangle=\langle lcm((X^3+X+1),\,(X+1)(X^3+X+1)\rangle=\langle(X+1)(X^3+X+1)\rangle.$$

3.4.1 | Characterization of cycic codes with the same hulls

In this subsection, we determine all cyclic codes of length n over $\mathbb{F}_q$ whose hulls equal C, where C is a fixed cyclic code of length n over $\mathbb{F}_q$.

Theorem 14. *Let C be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial*

$$L(X)=\prod_{\substack{j\,|\,\bar{n}\\ j\in\mathcal{N}_q}}\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{A_{ij}}\prod_{\substack{j\,|\,\bar{n}\\ j\notin\mathcal{N}_q}}\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{B_{ij}}f_{ij}^*(X)^{C_{ij}},$$

if $\lceil\frac{p^\alpha}{2}\rceil\le A_{ij}\le p^\alpha$ and $0\le B_{ij},\ C_{ij}\le p^\alpha$ are such that $p^\alpha\le B_{ij}+C_{ij}\le 2p^\alpha$, then the generator polynomials of cyclic codes whose hulls equal C are of the forms

$$g(X)=\prod_{\substack{j\,|\,\bar{n}\\ j\in\mathcal{N}_q}}\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{u_{ij}}\prod_{\substack{j\,|\,\bar{n}\\ j\notin\mathcal{N}_q}}\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{v_{ij}}f_{ij}^*(X)^{w_{ij}},$$

where $u_{ij}\in\{A_{ij},\ p^\alpha-A_{ij}\}$ and

$$\begin{cases}\{(B_{ij},C_{ij})\}, & \text{if } B_{ij}+C_{ij}=p^\alpha,\\ \{(B_{ij},C_{ij}),(p^\alpha-C_{ij},p^\alpha-B_{ij})\}, & \text{if } p^\alpha<B_{ij}+C_{ij}\le 2p^\alpha,\end{cases}$$

Otherwise, there are no cyclic codes of length n over $\mathbb{F}_q$ whose hulls equal C.

Proof. Let D be a cyclic code of length n over $\mathbb{F}_q$ with generator polynomial

$$g(X)=\prod_{\substack{j\,|\,\bar{n}\\ j\in\mathcal{N}_q}}\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{u_{ij}}\prod_{\substack{j\,|\,\bar{n}\\ j\notin\mathcal{N}_q}}\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{v_{ij}}f_{ij}^*(X)^{w_{ij}},$$

Assume that $\mathscr{H}(D)$, is with generator polynomial $k(X)$. Then we have

$$k(X)=\prod_{\substack{j\,|\,\bar{n}\\ j\in\mathcal{N}_q}}\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{\max\{u_{ij},\,p^\alpha-u_{ij}\}}\prod_{\substack{j\,|\,\bar{n}\\ j\notin\mathcal{N}_q}}\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\max\{v_{ij},\,p^\alpha-w_{ij}\}}f_{ij}^*(X)^{\max\{w_{ij},\,p^\alpha-v_{ij}\}}.$$

Comparing the coefficients, we have $\max\{u_{ij},\ p^\alpha-u_{ij}\}=A_{ij}$. Therefore, u_{ij} is equal to A_{ij} or $p^\alpha-A_{ij}$. Similarly, $\max\{v_{ij},\ p^\alpha-w_{ij}\}=B_{ij}$ and $\max\{w_{ij},\ p^\alpha-v_{ij}\}=C_{ij}$, and so $(B_{ij},C_{ij})=(\max\{v_{ij},\ p^\alpha-w_{ij}\},\max\{w_{ij},\ p^\alpha-v_{ij}\})$ is equal

to either (v_{ij}, w_{ij}) or $(p^\alpha - w_{ij}, p^\alpha - v_{ij})$.
If $B_{ij} + C_{ij} = p^\alpha$, then $(B_{ij}, C_{ij}) = (v_{ij}, w_{ij}) = (p^\alpha - w_{ij}, p^\alpha - v_{ij})$. If $p^\alpha < B_{ij} + C_{ij} \leq 2p^\alpha$, then $(B_{ij}, C_{ij}) = (v_{ij}, w_{ij})$ or $(p^\alpha - w_{ij}, p^\alpha - v_{ij})$. Hence, $(v_{ij}, w_{ij}) = (B_{ij}, C_{ij})$ or $(p^\alpha - C_{ij}, p^\alpha - B_{ij})$. If $0 \leq A_{ij} \leq \lceil \frac{p^\alpha}{2} \rceil - 1$, then there is no u_{ij} such that $0 \leq u_{ij} \leq p^\alpha$ and $\max\{u_{ij}, p^\alpha - u_{ij}\} = A_{ij}$. If $0 \leq B_{ij} + C_{ij} \leq p^\alpha - 1$, then there are no v_{ij} and w_{ij} where $0 \leq v_{ij}, w_{ij} \leq p^\alpha$, $\max\{v_{ij}, p^\alpha - w_{ij}\} = B_{ij}$ and $\max\{w_{ij}, p^\alpha - v_{ij}\} = C_{ij}$. Thus, there are no cyclic codes of length n over $\mathbb{F}_q$ when $0 \leq A_{ij} \leq \lceil \frac{p^\alpha}{2} \rceil - 1$ or $0 \leq B_{ij} + C_{ij} \leq p^\alpha - 1$. □

Corollary 3. *Let C be a cyclic codes of length n over $\mathbb{F}_q$ with generator polynomial*

$$k(X) = \prod_{\substack{j \mid \bar{n} \\ j \in \mathcal{N}_q}} \prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{\max\{u_{ij},\, p^\alpha - u_{ij}\}} \prod_{\substack{j \mid \bar{n} \\ j \notin \mathcal{N}_q}} \prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\max\{v_{ij},\, p^\alpha - w_{ij}\}} f_{ij}^*(X)^{\max\{w_{ij},\, p^\alpha - v_{ij}\}},$$

where $\lceil \frac{p^\alpha}{2} \rceil \leq A_{ij} \leq p^\alpha$ and $0 \leq B_{ij}, B_{ij} \leq p^\alpha$ are such that $p^\alpha \leq B_{ij} + C_{ij} \leq 2p^\alpha$.
Then the number of cyclic codes of length n over $\mathbb{F}_q$ whose hulls have $k(X)$ as generator polynomials is

$$\prod_{\substack{j \mid \bar{n} \\ j \in \mathcal{N}_q}} \prod_{i=1}^{\gamma(j;q)} |\{A_{ij},\, p^\alpha - A_{ij}\}| \prod_{\substack{j \mid \bar{n} \\ j \notin \mathcal{N}_q}} \prod_{i=1}^{\beta(j;q)} 2^{1 - \lfloor \frac{p^\alpha}{B_{ij} + C_{ij}} \rfloor}.$$

3.4.2 | The dimensions of the hulls of cyclic codes

The dimension of $\mathscr{H}(C)$, denoted by $\dim(\mathscr{H}(C))$ is the dimension of $\mathscr{H}(C)$ (so-called **hull dimension**) seen as linear space over $\mathbb{F}_q$.

An expression for the dimensions of the hulls of cyclic codes of length n over a finite field $\mathbb{F}_q$ is derived in Theorem 15 . The following lemma is required in its proof.

Lemma 3.4.1. *Let α be a nonnegative integer. Let $0 \leq x, y, z \leq p^\alpha$ be integers. Then the following statements hold.*

1. $0 \leq p^\alpha - \max\{x, p^\alpha - x\} \leq \lfloor \frac{p^\alpha}{2} \rfloor$.

2. $0 \leq 2p^{\alpha} - (\max\{y, p^{\alpha} - z\} + \max\{z, p^{\alpha} - y\}) \leq p^{\alpha}$.

Theorem 15. *[33] Let* n *be a positive integer and write* $n = p^{\alpha}\bar{n}$, *where* $\gcd(p, \bar{n}) = 1$ *and* $\alpha \geq 0$ *is an integer. The dimensions of the hull of cyclic codes of length* n *over* $\mathbb{F}_q$ *is of the form*

$$\sum_{\substack{j \mid \bar{n} \\ j \in \mathcal{N}_q}} ord_j(q) \cdot u_j + \sum_{\substack{j \mid \bar{n} \\ j \notin \mathcal{N}_q}} ord_j(q) \cdot v_j,$$

where $0 \leq u_j \leq \gamma(j;q)\left\lfloor \frac{p^{\alpha}}{2} \right\rfloor$ *and* $0 \leq v_j \leq \beta(j;q)p^{\alpha}$.

Proof. Let C be a cyclic code of length n over $\mathbb{F}_q$ generated by $\langle g(X) \rangle$, then $C^{\perp}$ is generated by $\langle h^*(X) \rangle$, where $g(X), h^*(X)$ are monic divisors of $X^n - 1$.
We have :

$$\begin{aligned}
g(X) &= \prod_{\substack{j \mid \bar{n} \\ j \in \mathcal{N}_q}} \prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{u_{ij}} \prod_{\substack{j \mid \bar{n} \\ j \notin \mathcal{N}_q}} \prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{v_{ij}} f_{ij}^*(X)^{w_{ij}}, \\
h(X) &= \prod_{\substack{j \mid \bar{n} \\ j \in \mathcal{N}_q}} \prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{p^{\alpha} - u_{ij}} \prod_{\substack{j \mid \bar{n} \\ j \notin \mathcal{N}_q}} \prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{p^{\alpha} - v_{ij}} f_{ij}^*(X)^{p^{\alpha} - w_{ij}}, \\
h^*(X) &= \prod_{\substack{j \mid \bar{n} \\ j \in \mathcal{N}_q}} \prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{p^{\alpha} - u_{ij}} \prod_{\substack{j \mid \bar{n} \\ j \notin \mathcal{N}_q}} \prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{p^{\alpha} - w_{ij}} f_{ij}^*(X)^{p^{\alpha} - v_{ij}},
\end{aligned}$$

for some $0 \le u_{ij}, v_{ij}, w_{ij} \le p^\alpha$. Since $\mathscr{H}(C) = \langle \mathtt{lcm}(g(X), h^*(X)) \rangle$, we have

$$\begin{aligned}
\dim(\mathscr{H}(C)) &= n - \deg \mathtt{lcm}(g(X), h^*(X)); \\
&= \sum_{\substack{j \mid \bar{n} \\ j \in \mathscr{N}_q}} \mathtt{ord}_j(q) \sum_{i=1}^{\gamma(j;q)} p^\alpha + \sum_{\substack{j \mid \bar{n} \\ j \notin \mathscr{N}_q}} \mathtt{ord}_j(q) \sum_{i=1}^{\beta(j;q)} 2p^\alpha \\
&\quad - \sum_{\substack{j \mid \bar{n} \\ j \in \mathscr{N}_q}} \mathtt{ord}_j(q) \sum_{i=1}^{\gamma(j;q)} \max\{u_{ij}, p^\alpha - u_{ij}\} \\
&\quad - \sum_{\substack{j \mid \bar{n} \\ j \notin \mathscr{N}_q}} \mathtt{ord}_j(q) \sum_{i=1}^{\beta(j;q)} (\max\{v_{ij}, p^\alpha - w_{ij}\} - \max\{w_{ij}, p^\alpha - v_{ij}\}) \\
&= \sum_{\substack{j \mid \bar{n} \\ j \in \mathscr{N}_q}} \mathtt{ord}_j(q) \sum_{i=1}^{\gamma(j;q)} (p^\alpha - \max\{u_{ij}, p^\alpha - u_{ij}\}) \\
&\quad + \sum_{\substack{j \mid \bar{n} \\ j \notin \mathscr{N}_q}} \mathtt{ord}_j(q) \sum_{i=1}^{\beta(j;q)} (2p^\alpha - (\max\{v_{ij}, p^\alpha - w_{ij}\} + \max\{w_{ij}, p^\alpha - v_{ij}\})) \\
&= \sum_{\substack{j \mid \bar{n} \\ j \in \mathscr{N}_q}} \mathtt{ord}_j(q) \cdot u_j + \sum_{\substack{j \mid \bar{n} \\ j \notin \mathscr{N}_q}} \mathtt{ord}_j(q) \cdot v_j, \text{ by lemma 3.4.1,}
\end{aligned}$$

where $0 \le u_j \le \gamma(j;q) \left\lfloor \frac{p^\alpha}{2} \right\rfloor$ and $0 \le v_j \le \beta(j;q) p^\alpha$. □

Example 3.4.2. *Let $n = 33$ and $p = 3$. Then $\bar{n} = 11$ and $v = 1$. The divisors of 11 are 1 and 11.*

1. *We have $1 \in \mathscr{N}_3$, so $ord_1(3) = 1$ and $\gamma(1;3) = 1$.*
2. *We have $11 \notin \mathscr{N}_3$, so $ord_{11}(3) = 5$ and $\beta(11;3) = 1$, by Theorem 15, the dimensions of the hulls of cyclic codes of length n over $\mathbb{F}_q$ is of the form*

$$u_1 + 5v_{11}, \quad \text{where } 0 \le u_1 \le 3 \text{ and } 0 \le v_{11} \le 6.$$

Hence, all possible dimensions of the hull of cylic codes of length 33 over $\mathbb{F}_3$:

$$\{0,1,3,5,6,8,10,11,13,15,16,18,20,21,23,25,26,28,30,31,33\}.$$

3.5 | The average dimension of the hull of cyclic Codes

Let $\mathscr{C}(n,\mathbb{F}_q)$ be the set of of all cyclic codes over length n over $\mathbb{F}_q$, and the average dimension of the hull of cyclic codes of length n over $\mathbb{F}_q$ is :

$$\mathrm{E}_{\mathbb{F}_q}(n) = \sum_{C\in\mathscr{C}(n,\mathbb{F}_q)} \frac{\mathtt{dim}(\mathscr{H}(C))}{|\mathscr{C}(n,\mathbb{F}_q)|}.$$

In this section we give a formula of $\mathrm{E}_{\mathbb{F}_q}(n)$ with its upper and lower bounds.

Lemma 3.5.1. *Let α be a nonnegative integer and let $0 \le u,v,w \le p^\alpha$ be integers. Then*

1. $E(\max\{u, p^\alpha - u\}) = \dfrac{3p^\alpha+1}{4} - \dfrac{\delta_{p^\alpha}}{4(p^\alpha+1)}$;
2. $E(\max\{v, p^\alpha - w\}) = \dfrac{p^\alpha(4p^\alpha+5)}{6(p^\alpha+1)}$, *where* $\delta_{p^\alpha} = 1$ *if* $\alpha > 0$ *and* $\delta_{p^\alpha} = 0$ *if* $\alpha = 0$.

The formula for the average dimension of the hull of cyclic codes of length n over $\mathbb{F}_q$ is given as follows.

Theorem 16. *[33] Let n be a positive integer and write $n = p^\alpha \bar{n}$, where $\gcd(p,\bar{n}) = 1$ and $\alpha \ge 0$ is an integer. The average dimensions of the hull of cyclic codes of length n over $\mathbb{F}_q$ is*

$$E_{\mathbb{F}_q}(n) = n\left(\frac{1}{3} - \frac{1}{6(p^\alpha+1)}\right) - \mathscr{B}_{\bar{n}}\left(\frac{p^\alpha+1}{12} + \frac{2-3\delta_{p^\alpha}}{12(p^\alpha+1)}\right).$$

Proof. Let C be a cyclic code of length n over $\mathbb{F}_q$, then $\mathscr{H}(C)$ is generated by:

$$\langle \mathtt{lcm}(g(X), h^*(X))\rangle,$$

and

$$\mathtt{dim}(\mathscr{H}(C)) \;=\; (n - \deg \mathtt{lcm}(g(X), h^*(X))).$$

Note that we can define $\mathrm{E}_{\mathbb{F}_q}(n)$ in terms of the probability theory. Let X be the random variable that takes as value $\dim(\mathscr{H}(C))$ where C is chosen randomly from $\mathscr{C}(n,\mathbb{F}_q)$ with uniform probability $\frac{1}{|\mathscr{C}(n,\mathbb{F}_q)|}$. The average dimension $\mathrm{E}_{\mathbb{F}_q}(n)$ can be determined in terms of the expectation $\mathrm{E}(X)$ as follows :

$$
\begin{aligned}
\mathrm{E}_{\mathbb{F}_q}(n)=\mathrm{E}(X) &= \mathrm{E}(n-\deg \mathrm{lcm}(g(X),h^*(X))) \\
&= n-\mathrm{E}\left(\sum_{\substack{j\mid \bar{n}\\ j\in\mathscr{N}_q}} \mathrm{ord}_j(q)\sum_{i=1}^{\gamma(j;q)}\max\{u_{ij},p^\alpha-u_{ij}\}\right) \\
&\quad +\mathrm{E}\left(\sum_{\substack{j\mid \bar{n}\\ j\notin\mathscr{N}_q}} \mathrm{ord}_j(q)\sum_{i=1}^{\beta(j;q)}(\max\{v_{ij},p^\alpha-w_{ij}\}+\max\{w_{ij},p^\alpha-v_{ij}\})\right) \\
&= n-\sum_{\substack{j\mid \bar{n}\\ j\in\mathscr{N}_q}} \mathrm{ord}_j(q).\gamma(j;q)\mathrm{E}(\max\{u_{ij},p^\alpha-u_{ij}\})- \\
&\quad \sum_{\substack{j\mid \bar{n}\\ j\notin\mathscr{N}_q}} \mathrm{ord}_j(q).\beta(j;q)\mathrm{E}(\max\{v_{ij},p^\alpha-w_{ij}\}+\max\{w_{ij},p^\alpha-v_{ij}\}) \\
&= n-\sum_{\substack{j\mid \bar{n}\\ j\in\mathscr{N}_q}} \phi(j).\mathrm{E}(\max\{u_{ij},p^\alpha-u_{ij}\}) \\
&\quad -\sum_{\substack{j\mid \bar{n}\\ j\notin\mathscr{N}_q}} \frac{\phi(j)}{2}\mathrm{E}(\max\{v_{ij},p^\alpha-w_{ij}\})+\max\{w_{ij},p^\alpha-v_{ij}\}) \\
&= (n-\mathscr{B}_{\bar{n}}.\mathrm{E}(\max\{u_{ij},p^\alpha-u_{ij}\}))-(\bar{n}-\mathscr{B}_{\bar{n}}).\mathrm{E}(\max\{v_{ij},p^\alpha-w_{ij}\}) \\
&= (n-\mathscr{B}_{\bar{n}}.\mathrm{E}(\max\{u_{ij},p^\alpha-u_{ij}\}))-(\bar{n}-\mathscr{B}_{\bar{n}}).\mathrm{E}(\max\{v_{ij},p^\alpha-w_{ij}\}) \\
&= (n-\mathscr{B}_{\bar{n}})\left(\frac{3p^\alpha+1}{4}-\frac{\delta_{p^\alpha}}{4(p^\alpha+1)}\right)-(\bar{n}-\mathscr{B}_{\bar{n}})\left(\frac{p^\alpha(4p^\alpha+5)}{6(p^\alpha+1)}\right) \\
&= n\left(\frac{1}{3}-\frac{1}{6(p^\alpha+1)}\right)-\mathscr{B}_{\bar{n}}\left(\frac{p^\alpha+1}{12}+\frac{2-3\delta_{p^\alpha}}{12(p^\alpha+1)}\right).
\end{aligned}
$$

□

Example 3.5.1. *Let* $n = 33$ *and* $p = 3$. *Then* $\bar{n} = 11$ *and* $\alpha = 1$. *The divisors of* 11 *are* 1 *and* 11.

1. *We have* $1 \in \mathcal{N}_3$ *and* $11 \notin \mathcal{N}_3$, *so* $\mathcal{B}_{11} = \phi(1) = 1$;

2. *And*

$$\begin{aligned} E_{\mathcal{R}_q}(33) &= 33\left(\frac{1}{3} - \frac{1}{6(3+1)}\right) - \mathcal{B}_{11}\left(\frac{3+1}{12} + \frac{2-3\delta_3}{12(3+1)}\right) \\ &= \frac{149}{16}. \end{aligned}$$

We have the following upper and lower bounds.

Corollary 4. *[34] Let* q *be a power of a prime* p, *let* $n \geq 1$. *Then:*

1. $E_{\mathbb{F}_q}(n) = 0$ *if and only if* $n \in N_q$.

2. $\frac{n}{12} \leq E_{\mathbb{F}_q}(n) \leq \frac{n}{3}$, *for all* $n \notin N_q$.

From Theorem 16, we can conclude that the average q-dimension of the hull of cyclic codes of length n over $\mathbb{F}_q$ is zero or grows the same rate as n.

4

Hull of cyclic codes over $\mathbb{Z}_{p^2}$

Cyclic codes over rings form an important class of linear codes due to their rich algebraic structure.
In this chapter, we consider the ring $\mathbb{Z}_{p^2}$, where p is a prime. $\mathbb{Z}_{p^2}$ is a local ring with unique maximal ideal $p\mathbb{Z}_{p^2}$. Here we extend results over $\mathbb{F}_q$ to $\mathbb{Z}_{p^2}$, we examine carefully the consequences of working over a ring, rather than a finite field.

4.1 | Cyclic codes over $\mathbb{Z}_{p^2}$

A $\mathbb{Z}_{p^2}$−linear code C of length n is a $\mathbb{Z}_{p^2}$-submodule of $\mathbb{Z}_{p^2}^n$. As with cyclic codes over a field, cyclic codes over $\mathbb{Z}_{p^2}$ form an important family of $\mathbb{Z}_{p^2}$-linear codes. C is called cyclic if for every codeword $c \in C$ the codeword obtained by a cyclic shift is also a codeword in C, we view codewords $c = c_0 c_1 \cdots c_{n-1}$ in a cyclic $\mathbb{Z}_{p^2}$-linear code of length n as polynomials $c(X) = c_0 + c_1 X + \cdots + c_{n1} X^{n-1} \in \mathbb{Z}_{p^2}[X]$. If we consider our polynomials as elements of the quotient ring $R_n = \mathbb{Z}_{p^2}[X]/\langle X^n - 1\rangle$, then $Xc(X)$ modulo $X^n - 1$ represents the cyclic shift of c.(See [18]).

A polynomial $f(X) \in \mathbb{Z}_{p^2}[X]$ is nilpotent if there exists a positive integer n such that $f^n(X) = 0$. Also, f is regular if it is not a zero divisor.Define $\mu : \mathbb{Z}_{p^2}[X] \to \mathbb{Z}_p[X]$, the ring homomorphism that maps $c + (p^2)$ to $c + (p)$ and the variable X to X. Observe that $f(X) \in \mathbb{Z}_{p^2}[X]$ is a unit if and only if $\mu(f)$ is a unit, f is regular if and only if $\mu(f(X)) \neq 0$ if and only if $f(X)$ is not nilpotent, if and only if c_i is not nilpotent for some i.

4.1.1 | Factorization of X^n-1 over $\mathbb{Z}_{p^2}$

- A polynomial $f(X) \in \mathbb{Z}_{p^2}[X]$ is irreducible in $\mathbb{Z}_{p^2}$ if whenever $f(X) = g(X)h(X)$ for two polynomials $g(X)$ and $h(X)$ in $\mathbb{Z}_{p^2}[X]$, one of $g(X)$ or $h(X)$ is a unit.
- A polynomial $f \in \mathbb{Z}_{p^2}[X]$ is basic irreducible if its $\mu(f)$ is irreducible in $\mathbb{Z}_p[X]$
- An ideal I of a ring $\mathbb{Z}_{p^2}$ is called a primary ideal provided $ab \in J$ implies that either $a \in J$ or $b^s \in J$ for some positive integer s.
- A polynomial $f \in \mathbb{Z}_{p^2}[X]$ is primary if the principal ideal $\langle f(X)\rangle = \{f(X)g(X)|g(X) \in \mathbb{Z}_{p^2}[X]\}$ is a primary ideal.

Lemma 4.1.1. *[18] If $f \in \mathbb{Z}_{p^2}[X]$ is a basic irreducible polynomial, then $f(X)$ is a primary polynomial.*

Proof. Suppose that $g(X)h(X) \in (f(X))$. As $\mu(f(X))$ is irreducible,

$$d = \gcd(\mu(g(X)), \mu(f(X))) \text{ is either } 1 \text{ or } \mu(f(X))$$

. If $d = 1$, then by the Euclidean Algorithm there exist polynomials $a(X)$ and $b(X) \in \mathbb{Z}_{p^2}[X]$ such that such that

$$\mu(a(X))\mu(g(X)) + \mu(b(X))\mu(f(X)) = 1$$

. Hence $a(X)g(X) + b(X)f(X) = 1 + 2s(X)$ for some $s(X) \in \mathbb{Z}_{p^2}[X]$.
Therefore $a(X)g(X)h(X)(1+2s(X)) + b(X)f(X)h(X)(1+2s(X)) = h(X)(1+2s(X))^2 = h(X)$, implying that $h(X) \in (f(X))$.
Suppose now that $d = \mu(f(X))$. Then there exists $a(X) \in \mathbb{Z}_{p^2}[X]$ such that $\mu(g(X)) = \mu(f(X))\mu(a(X))$, implying that

$$g(X) = f(X)a(X) + 2s(X) \text{ for some } s(X) \in \mathbb{Z}_{p^2}[X]$$

. Hence $g(X)^2 = (f(X)a(X))^2 \in (f(X))$. Thus $f(X)$ is a primary polynomial. □

Two polynomials $f(X)$ and $g(X)$ in $\mathbb{Z}_{p^2}[X]$ are coprime or relatively prime provided $\mathbb{Z}_{p^2}[X] = \langle f(X)\rangle + \langle g(X)\rangle$.

Lemma 4.1.2. *[18] Let $f(X)$ and $g(X)$ be polynomials in $\mathbb{Z}_{p^2}[X]$. Then $f(X)$ and $g(X)$ are coprime if and only if $\mu(f(X))$ and $\mu(g(X))$ are coprime polynomials in $\mathbb{Z}_p[X]$.*

Proof. If $f(X)$ and $g(X)$ are coprime, then

$$a(X)f(X)+b(X)g(X)=1 \text{ for some } a(X) \text{ and } b(X) \text{ in } \mathbb{Z}_{p^2}[x]$$

. Then $\mu(a(X))\mu(f(X))+\mu(b(X))\mu(g(X))=\mu(1)=1,$ implying that $\mu(f(X))$ and $\mu(g(X))$ are coprime.
Conversely, suppose that $\mu(f(X))$ and $\mu(g(X))$ are coprime. Then there exist

$$a(X) \text{ and } b(X) in \mathbb{Z}_{p^2}[X] \text{ such that } \mu(a(X))(f(X))+\mu(b(X))\mu(g(X))=1.$$

Thus $a(X)f(X)+b(X)g(X)=1+2s(X)$ for some $s(X)\in\mathbb{Z}_{p^2}[X]$. But then

$$a(X)(1+2s(X))f(X)+b(X)(1+2s(X))g(X)=(1+2s(X))^2=1$$

showing that $f(X)$ and $g(X)$ are coprime. □

The following result, which is a special case of Hensel's Lemma, shows how to get from a factorization of $\mu(f(X))$ to a factorization of $f(X)$.

Theorem 17. *(Hensel's Lemma) [14] Let $f(X)\in\mathbb{Z}_{p^2}[X]$. Suppose $\mu(f(X))=h_1(X)h_2(X)\cdots h_k(X)$,
where $h_1(X),h_2(X),\cdots,h_k(X)$ are pairwise coprime polynomials in $\mathbb{Z}_p[X]$. Then there exist $g_1(X),g_2(X),\cdots,g_k(X)$ in $\mathbb{Z}_{p^2}[X]$ such that :*

1. *$\mu(g_i(X))=h_i(X)$ for $1\le i\le k$.*
2. *$g_1(X),g_2(X),\cdots,g_k(X)$ are pairwise coprime.*
3. *$f(X)=g_1(X)g_2(X)\cdots g_k(X)$.*

Theorem 18. *[14] Let $(n,p)=1$ be coprime. Then $X^n-1=g_1(X)g_2(X)\cdots g_k(X)$ where $g_i(X)\in\mathbb{Z}_{p^2}[X]$ are unique monic irreducible (and basic irreducible) pairwise coprime polynomials in $\mathbb{Z}_{p^2}[X]$. Furthermore, $X^n-1=\mu(g_1(X))\mu(g_2(X))\cdots\mu(g_k(X))$ is a factorization into irreducible polynomials in $\mathbb{F}_q[X]$.*

In order to factor X^n-1 in $\mathbb{Z}_{p^2}[X]$, we first factor X^n-1 in $\mathbb{F}_q[X]$. The factorization of X^n-1 in $\mathbb{F}_q[X]$ is given by Eq.5.13 and by Theorem18 the factorization of X^n-1 over $\mathbb{Z}_{p^2}$ is:

$$X^n-1 = \prod_{\substack{j\mid n\\ j\in\mathcal{N}_p}}\left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)\right)\prod_{\substack{j\mid n\\ j\notin\mathcal{N}_p}}\left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)f_{ij}^*(X)\right) \tag{4.1}$$

Where

$$\gamma(j;p)=\frac{\phi(j)}{\mathtt{ord}_j(p)},\ \text{and}\ \beta(j;p)=\frac{\phi(j)}{2\mathtt{ord}_j(p)},$$

and $f_{ij}(X)$ and $f_{ij}^*(X)$ form a monic basic irreducible reciprocal polynomial pair and $g_{ij}(X)$ is a monic basic irreducible.

Example 4.1.1. *The factorization of $X^{13}-1$ over $\mathbb{Z}_9[X]$ into a product of basic irreducible polynomials is given by*

$$X^{13}-1=(X-1)(X^3+6X^2+2X+8)(X^3+7X^2+3X+8)(X^3+4X^2+7X+8)(X^3+2X^2+5X+8).$$

4.1.2 | Generating of cyclic codes over $\mathbb{Z}_{p^2}$

To study cyclic codes over $\mathbb{F}_q$ we need to find the ideals of $\mathbb{F}_q/\langle X^n-1\rangle$. Similarly, we need to find the ideals of R_n in order to study cyclic codes over $\mathbb{Z}_{p^2}$. We first need to know the ideal structure of $\mathbb{Z}_{p^2}/\langle f(X)\rangle$, where $f(X)$ is a basic irreducible polynomial.

Lemma 4.1.3. *[14] If $f(X)$ is in $\mathbb{Z}_{p^2}$ and is basic irreducible, then the only ideals of $\mathbb{Z}_{p^2}/\langle f(X)\rangle$ are $\langle 0\rangle, (1+\langle f(X)\rangle)$ and $(p+\langle f(X)\rangle)$.*

Theorem 19. *[14] Let $X^n-1=f_1(X)f_2(X)\cdots f_r(X)$, be a product of basic irreducible and pairwise-coprime polynomials, where $(p,n)=1$ and let $\widehat{f}_i(X)$ denote the product of all $f_j(X)$ except $f_i(X)$. Then any ideal in the ring R_n is a sum of ideal $\langle\widehat{f}_i(X)\rangle$ and $\langle p\widehat{f}_j(X)\rangle$.*

Proof. By Hensel's Lemma 17, such a factorization of X^n-1 exists and is unique. Since the $f_i(X)$ are basic irreducible and pairwise coprime we have

$$X^n-1=\langle f_1(X)\rangle\cap\langle f_2(X)\rangle\cap\langle f_3(X)\rangle\cap\cdots\cap\langle f_r(X)\rangle,$$

and for $1 \leq i, j \leq r, i \neq j$

$$\mathbb{Z}_{p^2}[X] = \langle f_i(X)\rangle + \langle f_j(X)\rangle.$$

Thus by Chinese Remainder

$$\begin{aligned} R_n &= \mathbb{Z}_{p^2}[x]/\langle f_1(X)\rangle \cap \mathbb{Z}_{p^2}[X]/\langle f_2(X)\rangle \cap \mathbb{Z}_{p^2}[X]/\langle f_3(X)\rangle \cap \cdots \cap \mathbb{Z}_{p^2}[X]/\langle f_r(X)\rangle \\ &\cong \bigoplus \sum_{i=1}^{r} \mathbb{Z}_{p^2}[X]/\langle f_i(X)\rangle \end{aligned}$$

Consequently, if I is an ideal of R_n, then

$$I = I_1 \oplus I_2 \oplus \cdots \oplus I_r,$$

where I_i is an ideal of the ring $\mathbb{Z}_{p^2}[X]/\langle f_i\rangle$, for $i = 1, 2, \cdots, r$. By lemma4.1.3

$$I_i = 0, \quad \mathbb{Z}_{p^2}[X]/\langle f_i(X)\rangle \text{ or } \quad (p + \langle f_i(X)\rangle).$$

If $I_i = \mathbb{Z}_{p^2}[X]/\langle f_i(X)\rangle$, then it corresponds to the ideal $\langle \widehat{f_i}(X)\rangle$ in the ring R_n, if $I_i = (p + \langle f_i(X)\rangle)$, then it corresponds to the ideal $\langle p\widehat{f_j}(X)\rangle$. In any case, the ideal I is a sum of $\langle \widehat{f_i}(X)\rangle$ and $\langle p\widehat{f_j}(X)\rangle$. □

Theorem 20. *[14] Suppose C is a cyclic code of length n over $\mathbb{Z}_{p^2}$. Let* $\gcd(n, p) = 1$, *then there exist unique monic polynomials f, g and h such that* $X^n - 1 = f(X)g(X)h(X)$ *and*
$C = \langle f(X)g(X)\rangle \oplus \langle pf(X)h(X)\rangle$. *Furthermore, C has type* $p^{2\deg(g(X))}p^{\deg(g(X)h(X))}$
When $g(X) = 1, C = \langle f(X)\rangle$ *and* $|C| = p^{n-\deg f(X)}$.
When $h(X) = 1, C = \langle pf(X)\rangle$ *and* $|C| = p^{n-\deg f(X)}$.

Proof. We know that $X^n - 1$ has a unique factorization such that $X^n - 1 = f_1(X)f_2(X)\cdots f_r(X)$, where the $f_i(X)$ are basic irreducible and pairwise coprime, We also know, by theorem 19, that C is a sum of $\langle \widehat{f_i}(X)\rangle$ and $\langle p\widehat{f_j}(X)\rangle$. By permuting the subscripts of $f_i(X)$, we can suppose that C is a sum of
$\langle \widehat{f}_{k+1}(X)\rangle, \langle \widehat{f}_{k+2}(X)\rangle, \cdots, \langle \widehat{f}_{k+l}(X)\rangle, \langle p\widehat{f}_{k+l+1}(X)\rangle, \langle p\widehat{f}_{k+l+2}(X)\rangle, \cdots, \langle p\widehat{f_r}(X)\rangle$
Then

$$C = \langle f_1(X)f_2(X)\cdots f_k(X)f_{k+l+1}(X)f_{k+l+2}(X)\cdots f_r(X), pf_1(X)f_2(X)\cdots f_k(X)f_{k+l}(X)\cdots f_{k+l}(X)\rangle$$

where

$$f_1(X)f_2(X)\cdots f_k(X),\ g = f_{k+1}(X)f_{k+2}(X)\cdots f_{k+l}(X) \text{ or } 1 \quad \text{if } l = 0$$

and

$$g(X) = f_{k+l+1}(X)f_{k+l+2}(X)\cdots f_r(X) \text{ or } 1 \quad \text{if } k+l = r$$

When $g(X) \neq 1, f(X)g(X)$ and $h(X)$ are coprime, $\langle f(X)g(X)\rangle \cap \langle pf(X)h(X)\rangle = 0$. Therefore

$$|C| = |f(X)g(X)||pf(X)h(X)| = (p^2)^{n-\deg(f(X))-\deg(g(X))}p^{n-\deg(f(X))-\deg(h(X))}.$$

When $g(X) = 1$, the above identity is still true because in this case $C = \langle f(X)\rangle$ and $|C| = (p^2)^{n-\deg(f(X))}$. When $g(X) = 1$, the above identity is still true because in this case $C = \langle pf(X)\rangle$ and $|C| = p^{n-\deg(f(X))}$. □

Corollary 5. *Let* $\gcd(n,p) = 1$. *Assume* $X^n - 1$ *is a product of* k *irreducible polynomial in* $\mathbb{Z}_{p^2}[X]$. *Then there are* 3^k *cyclic codes over* $\mathbb{Z}_{p^2}$ *of length* n.

The next theorem discusses the dual of C.

Theorem 21. *[14] Let* C *is a cyclic code of length* n *over* $\mathbb{Z}_{p^2}$. *Let* $\gcd(n,p) = 1$, *then there exist are unique monic polynomials* $f(X), g(X)$ *and* h *such that* $X^n - 1 = f(X)h(X)g(X)$ *and* $C = \langle f(X)g(X), pf(X)h(X)\rangle$. *Furthermore,* C *has type* $p^{2\deg(h(X))}p^{\deg(g(X)h(X)}$ *Then*

$$C^\perp = \langle g^*(X)h^*(X), ph^*(X)f^*(X)\rangle \text{ and } |C^\perp| = p^{2\deg(f(X))}p^{\deg(g(X))}.$$

- *If* $g(X) = 1$, *then* $C = \langle f(X)\rangle$ *and* $C^\perp = \langle h^*(X)\rangle$.
- *If* $h(X) = 1$, *then* $C = \langle pf(X)\rangle$ *and* $C^\perp = \langle g^*(X), pf^*(X)\rangle$, *where* $h^*(X), f^*(X), g^*(X)$ *are respectively reciprocal polynomials of* $f(X), h(X)$ *and* $g(X)$.

Proof. We know that

$$\langle g^*(X)h^*(X)\rangle \subseteq \langle g^*(X)\rangle \subseteq \langle f(X)g(X), pf(X)h(X)\rangle^\perp$$

and similarly

$$\langle ph^*(X)f^*(X)\rangle \subseteq \langle h^*(X)\rangle \subseteq \langle f(X)g(X), pf(X)h(X)\rangle^\perp.$$

Therefore,

$$\langle g^*(X)h^*(X), ph^*(X)f^*(X)\rangle \subseteq \langle h^*(X)\rangle \subseteq \langle f(X)g(X), pf(X)h(X)\rangle^{\perp}$$

Since

$$\begin{aligned} |\langle g^*(X)h^*(X), ph^*(X)f^*(X)\rangle| &= p^{2(n-\deg(h(x))-\deg(g(X)))}p^{n-\deg(h(X))-\deg(f(X))} \\ &= |\langle f(X)g(X), pf(X)h(X)\rangle^{\perp}|, \end{aligned}$$

we have $\langle g^*(X)h^*(X), ph^*(X)f^*(X)\rangle = \langle f(X)g(X), pf(X)h(X)\rangle^{\perp}$. □

4.1.3 | Characterization of the Hulls of cyclic codes

Here, we focus on algebraic structures of the hulls of cyclic codes of length n over $\mathbb{Z}_{p^2}$. The following lemma is useful in the study of their generators.

Lemma 4.1.4. *[17] Let $a = (u_0, u_1, \cdots, u_{n-1})$ and $b = (b_0, b_1, \cdots, b_{n-1})$ be vectors in $\mathbb{Z}_{p^2}^n$ with corresponding polynomial $a(X)$ and $b(X)$, respectively. Then a is orthogonal to b and all its shifts if and only if $a(X)b^*(X) = 0$ in $\mathbb{Z}_{p^2}[X]/\langle X^n - 1\rangle$.*

Theorem 22. *[17] Let C be a cyclic code of length n over $\mathbb{Z}_{p^2}$ generated by $\langle f(X)g(X), pf(X)h(X)\rangle = \langle f(X)g(X), pf(X)\rangle$, where $X^n - 1 = f(X)h(X)g(X)$ and $f(x), g(X)$ and $h(X)$ are monic pairwise coprime polynomials. Then $\mathscr{H}(C)$ is generated by*

$$\langle lcm(f(X)g(X), h^*(X)g^*(X)), p\,lcm(f^*(X), h^*(X))\rangle.$$

Furthermore, $\mathscr{H}(C)$ is of type $(p^2)^{\deg H(X)}p^{\deg G(X)}$, where

$$H(X) = \gcd(h(X), f^*(X)) \text{ and } G(X) = \frac{X^n - 1}{\gcd(h(X), f^*(X))\,lcm(f^*(X), h^*(X))}.$$

Proof. Note that $C^{\perp}$ is generated by $\langle h^*(X)g^*(X), ph^*(X)f^*(X)\rangle = \langle h^*(X)g^*(X), ph^*(X)\rangle$ Let C' be a cyclic code of length n over $\mathbb{Z}_{p^2}$ whose generators are of the form $\langle F(X)G(X), pF(X)\rangle$, where $F(X) = \mathtt{lcm}(f^*(X), h^*(X))$

$$G(X) = \frac{X^n - 1}{\gcd(h(X), f^*(X))\mathtt{lcm}(f^*(X), h^*(X))} \quad \text{and} \quad H(X) = \gcd(h(X), f^*(X)).$$

It is not difficult to see that $X^n-1 = F(X)G(X)H(X)$ and the polynomials $F(X), G(X)$ and $H(X)$ are monic pairwise coprime. Since $\langle F(X)G(X), pF(X)\rangle \subseteq \langle f(X)g(X), pf(X)\rangle$ and $\langle F(X)G(X), pF(X)\rangle \subseteq \langle h^*(X)g^*(X), ph^*(X)\rangle$, we have $C \subseteq \mathscr{H}(C)$.
Next, we show that $\mathscr{H}(C) \subseteq C^{'}$. Since $\mathscr{H}(C)$ is a cyclic code of length n over $\mathbb{Z}_{p^2}$, assume that $\mathscr{H}(C)$ has generators of the form $\langle A(X)B(X), pA(X)\rangle$ where $X^n-1 = A(X)B(X)C(X)$ and the polynomials $A(X), B(X)$ and $C(X)$ are pairwise coprime. Since $\mathscr{H}(C) \subseteq C^{\perp}$ is orthogonal to C, by Lemma 4.1.4, we have

$$A(X)B(X).pf^*(X) = 0 \text{ and } pA(X).f^*(X).g^*(X) = 0,$$

which imply that $h^*(X).g^*|A(X)B(X)$ and $h^*|A(X)$. Similarly, $\mathscr{H}(C) \subseteq C$is orthogonal to $C^{\perp}$ which implies that

$$A(X)B(X).ph(X) = 0 \text{ and } pA(X).h(X)g(X) = 0,$$

by Lemma 4.1.4. It follows that $f(X)g(X)|A(X)B(X)$ and $f(X)|A(X)$. Consequently, $\mathtt{lcm}(f(X)g(X), h^*(X)g^*(X))|A(X)B(X)$ and $\mathtt{lcm}(h^*(X), f(X))|A(X)$ which imply that $F(X)G(x)|A(X)B(X)$ and $F(X)|A(X)$. Hence, $\mathscr{H}(C) \subseteq C$. Therefore, $\mathscr{H}(C) = C$. □

Example 4.1.2. *The factorization of $X^{13}-1$ over $\mathbb{Z}_9[X]$ into a product of basic irreducible polynomials is given by*

$$X^{13}-1 = (X-1)(X^3+6X^2+2X+8)(X^3+7X^2+3X+8)(X^3+4X^2+7X+8)(X^3+2X^2+5X+8).$$

Let C be the cyclic code of length 13 over $\mathbb{Z}_9$ generated by

$$\begin{aligned} C &= \langle f(X)g(X), 3f(X)\rangle \\ &= \langle (X^3+6X^2+2X+8)(X^3+7X^2+3X+8)(X^3+4X^2+7X+8)(X^3+2X^2+5X+8), \\ &\quad 3(X^3+6X^2+2X+8)(X^3+4X^2+7X+8)\rangle, \end{aligned}$$

where $f(X) = (X^3+6X^2+2X+8)(X^3+4X^2+7X+8)$, $g(X) = (X^3+7X^2+3X+8)(X^3+2X^2+5X+8) = f^\star(X)$, and $h(X) = (X-1) = h^\star(X)$.
From Theorem 21, $C^{\perp}$ is of the form

$$\langle h^\star(X)g^\star(X), 3h^\star(X)\rangle = \langle (X-1)(X^3+6X^2+2X+8)(X^3+4X^2+7X+8), 3(X-1)\rangle.$$

By Theorem 22, $\mathscr{H}(C)$ is generated by

$$\begin{aligned}\mathscr{H}(C) &= \langle lcm(f(X)g(X), h^*(X)g^*(X)), p\,lcm(f^*(X), h^*(X))\rangle \\ &= \langle 3\,lcm((X^3+7X^2+3X+8)(X^3+2X^2+5X+8)\rangle.\end{aligned}$$

4.1.4 | Parameters and p-dimensions of hulls of cyclic codes

In this subsection, the parameters of the hulls of cyclic codes of length n where $\gcd(p,n)=1$ over $\mathbb{Z}_{p^2}$ are investigated and the $p-$dimensions of $\mathscr{H}(C)$ are determined. The parameters of the hulls of cyclic codes are given in Theorem 23 based on the following lemma. The following lemma is required in its proof.

Lemma 4.1.5. *[17] Let β be a positive integer. For $1 \le i \le \beta$, let (v_i, z_i), (w_i, d_i) and (u_i, b_i) be elements in $\{(0,0),(1,0),(0,1)\}$. Let $a_i = \min\{1-v_i-z_i, w_i\} + \min\{1-w_i-d_i, v_i\}$. Then $a_i \in \{0,1\}$. Moreover, the following statements hold.*

1. $2-\min\{1-v_i,z_i,w_i\}-\max\{v_i,1-w_i-d_i\}-\min\{1-w_i-d_i,v_i\}-\max\{w_i,1-v_i-z_i\} = z_i+d_i$.
2. *If $a_i = 0$, then $z_i + d_i \in \{0,1,2\}$.*
3. *If $a_i = 1$, then $z_i + d_i = 0$.*
4. *$a = \sum_{i=1}^{\beta} a_i$ then $\sum_{i=1}^{\beta}(z_i+d_i) = c$ for some $0 \le c \le 2(\beta - a)$.*

Theorem 23. *[17] Let n be a positive integer such that $\gcd(n,p)=1$. Then the parameters of the hull of a cyclic code of length n over $\mathbb{Z}_{p^2}$ are of the form $p^{2k_1}p^{k_2}$, where*

$$\begin{aligned}k_1 &= \sum_{\substack{j\,|\,n \\ j\notin\mathcal{N}_p}} ord_j(p).a_j; \\ k_2 &= \sum_{\substack{i\,|\,n \\ i\in\mathcal{N}_p}} ord_i(p)\cdot b_i + \sum_{\substack{j\,|\,n \\ j\notin\mathcal{N}_p}} ord_j(p)\cdot c_j,\end{aligned}$$

where $0 \le a_j \le \beta(j;p)$, $0 \le b_i \le \gamma(i;p)$, and $0 \le c_j \le 2(\beta(j;p)-a_j)$.

Proof. Let C bea cyclic code of length n over $\mathbb{Z}_{p^2}$ generated by $\langle f(X)g(X), pf(X)h(X)\rangle = \langle f(X)g(X), pf(X)\rangle$, where $X^n - 1 = f(x)g(X)h(X)$ and $f(X), g(X)$ and $h(X)$ are monic pairwise coprime polynomials. Then $\mathscr{H}(C)$ is generated by

$$\langle \mathtt{lcm}(f(X)g(X), h^*(X)g^*(X)), p\,\mathtt{lcm}(f^*(X), h^*(X))\rangle.$$

Furthermore, $\mathscr{H}(C)$ is of type $(p^2)^{\deg H(X)} p^{\deg G(X)}$, where

$$H(X) = \gcd(h(X), f^*(X)) \text{ and } G(X) = \frac{X^n-1}{\gcd(h(X), f*(X))\,\mathtt{lcm}(f*(X), h*(X)}.$$

We have

$$\begin{aligned}
f(X) &= \prod_{\substack{j\mid n\\ j\in\mathscr{N}_p}}\left(\prod_{i=1}^{\gamma(j;p)} g_{ij}(X)^{u_{ij}}\right)\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_p}}\left(\prod_{i=1}^{\beta(j;p)} f_{ij}(X)^{v_{ij}} f_{ij}^*(X)^{w_{ij}}\right);\\
g(X) &= \prod_{\substack{j\mid n\\ j\in\mathscr{N}_p}}\left(\prod_{i=1}^{\gamma(j;p)} g_{ij}(X)^{b_{ij}}\right)\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_p}}\left(\prod_{i=1}^{\beta(j;p)} f_{ij}(X)^{z_{ij}} f_{ij}^*(X)^{d_{ij}}\right);\\
h(X) &= \prod_{\substack{j\mid n\\ j\in\mathscr{N}_p}}\left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{\{1-u_{ij}-b_{ij}\}}\right)\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_p}}\left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\{1-v_{ij}-z_{ij}\}} f_{ij}^*(X)^{\{1-w_{ij}-d_{ij}\}}\right);\\
f^*(X) &= \prod_{\substack{j\mid n\\ j\in\mathscr{N}_p}}\left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{u_{ij}}\right)\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_p}}\left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{w_{ij}} f_{ij}^*(X)^{v_{ij}}\right);\\
g^*(X) &= \prod_{\substack{j\mid n\\ j\in\mathscr{N}_p}}\left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{b_{ij}}\right)\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_p}}\left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{d_{ij}} f_{ij}^*(X)^{z_{ij}}\right);\\
h^*(X) &= \prod_{\substack{j\mid n\\ j\in\mathscr{N}_p}}\left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{\{1-u_{ij}-b_{ij}\}}\right)\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_p}}\left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\{1-w_{ij}-d_{ij}\}} f_{ij}^*(X)^{\{1-v_{ij}-z_{ij}\}}\right);
\end{aligned}$$

where $(u_{ij}, b_{ij}), (v_{ij}, z_{ij}), (w-ij, d_{ij}) \in \{(0,0),(1,0),(0,1)\}$.
First we determine $\deg H(X)$. Observe that

$$\begin{aligned} H(X) &= \gcd(h(X), f^*(X)); \\ &= \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_p}} \left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\min\{1-v_{ij}-z_{ij}, w_{ij}\}} f_{ij}^*(X)^{\min\{1-w_{ij}-d_{ij}, v_{ij}\}} \right); \\ &= \sum_{\substack{i \mid n \\ i \notin \mathcal{N}_p}} \left(\sum_{i=1}^{\beta(j;q)} (\min\{1-v_{ij}-z_{ij}, w_{ij}\} + \min\{1-w_{ij}-d_{ij}, v_{ij}\}) \right); \\ &= \sum_{\substack{i \mid n \\ i \notin \mathcal{N}_p}} \mathtt{ord}_j(p).a_j, \end{aligned}$$

where $0 \leq a_j \leq \beta(j,p)$. Next we compute $\deg G(X)$. Since

$$\begin{aligned} \mathtt{lcm}(f(X), h^*(X)) &= \prod_{\substack{j \mid n \\ j \in \mathcal{N}_p}} \left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{\max\{u_{ij}, 1-u_{ij}-b_{ij}\}} \right) \\ &\times \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_p}} \left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\max\{v_{ij}, 1-w_{ij}-d_{ij}\}} f_{ij}^*(X)^{\max\{w_{ij}, 1-v_{ij}-z_{ij}\}} \right); \end{aligned}$$

and

$$\begin{aligned} \mathtt{gcd}(h(X), f^*(X)) \cdot \mathtt{lcm}(f(X), h^*(X)) &= \prod_{\substack{j \mid n \\ j \in \mathcal{N}_p}} \left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(x)^{\max\{u_{ij}, 1-u_{ij}-b_{ij}\}} \right) \\ \times \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_p}} \left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{\max\{v_{ij}, 1-w_{ij}-d_{ij}\}} f_{ij}^*(X)^{\min\{1-w_{ij}-d_{ij}, v_{ij}\} + \max\{w_{ij}, 1-v_{ij}-z_{ij}\}} \right). \end{aligned}$$

It can be deduced that

$$\begin{aligned} G(X) &= \frac{X^n-1}{\mathtt{gcd}(h(X),f^*(X))\mathtt{lcm}(f^*(X),h^*(X))} \\ &= \prod_{\substack{j\mid n \\ j\in\mathcal{N}_p}} \left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{1-\max\{u_{ij},1-u_{ij}-b_{ij}\}} \right) \\ &\times \prod_{\substack{j\mid n \\ j\notin\mathcal{N}_p}} \left(\prod_{i=1}^{\beta(j;q)} f_{ij}(X)^{1-\min\{1-v_{ij}-z_{ij},w_{ij}\}-\max\{v_{ij},1-w_{ij}-d_{ij}\}} \right); \\ &\times \prod_{\substack{j\mid n \\ j\notin\mathcal{N}_p}} \left(\prod_{i=1}^{\beta(j;q)} f^*_{ij}(X)^{1-\min\{1-w_{ij}-d_{ij},v_{ij}\}-\max\{w_{ij},1-v_{ij}-z_{ij}\}} \right); \end{aligned}$$

By Lemma 4.1.5, we can conclude that

$$
\begin{aligned}
\deg(G(X)) &= \deg\left(\frac{X^n-1}{\gcd(h(X),f^*(x))\,\mathtt{lcm}(f^*(X),h^*(X))}\right)\\
&= \prod_{\substack{j\mid n\\ j\in\mathcal{N}_p}}\left(\prod_{i=1}^{\gamma(j;q)} g_{ij}(X)^{1-\max\{u_{ij},1-u_{ij}-b_{ij}\}}\right)\\
&\quad\times\prod_{\substack{j\mid n\\ j\notin\mathcal{N}_p}}\prod_{i=1}^{\beta(j;q)} f_{ij}(x)^{1-\min\{1-v_{ij}-z_{ij},w_{ij}\}-\max\{v_{ij},1-w_{ij}-d_{ij}\}};\\
&\quad\times\prod_{\substack{j\mid n\\ j\notin\mathcal{N}_p}}\prod_{i=1}^{\beta(j;q)} f^*_{ij}(X)^{1-\min\{1-w_{ij}-d_{ij},v_{ij}\}-\max\{w_{ij},1-v_{ij}-z_{ij}\}};\\
&= \sum_{\substack{i\mid n\\ i\in\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\gamma(j;q)}(1-\max\{u_{ij},1-u_{ij}-b_{ij}\})\\
&\quad+\sum_{\substack{i\mid n\\ i\notin\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\beta(j;q)}(2-\min\{1-v_{ij}-z_{ij},w_{ij}\})\\
&\quad-\sum_{\substack{i\mid n\\ i\notin\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\beta(j;q)}\max\{v_{ij},1-w_{ij}-d_{ij}\}\\
&\quad-\sum_{\substack{i\mid n\\ i\notin\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\beta(j;q)}\min\{1-w_{ij}-d_{ij},v_{ij}\}\\
&\quad-\sum_{\substack{i\mid n\\ i\notin\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\beta(j;q)}\max\{w_{ij},1-v_{ij}-z_{ij}\})\\
&= \sum_{\substack{i\mid n\\ i\in\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\gamma(j;q)}(1-\max\{u_{ij},1-u_{ij}-b_{ij}\})\\
&\quad+\sum_{\substack{i\mid n\\ i\notin\mathcal{N}_p}}\mathtt{ord}_j(p)\sum_{i=1}^{\beta(j;q)}(z_{ij}+d_{ij})\\
&= \sum_{\substack{i\mid n\\ i\in\mathcal{N}_p}}\mathtt{ord}_i(p)\cdot b_i+\sum_{\substack{j\mid n\\ j\notin\mathcal{N}_p}}\mathtt{ord}_j(p)\cdot c_j,
\end{aligned}
$$

where $0 \le a_j \le \beta(j,p)$, $0 \le b_i \le \gamma(i,p)$, and $0 \le c_j \le 2(\beta(j,p) - a_j)$. □

Corollary 6. *Let n be an odd integer coprime with p such that $n \in N_p$. Then the parameters of the hull of a cyclic code of length n over $\mathbb{Z}_{p^2}$ are of the form $(p^2)^0 p^{k_2}$, where*

$$k_2 = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_p}} \mathtt{ord}_i(p) \cdot b_i, \quad 0 \le b_i \le \gamma(i,p).$$

The previous discussion leads to the Algorithm 11 and justifies its correctness. Examples 4.1.3, 4.1.4 show different outputs of the algorithm.

Algorithm 1: Parameters of the Euclidean hull of a cyclic codes over $\mathbb{Z}_{p^2}$.

Input: Length n, and a finite ring $\mathbb{Z}_{p^2}$ such that $\mathtt{gcd}(p,n) = 1$.
Output: All possible 2-tuples (k_1, k_2) describing the parameters of the Euclidean hull of a cyclic codes

1 .

1. For each divisor of n, consider the following case:
   (a) If $i \in \mathcal{N}_p$, compute $\mathtt{ord}_i(p)$ and $\gamma(i;p)$.
   (b) If $j \notin \mathcal{N}_p$, compute $\mathtt{ord}_j(p)$ and $\beta(j;p)$.
2. Compute $k_1 = \sum_{\substack{j \mid n \\ j \notin \mathcal{N}_p}} \mathtt{ord}_j(p) \cdot a_j$, where $0 \le a_j \le \beta(j;p)$.
3. For a fixed a_j in 2, compute : $k_2 = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_p}} \mathtt{ord}_i(p) \cdot b_i + \sum_{\substack{j \mid n \\ j \notin \mathcal{N}_p}} \mathtt{ord}_j(p) \cdot c_j$, where $0 \le b_i \le \gamma(i;p)$ and $0 \le c_j \le 2 \cdot (\beta(j;p) - a_j)$.

Example 4.1.3. *All the possible parameters (k_1, k_2) of the hull of a cyclic code of length 13 over $\mathbb{Z}_9$ are determined as follows.*

1. *The divisors of 13 are 1 and 13.*
   a) *We have $1 \in \mathcal{N}_3$, so $\mathtt{ord}_1(3) = 1$ and $\gamma(1;3) = 1$.*
   b) *We have $13 \notin \mathcal{N}_3$, so $\mathtt{ord}_1 3(3) = 3$ and $\beta(13;3) = 2$.*

2. *It follows that*

$$\begin{aligned} k_1 &= 3a_{13}, \text{ where } 0 \le a_{13} \le 2 \\ k_2 &= b_1 + 3c_{13} \text{ where } 0 \le b_1 \le 1 \text{ and } 0 \le c_{13} \le 2(2-a_{13}). \end{aligned}$$

Hence, the all possible parameters (k_1, k_2) of the hulls of cyclic codes of length 13 over $\mathbb{Z}_9$ are given in the following table

k_1	k_2
0	*0, 1, 3, 4, 6, 7, 9, 10, 12, 13*
3	*0, 1, 3, 4, 6, 7*
6	*0, 1*

Example 4.1.4. *All the possible parameters (k_1, k_2) of the hull of a cyclic code of length 21 over $\mathbb{Z}_4$ are determined as follows.*

1. *The divisors of 21 are* $\{1,3,7,21\}1$.

   a) *We have* $1,3 \in \mathcal{N}_2$, *so* $ord_1(2) = 1$, $ord_3(2) = 2$ *and* $\gamma(1;2) = 1 = \gamma(3;2)$.

   b) *We have* $7,21 \notin \mathcal{N}_3$, *so* $ord_7(2) = 3$, $ord_2 1(2) = 6$ *and* $\beta(7;2) = 1 = \beta(21;2)$.

2. *It follows that*
   $k_1 = 3a_7 + 6a_{21}$, *where* $0 \le a_7, a_{21} \le 0$
   For $(a_7, a_7) = (0,0)$, *we have* $k_1 = 0$ *and*

   $k_2 = b_1 + 2b_3 + 3c_7 + 6c_{21}$, *where* $0 \le b_1, b_3 \le 1$ *and* $0 \le c_7, c_{21} \le 2$. *So* $k_2 \in \{0, 1, \cdots, 21\}$.

   For $(a_7, a_{21}) = (1,0)$, *we have* $k_1 = 3$ *and*

   $k_2 = b_1 + 2b_3 + 3c_7 + 6c_{21}$, *where* $0 \le b_1, b_3 \le 1, c_7 = 0$ *and* $0 \le c_{21} \le 2$.

   Hence, $k_2 \in \{0,1,2,3,6,7,8,9,12,13,14,15\}$.
   For $(a_7, a_{21}) = (0,1)$, *we have* $k_1 = 6$ *and*

   $k_2 = b_1 + 2b_3 + 3c_7 + 6c_{21}$, *where* $0 \le b_1, b_3 \le 1, 0 \le c_7 \le 2$ *and* $c_{21} = 0$.

Thus $k_2 \in \{0,1,\cdots,9\}$.
For $(a_7,a_{21})=(1,1)$, *then* $k_1=9$ *and*

$$k_2 = b_1+2b_3+3c_7+6c_{21},\ \textit{where}\ 0\le b_1,b_3\le 1, c_7=0\ \textit{and}\ c_{21}=0.$$

Hence, $k_2 \in \{0,1,2,3\}$.

Hence, the all possible parameters (k_1,k_2) *of the hulls of cyclic codes of length* 21 *over* $\mathbb{Z}_4$ *are given in the following table*

k_1	k_2
0	*0, 1,*$\cdots$*,21*
3	*0, 1,2, 3, 6, 7, 8, 9, 12, 13, 14, 15*
6	*0, 1,*$\cdots$*,9*
9	*0, 1, 2, 3*

For a linear code C of length n over $\mathbb{Z}_{p^2}$, denote by $\dim_p(C)=\log_p(|C|)$ the p-dimension of C. A formula for the p-dimensions of the hulls of cyclic codes of length n over $\mathbb{Z}_{p^2}$ is given as follows.

Theorem 24. *[17] Let* $\gcd(n,p)=1$. *Then the* p*-dimensions of the hull of cyclic codes of length* n *over* $\mathbb{Z}_p^2$ *are of the form*

$$\sum_{\substack{i\,|\,n\\ i\in\mathcal{N}_p}} ord_j(p).\triangle_j + \sum_{\substack{i\,|\,n\\ i\notin\mathcal{N}_p}} ord_j(p).\blacktriangle_j,$$

where $0\le\triangle_j\le\gamma(j,q)$ *and* $0\le\blacktriangle\le 2\beta(j,q)$.

Proof. Let C be a cyclic code of length n over $\mathbb{Z}_{p^2}$ generated by
$\langle f(X)g(X), pf(X)h(X)\rangle = \langle f(X)g(X), pf(X)\rangle$,
where $X^n-1=f(X)g(X)h(X)$ and $f(X),g(X)$ and $h(X)$ are monic pairwise co-prime polynomials. Then $\mathscr{H}(C)$ is generated by

$$\langle \mathtt{lcm}(f(X)g(X),h^*(X)g^*(X)), p\,\mathtt{lcm}(f^*(X),h^*(X))\rangle.$$

Furthermore, $\mathscr{H}(C)$ is of type $(p^2)^{\deg H(X)} p^{\deg G(X)}$, and the p-dimension of $Hull(C)$ is $2\deg H(X)+\deg G(X)$, where

$$H(X)=\gcd(h(X),f^*(X)) \text{ and } G(X)=\frac{X^n-1}{\gcd(h(X),f^*(X))\,\mathtt{lcm}(f^*(X),h^*(X))}.$$

It can be deduced that

$$\begin{aligned}
\mathtt{dim}_p(\mathscr{H}(C)) &= 2\deg H(X)+\deg G(X);\\
&= 2\sum_{\substack{i\mid n\\ i\notin\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\beta(j;q)} (\min\{1-v_{ij}-z_{ij},w_{ij}\}+\min\{1-w_{ij}-d_{ij},v_{ij}\})\\
&\quad+\sum_{\substack{i\mid n\\ i\in\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\gamma(j;q)} (1-\max\{u_{ij},1-u_{ij}-b_{ij}\})\\
&\quad+\sum_{\substack{i\mid n\\ i\notin\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\beta(j;q)} (2-\min\{1-v_{ij}-z_{ij},w_{ij}\}-\max\{v_{ij},1-w_{ij}-d_{ij}\}\\
&\quad-\min\{1-w_{ij}-d_{ij},v_{ij}\}-\max\{w_{ij},1-v_{ij}-z_{ij}\})\\
&= \sum_{\substack{i\mid n\\ i\in\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\gamma(j;q)} (1-\max\{u_{ij},1-u_{ij}-b_{ij}\})\\
&\quad+\sum_{\substack{i\mid n\\ i\notin\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\beta(j;q)} (2+\min\{1-v_{ij}-z_{ij},w_{ij}\}-\max\{v_{ij},1-w_{ij}-d_{ij}\}\\
&\quad+\min\{1-w_{ij}-d_{ij},v_{ij}\}-\max\{w_{ij},1-v_{ij}-z_{ij}\})\\
&= \sum_{\substack{i\mid n\\ i\in\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\gamma(j;q)} .\,\triangle_{ij}+\sum_{\substack{i\mid n\\ i\notin\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\beta(j;q)} \blacktriangle_{ij},
\end{aligned}$$

where

$$\begin{aligned}
\triangle_{ij} &= (1-\max\{u_{ij},1-u_{ij}-b_{ij}\}),\\
\blacktriangle_{ij} &= (2+\min\{1-v_{ij}-z_{ij},w_{ij}\}-\max\{v_{ij},1-w_{ij}-d_{ij}\}\\
&\quad+\min\{1-w_{ij}-d_{ij},v_{ij}\}-\max\{w_{ij},1-v_{ij}-z_{ij}\}).
\end{aligned}$$

It is not difficult to see that $0 \leq \triangle_{ij} \leq 1$ and $0 \leq \blacktriangle_{ij} \leq 2$. Then we have

$$\begin{aligned}\dim_p(\mathscr{H}(C)) &= \sum_{\substack{i|n \\ i\in\mathscr{N}_p}} \mathrm{ord}_j(p) \sum_{i=1}^{\gamma(j;p)} \triangle_{ij} + \sum_{\substack{i|n \\ i\notin\mathscr{N}_p}} \mathrm{ord}_j(p) \sum_{i=1}^{\beta(j;p)} \blacktriangle_{ij}. \\ &= \sum_{\substack{i|n \\ i\in\mathscr{N}_p}} \mathrm{ord}_j(p).\triangle_j + \sum_{\substack{i|n \\ i\notin\mathscr{N}_p}} \mathrm{ord}_j(p).\blacktriangle_j,\end{aligned}$$

where $\triangle_j = \sum_{i=1}^{\gamma(j;q)} \triangle_{ij}$ and $\blacktriangle_j = \sum_{i=1}^{\beta(j;q)} \blacktriangle_{ij}$ □

4.1.5 | The average p-dimensions $\mathrm{E}_p(n)$

The average p-dimension of the hull of cyclic codes of length n over $\mathbb{Z}_{p^2}$ is defined to be

$$\mathrm{E}_p(n) = \sum_{C\in\mathscr{C}(n,p^2)} \frac{\dim_p(\mathscr{H}(C))}{|\mathscr{C}(n,p^2)|},$$

where $\mathscr{C}(n,p^2)$ denote the set of all cyclic codes over length n over $\mathbb{Z}_{p^2}$. The average p-dimension of $\mathscr{H}(C)$ is based on the following lemma. The following lemma is required in its proof.

Lemma 4.1.6. *Let $(v,z),(w,d),(u,b) \in \{(0,0),(1,0),(0,1)\}$. Then*

1. $E(1-\max\{u,1-u-b\}) = \frac{1}{3}$
2. $E(2+\min\{1-v-z,w\}-\max\{v,1-w-d\}+\min\{1-w-d,v\}-\max\{w,1-v-z\}) = \frac{10}{9}$.

Theorem 25. *[17] Let p be a prime number and let n be a positive integer such that $p \nmid n$. Then the average p-dimension of the hull of cyclic codes of length n over $\mathbb{Z}_{p^2}$ is*

$$E_p(n) = \frac{5}{9}n - \frac{2}{9}\mathscr{B}_n.$$

Proof. Let C be a cyclic code of length n over $\mathbb{Z}_{p^2}$ generated by $\langle f(X)g(X), pf(X)h(X)\rangle = \langle f(X)g(X), pf(X)\rangle$,

where $X^n-1 = f(X)g(X)h(X)$ and $f(X), g(X)$ and $h(X)$ are monic pairwise coprime polynomials. Then $\mathscr{H}(C)$ is generated by

$$\langle \mathtt{lcm}(f(X)g(X), h^*(X)g^*(X)), p\,\mathtt{lcm}(f^*(X), h^*(X))\rangle.$$

Furthermore, $\mathscr{H}(C)$ is of type $(p^2)^{\deg H(X)} p^{\deg G(X)}$, and the p-dimension of $Hull(C)$ is $2\deg H(X) + \deg G(X)$, where

$$H(X) = \gcd(h(X), f^*(X)) \text{ and } G(X) = \frac{X^n-1}{\gcd(h(X), f^*(X))\,\mathtt{lcm}(f^*(X), h^*(X))}.$$

Let Y be the random variable of the $\mathtt{dim}_p(\mathscr{H}(C))$, where C is chosen randomly from $\mathscr{C}(n,p^2)$ with uniform probability. Let $\mathtt{E}(Y)$ be the expectation of Y. Thus $\mathtt{E}_p(n) = \mathtt{E}(Y)$. Therefore, choosing a cyclic code C from $\mathscr{C}(n,p^2)$ with uniform probability $\frac{1}{|\mathscr{C}(n,p^2)|}$. The average dimension $\mathtt{E}_p(n)$ can be determined in terms of the expectation $\mathtt{E}(Y)$ as follows :

$$\begin{aligned}
\mathtt{E}_P(n) &= \mathtt{E}(Y) = \mathtt{E}(2\deg H(X) + \deg G(X)) \\
&= \mathtt{E}\Big(\sum_{\substack{i\mid n \\ i\in\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\gamma(j;q)} (1-\max\{u_{ij}, 1-u_{ij}-b_{ij}\})\Big) \\
&\quad + \mathtt{E}\Big(\sum_{\substack{i\mid n \\ i\notin\mathscr{N}_p}} \mathtt{ord}_j(p) \sum_{i=1}^{\beta(j;q)} (2+\min\{1-v_{ij}-z_{ij}, w_{ij}\} - \max\{v_{ij}, 1-w_{ij}-d_{ij}\} \\
&\quad + \min\{1-w_{ij}-d_{ij}, v_{ij}\} - \max\{w_{ij}, 1-v_{ij}-z_{ij}\})\Big) \\
&= \sum_{\substack{i\mid n \\ i\in\mathscr{N}_p}} \mathtt{ord}_j(p)\gamma(j;q)\mathtt{E}(1-\max\{u_{ij}, 1-u_{ij}-b_{ij}\}) + \sum_{\substack{i\mid n \\ i\notin\mathscr{N}_p}} \mathtt{ord}_j(p)\beta(j;q) \\
&\quad .\mathtt{E}(2+\min\{1-v_{ij}-z_{ij}, w_{ij}\} - \max\{v_{ij}, 1-w_{ij}-d_{ij}\} \\
&\quad + \min\{1-w_{ij}-d_{ij}, v_{ij}\} - \max\{w_{ij}, 1-v_{ij}-z_{ij}\}) \\
&= \sum_{\substack{i\mid n \\ i\in\mathscr{N}_p}} \phi(i).\frac{1}{3} + \sum_{\substack{i\mid n \\ i\notin\mathscr{N}_p}} \frac{\phi(i)}{2}.\frac{10}{9} \\
&= \frac{\mathscr{B}_n}{3} + \frac{5(n-\mathscr{B}_n)}{9} \\
&= \frac{5}{9}n - \frac{2}{9}\mathscr{B}_n.
\end{aligned}$$

□

We have $0 < \mathscr{B}_n < \frac{2n}{3}$, if $n \in \mathscr{N}_p$, and $\mathscr{B}_n = n$ otherwise. Hence, we have the following rough bounds.

Corollary 7. *Let p be a prime number and let n be a positive integer such that $p \nmid n$. The following statements hold.*

1. $n \in \mathscr{N}_p$ *if and only if* $E_P(n) = \frac{n}{3}$.
2. $n \notin \mathscr{N}_p$, *then* $\frac{11n}{27} < E_P(n) < \frac{5n}{9}$.

5

Galois Hulls of cyclic serial codes over finite chain rings

In this chapter, we characterize Galois hulls of cyclic serial code over finite chain rings. we shows the parameters and the q-dimensions of the Euclidean hull of cyclic serial codes. Finally, the average dimension of the Euclidean hull of cyclic serial codes is computed

5.1 | Factorization of X^n-1

Let $\mathbb{N}$ be the set of nonnegative integers and n be a positive integer such that $\gcd(n,q)=1$. Set $[|a;b|]=\{a,a+1,\cdots,b\}$ where $(a,b)\in\mathbb{N}^2$ such that $a<b$. Let A and B be two subsets in $[|0;n-1|]$, as usual, the opposite of A, denoted $-$A, is defined as $-\mathrm{A}=\{n-z\ :\ z\in\mathrm{A}\}$ and its complementary, denoted $\overline{\mathrm{A}}$, is defined as: $\overline{\mathrm{A}}=\{z\in[|0;n-1|]\ :\ z\notin\mathrm{A}\}$. The set A is symmetric, if $\mathrm{A}=-\mathrm{A}$, and the pair $\{\mathrm{A},\mathrm{B}\}$ is asymmetric, if $\mathrm{B}=-\mathrm{A}$. Recall that the pair is a set with two elements. If $u\in\mathbb{N}\backslash\{0\}$, then $u\mathrm{A}=\left\{i\in[|0;n-1|]:(\exists z\in\mathrm{A})(uz\equiv i(\mathrm{mod}\,n)\right\}$. It defines the binary relation on $[|0;n-1|]$ by $x\sim_q y$ if there is i in $\mathbb{N}$ such that $y\equiv q^i x(\mathrm{mod}\,n)$. Obviously, the binary relation $\sim_q$ is an equivalence relation on $[|0;n-1|]$. The cosets of $\sim_q$, are called q-cyclotomic cosets modulo n. Denote by $[|0;n-1|]_q$, a complete system of representatives of $\sim_q$. A subset Z of $[|0;n-1|]$ is a q-closed set modulo n, if $\mathrm{Z}=q\mathrm{Z}$. The smallest q-closed set modulo n, containing a subset Z of $[|0;n-1|]$ is $\bigcup_{i\in\mathbb{N}}q^i\mathrm{Z}$ and we will denote it by $\mathcal{C}_q(\mathrm{Z})$. In particular, the set of q-cyclotomic cosets modulo n which is $\left\{\mathcal{C}_q(\{z\}):z\in[|0;n-1|]_q\right\}$, forms a partition

of $[|0;n-1|]$. Since $\mathtt{C}_q(\{z\}) = \{x \in [|0;n-1|] \ : \ x \sim_q z\}$ for any z in $[|0;n-1|]$. We will take $\mathtt{C}_q(\emptyset) = \emptyset$ by convention. Let j be a divisor of n, we will use the following notation

- $\omega(n;q)$ the number of q-cyclotomic cosets modulo n;
- Λ_j the set of symmetric q-cyclotomic cosets modulo n of size $\mathtt{ord}_j(q)$ and $\gamma(j;q) := |\Lambda_j|$;
- $\overline{\Lambda}_j$ the set of asymmetric pairs of q-cyclotomic cosets modulo n of size $\mathtt{ord}_j(q)$ and $\beta(j;q) := |\overline{\Lambda}_j|$.

Let δ be a generator of the cyclic multiplicative subgroup $\Gamma(\mathtt{GR}(p^a,m))\backslash\{0\}$ of $(\mathtt{GR}(p^a,m))^\times$, where $m = \mathtt{ord}_n(q)$. The following result is straight forward from Hensel's Lemma [23], which guarantees the uniqueness of this monic basic-irreducible factorization of X^n-1, and $X^n-1 = \prod_{z\in[|0;n-1|]_q} m_z$ where $m_z := \prod_{a\in\mathtt{C}_q(\{z\})}(X-\delta^a)$. Obviously, for any z in $[|0;n-1|]_q$, the polynomial m_z is monic basic-irreducible over R.

The following lemma shows that the irreducible factors of x^n-1 are in correspondence with the cyclotomic cosets.

Lemma 5.1.1. *The map*

$$\begin{array}{rccc} \Omega: & \{\mathtt{C}_q(Z) : Z \subseteq [|0;n-1|]_q\} & \to & \{f \in GR(p^a,r)[X] : f \text{ is monic and } f|X^n-1\} \\ & A & \mapsto & \prod_{a\in A}(X-\delta^a) \end{array} \tag{5.1}$$

where $\Omega(\emptyset) = 1$, *is bijective. Moreover, for any* $z \in [|0;n-1|]$ *and for all* q*-closure sets* A *and* B *modulo* n, *we have*

1. $\Omega\big(\mathtt{C}_q(\{z\})\big)$ *is a monic basic-irreducible polynomial over* $GR(p^a,r)$ *of degree* $\big|\mathtt{C}_q(\{z\})\big|$;
2. $lcm(\Omega(A),\Omega(B)) = \Omega(A\cup B)$ *and* $gcd(\Omega(A),\Omega(B)) = \Omega(A\cap B)$;
3. *if* $A\cap B = \emptyset$, *then* $\Omega(A\cup B) = \Omega(A)\Omega(B)$.

Proof. Since $\delta \in \Gamma(\mathtt{GR}(p^a,m))\backslash\{0\} \subset \mathtt{GR}(p^a,m)$ and $\mathtt{GR}(p^a,m)$ is a Galois extension of $\mathtt{GR}(p^a,r)$, it follows that for any q-cyclotomic cosets A modulo n, the monic polynomial $\prod_{a\in \mathrm{A}}(X-\delta^a)$ is basic-irreducible over $\mathtt{GR}(p^a,r)$. Therefore, the correspondence Ω is well-defined, and by Hensel lemma, X^n-1 admits a unique monic basic-irreducible factorization in $\mathtt{GR}(p^a,r)[X]$. Thus the existence and the uniqueness of this basic-irreducible factorization over $\mathtt{GR}(p^a,r)$, the map Ω is bijective. Items 2. and 3. are straight forward to prove. □

Proposition 5.1.1. *[33, Subsection 2.2] Let j be a divisor of n. Then*

$$\gamma(j;q)=\begin{cases}\frac{\phi(j)}{ord_j(q)}, & \text{if } j\in\mathscr{N}_q;\\ 0, & \text{otherwise,}\end{cases} \quad \text{and } \beta(j;q)=\begin{cases}\frac{\phi(j)}{2ord_j(q)}, & \text{if } j\notin\mathscr{N}_q,\\ 0, & \text{otherwise.}\end{cases}$$

Moreover, $\omega(n;q)=\sum_{\substack{i\mid n\\ i\in\mathscr{N}_q}}\gamma(i;q)+2\sum_{\substack{j\mid n\\ j\notin\mathscr{N}_q}}\beta(j;q)$.

We will introduce the following notation

$$\mathscr{E}_n(q,s)=\mathscr{I}_n(q,s)\times(\mathscr{J}_n(q,s))^2, \tag{5.2}$$

where $\mathscr{I}_n(q,s)=\prod_{\substack{i\mid n\\ i\in\mathscr{N}_q}}\mathscr{E}_s^{\gamma(i;q)}$ and $\mathscr{J}_n(q,s)=\prod_{\substack{j\mid n\\ j\notin\mathscr{N}_q}}\mathscr{E}_s^{\beta(j;q)}$, with

$$\mathscr{E}_s=\left\{(x^{(0)},x^{(1)},\cdots,x^{(s-1)})\in\{0;1\}^s \,:\, \sum_{a=0}^{s-1}x^{(a)}\in\{0;1\}\right\}. \tag{5.3}$$

Note that $\mathscr{E}_s=\{(0,\cdots,0)\}\cup\left\{\left(0,\cdots,0,\underbrace{1}_{j\text{-i th position}},0,\cdots,0\right) : j\in\{1;\cdots;s\}\right\}\subseteq \{0;1\}^s$ and $|\mathscr{E}_s|=s+1$.

The elements in $\mathscr{I}_n(q,s)$ are arrays of the form $(((u_{il}^{(a)})_{0\le a<s})^\circ)$ where $(u_{il}^{(a)})_{0\le a<s}$ are in $\mathscr{E}_s$ and the indices i and l satisfy $i\mid n, i\in\mathscr{N}_q$ and $1\le l\le\gamma(i;q)$, i.e.,

$$(((u_{il}^{(a)})_{0\le a<s})^\circ)=\left(\left((u_{il}^{(a)})_{0\le a<s}\right)_{1\le l\le\gamma(i;q)}\right)_{i\mid n,i\in\mathscr{N}_q}\in\mathscr{I}_n(q,s).$$

Similarly, $(((v_{jh}^{(a)})_{0\le a<s})^\bullet)=\left(\left((v_{jh}^{(a)})_{0\le a<s}\right)_{1\le h\le\beta(j;q)}\right)_{j\mid n,j\notin\mathscr{N}_q}\in\mathscr{J}_n(q,s)$. Note that if $s=1$, then $\mathscr{E}_1=\{0;1\}$, and in this case, we write $((u_{il})^\circ)=(((u_{il}^{(a)})_{0\le a<1})^\circ)$ and $((v_{jh})^\bullet)=(((v_{jh}^{(a)})_{0\le a<1})^\bullet)$.

Let i and j be positive integers such that $i \mid n, i \in \mathcal{N}_q$, and $j \mid n, j \notin \mathcal{N}_q$. From now on,

$$\Lambda_i = \{G_{il} : 1 \le l \le \gamma(i;q)\} \qquad \text{and} \qquad \overline{\Lambda_j} = \{\{F_{jh}, -F_{jh}\} : 1 \le h \le \beta(j;q)\}.$$

Of course, all the polynomials in $\{\Omega(G_{il}) : 1 \le l \le \gamma(i;q)\}$ are basic-irreducible in $R[X]$ of degree $\mathtt{ord}_i(q)$, and all the elements in $\{\{\Omega(F_{jh}), \Omega(-F_{jh})\} : 1 \le h \le \beta(j;q)\}$ are pairs of monic basic-irreducible reciprocal polynomials (up to a unit) in $R[X]$ of the same degree $\mathtt{ord}_j(q)$. The basic-irreducible factorization of $X^n - 1$ in $R[X]$ is given as

$$X^n - 1 = \prod_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \left(\prod_{l=1}^{\gamma(i;q)} \Omega(G_{il}) \right) \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_q}} \left(\prod_{h=1}^{\beta(j;q)} \Omega(F_{jh}) \Omega(-F_{jh}) \right). \tag{5.4}$$

Thus, for any monic factor of $X^n - 1 \in R[X]$, there is a unique $(((u_{il})^\circ), ((v_{jh})^\bullet), ((w_{jh})^\bullet))$ in $\mathcal{E}_n(q,1)$ such that

$$f = \prod_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \left(\prod_{l=1}^{\gamma(i;q)} \Omega(G_{il})^{u_{il}} \right) \prod_{\substack{j \mid n \\ j \notin \mathcal{N}_q}} \left(\prod_{h=1}^{\beta(j;q)} \Omega(F_{jh})^{v_{jh}} \Omega(-F_{jh})^{w_{jh}} \right), \tag{5.5}$$

and conversely. Denote the right-hand side of Equation (5.5) by $\partial(((u_{il})^\circ), ((v_{jh})^\bullet), ((w_{jh})^\bullet))$. Note that $\partial(((1)^\circ), ((1)^\bullet), ((1)^\bullet)) = X^n - 1$ and $\partial(((0)^\circ), ((0)^\bullet), ((0)^\bullet)) = 1$. If we are given $f_1 = \partial(((u_{il})^\circ), ((v_{jh})^\bullet), ((w_{jh})^\bullet))$ and $f_2 = \partial(((u'_{il})^\circ), ((v'_{jh})^\bullet), ((w'_{jh})^\bullet))$, we have that

$$\begin{aligned} \mathtt{lcm}(f_1; f_2) &= \partial(((\max\{u_{il}, u'_{il}\})^\circ), ((\max\{v_{jh}, v'_{jh}\})^\bullet), ((\max\{w_{jh}, w'_{jh}\})^\bullet)); \\ \mathtt{gcd}(f_1; f_2) &= \partial(((\min\{u_{il}, u'_{il}\})^\circ), ((\min\{v_{jh}, v'_{jh}\})^\bullet), ((\min\{w_{jh}, w'_{jh}\})^\bullet)), \end{aligned}$$

and if all $(u_{il} + u'_{il}, v_{jh} + v'_{jh}, w_{jh} + w'_{jh})$ are in $\{0;1\}^3$ then

$$f_1 f_2 = \partial(((u_{il} + u'_{il})^\circ), ((v_{jh} + v'_{jh})^\bullet), ((w_{jh} + w'_{jh})^\bullet)).$$

5.2 | Cyclic serial codes

A *cyclic code* C of length n over R is a linear code that is invariant under the transformation $\tau((c_0, c_1, \cdots, c_{n-1})) = (c_{n-1}, c_0, \cdots, c_{n-2})$. If we denote by $\langle X^n - 1 \rangle$ the ideal

of $R[X]$ generated by X^n-1, it is well-known that any cyclic code of length n over R can be represented as an ideal of the quotient ring $R[X]/\langle X^n-1\rangle$ via the R-module isomorphism $\overline{\Psi}: R^n \to R[X]/\langle X^n-1\rangle$, where $\overline{\Psi}(\mathbf{c}) = \Psi(\mathbf{c}) + \langle X^n-1\rangle$ and

$$\begin{array}{rccc} \Psi: & R^n & \to & R[X] \\ & \mathbf{u}=(u_0,u_1,\cdots,u_{n-1}) & \mapsto & \mathbf{u}(X)=u_0+u_1X+\cdots+u_{n-1}X^{n-1}, \end{array} \tag{5.6}$$

which is an R-module homomorphism. We will slightly abuse notation, identifying vectors in R^n as polynomials in $R[X]$ of degree less than n, and vice versa when the context is clear. It is well-known that $R[X]/\langle X^n-1\rangle$ is a principal ideal ring and C is a cyclic code of length n over R if and only if $\overline{\Psi}(C)$ is an ideal of $R[X]/\langle X^n-1\rangle$, (see [10] and references therein). Thus, the generator polynomial of a cyclic code C of R^n, is the monic polynomial f in $R[X]$ such that $\overline{\Psi}(C) = \langle f(x)\rangle$, where $\langle f(x)\rangle$ is the ideal of $R[X]/\langle X^n-1\rangle$ generated by f.

A cyclic code over R of length n, is uniserial if its cyclic subcodes over R are totally ordered by inclusion (see the definition of serial modules in [39]). A cyclic code over R of length n, is serial if it is a direct sum of uniserial cyclic codes over R of length n. Note that, over a finite chain ring R, any cyclic code of length n is serial, if and only if $\gcd(p,n)=1$.

For a polynomial f of degree k its reciprocal polynomial $X^k f(X^{-1})$ will be denoted by f^* and if f is a factor of X^n-1 we denote $\widehat{f} = \frac{X^n-1}{f}$. A polynomial f is *self-reciprocal* if $f = f^*$, otherwise f and f^* are called a *reciprocal polynomial pair*.

In order to make the comparison we take $\Omega(\mathrm{A})^* = \Omega(-\mathrm{A})$ and $\widehat{\Omega(\mathrm{A})} = \Omega(\overline{\mathrm{A}})$, for any union A of q-cyclotomic cosets modulo n.
The $(s+1)$-tuple $(\mathrm{A}_0,\mathrm{A}_1,\cdots,\mathrm{A}_s)$ is called to be an ordered (q,s)-partition cyclotomic modulo n, if $\mathrm{A}_0,\mathrm{A}_1,\cdots,\mathrm{A}_s$ are unions of q-cyclotomic cosets modulo n whose $\{\mathrm{A}_t : \mathrm{A}_t \neq \emptyset, \text{ for } 0 \le t \le s\}$ forms a partition of $[|0;n-1|]$. Denote by $\mathfrak{R}_n(q,s)$ the set of ordered (q,s)-partition cyclotomic modulo n. Note that

$$\mathfrak{R}_n(q,s) = \left\{\left(\mathcal{C}_q(\lambda^{-1}(\{0\})),\mathcal{C}_q(\lambda^{-1}(\{1\})),\ldots,\mathcal{C}_q(\lambda^{-1}(\{s\}))\right) : \lambda \in [|0;s|]^{[|0;n-1|]_q}\right\}.$$

It follows that $|\mathfrak{R}_n(q,s)| = (s+1)^{\omega(n;q)}$. Let $\underline{\mathbf{A}} = (\mathrm{A}_0,\mathrm{A}_1,\cdots,\mathrm{A}_s)$ be in $\mathfrak{R}_n(q,s)$. For a positive integer u we denote by $u\underline{\mathbf{A}} = (u\mathrm{A}_0, u\mathrm{A}_1,\cdots, u\mathrm{A}_{s-1})$. Now, the $\mathrm{A}_0,\mathrm{A}_1,\cdots,\mathrm{A}_s$ are unions of q-cyclotomic cosets modulo n, therefore $p^\ell \mathrm{A}_t$ is also another union

of q-cyclotomic cosets modulo n, for any t in $\{0;1;\cdots;s-1\}$ and for any ℓ in $\{0;1;\cdots;r-1\}$. Hence, $p^\ell \underline{\mathbf{A}} \in \mathfrak{R}_n(q,s)$ for any $0 \le \ell < r$. From [10, Theorems 3.4, 3.5 and 3.8], we have the following result.

Lemma 5.2.1. *For any cyclic serial code C over R of length n, there is a unique $(s+1)$-tuple $(\mathrm{A}_0,\mathrm{A}_1,\cdots,\mathrm{A}_s)$ in $\mathfrak{R}_n(q,s)$ such that*

$$\overline{\Psi}(C) = \bigoplus_{t=0}^{s-1} \theta^t \left\langle \Omega(\overline{\mathrm{A}_t}) \right\rangle = \left\langle \left\{ \theta^t \prod_{a=t+1}^{s} \Omega(\mathrm{A}_a) : 0 \le t \le s-1 \right\} \right\rangle. \tag{5.7}$$

Moreover, $\overline{\Psi}(C^{\perp_0}) = \bigoplus_{t=0}^{s-1} \theta^t \left\langle \Omega(-\overline{\mathrm{A}_{s-t}}) \right\rangle$.

Let A be a union of q-cyclotomic cosets modulo n. From now on, we will consider the code

$$\mathscr{C}(\mathrm{A}) = \left\{ \mathbf{c} \in R^n : \Omega(\overline{\mathrm{A}}) \text{ divides } \Psi(\mathbf{c}) \right\}, \tag{5.8}$$

thus it is clear that $\overline{\Psi}(\mathscr{C}(\mathrm{A})) = \left\langle \Omega(\overline{\mathrm{A}}) \right\rangle$.

Remark 5.2.1. *Free cyclic serial codes over a finite chain ring have been studied in [11] using the cyclotomic cosets and the trace map. Note that $\mathscr{C}([|0;n-1|]) = \{\mathbf{0}\}$ and $\mathscr{C}(\emptyset) = R^n$. From Lemma 5.2.1, for any free cyclic serial code C of length n over R there exists a unique set A which is a union of q-cyclotomic cosets modulo n such that $C = \mathscr{C}(\mathrm{A})$. Moreover, $\mathscr{C}(\mathrm{A})^{\perp_0} = \mathscr{C}(-\overline{\mathrm{A}})$, the generator polynomial of $\mathscr{C}(\mathrm{A})$ is $\Omega(\overline{\mathrm{A}})$, and $\mathtt{rank}_R(\mathscr{C}(\mathrm{A})) = |\mathrm{A}|$.*

Proposition 5.2.1. *If A and B are unions of q-cyclotomic cosets modulo n, then*

1. *$\mathrm{A} \subseteq \mathrm{B}$ if and only $\mathscr{C}(\mathrm{A}) \subseteq \mathscr{C}(\mathrm{B})$;*
2. *$\mathscr{C}(\mathrm{A} \cap \mathrm{B}) = \mathscr{C}(\mathrm{A}) \cap \mathscr{C}(\mathrm{B})$, and $\mathscr{C}(\mathrm{A} \cup \mathrm{B}) = \mathscr{C}(\mathrm{A}) + \mathscr{C}(\mathrm{B})$;*
3. *$\sigma^\ell(\mathscr{C}(\mathrm{A})) = \mathscr{C}(p^\ell \mathrm{A})$ and $\mathscr{C}(\mathrm{A})^{\perp_\ell} = \mathscr{C}(-p^\ell \overline{\mathrm{A}})$, for all $0 \le \ell \le r-1$.*

Proof. Item (1) follows from the definition of $\mathscr{C}(\mathrm{A})$ and $\mathscr{C}(\mathrm{B})$ and the fact that $\mathrm{A} \subseteq \mathrm{B}$ if and only $\Omega(\overline{\mathrm{B}})$ divides $\Omega(\overline{\mathrm{A}})$. To prove (2), we note that since $\mathrm{A} \cap \mathrm{B} \subseteq \mathrm{A} \subseteq \mathrm{A} \cup \mathrm{B}$, and $\mathrm{A} \cap \mathrm{B} \subseteq \mathrm{B} \subseteq \mathrm{A} \cup \mathrm{B}$, from item (1), we have $\mathscr{C}(\mathrm{A} \cap \mathrm{B}) \subseteq \mathscr{C}(\mathrm{A}) \cap \mathscr{C}(\mathrm{B})$ and $\mathscr{C}(\mathrm{A}) + \mathscr{C}(\mathrm{B}) \subseteq \mathscr{C}(\mathrm{A} \cup \mathrm{B})$. Conversely, if $\mathbf{c} \in \mathscr{C}(\mathrm{A}) \cap \mathscr{C}(\mathrm{B})$ then $\Omega(\overline{\mathrm{A}})$ and $\Omega(\overline{\mathrm{B}})$ divide $\Psi(\mathbf{c})$. Thus

$\mathtt{lcm}(\Omega(\overline{\mathrm{A}}),\Omega(\overline{\mathrm{B}}))$ divides $\Psi(\mathbf{c})$. Now, $\mathtt{lcm}(\Omega(\overline{\mathrm{A}}),\Omega(\overline{\mathrm{B}})) = \Omega(\overline{\mathrm{A}}\cup\overline{\mathrm{B}}) = \Omega(\overline{\mathrm{A}\cap\mathrm{B}})$, so we have $\mathscr{C}(\mathrm{A})\cap\mathscr{C}(\mathrm{B}) \subseteq \mathscr{C}(\mathrm{A}\cap\mathrm{B})$. Since $\mathtt{gcd}(\Omega(\overline{\mathrm{A}}),\Omega(\overline{\mathrm{B}})) = \Omega(\overline{\mathrm{A}}\cap\overline{\mathrm{B}}) = \Omega(\overline{\mathrm{A}\cup\mathrm{B}})$, hence $\mathscr{C}(\mathrm{A})+\mathscr{C}(\mathrm{B}) \supseteq \mathscr{C}(\mathrm{A}\cup\mathrm{B})$. To finish with the proof of the item (3), we have $\sigma^{\ell}(\mathscr{C}(\mathrm{A})) = \{\mathbf{c}\in R^n : \sigma^{\ell}(\Omega(\overline{\mathrm{A}}) \text{ divides } \Psi(\mathbf{c})\}$, thus $\sigma^{\ell}(\mathscr{C}(\mathrm{A})) = \mathscr{C}(p^{\ell}\mathrm{A})$, since $\sigma^{\ell}(\Omega(\overline{\mathrm{A}})) = \Omega(p^{\ell}\overline{\mathrm{A}})$. Finally, for any $0\le\ell\le r-1$ we have

$$\begin{aligned}\mathscr{C}(\mathrm{A})^{\perp_\ell} &= \left(\sigma^{\ell}(\mathscr{C}(\mathrm{A}))\right)^{\perp_0}, \text{ from Proposition 2.2.3;}\\ &= \left(\mathscr{C}(p^{\ell}\mathrm{A})\right)^{\perp_0};\\ &= \mathscr{C}(-p^{\ell}\overline{\mathrm{A}}), \text{ from Remark 5.2.1.}\end{aligned}$$

□

5.3 | Galois hulls of cyclic serial codes

Let $\underline{\mathbf{A}} = (\mathrm{A}_0,\mathrm{A}_1,\ldots,\mathrm{A}_s)$ and $\underline{\mathbf{B}} = (\mathrm{B}_0,\mathrm{B}_1,\ldots,\mathrm{B}_s)$ be elements in $\mathfrak{R}_n(q,s)$. We will define the following set in R^n

$$\mathbb{C}(\underline{\mathbf{A}}) = \bigoplus_{t=0}^{s-1}\theta^t\mathscr{C}(\mathrm{A}_t).$$

Taking into account the map Ψ in Equation (5.6) and from [10, Theorem 3.4], it follows that $\mathbb{C}(\underline{\mathbf{A}})$ is a direct sum of cyclic serial codes of length n over R. Therefore, $\mathbb{C}(\underline{\mathbf{A}})$ is a cyclic serial code of length n over R. The parameters of $\mathbb{C}(\underline{\mathbf{A}})$ are given by the entries in $(|\mathrm{A}_0|,|\mathrm{A}_1|,\cdots,|\mathrm{A}_s|)$ and from Lemma 5.2.1 it follows that for any cyclic serial code C over R of length n, there is a unique $\underline{\mathbf{A}}$ in $\mathfrak{R}_n(q,s)$ such that $C = \mathbb{C}(\underline{\mathbf{A}})$. Thus $\underline{\mathbf{A}}$ is called the defining multiset of $\mathbb{C}(\underline{\mathbf{A}})$.

Let us denote by

$$\underline{\mathbf{A}}^{\diamond} = (\mathrm{A}_s,\mathrm{A}_{s-1},\ldots,\mathrm{A}_0), \quad \underline{\mathbf{A}}\sqcup\underline{\mathbf{B}} = (\mathrm{E}_0,\mathrm{E}_1,\ldots,\mathrm{E}_s)$$

where $\mathrm{E}_0 = \mathrm{A}_0\cup\mathrm{B}_0$, and $\mathrm{E}_t = (\mathrm{A}_t\cup\mathrm{B}_t)\setminus\left(\bigcup_{i=0}^{t-1}(\mathrm{A}_i\cup\mathrm{B}_i)\right)$ for all $0<t\le s$. It is easy to see that $\underline{\mathbf{A}}^{\diamond}$ and $\underline{\mathbf{A}}\sqcup\underline{\mathbf{B}}$ are in $\mathfrak{R}_n(q,s)$. Moreover, $C^{\perp_\ell} = \mathbb{C}(-p^{\ell}\underline{\mathbf{A}}^{\diamond})$, and $\mathtt{dim}_q(C) = \sum_{t=0}^{s-1}(s-t)|\mathrm{A}_t|$. Note that if $\underline{\mathbf{A}}\sqcap\underline{\mathbf{B}} = (\underline{\mathbf{A}}^{\diamond}\sqcup\underline{\mathbf{B}}^{\diamond})^{\diamond} = (\mathrm{E}_0,\mathrm{E}_1,\cdots,\mathrm{E}_s)$, then $\mathrm{E}_s = \mathrm{A}_s\cup\mathrm{B}_s$ and $\mathrm{E}_{s-t} = (\mathrm{A}_{s-t}\cup\mathrm{B}_{s-t})\setminus\left(\bigcup_{i=0}^{t-1}(\mathrm{A}_{s-i}\cup\mathrm{B}_{s-i})\right)$, for all $0<t\le s$. .

Proposition 5.3.1. *[11, Theorem 6] Let* $\underline{\boldsymbol{A}} = (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$ *and* $\underline{\boldsymbol{B}} = (\mathrm{B}_0, \mathrm{B}_1, \ldots, \mathrm{B}_s)$ *in* $\mathfrak{R}_n(q,s)$. *Then* $\mathbb{C}(\underline{\boldsymbol{A}}) + \mathbb{C}(\underline{\boldsymbol{B}}) = \mathbb{C}(\underline{\boldsymbol{A}} \sqcup \underline{\boldsymbol{B}})$ *and* $\mathbb{C}(\underline{\boldsymbol{A}}) \cap \mathbb{C}(\underline{\boldsymbol{B}}) = \mathbb{C}(\underline{\boldsymbol{A}} \sqcap \underline{\boldsymbol{B}})$.

Corollary 8. *Let* $\underline{\boldsymbol{A}} = (\mathrm{A}_0, \mathrm{A}_1, \ldots, \mathrm{A}_s)$ *and* $\underline{\boldsymbol{B}} = (\mathrm{B}_0, \mathrm{B}_1, \ldots, \mathrm{B}_s)$ *in* $\mathfrak{R}_n(q,s)$, *and define* $g_t = \prod_{a=t+1}^{s} \Omega(\mathrm{A}_a)$ *and* $h_t = \prod_{a=t+1}^{s} \Omega(\mathrm{B}_a)$, *for all* $0 \le t < s$. *Then*

1. $\overline{\Psi}(\mathbb{C}(\underline{\boldsymbol{A}})) = \left\langle \{\theta^t g_t(x) : 0 \le t < s\} \right\rangle$, *and* $\overline{\Psi}(\mathbb{C}(\underline{\boldsymbol{B}})) = \left\langle \{\theta^t h_t(x) : 0 \le t < s\} \right\rangle$;
2. $\overline{\Psi}(\mathbb{C}(\underline{\boldsymbol{A}} \sqcap \underline{\boldsymbol{B}})) = \left\langle \{\theta^t \, \mathtt{lcm}(g_t, h_t) : 0 \le t < s\} \right\rangle$.

Proof. We have $\underline{\mathrm{A}} \sqcap \underline{\mathrm{B}} = (\mathrm{E}_0, \mathrm{E}_1, \ldots, \mathrm{E}_s)$, where $\mathrm{E}_s = \mathrm{A}_s \cup \mathrm{B}_s$ and $\mathrm{E}_{s-t} = (\mathrm{A}_{s-t} \cup \mathrm{B}_{s-t}) \setminus \left(\bigcup_{i=0}^{t-1} (\mathrm{A}_{s-i} \cup \mathrm{B}_{s-i}) \right)$, for all $0 < t \le s$. From Lemma 5.2.1 it follows that $\overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}})) = \left\langle \{\theta^t g_t(x) : 0 \le t < s\} \right\rangle$, and $\overline{\Psi}(\mathbb{C}(\underline{\mathbf{B}})) = \left\langle \{\theta^t h_t(x) : 0 \le t < s\} \right\rangle$. Since $\overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}} \sqcap \underline{\mathbf{B}})) = \overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}})) \cap \overline{\Psi}(\mathbb{C}(\underline{\mathbf{B}}))$, using again Lemma 5.2.1 and Proposition 5.3.1 it follows that

$$\overline{\Psi}(\mathbb{C}(\underline{\mathbf{A}} \sqcap \underline{\mathbf{B}})) = \left\langle f_0(x), \theta f_1(x), \ldots, \theta^{s-1} f_{s-1}(x) \right\rangle,$$

where $f_t = \prod_{a=t+1}^{s} \Omega(\mathrm{E}_a)$. Thus for all $0 \le t < s$, $f_t = \Omega\left(\bigcup_{a=t+1}^{s} \mathrm{E}_a \right)$ and $\bigcup_{a=t+1}^{s} \mathrm{E}_a = \bigcup_{a=t+1}^{s} (\mathrm{A}_{s-t-1} \cup \mathrm{B}_{s-t-1})$. Then $f_t = \Omega\left(\bigcup_{a=t+1}^{s} (\mathrm{A}_{s-t-1} \cup \mathrm{B}_{s-t-1}) \right) = \mathtt{lcm}(g_t, h_t)$. □

Theorem 26. *Let* $\underline{\boldsymbol{A}}$ *in* $\mathfrak{R}_n(q,s)$. *Then*

$$\mathscr{H}_\ell(\mathbb{C}(\underline{\boldsymbol{A}})) = \mathbb{C}\left(\underline{\boldsymbol{A}} \sqcap -p^\ell \underline{\boldsymbol{A}}^\diamond\right). \tag{5.9}$$

Proof. Let $\underline{\mathbf{A}}$ in $\mathfrak{R}_n(q,s)$ and $0 \le \ell < r$. We have

$$\begin{aligned} \mathscr{H}_\ell(\mathbb{C}(\underline{\mathbf{A}})) &= \mathbb{C}(\underline{\mathbf{A}}) \cap \mathbb{C}(\underline{\mathbf{A}})^{\perp_\ell}, \text{ from Definition 2.2.7 ;} \\ &= \mathbb{C}(\underline{\mathbf{A}}) \cap \mathbb{C}(-p^\ell \underline{\mathbf{A}}^\diamond), \text{ since } \mathbb{C}(\underline{\mathbf{A}})^{\perp_\ell} = \mathbb{C}(-p^\ell \underline{\mathbf{A}}^\diamond); \\ &= \mathbb{C}\left(\underline{\mathbf{A}} \sqcap -p^\ell \underline{\mathbf{A}}^\diamond\right), \text{ from Proposition 5.3.1.} \end{aligned}$$

□

Example 5.3.1. *Let* $R = \mathbb{Z}_{2^a}[\theta]$ *with* $1 \le a \le 2$ *be the finite chain ring of parameters* $(2, a, 1, e, 2)$. *Consider the* 2*-cyclotomic cosets modulo* 7 *given by* $\mathfrak{C}_2(\{0\}) =$

$\{0\}, \mathtt{C}_2(\{1\}) = \{1;2;4\}$, *and* $\mathtt{C}_2(\{3\}) = \{3;5;6\}$. *Note that* $\{\mathtt{C}_2(\{1\}), \mathtt{C}_2(\{3\})\}$ *is an asymmetric set, and* $\mathtt{C}_2(\{0\})$ *is a symmetric set. Consider the cyclic serial code over* R *of length* 7 *with defining multiset* $\underline{\boldsymbol{A}} = (\mathtt{C}_2(\{0\}), \mathtt{C}_2(\{3\}), \mathtt{C}_2(\{1\}))$.
Then $-\underline{\boldsymbol{A}}^{\diamond} = (\mathtt{C}_2(\{3\}), \mathtt{C}_2(\{1\}), \mathtt{C}_2(\{0\}))$, *and* $\mathbb{C}(\underline{\boldsymbol{A}}) = \mathscr{C}(\mathtt{C}_2(\{0\})) \oplus \theta\mathscr{C}(\mathtt{C}_2(\{3\}))$. *Thus* $\mathbb{C}(\underline{\boldsymbol{A}})^{\perp_0} = \mathbb{C}(-\underline{\boldsymbol{A}}^{\diamond}) = \mathscr{C}(\mathtt{C}_2(\{3\})) \oplus \theta\mathscr{C}(\mathtt{C}_2(\{1\}))$. *Finally,* $\underline{\boldsymbol{A}} \sqcap -\underline{\boldsymbol{A}}^{\diamond} = (\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_2)$ *where* $\mathrm{F}_0 = \emptyset, \mathrm{F}_1 = \mathtt{C}_2(\{3\})$, *and* $\mathrm{F}_2 = \mathtt{C}_2(\{0;1\})$. *Therefore* $\mathscr{H}_0(\mathbb{C}(\underline{\boldsymbol{A}})) = \mathbb{C}(\underline{\boldsymbol{A}} \sqcap -\underline{\boldsymbol{A}}^{\diamond}) = \mathbb{C}(\emptyset, \mathtt{C}_2(\{3\}), \mathtt{C}_2(\{0;1\})) = \theta\mathscr{C}(\mathtt{C}_2(\{3\}))$.

5.3.1 | Euclidean hulls

From now on, $\ell = 0$. The following result provides us a way of checking whether a given cyclic serial code D is the Euclidean hull of a cyclic code C or not. Of course, if $\mathscr{H}_0(C) = D$, then D is a serial cyclic code if, and only if C is also a serial code. In the sequel, for each $\underline{\mathbf{X}} = (\mathrm{X}_0, \mathrm{X}_1, \cdots, \mathrm{X}_s) \in \mathfrak{R}_n(q,s)$, we will denote $\Omega(\mathrm{X}_a) = \partial\left(((x_{il}^{(a)})^{\circ}), ((y_{jh}^{(a)})^{\bullet}), ((z_{jh}^{(a)})^{\bullet})\right)$, for a in $\{0;1;\cdots;s\}$. Thus $\Omega(-\mathrm{X}_a) = \partial\left(((x_{il}^{(a)})^{\circ}), ((z_{jh}^{(a)})^{\bullet}), ((y_{jh}^{(a)})^{\bullet})\right)$, and from Equation 5.6, we have for $0 \le t \le s-1$,

$$\prod_{a=t+1}^{s} \Omega(\mathrm{X}_a) = \partial\left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)}\right)^{\bullet}\right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)}\right)^{\bullet}\right)\right).$$

Since $\partial(((1)^{\circ}), ((1)^{\bullet}), ((1))^{\bullet}) = X^n - 1 = g_0 \cdot \partial(((x_{il}^{(0)})^{\circ}), ((y_{jh}^{(0)})^{\bullet}), ((z_{jh}^{(0)})^{\bullet}))$, it follows that

$$\sum_{a=0}^{s} x_{il}^{(a)} = \sum_{a=0}^{s} y_{jh}^{(a)} = \sum_{a=0}^{s} z_{jh}^{(a)} = 1.$$

From Eqs. (5.5) and (5.7), there exists a unique

$$\left(((x_{il}^{(a)})_{0\le a<s})^{\circ}), (((y_{jh}^{(a)})_{0\le a<s})^{\bullet}), (((z_{jh}^{(a)})_{0\le a<s})^{\bullet})\right)$$

in $\mathscr{E}_n(q,s)$ such that

$$\overline{\Psi}(\mathbb{C}(\underline{\mathbf{X}})) = \left\langle \left\{ \theta^t \cdot \partial\left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)}\right)^{\bullet}\right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)}\right)^{\bullet}\right)\right) : 0 \le t \le s-1 \right\} \right\rangle.$$

From Eqs. (5.4), (5.5), and (5.7), the following lemma follows.

Lemma 5.3.1. *There is a bijection between the set* $\mathscr{C}(n;R)$ *of cyclic serial codes of length* n *over* R *and the set* $\mathscr{E}_n(q,s)$.

When $\ell = 0$, and with the triple-sequence of a cyclic serial code, by comparing the two sides of Equation (5.9) in Theorem 26, the following result is obtained.

Corollary 9. *Let*

$$\left(\left(\left(x_{il}^{(a)}\right)_{0\le a<2}\right)^{\circ}\right),\left(\left(\left(y_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right),\left(\left(\left(z_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right)\Big)$$

and

$$\left(\left(\left(u_{il}^{(a)}\right)_{0\le a<2}\right)^{\circ}\right),\left(\left(\left(v_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right),\left(\left(\left(w_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right)\Big)$$

in $\mathcal{E}_n(q,s)$ *such that*

$$\overline{\Psi}(C)=\left\langle\left\{\theta^t\cdot\partial\left(\left(\left(\sum_{a=t+1}^{s}x_{il}^{(a)}\right)^{\circ}\right),\left(\left(\sum_{a=t+1}^{s}y_{jh}^{(a)}\right)^{\bullet}\right),\left(\left(\sum_{a=t+1}^{s}z_{jh}^{(a)}\right)^{\bullet}\right)\right):0\le t\le s-1\right\}\right\rangle,$$

and

$$\overline{\Psi}(D)=\left\langle\left\{\theta^t\cdot\partial\left(\left(\left(\sum_{a=t+1}^{s}u_{il}^{(a)}\right)^{\circ}\right),\left(\left(\sum_{a=t+1}^{s}v_{jh}^{(a)}\right)^{\circ}\right),\left(\left(\sum_{a=t+1}^{s}w_{jh}^{(a)}\right)^{\circ}\right)\right):0\le t\le s-1\right\}\right\rangle.$$

Then $\mathscr{H}_0(C)=D$ *if, and only if for all* $0\le t\le s-1$,

$$\begin{cases}\displaystyle\sum_{a=t+1}^{s}u_{il}^{(a)}=\max\left\{\sum_{a=t+1}^{s}x_{il}^{(a)};\sum_{a=t+1}^{s}x_{il}^{(s-a)}\right\};\\ \displaystyle\sum_{a=t+1}^{s}v_{jh}^{(a)}=\max\left\{\sum_{a=t+1}^{s}y_{jh}^{(a)};\sum_{a=t+1}^{s}z_{jh}^{(s-a)}\right\};\\ \displaystyle\sum_{a=t+1}^{s}w_{jh}^{(a)}=\max\left\{\sum_{a=t+1}^{s}z_{jh}^{(a)};\sum_{a=t+1}^{s}y_{jh}^{(s-a)}\right\}.\end{cases}\tag{5.10}$$

In such a case, for all $0\le t\le s-1$, *if* $2t\le s-1$, *then*

$$\sum_{a=t+1}^{s}u_{il}^{(a)}=\max\left\{\sum_{a=t+1}^{s}x_{il}^{(a)};\sum_{a=t+1}^{s}x_{il}^{(s-a)}\right\}=1,$$

and

$$\left(\sum_{a=t+1}^{s}v_{jh}^{(a)};\sum_{a=t+1}^{s}w_{jh}^{(a)}\right)\in\{(1;0),(0;1),(1;1)\},$$

since $\sum_{a=0}^{s}x_{il}^{(a)}=1$.

From Corollary 9, we recover the characterization of LCD cyclic codes and of self-orthogonal cyclic codes in [17, Theorem 3.4, and Corollaries 3.5 and 3.6] and we naturally extend it to finite chain rings of nilpotency index 2. The following remark provides this generalization.

Remark 5.3.1. *Let*

$$\left(\left(\left(x_{il}^{(a)}\right)_{0\le a<2}\right)^{\circ}\right),\left(\left(\left(y_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right),\left(\left(\left(z_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right)\Big)$$

and

$$\left(\left(\left(u_{il}^{(a)}\right)_{0\le a<2}\right)^{\circ}\right),\left(\left(\left(v_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right),\left(\left(\left(w_{jh}^{(a)}\right)_{0\le a<2}\right)^{\bullet}\right)\Big)$$

in $\mathcal{E}_n(q,2)$ *such that*

$$\overline{\Psi}(C)=\left\langle\left\{\partial\left(\left((x_{il}^{(1)}+x_{il}^{(2)})^{\circ}\right),\left((y_{jh}^{(1)}+y_{jh}^{(2)})^{\bullet}\right),\left((z_{jh}^{(1)}+z_{jh}^{(2)})^{\bullet}\right)\right),\theta\cdot\partial\left(\left((x_{il}^{(2)})^{\circ}\right),\left((y_{jh}^{(2)})^{\bullet}\right),\left((z_{jh}^{(2)})^{\bullet}\right)\right)\right.$$

and

$$\overline{\Psi}(D)=\left\langle\left\{\partial\left(\left((u_{il}^{(1)}+u_{il}^{(2)})^{\circ}\right),\left((v_{jh}^{(1)}+v_{jh}^{(2)})^{\bullet}\right),\left((w_{jh}^{(1)})^{\bullet}+w_{jh}^{(2)})^{\bullet}\right)\right),\theta\cdot\partial\left(\left((u_{il}^{(2)})^{\circ}\right),\left((v_{jh}^{(2)})^{\bullet}\right),\left((w_{jh}^{(2)}\right.\right.\right.$$

Then $\mathscr{H}_0(C)=D$ *if, and only if* $(x_{il}^{(1)};x_{il}^{(2)})\in\begin{cases}\{(0;1)\}, & \text{if } u_{il}^{(2)}=0;\\ \{(0;0),(1;0)\}, & \text{if } u_{il}^{(2)}=1,\end{cases}$ *and*
$(y_{jh}^{(1)};y_{jh}^{(2)};z_{jh}^{(1)};z_{jh}^{(2)})$ *belongs to*

$$\begin{cases}\{(0;0;0;0),(1;0;1;0)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;1;1);\\ \{(0;1;1;0),(1;0;1;1)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;0;1);\\ \{(0;1;0;0),(1;0;0;1)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;1;0);\\ \{(1;0;0;0)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;0;1;0);\\ \{(0;0;1;0)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;0;1;0;1);\\ \{(0;1;0;1)\}, & \text{if } (u_{il}^{(1)}+u_{il}^{(2)};v_{jh}^{(1)}+v_{jh}^{(2)};w_{jh}^{(1)}+w_{jh}^{(2)};v_{jh}^{(2)};w_{jh}^{(2)})=(1;1;1;0;0),\end{cases}$$

for all i,l,j,h. *Moreover,*

1. *C is LCD if, and only if* $x_{il}^{(2)}=x_{il}^{(1)},y_{jh}^{(2)}=y_{jh}^{(1)},z_{jh}^{(2)}=z_{jh}^{(1)}$ *and* $(x_{il}^{(2)};y_{jh}^{(2)};z_{jh}^{(2)})\in\{(0;0;0),(0;1;1),(1;0;0),(1;1;1)\}$, *for all* i,l,j,h.

2. *C is self-orthogonal if, and only if* $(x_{il}^{(2)}; x_{il}^{(1)}) \in \{(0;1),(1;0)\}$ *and*

   $(y_{jh}^{(2)}; y_{jh}^{(1)}; z_{jh}^{(2)}; z_{jh}^{(1)}) \in \{(1;0;1;0),(0;1;1;0),(1;0;0;1),(1;0;0;0),(0;0;1;0),(0;1;0;1)\}$,

   for all i, l, j, h.

Note that Corollary 9 is insufficient to characterize the nontrivial self-dual cyclic codes over R when s is even (see [10, Theorem 4.4]).

5.4 | The q-dimensions of Euclidean hulls of cyclic serial codes

In this section, C is a cyclic serial code of length n over R with triple-sequence

$$\left(((x_{il}^{(a)})_{0\le a<s})^{\circ}), (((y_{jh}^{(a)})_{0\le a<s})^{\bullet}), (((z_{jh}^{(a)})_{0\le a<s})^{\bullet})\right)$$

in $\mathscr{E}_n(q,s)$. Then

$$\overline{\Psi}(C) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} x_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} y_{jh}^{(a)} \right)^{\bullet} \right), \left(\left(\sum_{a=t+1}^{s} z_{jh}^{(a)} \right)^{\bullet} \right) \right) : 0 \le t \le s-1 \right\} \right\rangle.$$

From Corollary 9,

$$\overline{\Psi}(\mathscr{H}_0(C)) = \left\langle \left\{ \theta^t \cdot \partial \left(\left(\left(\sum_{a=t+1}^{s} u_{il}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} v_{jh}^{(a)} \right)^{\circ} \right), \left(\left(\sum_{a=t+1}^{s} w_{jh}^{(a)} \right)^{\circ} \right) \right) : 0 \le t \le s-1 \right\} \right\rangle,$$

where

$$\begin{cases} \sum_{a=t+1}^{s} u_{il}^{(a)} = 1 - \min\left\{ \sum_{a=0}^{t} x_{il}^{(a)}; 1 - \sum_{a=0}^{s-t-1} x_{il}^{(a)} \right\}; \\ \sum_{a=t+1}^{s} v_{jh}^{(a)} = 1 - \min\left\{ \sum_{a=0}^{t} y_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} z_{jh}^{(a)} \right\}; \\ \sum_{a=t+1}^{s} w_{jh}^{(a)} = 1 - \min\left\{ \sum_{a=0}^{t} z_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} y_{jh}^{(a)} \right\}, \end{cases}$$

for all $0 \le t \le s-1$. The following notations are important for the sequel of this paper. For all $0 \le t \le s-1$, $1 \le l \le \gamma(i;q)$ and $1 \le h \le \beta(j;q)$, denote by:

$$\varepsilon_{jh}^{(t)} = \sum_{a=t+1}^{s} (v_{jh}^{(a)} + w_{jh}^{(a)}). \tag{5.11}$$

Note that $\varepsilon_{jh}^{(-1)} = 2$. Let us consider now

$$\triangle_{il} = \sum_{t=0}^{s-1} (s-t)\, u_{il}^{(t)}, \text{ and } \blacktriangle_{jh} = \sum_{t=0}^{s-1} (s-t)(\varepsilon_{il}^{(t-1)} - \varepsilon_{il}^{(t)}). \tag{5.12}$$

Obviously, $\triangle_{il} = \sum_{t=0}^{s-1} \triangle_{il}^{(t)}$, where $\triangle_{il}^{(t)} = \min\left\{\sum_{a=0}^{t} x_{il}^{(a)}; 1 - \sum_{a=0}^{s-t-1} x_{il}^{(a)}\right\}$, and $\blacktriangle_{jh} = \sum_{t=0}^{s-1} \blacktriangle_{jh}^{(t)}$, where

$$\blacktriangle_{jh}^{(t)} = \min\left\{\sum_{a=0}^{t} y_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} z_{jh}^{(a)}\right\} + \min\left\{\sum_{a=0}^{t} z_{jh}^{(a)}; 1 - \sum_{a=0}^{s-t-1} y_{jh}^{(a)}\right\}.$$

Thus, we set $\triangle_i := \sum_{l=1}^{\gamma(i;q)} \triangle_{il}$, $\varepsilon_j^{(t)} := \sum_{h=1}^{\beta(j;q)} \varepsilon_{jh}^{(t)}$ and $\blacktriangle_j := \sum_{h=1}^{\beta(j;q)} \blacktriangle_{jh}$.

Remark 5.4.1. *Let* $0 \le t \le s-1$.

1. $\triangle_{il}^{(t)} \in \{0;1\}$ *and* $\blacktriangle_{jh}^{(t)} \in \{0;1;2\}$.
2. *If* $0 < t < s$, *then* $\triangle_{il}^{(t-1)} \le \triangle_{il}^{(t)}$ *and* $\blacktriangle_{jh}^{(t-1)} \le \blacktriangle_{jh}^{(t)}$.
3. *If* $2t < s$, *then* $\triangle_{il}^{(t)} = 0$ *and* $\blacktriangle_{jh}^{(t)} \le 1$.

Lemma 5.4.1. *Let* j *be a divisor of* n *such that* $j \notin \mathscr{N}_q$. *Then*

$$\begin{cases} 0 \le \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \le \beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)}), & \text{if } t < \lceil \frac{s}{2} \rceil; \\ 0 \le \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \le 2\Big(\beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)})\Big), & \text{if } t \ge \lceil \frac{s}{2} \rceil. \end{cases}$$

Proof. Let $0 \le t \le s-1$ and $\blacktriangle_j^{(t)} = \sum_{h=1}^{\beta(j;q)} \blacktriangle_{jh}^{(t)}$. We have $\varepsilon_{jh}^{(t)} = 2 - \blacktriangle_{jh}^{(t)}$. From Remark 5.4.1, two cases are considered. Let $\varpi_j^{(t-1)} := |\{h \in \mathbb{N} : 1 \le h \le \beta(j;q) \text{ and } \varepsilon_{jh}^{(t-1)} = \varepsilon_{jh}^{(t)} = 1\}|$. Then there is a permutation τ in $\mathbb{S}_{\beta(j;q)}$ such that $\varepsilon_{jh}^{(t-1)} = \varepsilon_{jh}^{(t)} = 1$, for all $h \in \{\tau(1), \cdots, \tau(\varpi_j^{(t-1)})\}$. Obviously, $\varepsilon_j^{(t-2)} \le 2\beta(j;q)$. For that $\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)} \le \varpi_j^{(t-1)}$.

Case 1: $t < \lceil \frac{s}{2} \rceil$. We have $\varepsilon_{jh}^{(t)} \in \{1;2\}$, and $\begin{cases} \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \in \{0;1\}, & \text{if } \varepsilon_{jh}^{(t-1)} = 2; \\ \varepsilon_{jh}^{(t)} = \varepsilon^{(t-1)}, & \text{if } \varepsilon_{jh}^{(t-1)} = 1. \end{cases}$

Thus

$$\begin{aligned} \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} &= \left(\sum_{h \in \{\tau(1), \cdots, \tau(\varpi_j^{(t-1)})\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right) \\ &\quad + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right); \\ &= 0 + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right), \text{ since } 0 \le \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \le 1 \end{aligned}$$

Hence $0 \le \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \le \beta(j;q) - \varpi_j^{(t-1)} \le \beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)})$.

Case 2: $t \ge \lceil \frac{s}{2} \rceil$. We have $\begin{cases} \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \in \{0;1;2\}, & \text{if } \varepsilon_{jh}^{(t-1)} \in \{1;2\}; \\ \varepsilon_{jh}^{(t)} = \varepsilon_{jh}^{(t-1)}, & \text{if } \varepsilon_{jh}^{(t-1)} = 0. \end{cases}$ Thus

$$\begin{aligned} \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} &= \left(\sum_{h \in \{\tau(1), \cdots, \tau(\varpi_j^{(t-1)})\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right) \\ &\quad + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right); \\ &= 0 + \left(\sum_{h \in \{\tau(\varpi_j^{(t-1)}+1), \cdots, \tau(\beta(j;q))\}} (\varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)}) \right), \text{ since } 0 \le \varepsilon_{jh}^{(t-1)} - \varepsilon_{jh}^{(t)} \le 2 \end{aligned}$$

Therefore $0 \le \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)} \le 2(\beta(j;q) - \varpi_j^{(t-1)}) \le 2\left(\beta(j;q) - (\varepsilon_j^{(t-2)} - \varepsilon_j^{(t-1)})\right)$.

□

Theorem 27. *The parameters of the Euclidean hull of a cyclic serial code over R of length n are given by $(k_0, k_1, \cdots, k_{s-1})$ where $2k_0 + k_1 + \cdots + k_{s-1} \leq n$,*

$$k_t = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \mathtt{ord}_i(q) \cdot u_i^{(t)} + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \mathtt{ord}_j(q) \cdot v_j^{(t)},$$

with

$$\begin{cases} u_i^{(t)} = 0, & \text{if } t < \lceil \frac{s}{2} \rceil; \\ 0 \leq u_i^{(t)} \leq \gamma(i;q), & \text{if } t \geq \lceil \frac{s}{2} \rceil, \end{cases} \text{, and } \begin{cases} \varepsilon_j^{(t)} = 0, & \text{if } n \in \mathcal{N}_q; \\ 0 \leq v_j^{(t)} \leq \beta(j;q) - v_j^{(t-1)}, & \text{if } n \notin \mathcal{N}_q, \text{ and } t < \lceil \frac{s}{2} \rceil; \\ 0 \leq v_j^{(t)} \leq 2(\beta(j;q) - v_j^{(t-1)}), & \text{if } n \notin \mathcal{N}_q, \text{ and } t \geq \lceil \frac{s}{2} \rceil. \end{cases}$$

Moreover $v_j^{(-1)} = 0$.

Proof. Let $(k_0, k_1, \cdots, k_{s-1})$ be the parameters of $\mathscr{H}_0(C)$. When $\mathscr{H}_0(C) = C$, we have $2k_0 + k_1 + \cdots + k_{s-1} \leq n$. Then for all $0 \leq t \leq s-1$,

$$\begin{aligned} k_t &= \mathtt{deg}\left(\partial\left(\left(\left(\sum_{a=t}^{s} u_{il}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t}^{s} v_{ij}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t}^{s} w_{jh}^{(a)}\right)^{\circ}\right)\right)\right) \\ &\quad - \mathtt{deg}\left(\partial\left(\left(\left(\sum_{a=t+1}^{s} u_{il}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t+1}^{s} v_{jh}^{(a)}\right)^{\circ}\right), \left(\left(\sum_{a=t+1}^{s} w_{jh}^{(a)}\right)^{\circ}\right)\right)\right); \\ &= \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \mathtt{ord}_i(q) \cdot u_i^{(t)} + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \mathtt{ord}_j(q) \cdot (\varepsilon_j^{(t-1)} - \varepsilon_j^{(t)}), \qquad \text{where } u_i^{(t)} = \sum_{l=1}^{\gamma(i;q)} u_{il}^{(t)}. \end{aligned}$$

Since $\begin{cases} u_i^{(t)} = 0, & \text{if } t < \lceil \frac{s}{2} \rceil; \\ 0 \leq u_i^{(t)} \leq \gamma(i;q), & \text{if } t \geq \lceil \frac{s}{2} \rceil, \end{cases}$, it follows that $\begin{cases} u_i^{(t)} = 0, & \text{if } 2t < s; \\ 0 \leq u_i^{(t)} \leq \gamma(i;q), & \text{if } s \leq 2t. \end{cases}$ On the other hand, one notes that if $n \in \mathcal{N}_q$, then any positive divisor of n is in then $\mathcal{N}_q$. By Lemma 5.4.1, we obtain

$$\begin{cases} \varepsilon_j^{(t)} = 0, & \text{if } n \in \mathcal{N}_q; \\ 0 \leq v_j^{(t)} \leq \beta(j;q) - v_j^{(t-1)}, & \text{if } n \notin \mathcal{N}_q, \text{ and } t < \lceil \frac{s}{2} \rceil; \\ 0 \leq v_j^{(t)} \leq 2(\beta(j;q) - v_j^{(t-1)}), & \text{if } n \notin \mathcal{N}_q, \text{ and } t \geq \lceil \frac{s}{2} \rceil. \end{cases}$$

where $v_j^{(t)} = \varepsilon_j^{(t-1)} - \varepsilon_j^{(t)}$. Obviously $v_j^{(-1)} = \varepsilon_j^{(-2)} - \varepsilon_j^{(-1)} = 0$. □

The previous discussion leads to the Algorithm 1 and justifies its correctness. Examples 5.4.1, 5.4.2, 5.4.3 show different outputs of the algorithm.

Example 5.4.1. *All possible parameters of Euclidean hulls of cyclic codes of length* 11 *over* $\mathbb{Z}_{27}$ *are determined as follows.*

1. *The divisors of* 11 *are* 1 *and* 11.

   a) *We have* $1 \in \mathcal{N}_3$, *so* $\mathtt{ord}_1(3) = 1$ *and* $\gamma(1;3) = 1$.

   b) *We have* $11 \notin \mathcal{N}_3$, *so* $\mathtt{ord}_{11}(3) = 5$ *and* $\beta(11;3) = 1$.

2. *It follows that*

$$\begin{aligned} k_0 &= 5\nu_{11}^{(0)},\ \text{where } 0 \le \nu_{11}^{(0)} \le 1 \\ k_1 &= 5\nu_{11}^{(1)},\ \text{where } 0 \le \nu_{11}^{(1)} \le 1-\nu_{11}^{(0)} \\ k_2 &= u_1^{(2)} + 5\nu_{11}^{(2)} \text{ where } 0 \le u_1^{(2)} \le 1 \text{ and } 0 \le \nu_{11}^{(2)} \le 2(1-\nu_{11}^{(1)}). \end{aligned}$$

   Hence, the all possible parameters (k_0, k_1, k_2) *of the Euclidean hulls of cyclic codes of length* 7 *over* $\mathbb{Z}_8$ *are given in the following table*

k_0	k_1	k_2
0	*0*	*0, 1, 5, 6, 10, 11*
	5	*0, 1*
5	*0*	*0, 1*

Example 5.4.2. *All the possible parameters* (k_0, k_1, k_2) *of the Euclidean hull of a cyclic code of length* 7 *over* $\mathbb{Z}_8$ *are determined as follows.*

1. *The divisors of* 7 *are* 1 *and* 7.

   a) *We have* $1 \in \mathcal{N}_2$, *so* $\mathtt{ord}_1(2) = 1$ *and* $\gamma(1;2) = 1$.

   b) *We have* $7 \notin \mathcal{N}_2$, *so* $\mathtt{ord}_7(2) = 3$ *and* $\beta(7;2) = 1$.

2. *It follows that*

$$\begin{aligned} k_0 &= 3\nu_7^{(0)},\ \text{where } 0 \le \nu_7^{(0)} \le 1 \\ k_1 &= 3\nu_7^{(1)},\ \text{where } 0 \le \nu_7^{(1)} \le 1-\nu_7^{(0)} \\ k_2 &= u_1^{(2)} + 3\nu_7^{(2)} \text{ where } 0 \le u_1^{(2)} \le 1 \text{ and } 0 \le \nu_7^{(2)} \le 2(1-\nu_7^{(1)}). \end{aligned}$$

Algorithm 2: Parameters of the Euclidean hull of a cyclic serial code over R.

Input: Length n, and a finite chain ring R of parameters (p,a,r,e,s) such that $\gcd(p,n)=1$.

Output: All possible s-tuples $(k_0,k_1,\cdots,k_{s-1})$ describing the parameters of the Euclidean hull of a cyclic serial code

. **if** $n \in \mathcal{N}_q$ **then**
  for $0 \le t < s$ **do**
    if $t < \lceil \frac{s}{2} \rceil$ **then**
      $k_t = 0$.
    else
      For each $i \mid n$, compute $\mathtt{ord}_i(q)$, and $\gamma(i;q)$,
      therefore all the possible values of k_t, such that
      $$k_t = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \mathtt{ord}_i(q) \cdot u_i^{(t)},$$
      with $0 \le u_i^{(t)} \le \gamma(i;q)$.
  return *The possible parameters* $(0,\cdots,0,k_{\lceil \frac{s}{2} \rceil},\cdots,k_{s-1})$ *such that* $k_{\lceil \frac{s}{2} \rceil} + \cdots + k_{s-1} \le n$.
else
  For each $i \mid n$, if $i \in \mathcal{N}_q$, then compute $\mathtt{ord}_i(q)$, and $\gamma(i;q)$.
  For each $j \mid n$, if $j \notin \mathcal{N}_q$, then compute $\mathtt{ord}_j(q)$, and $\beta(j;q)$.
  for $0 \le t < s$, **do**
    if $t = 0$ **then**
      compute $k_0 = \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \mathtt{ord}_j(q) \cdot v_j^{(0)}$, where $0 \le v_j^{(0)} \le \beta(j;q)$
    else
      while $0 < t < \lceil \frac{s}{2} \rceil$ **do**
        For a fixed $v_j^{(t-1)}$ in k_{t-1}, compute $k_t = \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \mathtt{ord}_j(q) \cdot v_j^{(t)}$,
        where $0 \le v_j^{(t)} \le \beta(j;q) - v_j^{(t-1)}$,
        if $2k_0 + k_1 + \cdots + k_t \le n$ **then**
          consider k_t,
        else
          reject k_t
      while $t \ge \lceil \frac{s}{2} \rceil$ **do**
        For a fixed $v_j^{(t-1)}$ in k_{t-1}, compute
        $k_t = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \mathtt{ord}_i(q) \cdot u_i^{(t)} + \sum_{\substack{j \mid n \\ i \notin \mathcal{N}_q}} \mathtt{ord}_j(q) \cdot v_j^{(t)}$, where
        $0 \le u_i^{(t)} \le \gamma(i;q)$ and $0 \le v_j^{(t)} \le 2 \cdot (\beta(j;q) - v_j^{(t-1)})$.
        if $2k_0 + k_1 + \cdots + k_t \le n$ **then**
          consider k_t,
        else
          reject k_t

Hence, the all possible parameters (k_0, k_1, k_2) *of the Euclidean hulls of cyclic codes of length* 7 *over* $\mathbb{Z}_8$ *are given in the following table*

k_0	k_1	k_2
0	*0*	*0, 1, 3, 4, 6, 7*
	3	*0, 1*
3	*0*	*0, 1*

Example 5.4.3. *The parameters of the Euclidean hulls of cyclic codes of length* 21 *over* $\mathbb{Z}_8$ *are given by*

1. *The divisors of* 21 *are* $\{1,3,7,21\}$.

   (a) $1;3 \in \mathscr{N}_2$, *we have* $\mathtt{ord}_1(2) = 1, \mathtt{ord}_3(2) = 2$ *and* $\gamma(1;2) = \gamma(3;2) = 1$.

   (b) $7;21 \notin \mathscr{N}_2$, *we have* $\mathtt{ord}_7(2) = 3, \mathtt{ord}_{21}(2) = 6$ *and* $\beta(7;2) = \beta(21;2) = 1$.

2. *It follows that*

$$\begin{aligned} k_0 &= 3\nu_7^{(0)} + 6\nu_{21}^{(0)}, \text{ with } 0 \le \nu_j^{(0)} \le 1, \text{ where } j \in \{7;21\}. \\ k_1 &= 3\nu_7^{(1)} + 6\nu_{21}^{(1)}, \text{ with } 0 \le \nu_j^{(1)} \le 1 - \nu_j^{(0)}, \text{ where } j \in \{7;21\}. \\ k_2 &= u_1^{(2)} + 2u_3^{(2)} + 3\nu_7^{(2)} + 6\nu_{21}^{(2)}, \text{ with } 0 \le u_i^{(2)} \le 1 \text{ and } 0 \le \nu_j^{(2)} \le 2(1 - \nu_j^{(1)}), \\ &\quad \text{where } i \in \{1;3\}, \text{ and } j \in \{7;21\}. \end{aligned}$$

Hence, the all possible parameters (k_0, k_1, k_2) *of the Euclidean hulls of cyclic codes of length* 21 *over* $\mathbb{Z}_8$ *are given in the following table*

k_0	k_1	k_2
0	*0*	*0, 1, 2, 3, ⋯ , 21*
	3	*0, 1, 2, 3, 6, 7, 8, 9, 12, 13, 14, 15*
	6	*0, 1, 2, 3, 4, 5, 6, 7, 8, 9*
	9	*0, 1, 2, 3*
3	*0*	*0, 1, 3, ⋯, 15*
	6	*0, 1, 2, 3, 4, 5, 6, 7, 8, 9*
6	*0*	*0, 1, 3, ⋯, 9*
	3	*0, 1, 2, 3, 6, 7, 8, 9, 12, 13, 14, 15*
9	*0*	*0, 1, 2, 3*

Corollary 10. *The set $\aleph(n,s,q)$ of q-dimensions of the Euclidean hull of a cyclic serial code of length n over R, is given by*

$$\aleph(n,s,q)=\left\{\sum_{\substack{i\mid n\\ i\in\mathcal{N}_q}}ord_i(q)\left(\sum_{l=1}^{\gamma(i;q)}\triangle_{il}\right)+\sum_{\substack{j\mid n\\ i\notin\mathcal{N}_q}}ord_j(q)\left(\sum_{h=1}^{\beta(j;q)}\blacktriangle_{jh}\right)\Big|\ \begin{array}{l}0\le\triangle_{il}\le s-\lceil\frac{s}{2}\rceil\\ 0\le\blacktriangle_{jh}\le s\end{array}\right\}.$$

Proof. Let C be a cyclic serial code of length n over R with triple-sequence

$$\left(((x_{il}^{(a)})_{0\le a<s})^{\circ}),(((y_{jh}^{(a)})_{0\le a<s})^{\bullet}),(((z_{jh}^{(a)})_{0\le a<s})^{\bullet})\right)$$

in $\mathscr{E}_n(q,s)$. From Theorem 27, the parameters $(k_0,k_1,\cdots,k_{s-1})$ of $\mathscr{H}_0(C)$ where for all $0\le t\le s-1$,

$$k_t=\sum_{\substack{i\mid n\\ i\in\mathcal{N}_q}}\mathtt{ord}_i(q)\cdot\left(\sum_{i=1}^{\gamma(i;q)}u_{il}^{(t)}\right)+\sum_{\substack{j\mid n\\ i\notin\mathcal{N}_q}}\mathtt{ord}_j(q)\cdot\left(\sum_{h=1}^{\beta(j;q)}(\varepsilon_{jh}^{(t-1)}-\varepsilon_{jh}^{(t)})\right).$$

Thus the q-dimension of $\mathscr{H}_0(C)$ is $\sum_{t=0}^{s-1}(s-t)k_t$. It follows that

$$\mathtt{dim}_q(C)=\sum_{\substack{i\mid n\\ i\in\mathcal{N}_q}}\mathtt{ord}_i(q)\cdot\left(\sum_{i=1}^{\gamma(i;q)}\triangle_{il}\right)+\sum_{\substack{j\mid n\\ i\notin\mathcal{N}_q}}\mathtt{ord}_j(q)\cdot\left(\sum_{h=1}^{\beta(j;q)}\blacktriangle_{jh}\right).$$

From Remark 5.4.1,

$$\triangle_{il}=\sum_{t=0}^{s-1}\triangle_{il}^{(t)}=\sum_{t=\lceil\frac{s}{2}\rceil}^{s-1}\triangle_{il}^{(t)}\le s-\left\lceil\frac{s}{2}\right\rceil,$$

and if $j \in \mathcal{N}_q$ then $\blacktriangle_j = 0$. Otherwise,

$$\blacktriangle_{jh} = \sum_{t=0}^{s-1} \blacktriangle_{jh}^{(t)} = \sum_{t=0}^{\lceil \frac{s}{2} \rceil - 1} \blacktriangle_{jh}^{(t)} + \sum_{t=\lceil \frac{s}{2} \rceil}^{s-1} \blacktriangle_{jh}^{(t)} \leq \max_{0 \leq b \leq s-\lceil \frac{s}{2} \rceil} \left\{ \left(\left\lceil \frac{s}{2} \right\rceil + b \right) + 2\left(s - \left\lceil \frac{s}{2} \right\rceil - b \right) \right\} = s.$$

□

5.5 | The average q-dimension

We will denote by $\mathscr{C}(n;R)$ the set of all cyclic serial codes over length n over R. The average q-dimension of the Euclidean hull of cyclic of length n over R is

$$\mathtt{E}_R(n) = \sum_{C \in \mathscr{C}(n;R)} \frac{\mathtt{dim}_q(\mathscr{H}_0(C))}{|\mathscr{C}(n;R)|}.$$

In this section, an explicit formula for $\mathtt{E}_R(n)$ and bounds are given in terms of $\mathtt{B}_{n,q}$ where

$$\mathtt{B}_{n,q} = \mathtt{deg} \prod_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \left(\prod_{l=1}^{\gamma(i;q)} \Omega(G_{il}) \right) = \sum_{\substack{i \mid n \\ i \in \mathcal{N}_q}} \phi(i),$$

where G_{il} are symmetric q-cyclotomic cosets modulo n of size $\mathtt{ord}_j(q)$, as defined in (5.4).

Consider the maps

$$\begin{array}{rccc} \Delta: & \mathscr{E}_s & \to & \mathbb{N} \\ & (x^{(0)}, \cdots, x^{(s-1)}) & \mapsto & \displaystyle\sum_{t=0}^{s-1} \min \left\{ \sum_{a=0}^{t} x^{(a)}; 1 - \sum_{a=0}^{s-t-1} x^{(a)} \right\}, \end{array} \tag{5.13}$$

and $\blacktriangle : \mathscr{E}_s \times \mathscr{E}_s \to \mathbb{N}$ defined as

$$\blacktriangle(\mathbf{y},\mathbf{z}) = \sum_{t=0}^{s-1} \left(\min \left\{ \sum_{a=0}^{t} y^{(a)}; 1 - \sum_{a=0}^{s-t-1} z^{(a)} \right\} + \min \left\{ \sum_{a=0}^{t} z^{(a)}; 1 - \sum_{a=0}^{s-t-1} y^{(a)} \right\} \right), \tag{5.14}$$

where $(\mathbf{y},\mathbf{z}) = ((y^{(0)}, \cdots, y^{(s-1)}), (z^{(0)}, \cdots, z^{(s-1)}))$.

Let $\tau \in \aleph(n,s,q)$ be an element in the set defined in Corollary 10. Then τ is the q-dimension of the Euclidean hull of a cyclic serial code of length n over R. The following result gives the number of cyclic serial codes of length n over R whose Euclidean hulls have q-dimension τ.

Proposition 5.5.1. *Let n be a positive integer such that $gcd(n,p)=1$ and $\tau \in \aleph(n,s,q)$ where $\aleph(n,s,q)$ is described in Corollary 10. The number $\wp(n,\tau;R)$ of cyclic serial codes of length n over R whose Euclidean hulls have q-dimension τ is given by:*

$$\wp(n,\tau;R)=\sum_{(((\triangle_{il})^{\circ}),((\blacktriangle_{jh})^{\bullet}))\in\Upsilon(\tau)}\left(\prod_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}\prod_{l=1}^{\gamma(i;q)}\psi_s(\triangle_{il})\right)\left(\prod_{\substack{j\,|\,n\\ j\notin\mathcal{N}_q}}\prod_{h=1}^{\beta(j;q)}\rho_s(\blacktriangle_{jh})\right),$$

where

$$\psi_s(\triangle_{il})=|\{\boldsymbol{x}\in\mathscr{E}_s:\triangle(\boldsymbol{x})=\triangle_{il}\}|,\ \rho_s(\blacktriangle_{jh})=|\{(\boldsymbol{y},\boldsymbol{z})\in\mathscr{E}_s\times\mathscr{E}_s:\blacktriangle(\boldsymbol{y},\boldsymbol{z})=\blacktriangle_{jh}\}|,$$

and

$$\Upsilon(\tau)=\left\{(((\triangle_{il})^{\circ}),((\blacktriangle_{jh})^{\bullet})):\sum_{\substack{i\,|\,n\\ i\in\mathcal{N}_q}}ord_i(q)\left(\sum_{l=1}^{\gamma(i;q)}\triangle_{il}\right)+\sum_{\substack{j\,|\,n\\ i\notin\mathcal{N}_q}}ord_j(q)\left(\sum_{h=1}^{\beta(j;q)}\blacktriangle_{jh}\right)=\tau\right\}.$$

The above expression of $\mathrm{E}_R(n)=\sum_{\tau\in\aleph(n,s,q)}\frac{\tau\cdot\wp(n,\tau;R)}{|C\in\mathscr{C}(n;R)|}$, might lead to a tedious and lengthy computation. The remainder of the section will show an alternative simpler expression for the expected value.

Lemma 5.5.1. *Consider the random variable $\triangle$ defined in (5.13) with uniform probability. The expected value $E(\triangle)$ is given by:*

$$E(\triangle)=\frac{\lceil\frac{s}{2}\rceil\left(s-\lceil\frac{s}{2}\rceil\right)}{s+1}=\begin{cases}\frac{s^2}{4(s+1)}, & \text{if } s \text{ even;}\\ \frac{s-1}{4}, & \text{if } s \text{ odd.}\end{cases}$$

Proof. Let $t\in\{0;1;\cdots;s-1\}$ and $\mathbf{x}=(x^{(0)},\cdots,x^{(s-1)})\in\mathscr{E}_s$. Set

$$\triangle_{(\mathbf{x})}^{(t)}=\min\left\{\sum_{a=0}^{t}x^{(a)};1-\sum_{a=0}^{s-t-1}x^{(a)}\right\}\in\{0;1\}.$$

Then $\triangle_{(\mathbf{x})}^{(t)}=1$ if and only if $2t\geq s$ and , $\sum_{a=s-t}^{t}x_{il}^{(a)}=1$. Thus for all $\eta\in\mathbb{N}$, we have

$$|\{\mathbf{x}\in\mathscr{E}_s:\triangle_{(\mathbf{x})}^{(t)}=\eta\}|=\begin{cases}2t-s+1, & \text{if } t\geq\lceil\frac{s}{2}\rceil \text{ and } \eta=1;\\ 0, & \text{otherwise.}\end{cases}$$

Therefore,

$$\begin{aligned}|\{\mathbf{x}\in\mathscr{E}_s : \triangle(\mathbf{x})=\eta\}| &= \begin{cases}\sum_{t=\lceil\frac{s}{2}\rceil}^{s-1}(2t-s+1), & \text{if } \eta=s-\lceil\frac{s}{2}\rceil;\\ 0, & \text{otherwise.}\end{cases}\\ &= \begin{cases}\lceil\frac{s}{2}\rceil\big(s-\lceil\frac{s}{2}\rceil\big), & \text{if } \eta=s-\lceil\frac{s}{2}\rceil;\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

Since $|\mathscr{E}_s|=s+1$ and $\mathtt{P}(\{\mathbf{x}\in\mathscr{E}_s : \triangle(\mathbf{x})=\eta\})=\frac{|\{\triangle(\mathbf{x})=\eta\}|}{|\mathscr{E}_s|}$, it follows that,

$$\mathtt{E}(\triangle)=\sum_{\eta\in\mathbb{N}}\eta\mathtt{P}(\{\mathbf{x}\in\mathscr{E}_s : \triangle(\mathbf{x})=\eta\})=\frac{\lceil\frac{s}{2}\rceil\big(s-\lceil\frac{s}{2}\rceil\big)}{s+1}.$$

□

Lemma 5.5.2. *Consider the random variable $\blacktriangle : \mathscr{E}_s\times\mathscr{E}_s\to\mathbb{N}$ defined in (5.14) with uniform distribution. The expected value $E(\blacktriangle)$ si given by*

$$E(\blacktriangle)=\frac{s(2s+1)}{3(s+1)}.$$

Proof. From Corollary 10, for any $(\mathbf{y},\mathbf{z})\in\mathscr{E}_s\times\mathscr{E}_s$, $0\le\blacktriangle(\mathbf{y},\mathbf{z})\le s$. Let

$$\mathscr{E}_s(\eta)=\{(\mathbf{y},\mathbf{z})\in\mathscr{E}_s\times\mathscr{E}_s : \blacktriangle(\mathbf{y},\mathbf{z})=\eta\},$$

for $0\le\eta\le s$. Now,

$$|\mathscr{E}_s(\eta)|=\begin{cases}2(\eta+1), & \text{if } 0\le\eta\le s-1;\\ s+1, & \text{if } \eta=s.\end{cases}$$

Thus

$$\begin{aligned}\mathtt{E}(\blacktriangle) &= \frac{1}{(s+1)^2}\sum_{\eta=0}^{s}\eta|\mathscr{E}_s(\eta)|;\\ &= \frac{1}{(s+1)^2}\left(\sum_{\eta=1}^{s-1}2\eta(\eta+1)+s(s+1)\right);\\ &= \frac{s(2s^2+3s+1)}{3(s+1)^2}.\end{aligned}$$

□

Theorem 28. *The average q-dimension of the Euclidean hull of cyclic serial codes from $\mathscr{C}(n;R)$ is*

$$E_R(n) = \begin{cases} \left(\frac{(2s+1)s}{6(s+1)}\right)n - \left(\frac{(s+2)s}{12(s+1)}\right)B_{n,q}, & \text{if } s \text{ even;} \\ \left(\frac{(2s+1)s}{6(s+1)}\right)n - \left(\frac{s^2+2s+3}{12(s+1)}\right)B_{n,q}, & \text{if } s \text{ odd.} \end{cases}$$

where $B_{n,q} = \sum_{\substack{i \mid n \\ i \in \mathscr{N}_q}} \phi(i)$.

Proof. Let Y be the random variable that takes as value $\mathtt{dim}_q(\mathscr{H}_0(C))$ when we choose at random a cyclic serial code from $\mathscr{C}(n;R)$ with uniform probability. Then $\mathtt{E}(Y) = \mathtt{E}_R(n)$. By Lemma 5.3.1, there exists an one-to-one correspondence between $\mathscr{C}(n;R)$, and $\mathscr{E}_n(q,s)$. Therefore, choosing a cyclic serial code C from $\mathscr{C}(n,R)$ their probabilities are identical. By Corollary 10, we obtain

$$Y = \sum_{\substack{i \mid n \\ i \in \mathscr{N}_q}} \mathtt{ord}_i(q) \left(\sum_{l=1}^{\gamma(i;q)} \vartriangle_{il} \right) + \sum_{\substack{j \mid n \\ i \notin \mathscr{N}_q}} \mathtt{ord}_j(q) \left(\sum_{h=1}^{\beta(j;q)} \blacktriangle_{jh} \right).$$

For all i and j dividing n such that $i \in \mathscr{N}_q$ and $j \notin \mathscr{N}_q$, from Lemmas 5.5.1 and 5.5.2, we note that $\mathtt{E}(\vartriangle_{il}) = \mathtt{E}(\vartriangle)$ and $\mathtt{E}(\blacktriangle_{jh}) = \mathtt{E}(\blacktriangle)$. So, we get

$$\begin{aligned} \mathtt{E}(Y) &= \sum_{\substack{i \mid n \\ i \in \mathscr{N}_q}} \mathtt{ord}_i(q) \left(\sum_{l=1}^{\gamma(i;q)} \mathtt{E}(\vartriangle) \right) + \sum_{\substack{j \mid n \\ i \notin \mathscr{N}_q}} \mathtt{ord}_j(q) \left(\sum_{h=1}^{\beta(j;q)} \mathtt{E}(\blacktriangle) \right); \\ &= \sum_{\substack{i \mid n \\ i \in \mathscr{N}_q}} \phi(i)\mathtt{E}(\vartriangle_{il}) + \sum_{\substack{j \mid n \\ i \notin \mathscr{N}_q}} \frac{\phi(j)}{2} \mathtt{E}(\blacktriangle_{jh}); \\ &= \mathtt{B}_{n,q}\mathtt{E}(\vartriangle) + \left(\frac{n - \mathtt{B}_{n,q}}{2}\right)\mathtt{E}(\blacktriangle); \\ &= \frac{n}{2}\mathtt{E}(\blacktriangle) - \mathtt{B}_{n,q} \cdot \left(\frac{1}{2}\mathtt{E}(\blacktriangle) - \mathtt{E}(\vartriangle)\right). \end{aligned}$$

From Lemmas 5.5.1 and 5.5.2, we have

$$\mathtt{E}_R(n) = \begin{cases} \left(\frac{(2s+1)s}{6(s+1)}\right)n - \left(\frac{(s+2)s}{12(s+1)}\right)\mathtt{B}_{n,q}, & \text{if } s \text{ even;} \\ \left(\frac{(2s+1)s}{6(s+1)}\right)n - \left(\frac{s^2+2s+3}{12(s+1)}\right)\mathtt{B}_{n,q}, & \text{if } s \text{ odd.} \end{cases}$$

□

From [34], we have $\mathtt{B}_{n,q} = n$ if $n \in \mathscr{N}_q$ and $1 \leq \mathtt{B}_{n,q} \leq \frac{2n}{3}$ if $n \notin \mathscr{N}_q$. Thus

- If $n \in \mathscr{N}_q$, then
$$\mathtt{E}_R(n) = \begin{cases} \frac{s^2 n}{4(s+1)}, & \text{if } s \text{ even;} \\ \frac{n(s-1)}{4}, & \text{if } s \text{ odd.} \end{cases}$$
- If $n \notin \mathscr{N}_q$, then
$$\begin{cases} \frac{(5s+1)sn}{18(s+1)} \leq \mathtt{E}_R(n) \leq \frac{2n(2s+1)s-(s+2)s}{12(s+1)}, & \text{if } s \text{ even;} \\ \frac{(5s^2+s-3)n}{18(s+1)} \leq \mathtt{E}_R(n) \leq \frac{2ns(2s+1)-(s^2+2s+3)}{12(s+1)}, & \text{if } s \text{ odd.} \end{cases}$$

Remark 5.5.1. *$E_R(n)$ grows at the same rate with ns as s and n is coprime with p and tend to infinity. Thus, the upper limit of the sequence $\left(\frac{E_R(n)}{sn}\right)_{\substack{(s,n)\in(\mathbb{N}\setminus\{0\})^2 \\ gcd(p,n)=1}}$ is at most $\frac{1}{3}$ and its its lower limit is at least $\frac{5}{18}$.*

6

Conclusions and future works

Summing up, during this dissertation we have focused on the hull and the dimension of the hull of cyclic codes. First we recalled some basic consepts and key results on cyclic codes over finite fields and rings, we gave the characterization of the hull of cyclic codes in terms of their generator polynomials with respect to the Euclidean inner product over finite fields and rings. We discussed recepectively about the type of the hulls of cyclic codes over $\mathbb{F}_q$ and $\mathbb{Z}_4$ and we gave a formula of the average q-dimensions of the hull of cyclic codes. We generalized the notion of the hull of cyclic code over over $\mathbb{F}_q$ and $\mathbb{Z}_4$ to an arbitrary finite chain ring R. Moreover, we explored some properties of hulls of cyclic serial codes over a fnite chain ring. As special cases, we gave some results about LCD and self orthogonal codes. We provided an algorithm for computing all the possible parameters of the Euclidean hulls of that codes and we gave an expression of the set $\aleph(n,s,q)$ of q-dimensions of the Euclidean hulls of cyclic serial codes of length n over R. We determined the number $\wp(n,\tau;R)$ of cyclic serial codes of length n over finite chain rings having hulls of a given q-dimension. Finaly, We established an alternative simpler expression of $\mathbb{E}_R(n)$, the average q-dimensions of the Euclidean hulls of cyclic serial codes over finite chain rings with its upper and lower bounds. We showed that $\mathbb{E}_R(n)$, grows at the same rate with ns as n and s are coprime with p. Based on our survey and study, now we present a few open directions for future investigation.

1. It would be an interesting problem to determine dual codes of constacyclic codes over finite chain ring R and to study the hull of constacyclic codes R.

2. Another interesting problem would be to study the properties the hulls of repeated-root cyclic codes over finite chain rings.

3. It would be also interesting to study the hull of nnegacyclic serial codes over finite chain rings.

References

[1] E.F. Assmus, J.D. Key, *Affine and projective planes*, Discrete Math. **83** (1990), 161-187.

[2] G. Bini and F. Flamini, *Finite commutative rings and their a pplications*, University of Michigan, Universita degli Studi Roma Tre,U.S.A and Italy, 2002.

[3] A. Batoul, K. Guenda, T. A. Gulliver, *On self-dual codes over finite chaing rings*, Des. Codes and Cryptogr. **70** (2014) 347-358.

[4] S. Bhowmick, A. Fotue-Tabue, E. Martínez-Moro, R. Bandi, S. Bagchi, *Do non-free LCD codes over finite commutative Frobenius rings exist*, Des. Codes Cryptogr. **88** (2020), 825-840.

[5] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Appl. Discr. Math., **128** 27–46, 2003.

[6] T. Blackford, *Negacyclic codes over $\mathbb{Z}_4$ of even length*, IEEE. Trans. Inform. Theory, **49**(6) 1417–1424, June 2003.

[7] A. Bonnecaze, P. Solé, and A. R. Calderbank, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory, **41**(2) 366–377, Mar. 1995.

[8] A. Bonnecaze and P. Udaya, *cyclic codes and self-Dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$*, 1998.

[9] A.R. Calderbank and N.J.A. Sloane, *Modular and p-adic cyclic codes*, Designs, Codes, Cryptogr., 6, 1995, 21–35.

[10] H. Q. Dinh, S. R. López-Permouth, *Cyclic and Negacyclic Codes Over Finite Chain Rings*, IEEE Trans. Inform. Theory, **50** (2004),1728-1744.

[11] A. Fotue-Tabue, C. Mouaha, *On the Lattice of Cyclic Linear Codes Over Finite Chain Rings*, Algebra and Discrete Math. **27** (2019), 252-268.

[12] A. Fotue Tabue, E. Martínez-Moro, C. Mouaha, *Galois correspondence on linear codes over finite chain rings*, Discrete Math. **343** (2020) 111653, https://doi.org/10.1016/j.disc.2019.111653

[13] T. Honold, I. Landjev, *Linear Codes over Finite Chain Rings*, The electronic journal of combinatorics 7 (2000),

[14] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes,* Cambridge, 2003.

[15] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z_4 linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, 40(2) 301–319, Mar. 1994.

[16] S. Jitman, E. Sangwisut, *The Average Hull Dimension of Negacyclic Codes over Finite Fields*, Math. Comput. Appl. **23**, no. 3: 41. https://doi.org/10.3390/mca23030041

[17] S. Jitman, E. Sangwisut, P. Udomkavanich, *Hulls of Cyclic Codes over $\mathbb{Z}_4$*, Discrete Math. **343**, (2020) 111621, https://doi.org/10.1016/j.disc.2019.111621

[18] P. Kanwar and S. R. López-Permouth, Cyclic codes over the integers modulo p^m, Finite Fields Appl., 3(4) 334–352, Oct. 1997.

[19] A.Klapper and M.Goresky,An introduction to abstract algebra.

[20] H. Liu, X. Pan, *Galois hulls of linear codes over finite fields*. Des. Codes Cryptogr. **88** (2020), 241–255 .

[21] J. S. Leon, *Computing automorphism groups of error-correcting codes*, IEEE Trans. Inf. Theory **28**(3) (1982) 496-511.

[22] S. López-Permouth and S. Szabo, *Repeated root cyclic and negacyclic codes over Galois rings*, Applied Algebra, Albebraic Algorithms and Error-Correcting Codes, Springer Lecture Notes in Computer Science, 5527 219–222, 2009.

[23] B. R. McDonald, *Finite Rings with Identity* Marcel Dekker Inc., New York (1974)

[24] E. Martínez-Moro, I. F. Rúa, *Multivariable Codes Over Finite Chain Rings: Serial Codes* SIAM J. Discrete Math., **20** (2006), 947-959.

[25] F. J. Macwilliams and N.J.A Sloane, *Thetheory of error correcting-codes,* Benjamin, Inc. Amsterdam,North-Holland, 1977

[26] G. H. Norton and A. Sălăgean, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engr. Comm. Comput., 10(6) 489–506, 2000. S. Ling et C. Xing,Coding Theory, Cambridge, 2004.

[27] G. H. Norton, A. Salagean, *On the Structure of Linear and Cyclic Codes over a Finite Chain Ring*, AAECC. **10** (2000), 489-506 .

[28] E. Petrank, R. M. Roth, *Is code equivalence easy to decide?*, IEEE Trans. Inf. Theory, **43**(1997), 1602-1604

[29] E. Rains and N.J.A. Sloane, *Self-dual codes*, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 177–294, 1998.

[30] S. Roman, Coding and Information Theory, Graduate Texts in Mathematics, 134, Springer-Verlag, New-York, 1992.

[31] N. Sendrier, *Finding the permutation between equivalent codes: the support splitting algorithm*, IEEE Trans. Inf. Theory, **46** (2000), 1193-1203.

[32] N. Sendrier, *On the dimension of the hull*, SIAM J. Appl. Math. **10** (1997), 282-293.

[33] E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, *Hulls of cyclic and negacyclic codes over finite fields*, Finite Fields Appl. 33 (2015) 232-257.

[34] G. Skersys, *The average dimension of the hull of cyclic codes*, Discrete Appl. Math. **128**(2003), 275-292.

[35] A.K. Singh, N. Kumar, K.P. Shum, *Cyclic self-orthogonal codes over finite chain rings*, Asian-Eur. J. Math. **11**(2018), 1850078.

[36] C.E. Shannon, *A mathematical theory of communication*, The Bell system technical journal **27** (1948): 379-423.

[37] G. Skersys, *Calcul du group d'automorphismes des codes*, PhD Thesis, Laco, Limoges, 1999.

[38] N. J. A. Sloane and J. G. Thompson, Cyclic self-dual codes, IEEE. Trans. Inform. Theory, 29(3) 364–366, May 1983.

[39] Jr. Warfield, B. Robert, *Serial rings and finitely presented modules*, J. Algebra, **37** (1975), 187-222. doi:10.1016/0021-8693(75)90074-5

[40] E.A. Whelan, *A note on finite local rings*, Rocky Mountain J. Math., **22**(1992), 757-759.

[41] J. L. Yucas and G. L. Mullin, *Self-reciprocal irreducible polynomials over finite fields*, Designs, Codes, Crypt., 33(3) 275–281, 2004.

[42] O. Zariski and P. Samuel, *Commutative Algebra*. New York: Van Nostrand, 1958