REPEATED-ROOT CYLIC CODES AND MATRIX PRODUCT CODES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

HAKAN ÖZADAM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

DECEMBER 2012

Approval of the thesis:

REPEATED-ROOT CYLIC CODES AND MATRIX PRODUCT CODES

submitted by **HAKAN ÖZADAM** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen ________________
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak ________________
Head of Department, **Cryptography**

Prof. Dr. Ferruh Özbudak ________________
Supervisor, **Department of Mathematics, METU**

Examining Committee Members:

Assoc. Prof. Dr. Ali Doğanaksoy (Head of the examining com.) ________________
Department of Mathematics, METU

Prof. Dr. Ferruh Özbudak (Supervisor) ________________
Department of Mathematics, METU

Asst. Prof. Dr. Ömer Küçüksakallı ________________
Department of Mathematics, METU

Asst. Prof. Dr. Burcu Gülmez Temür ________________
Department of Mathematics, Atılım University

Dr. Muhiddin Uğuz ________________
Department of Mathematics, METU

Date: ________________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: HAKAN ÖZADAM

Signature :

ABSTRACT

REPEATED-ROOT CYLIC CODES AND MATRIX PRODUCT CODES

Özadam, Hakan
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

December 2012, 82 pages

We study the Hamming distance and the structure of repeated-root cyclic codes, and their generalizations to constacyclic and polycyclic codes, over finite fields and Galois rings. We develop a method to compute the Hamming distance of these codes. Our computation gives the Hamming distance of constacyclic codes of length np^s in many cases. In particular, we determine the Hamming distance of all constacyclic, and therefore cyclic and negacyclic, codes of lengths p^s and $2p^s$ over a finite field of characteristic p. It turns out that the generating sets for the ambient space obtained by torsional degrees and strong Groebner basis for the ambient space are essentially the same and one can be obtained from the other.

In the second part of the thesis, we study matrix product codes. We show that using nested constituent codes and a non-constant matrix in the construction of matrix product codes with polynomial units is a crucial part of the construction. We prove a lower bound on the Hamming distance of matrix product codes with polynomial units when the constituent codes are nested. This generalizes the technique used to construct the record-breaking examples of Hernando and Ruano. Contrary to a similar construction previously introduced, this bound is not sharp and need not hold when the constituent codes are not nested. We give a comparison of this construction with a previous one. We also construct new binary codes having the same parameters, of the examples of Hernando and Ruano, but non-equivalent to them.

Keywords: Coding Theory, Linear Codes, Cyclic Codes, Constacyclic Codes, Repeated-Root Cyclic Codes, Optimal Codes, Matrix Product Codes, Code Construction

ÖZ

ÇOK KATLI DÖNGÜSEL KODLAR VE MATRİS ÇARPIM KODLARI

Özadam, Hakan
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Ferruh Özbudak

Aralık 2012 , 82 sayfa

Bu çalışmada Galois halkaları ve sonlu cisimler üzerinde tanımlanan çok katlı döngüsel ve sabit döngüsel kodları ve polidöngüsel kodların yapılarını ve Hamming mesafelerini inceledik. Bu kodların Hamming mesafesini bulmak için bir yöntem geliştirdik. Bu yöntemi kullanarak, uzunluğu np^s olan pek çok sabit döngüsel kodun Hamming mesafesini bulabildiğimizi gördük. Hesaplamalarımız sonucunda karakteristiği p'nin kuvveti olan bir alfabe üzerinde tanımlı, uzunlukları p^s veya $2p^s$ olan bütün döngüsel ve negatif döngüsel kodların Hamming mesafesini elde ettik. Çalıştığımız kodların ambiyant uzaylarını üretmek için literatürde birbirinden bağımsız olarak yayımlanmış iki çalışmada kullanılan torsiyonal dereceler ve Gröbner tabanları tekniklerinin aslında aynı üreteç kümeyi verdiklerini gözlemledik. Ayrıca görünürde farklı bu iki üreteç kümenin birbirlerinden nasıl elde edileceğini gösterdik.

Tezin ikinci kısmında ise matris çarpım kodlarını inceledik. Polinom birimli matris çarpma yönteminde, iç içe geçmiş kodlar kullanmanın ve sadece sabitlerden oluşmayan bir matrisin kullanılmasının nasıl bir fark yaratacağını ortaya koyduk. Kullanılan kodlar iç içe geçmiş olduklarında, üretilen yeni kodun Hamming mesafesi için bir alt sınır bulduk. Bu şekilde Hernando ve Ruano'nun çalışmasındaki en iyi parametrelere sahip bir takım kodları üreten yöntemi genelleştirmiş olduk. Önceden sunulan başka bir yöntemin aksine, kullanılan kodlar iç içe geçmemiş olduklarında bulduğumuz bu alt sınıra ulaşılamayacağını ve ayrıca bu alt sınırın geçerli olmayabileceğini de gözlemledik. Bunların yanında, Hernando ve Ruano'nun çalışmasında sunulan kodlarla aynı parametrelere sahip fakat bu kodlara denk olmayan yeni lineer kodlar elde ettik.

Anahtar Kelimeler: Kodlama Teorisi, Lineer kodlar, Döngüsel Kodlar, Sabit Döngüsel Kodlar, Çok Katlı Döngüsel Kodlar, Optimal Kodlar, Matris Çarpım Kodları, Kod Oluşturma

ACKNOWLEDGMENTS

First and foremost, I would like to thank my supervisor Ferruh Özbudak. He always came to me with very interesting research problems and brilliant ways of approaching them. I benefited a lot from his enthusiasm, insight, knowledge, wisdom, encouragement and support throughout my graduate studies.

I am greatly indebted to Sergio R. López Permouth for his kindness, thoughtfulness, collaboration, guidance and support. My stay in Ohio turned out to be a marvelous experience thanks to the hospitality of his lovely family.

Most of the material in this thesis is the result of many fruitful conversations with Steve Szabo and José Ignacio Iglesias Curto. I would like to thank them for being great collaborators and friends.

I was influenced and inspired by the summer schools on algebra and coding theory, which were organized by Edgar Martínez-Moro. He was also my host when I was a visiting researcher in Spain. I would like to thank him for his support, help, kindness and hospitality.

Oğuz Yayla helped me a lot in finishing up this thesis with great patience. I would like to express my appreciation to him for his invaluable help.

During my graduate and undergraduate studies, my dear friends Alp Bassa, Devrim Kaba and Ayberk Zeytin spent their precious time generously for answering my mathematics related questions. I would like to thank them for sharing their knowledge and ideas with me.

I was very fortunate for having the excellent teachers: Sefa Feza Arslan, Mehpare Bilhan, Emrah Çakçak and Mahmut Kuzucuoğlu who taught me Algebra and made me love it. I would like to express my sincere gratitude to them.

Murat Akman and Hakan Güntürkün were not only ideal office mates but also great friends. I would like to thank them for their uplifting company throughout my graduate life.

I am indebted to Ali Doğanaksoy. He kept motivating me and amusing me during my graduate

life in METU. Working with him was a great pleasure and fun. Assisting him in mathematics courses was a charming and unforgettable experience.

I would like to thank the members of the Department of Mathematics for the friendly working atmosphere in my research assistantship years in METU.

I would like to thank the following people for their support in various ways during my graduate studies: San Ling, Melissa Moore, Heide Gluesing-Luerssen.

I would like to express my gratitude to my thesis Committee members for their feedback and attention.

Last but not least, I would like to thank my mother for her support and endless love.

PREFACE

This thesis consists of two projects on coding theory. In the first project, we study repeated-root cyclic, constacyclic and polycyclic codes. This part is based on the publications [47, 48, 49] of the author. The other project is on the construction of linear codes having best known parameters. The related results are compiled in [13] and submitted for publication.

Linear codes have many applications in computer science such as source coding, cryptography, secret sharing, computer networks, distributed storage and etc. Linear codes are chosen over nonlinear codes as their structure allows efficient encoding / decoding algorithms and easier study of their features like minimum Hamming distance. One very important class of linear codes is cyclic codes. They have an additional algebraic structure and this makes them more interesting for theoretical and practical purposes. Cyclic codes can be grouped into two sub-classes: simple-root cyclic codes and repeated-root cyclic codes. Simple-root cyclic codes are those with codeword length coprime to the characteristic of the alphabet. Repeated-root cyclic codes are those with codeword length having a common prime divisor with the characteristic of the alphabet. Most of the studies in the literature on cyclic codes are focused on the simple-root case. However, coding theory has unprecedented applications in various areas of computer science which are not just limited to reliable communication. For this reason, repeated-root cyclic codes also deserve attention. In this thesis, we study the Hamming distance and the structure of repeated-root cyclic codes, and their generalizations to constacyclic and polycyclic codes, over finite fields and Galois rings. We consider constacyclic codes of length np^s over an alphabet whose characteristic is a power of p. We develop a method to compute the Hamming distance of these codes. Our computations give the Hamming distance of constacyclic codes of length np^s in many cases. In particular, we determine the Hamming distance of all constacyclic, and therefore cyclic and negacyclic, codes of length p^s and $2p^s$ over a finite field of characteristic p. We also study the structure of the ambient space of these codes over Galois rings. There are two approaches to this in the literature. One approach is studying the ambient space via Groebner basis. The other is based on using torsional degrees in order to find nice generating sets. We unify these two approaches and observe that the two sets are essentially the same and one can be obtained from the other. Us-

ing this, we give a method to find the Hamming distance of polycyclic codes if the Hamming distance of the residue code is known.

In the second part of the thesis, we study the construction of codes having best known parameters using matrix product codes with polynomial units. We show that using nested constituent codes and a non-constant matrix in the construction of matrix product codes with polynomial units, which were recently introduced in [4], is a crucial part of the construction. We prove a lower bound on the Hamming distance of matrix product codes with polynomial units when the constituent codes are nested. This generalizes the technique used to construct the record-breaking examples of [27]. Contrary to a similar construction previously introduced, this bound is not sharp and need not hold when the constituent codes are not nested. We give a comparison of this construction with a previous one. We also construct new binary codes having the same parameters, of the examples of [27], but non-equivalent to them. The codes in our examples have less codewords with the minimum Hamming weight of the code compared to the examples of [27].

In Chapter 1, we give some background on algebra and coding theory. We study polycyclic and repeated-root constacyclic codes in Chapter 2 and Chapter 3. First we study the structure of the ambient space of these codes in Chapter 2. Next we compute their Hamming distance in Chapter 3. Chapter 4 is about methods to construct linear codes having good parameters.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

TABLES

CHAPTER 1

Preliminaries

1.1 Algebraic Background

Linear codes have important advantages over nonlinear codes. For example there are much more efficient encoding and decoding algorithms for linear codes compared to nonlinear ones. We can also study their features such as Hamming distance and weight distribution systematically whereas brute force is needed for most of the nonlinear codes. The superiority of linear codes comes from their algebraic structure. Linear codes can be viewed as vector spaces over finite fields or modules over Galois rings. Moreover, cyclic codes can be viewed as ideals of a quotient ring. In this chapter, we briefly give the necessary algebraic background to study the algebraic structure of linear codes. We begin with groups, rings, fields, modules and vector spaces and continue with finite fields and Galois rings. Then we define linear and cyclic codes and state some of their properties.

Though groups and rings are not commutative in general, we will be working with commutative ones in this thesis. So, throughout we will assume that the groups and rings we are dealing with are all commutative. We will give the definitions and properties built on them based on this assumption. A more general and detailed treatment of the topic can be found in textbooks on Algebra such as [22, 30, 35].

1.1.1 Groups

Let S be a nonempty set. A *binary operation* $\star$ is a function from $S \times S$ to S. It is said to be *associative* if $(a \star b) \star c = a \star (b \star c)$ for all $a, b, c \in S$. A *group* G is a set equipped with an associative binary operation $\star$ satisfying the following two properties.

- There is an element $e \in G$ such that $a \star e = e \star a$ for all $a \in G$.
- For every $a \in G$, there is an element $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$. The element a^{-1} is called *the inverse* of a.

The group G is called *commutative* if $a \star b = b \star a$ for all $a, b \in G$. Commutative groups are also called *abelian* groups. Most of the groups we will be working with are commutative.

Let $(G, \star)$ be a group and $H \subset G$ be a subset of G. If H is itself a group under the binary operation inherited from G, then H is called a *subgroup* of G. In other words, H is a subgroup of G if H is closed under $\star$ and H has the identity element.

1.1.2 Rings

Let G be a group with two binary operations $+$ and $\times$, called addition and multiplication respectively. The tuple $(G, +)$ is called an *additive group* and $(G, \times)$ is called a *multiplicative group*.

Let R be a set with two binary operations $+, \times$ defined on it. The set R is called a *ring* if the following hold.

- $(R, +)$ is a commutative group.
- The multiplication operation $\times$ is associative.
- The two binary operations are distributive over each other. More explicitly, for every $a, b, c \in R$, we have $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$.

The ring R is called *commutative* if the multiplication operation $\times$ is commutative. The ring R is said to be *with unity* if there is an element 1_R such that $1_R \times a = a \times 1_R = a$ for all $a \in R$. By convention, we denote the identity element of the additive group by 0_R. Throughout, if the binary operation symbol is omitted, it is assumed to be multiplication. Namely we simply write ab to denote $a \times b$.

Let F be a commutative ring with unity, say 1_F. Then F is called a *field* if every nonzero element has a multiplicative inverse. In other words, for every $a \in F$ with $a \neq 0_F$, there is $a^{-1} \in F$ with $a^{-1} \neq 0$ such that $aa^{-1} = a^{-1}a = 1_F$.

Let R be a commutative ring. Let I be a subset of R. Then I is called an *ideal* of R if I is itself a ring under the binary operations inherited from R and I is closed under multiplication by the elements of R. More explicitly, $I \subset R$ is called an ideal of R if I is a ring and for each $a \in I$ and $r \in R$, we have $ra \in R$. We also write $I \lhd R$ to indicate that I is an ideal of R. Let $r_1, \ldots, r_n \in R$. An ideal $J \subset R$ is said to be *generated* by the set $\{a_1, \ldots, a_n\}$ if $J = \{r_1a_1 + \cdots + r_na_n : \quad r_1, \ldots, r_n \in R\}$. We denote it by $J = \langle a_1, \ldots, a_n \rangle$. If J is generated by one element, i.e. $J = \langle a \rangle$, then J is said to be a *principal ideal*.

R is called a *chain ring* if all its ideals are linearly ordered with respect to set inclusion.

An ideal $P \subsetneq R$ is called a *prime ideal* of R if $rs \in P$ implies $r \in P$ or $s \in P$ for every $r, s \in R$.

An ideal $I \lhd R$ is called a *primary ideal* if for all $uv \in I$, we have $u^n \in I$ or $v \in I$ for some positive integer n.

An ideal $M \subsetneq R$ is called a *maximal ideal* of R if the only ideals containing M are M and R. The *Jacobson Radical* of R is the intersection of all maximal ideals of R. A ring is called a *local ring* if it has only one maximal ideal.

The *socle* of R, denoted by $soc(R)$, is the sum of all ideals of R containing only themselves and the zero ideal.

Let R and S be two rings. A *ring homomorphism* is a map $\varphi : R \to S$ that preserves addition and multiplication. That is $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$ for every $x, y \in R$. The map φ is called *ring isomorphism* if φ is a bijection.

Let R be a ring and $a, b \in R$.

- a is called a *unit* if there is $c \in R$ such that $ac = 1$.

- a is called a *zero divisor* if a is nonzero and there is a nonzero element $w \in R$ such that $aw = 0$.

- a is called *nilpotent* if there is a positive integer n such that $a^n = 0$. The least positive integer m with $a^m = 0$ is called the *nilpotency index* of a.

- a and b be are called *coprime* if there exist $\alpha, \beta \in R$ such that $\alpha a + \beta b = 1$.
- a is called *prime* if $\langle a \rangle$ is a proper prime ideal of R.
- a is called *irreducible* if $a = \alpha\beta$, then α is a unit or β is a unit.
- a is called *primary* if $\langle a \rangle$ is a primary ideal.

Let $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \,:\, a_0, \ldots, a_n \in R,\ n \in \mathbb{Z}^+ \cup \{0\}\}$ be the ring of polynomials in one variable over the ring R. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. The term $a_n x^n$ is called the *leading term* of $f(x)$ and a_n is called the *leading coefficient* of $f(x)$. The polynomial $f(x)$ is called *monic* if $a_n = 1$. The term a_0 is called the *constant term* of $f(x)$.

1.1.3 Fields

A *field* is a commutative ring with unity such that every nonzero element has an inverse with respect to multiplication. In other words, a field F is a commutative ring with unity with the binary operations + and × such that $(F, \times)$ is a commutative group. A subset E of F is called a *subfield* if F is a field itself. The field F is called an *extension* of E.

Let R be a ring and I be its ideal. We denote the set of the equivalence classes of I by R/I. If I is a maximal ideal then R/I is a field and it is called the *residue field* of I.

Let F and K be two fields. A *field homomorphism* is a map $\psi : F \to K$ that preserves addition and multiplication. The map ψ is called a *field isomorphism* if ψ is a bijection.

1.1.4 Modules & Vector Spaces

Let R be a commutative ring with unity. A *module over* R is a set M having the following properties.

- There is a binary operation + on M such that $(M, +)$ is a commutative group.
- There is a map from $R \times M$ to M. For $r \in R$ and $m \in M$, we denote the image of (r, m) by rm. For all $r, s \in R$ and $m, n \in M$, this map has the following properties.

- ♦ $(r+s)m = rm + sm$.
- ♦ $(rs)m = r(sm)$.
- ♦ $r(m+n) = rm + rn$.
- ♦ $1_R m = m$.

Let $N \subset M$. Then N is called a *submodule* of M if N is itself an R-module.

Let F be a field. A set V is called a *Vector Space over F* if V is a module over F.

Let M be a an R-module and $S \subset M$. The set S is said to be *linearly independent* if for every $r_1, \ldots, r_n \in R$ and $s_1, \ldots, s_n \in S$, $r_1 s_1 + r_2 s_2 + \cdots + r_n s_n = 0$ implies $r_1 = r_2 = \cdots = r_n = 0$.

1.1.5 Finite Fields

Linear codes are constructed using a finite alphabet which is customarily a Finite Field. In this subsection, we cover the basics of finite fields and fix our notation. We refer to [36] as a standard text on finite fields.

The simplest finite fields are integers modulo a prime number p. They are denoted by $\mathbb{Z}_p$ or $\mathbb{F}_p$. All other finite fields are constructed by adjoining a root of an irreducible polynomial to them. Here we briefly explain this construction. A more detailed treatment of this topic can be found in the second chapter of [36].

It is well-known that for every positive integer n, we can find an irreducible polynomial of degree n over a Finite Field. It is also well-known that every polynomial over a finite field can be factored linearly over an appropriate extension. So, every polynomial over $\mathbb{F}_p$ has a root over some extension of $\mathbb{F}_p$. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}_p[x]$ be an irreducible polynomial over $\mathbb{F}_p$. Let α be a root of $f(x)$. Then it can be shown that the smallest field containing $\mathbb{F}_p$ and α, denoted by $\mathbb{F}_p(\alpha)$, has p^n elements. Clearly, $\mathbb{F}_p \subset \mathbb{F}_{p^n}$, so $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_p$. All finite fields can be constructed this way. If we pick another root of $f(x)$, say β, then we get essentially the same field. Namely, the fields $\mathbb{F}_p(\alpha)$ and $\mathbb{F}_p(\beta)$ are isomorphic. So, in this sense, there is a unique Finite Field having p^n elements. It is common practice to denote the finite field having q elements by $\mathbb{F}_q$, where $q = p^n$. Hence

$$\mathbb{F}_q \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_p(\beta) \cong \frac{\mathbb{F}_p[x]}{\langle f(x) \rangle}.$$

So, for each prime power q there is a unique Finite Field having q elements, namely $\mathbb{F}_q$. Conversely, the cardinality of any finite field field is a power of a prime number.

We denote the multiplicative group of $\mathbb{F}_q$ by $\mathbb{F}_q^*$. Clearly, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The multiplicative group of $\mathbb{F}_q$ is cyclic, that is $\mathbb{F}_q^* = \{\xi, \xi^2, \ldots, \xi^{q-1}\}$ for some $\xi \in \mathbb{F}_q^*$.

1.1.6 Galois Rings

The theory of Galois rings has similarities with finite fields. For a rigorous treatment of this topic, we refer to [40] as a standard text. We begin with preliminaries and define Galois rings and then mention some of their properties.

Throughout this subsection, R denotes a finite commutative ring with unity.

A polynomial $f(x) \in R[x]$ is called *regular* if $f(x)$ is not a zero divisor.

If R is a local ring with the maximal ideal M, then $F = R/M$ is a field and F is called the *residue field* of R. There is a natural homomorphism μ, called the *canonical projection*, from R to F given by $r \mapsto r + F$. This map extends to a homomorphism of the polynomial rings $R[x]$ and $F[x]$. For this we define, abusing notation,

$$\begin{aligned} \mu : R[x] &\rightarrow F[x] \\ a_n x^n + \cdots + a_1 x + a_0 &\mapsto \mu(a_n)x^n + \cdots + \mu(a_1)x + \mu(a_0) \end{aligned}$$

We denote $\mu(f(x))$ by $\bar{f}(x)$. Note also that μ maps the ideals of $R[x]$ to the ideals of $F[x]$ and we denote the canonical projection of the ideal I by $\bar{I}$.

If $\mu(f(x))$ is irreducible over the residue field F, then $f(x)$ is called *basic irreducible*.

Recall that finite fields can be described as extensions of $\mathbb{F}_p$, where an extension is obtained by the quotient ring $\mathbb{F}_p[x]/\langle g(x)\rangle$ where $g(x)$ is an irreducible polynomial. Similarly, Galois rings can be described as finite extensions of $\mathbb{Z}_{p^a}$. Let $f(x) \in \mathbb{Z}_{p^a}[x]$ be a basic irreducible polynomial of degree m, i.e., $\mu(f(x))$ is irreducible over $\mathbb{F}_p$. Then the *Galois Ring of characteristic p^a having p^{am} elements*, denoted by $GR(p^a, m)$ is the quotient ring $\mathbb{Z}_{p^a}[x]/\langle f(x)\rangle$. Clearly, $GR(p, m) = \mathbb{F}_{p^m}$ and $GR(p^a, 1) = \mathbb{Z}_{p^a}$.

It is well-known that the Galois ring $GR(p^a, m)$ is a local ring with the maximal ideal $\langle p \rangle$. Moreover $GR(p^a, m)$ is a finite chain ring and its ideals are $\langle p^i \rangle$ where $i \in \{0, 1, \ldots, a\}$. A characterization of finite chain rings is as follows.

Lemma 1.1.1 ([20, Proposition 2.1]) *Let R be a finite commutative ring. The following are equivalent.*

1. *R is a chain ring.*
2. *R is a local principal ideal ring.*
3. *R is a local ring and the maximal ideal of R is principal.*

Furthermore, if R is a finite commutative chain ring with the maximal ideal $\langle v \rangle$, then the ideals of R are exactly $\langle v^i \rangle$ where $i \in \{0, 1, \ldots, t\}$ and t is the nilpotency index of v.

The residue field of $GR(p^a, m)$ is $\mathbb{F}_{p^m}$. Let ζ be a generator of the multiplicative group $\mathbb{F}_{p^m} \setminus \{0\}$. The fact that $\mathbb{Z}_{p^a}[\zeta] \cong GR(p^a, m)$ is a classical result of finite ring theory. We can express an element $z \in GR(p^a, m)$ as $z = \sum_{j=0}^{p^m-2} v_j \zeta^j$ where $v_j \in \mathbb{Z}_{p^a}$. Let $\mathcal{T}_m = \{0, 1, \zeta, \ldots, \zeta^{p^m-2}\}$. The set $\mathcal{T}_m$ is called the *Teichmüller set*. Alternatively, we can uniquely express $z \in GR(p^a, m)$ as

$$z = z_0 + pz_1 + \cdots + p^{a-1} z_{a-1}, \quad z_i \in \mathcal{T}_m,$$

which is called the *p-adic expansion* of z.

By the characterization given in [40, Theorem XIII.2], $f(x)$ is regular if and only if one of its coefficients is a unit in $GR(p^a, m)$. As the following theorem says, regular polynomials over Galois rings can be factored uniquely.

Theorem 1.1.2 ([40, Theorem XIII.11]) *Let $f(x) \in GR(p^a, m)[x]$ be a regular polynomial. Then $f(x) = \delta g_1(x) \cdots g_r(x)$ where δ is a unit and $g_1(x), \ldots, g_r(x)$ are regular primary coprime polynomials. Moreover, this factorization is unique up to reordering terms and multiplication by units.*

Now we recall the division algorithm in $\mathbb{F}_{p^m}[x]$ and $GR(p^a, m)[x]$. Since $\mathbb{F}_{p^m}[x]$ is a Euclidean domain, for any $v(x)$ and $0 \neq g(x) \in \mathbb{F}_{p^m}[x]$, there exist unique polynomials $y(x), r(x) \in \mathbb{F}_{p^m}[x]$

such that

$$v(x) = g(x)y(x) + r(x)$$

where either $0 \leq \deg(r(x)) < \deg(g(x))$ or $r(x) = 0$. We define $v(x) \mod g(x)$ as $r(x)$, and we use the notation $v(x) \equiv r(x) \mod g(x)$ in the usual sense.

There is also a division algorithm for polynomials in $GR(p^a, m)[x]$ (see, for example, [40, Exercise XIII.6] or [4, Proposition 3.4.4]). Let $f(x) \in GR(p^a, m)[x]$ and let $h(x) \in GR(p^a, m)[x]$ be a regular polynomial. Then there exist polynomials $z(x), b(x) \in GR(p^a, m)[x]$ such that

$$f(x) = z(x)h(x) + b(x)$$

and $\deg(b(x)) < \deg(h(x))$ or $b(x) = 0$.

1.2 Basics of Coding Theory

Traditionally, linear codes are defined and studied over finite fields. In mid 1990's, linear codes over finite commutative rings, and in particular, over Galois rings, became popular after the seminal paper [25] of Hammons et. al. Yet in the literature, there exist studies on codes over noncommutative rings such as [1]. In this thesis, we study codes over Galois rings and finite fields. So, throughout, we assume that linear codes are defined over commutative rings. A rigorous and in-depth treatment of coding theory can be found in the books [3, 28, 38].

1.2.1 Linear Codes

Let R be a finite commutative ring. A *linear code* C of length n over R is an R-submodule of R^n. If the alphabet is a finite field, i.e. $R = \mathbb{F}_q$, then C is a subspace of the vector space $\mathbb{F}_q^n$. The elements of C are called *codewords*. We can view a codeword $c \in C$ as an n-tuple $c = (c_1, c_2, \ldots, c_n)$ where $c_i \in R$ for $1 \leq i \leq n$.

Let $v = (v_1, \ldots, v_n), w = (w_1, \ldots, w_n) \in C$ be two codewords. The *Hamming distance* between v and w is defined as $d_H(v, w) = |\{i : v_i \neq w_i\}|$. In other words, the Hamming distance between two codewords is the number of different entries in v and w having the same index. The *Hamming weight* of v is defined as the number of nonzero entries of v, i.e., $w_H(v) = |\{i : v_i \neq 0\}|$.

The *minimum Hamming distance*, or, simply *the Hamming distance*, $d_H(C)$ of a linear code C is the minimum of all distances between distinct codewords of C. That is $d_H(C) = \min\{d_H(v,w) : v,w \in C \text{ and } v \neq w\}$. For a linear code C, it can easily be shown, that $d_H(C)$ is equal to the minimum of the Hamming weights of its nonzero codewords. In other words $d_H(C) = \min\{w_H(v) : v \in C \text{ and } v \neq 0\}$.

Let C be a linear code over $\mathbb{F}_q$. The number of elements of a basis of C is called its *dimension*. If C is a linear code C of length n, dimension k and Hamming distance d, then C is referred to as an $[n,k,d]$ code. The integers n,k,d are called the *parameters* of C.

Let C be an $[n,k,d]$ code over $\mathbb{F}_q$. Let $\mathcal{B} = \{w_1, w_2, \ldots, w_k\}$ be a basis for C and $w_i = (w_{i1}, w_{i2}, \ldots, w_{in})$, for all $1 \leq i \leq k$. We define

$$G = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ w_{k1} & w_{k2} & \cdots & w_{kn} \end{bmatrix}.$$

The matrix G is called a *Generator Matrix* for C. So, the linear combinations of the rows of G are exactly the elements of C. Note that, in general, C has more than one generator matrix. On the other hand, a generator matrix uniquely defines a linear code.

1.2.2 Cyclic Codes

Cyclic Codes are obtained by imposing an additional algebraic structure on linear codes. This additional structure allows us to use more algebra to study the structure and the Hamming distance of these codes.

Let $w = (w_0, w_1, \ldots, w_n) \in GR(p^a, m)^n$. The *cyclic shift* of w is defined to be $(w_{n-1}, w_0, w_1, \ldots, w_{n-2}) \in GR(p^a, m)$. Let C be a linear code of length n over $GR(p^a, m)$. C is called a *cyclic code* if C is closed under cyclic shifts. In other words, C is cyclic if

$$(w_0, w_1, \ldots, w_n) \in C \Rightarrow (w_{n-1}, w_0, w_1, \ldots, w_{n-2}) \in C.$$

In order to see the algebraic structure of cyclic codes, we identify the codeword $w = (w_0, w_1, \ldots, w_{n-1})$, over $GR(p^a, m)$, with the polynomial $w(x) = w_0 + w_1x + \cdots + w_{n-1}x^{n-1} \in GR(p^a, m)[x]$. Recall that all of the equivalence classes of $\frac{GR(p^a,m)[x]}{\langle x^n-1 \rangle}$ can be represented by polynomials of degree less than or equal to $n-1$. So, there is a one-to-one correspondence between the elements of the quotient ring $\frac{GR(p^a,m)[x]}{\langle x^n-1\rangle}$ and n-tuples over $GR(p^a, m)$ given by

$$(w_0, w_1, \ldots, w_{n-1}) \leftrightarrow w_0 + w_1 x + \cdots + w_{n-1} x^{n-1}.$$

Then, with respect to the above identification, the cyclic shift of w is obtained by multiplying the corresponding polynomial by x modulo $x^n - 1$. Namely, for $w = (w_0, w_1, \ldots, w_{n-1})$,

$$xw(x) \equiv w_{n-1} + w_0 x + w_1 x^2 + \cdots + w_{n-2} x^{n-1} \mod (x^n - 1).$$

This motivates us to consider the codewords of a cyclic code C of length n over $GR(p^a, m)$ as the elements of the quotient ring

$$\mathcal{S} = \frac{GR(p^a, m)[x]}{\langle x^n - 1\rangle}.$$

It is not hard to show that there is a one-to-one correspondence between the ideals of $\mathcal{S}$ and cyclic codes of length n over $GR(p^a, m)$ in the following sense. Let C be a cyclic code of length n over $GR(p^a, m)$. Let I be the set obtained by expressing all codewords of C as polynomials. Then I is and ideal of $\mathcal{S}$. Conversely, if J is an ideal of $\mathcal{S}$, then we obtain a cyclic code of length n over $GR(p^a, m)$ when we view the elements of J as codewords in the above sense.

A natural generalization of cyclic codes is the so-called constacyclic codes. The *λ-shift* of the codeword $(w_0, w_1, \ldots, w_{n-1})$ is defined to be $(\lambda w_{n-1}, w_0, w_1, \cdots, w_{n-2})$. If a linear code C is closed under λ-shifts, then C is called a λ-cyclic code and in general, such codes are called *constacyclic* codes. It is also well-known that λ-cyclic codes, of length n, over $GR(p^a, m)$ correspond to the ideals of the quotient ring

$$\mathcal{S}_c = \frac{GR(p^a, m)[x]}{\langle x^n - \lambda\rangle}.$$

Clearly, when $\lambda = 1$, the ideals of $\mathcal{S}_c$ are cyclic codes. When $\lambda = -1$, the ideals of $\mathcal{S}_c$ are called *negacyclic* codes.

Constacyclic codes can be grouped into two classes. If the codeword length, namely n, is coprime to the characteristic of the alphabet, then the ideals of $\mathcal{S}_c$ are called *simple-root* constacyclic codes, i.e., if the greatest common divisor of n and p is 1, then the ideals of $\mathcal{S}_c$ are called simple-root cyclic codes. If the codeword length and the characteristic of the alphabet are not coprime, i.e., if p divides n, then such constacyclic codes are called *repeated-root* constacyclic codes.

1.2.3 Polycyclic Codes

Constacyclic codes are defined to be the ideals of the quotient ring $\frac{GR(p^a,m)[x]}{\langle x^n-\lambda\rangle}$. Constacyclic codes can be generalized by considering a regular polynomial as the generator of the ideal in the denominator of this quotient ring.

Let $f(x)$ be a regular polynomial of degree n over $GR(p^a, m)[x]$. The ideals of the quotient ring

$$\mathcal{R} = \frac{GR(p^a, m)[x]}{\langle f(x)\rangle}$$

are called *polycyclic* codes. The elements of $\mathcal{R}$ are cosets of the equivalence class induced by $f(x)$. Each coset is identified uniquely with a polynomial of degree less than $\deg(f(x))$. So, throughout, we identify the elements of $\mathcal{R}$ with polynomials of degree less than $\deg(f(x))$. Let $w(x) = w_0 + w_1x + \cdots + w_{n-1}x^{n-1} \in \mathcal{R}$. As described in the previous subsection, we identify $w(x)$ with $(w_0, w_1, \ldots, w_{n-1}) \in (GR(p^a, m))^n$. Then the ideals of $\mathcal{R}$ are linear codes of length n over $GR(p^a, m)$. Such codes are called *Polycyclic* Codes. The ring $\mathcal{R}$ is called the *ambient space*.

When $GR(p^a, m)$ is a field, i.e., when $a = 1$, the ring $\mathcal{R}$ is a principal ideal ring and it is ideals are generated by the divisors of $f(x)$. When $GR(p^a, m)$ is not a field, i.e., when $a > 1$, the ideals of $\mathcal{R}$ is not necessarily generated by one polynomial. We study these ideals in Section 2 in detail.

Let $\bar{\mathcal{R}} = \frac{\mathbb{F}_{p^m}[x]}{\langle \bar{f}(x)\rangle}$. The map μ, defined above, extends to an onto ring homomorphism as $\mu : \mathcal{R} \to \bar{\mathcal{R}}$ where $\mu(g(x)) = \bar{g}(x)$. Also, for $c = (c_0, c_1 \ldots, c_{n-1}) \in GR(p^a, m)^n$, we define $\mu(c) = \bar{c} = (\bar{c}_0, \bar{c}_1, \ldots, \bar{c}_{n-1})$. Let $r \in \mathcal{R}$ and $w \in \bar{\mathcal{R}}$. We define the scalar multiplication by rw $(mod\ p)$ where we consider the multiplication in $\mathcal{R}$. This makes $\bar{\mathcal{R}}$ an $\mathcal{R}$-module.

Let C be a linear code over $GR(p^a, m)$. We define $\bar{C} = \{\mu(c) : c \in C\}$. The following lemma tells us that the Hamming distance of nontrivial codes is greater than 2 and $d_H(C) = d_H(\bar{C})$.

Lemma 1.2.1 *Let $\{0\} \neq C \lhd \mathcal{R}$ be a constacyclic code of length greater than 1 over $GR(p^a, m)$ with $C \neq \{0\}$ and $C \neq \langle 1\rangle$, and let $\bar{C} \lhd \bar{\mathcal{R}}$ be its canonical projection. Then $d_H(C) = d_H(\bar{C})$ as the $\mathcal{R}$-modules $p^{a-1}\mathcal{R}$ and $\bar{\mathcal{R}}$ are isomorphic. Moreover $d_H(\bar{C}), d_H(C) \geq 2$.*

Proof. The isomorphism is established by sending $f(x) \in \bar{\mathcal{R}}$ to $p^{a-1}f(x) \in p^{a-1}\mathcal{R}$. The bound

$d_H(\bar{C}), d_H(C) \geq 2$ follows from the facts that $d_H(C) = d_H(\bar{C})$ and a proper ideal can not contain a unit. ■

CHAPTER 2

The Ambient Space of Polycyclic Codes

Polycyclic codes are defined to be the ideals of the ring

$$\mathcal{R} = \frac{GR(p^a, m)[x]}{\langle f(x) \rangle},$$

where $f(x) \in GR(p^a, m)[x]$ is a regular polynomial. In this section, we study the ideal structure of the ambient space $\mathcal{R}$.

First, in Section 2.1, we assume $f(x)$ to be primary. Then we use the results there to study the general case in Section 2.2 where $f(x)$ is not necessarily primary. In Section 2.3, we observe that finer results can be obtained in characteristic p^2.

2.1 Structure of the Ambient Space: Primary Case

Let $f(x) \in GR(p^a, m)[x]$ be a regular primary polynomial which is not a unit. Let

$$\mathcal{R} = \frac{GR(p^a, m)[x]}{\langle f(x) \rangle}.$$

First we show that $\mathcal{R}$ is a local ring and determine its maximal ideal, we determine the socle of $\mathcal{R}$, for $a \geq 1$, we give necessary and sufficient conditions for $\mathcal{R}$ to be a chain ring in Lemma 2.1.4. Then, using the notion of torsional code and torsional degree, we determine a unique generating set for any ideal of $\mathcal{R}$ in Theorem 2.1.11. Next we observe, in Corollary 2.1.13, that such a generating set is a strong Groebner basis and if we remove the redundant generators, we obtain a generating set in standard form which is a minimal strong Groebner basis. Finally, we show that the torsional degrees of a polycyclic code can immediately be obtained from a generating set in standard form.

By [40, Theorem XIII.6], $f(x) = vf^*(x)$ where v is a unit and $f^*(x)$ is monic and regular. Since $\langle f(x)\rangle = \langle vf^*(x)\rangle$ and because of our interest in $\mathcal{R}$, assume $f(x)$ is monic. By Proposition [40, XIII.12], $f(x) = \delta(x)h(x)^t + p\beta(x)$ for some $\delta(x), h(x), \beta(x) \in GR(p^a, m)[x]$ where $\delta(x)$ is a unit and $h(x)$ is a basic irreducible polynomial. Since $\delta(x)$ is a unit, by [40, Theorem XIII.2], $\delta(x) = \delta_0 + p\delta'(x)$ for some $\delta_0 \in GR(p^a, m)$ that is a unit and some $\delta'(x) \in GR(p^a, m)[x]$. Also, since $h(x)$ is basic, $h(x) = \overline{h}(x) + p\alpha(x)$ for some $\alpha(x) \in GR(p^a, m)[x]$. So, $\overline{f}(x) = \delta_0\overline{h}(x)^t$ and $f(x) = \delta_0\overline{h}(x)^t + p\beta'(x)$ for some $\beta'(x) \in GR(p^a, m)[x]$.

Assume $f(x) = \delta h(x)^t + p\beta(x)$ where $\delta \in GR(p^a, m)$ is a unit and $h(x)$ is a basic irreducible polynomial such that $\overline{h}(x) = h(x)$. By the fact that $f(x)$ is monic, we know that $t \deg h(x) > \deg \beta(x)$. Furthermore, without loss of generality, we may assume $h(x)$ is monic. By this assumption, $\delta = 1$ since $f(x)$ is monic. Hence, $f(x)$ is a monic regular primary polynomial such that $f(x) = h(x)^t + p\beta(x)$ where $h(x)$ is a monic basic irreducible polynomial such that $\bar{h}(x) = h(x)$.

We show that $\langle p, h(x)\rangle$ is the unique maximal ideal of $\mathcal{R}$.

Lemma 2.1.1 *The ring $\mathcal{R}$ is local with maximal ideal $J(\mathcal{R}) = \langle p + \langle f\rangle, h(x) + \langle f\rangle\rangle$.*

Proof. As discussed in page 262 of [40], any maximal ideal in $GR(p^a, m)[x]$ is of the form $\langle p, g(x)\rangle$ where $g(x)$ is a basic irreducible polynomial. Assume $f(x) \in \langle p, g(x)\rangle$ where $g(x) \in GR(p^a, m)[x]$ is a basic irreducible polynomial. Then for some $a(x), b(x) \in GR(p^a, m)[x]$

$$\begin{aligned} f(x) &= a(x)p + b(x)g(x), \\ \bar{f}(x) &= \bar{b}(x)\bar{g}(x), \\ \bar{h}(x)^t &= \bar{b}(x)\bar{g}(x). \end{aligned}$$

This shows that $\bar{h}(x)|\bar{g}(x)$ which implies $\bar{g}(x)|\bar{h}(x)$ and $g(x) = h(x) + pc(x)$ for some $c(x) \in GR(p^a, m)[x]$. So, $\langle p, g(x)\rangle = \langle p, h(x)\rangle$ meaning $\langle p, h(x)\rangle$ is the only maximal ideal containing $f(x)$. Hence, $\langle p + \langle f\rangle, h(x) + \langle f\rangle\rangle$ is the unique maximal ideal of $\mathcal{R}$. ■

In the case of finite fields, $\mathcal{R}$ is a chain ring.

Lemma 2.1.2 *The quotient ring $\frac{GR(p,m)[x]}{\langle f(x)\rangle}$ is a chain ring with exactly the following ideals*

$$\frac{GR(p,m)[x]}{\langle f(x)\rangle} = \langle h(x)^0 + \langle f\rangle\rangle \supsetneq \langle h(x)^1 + \langle f\rangle\rangle \supsetneq \cdots \supsetneq \langle h(x)^t + \langle f\rangle\rangle = 0.$$

Proof. By Lemma 2.1.1, $\frac{GR(p,m)[x]}{\langle f(x)\rangle}$ is local with $J\left(\frac{GR(p,m)[x]}{\langle f(x)\rangle}\right) = \langle h(x)+\langle f\rangle\rangle$. By Lemma 1.1.1, the result follows. ■

Now we determine the socle of $\mathcal{R}$ and show that it is simple.

Lemma 2.1.3 *The ring $\mathcal{R}$ has simple socle with $soc\,(\mathcal{R}) = \langle p^{a-1}h(x)^{t-1} + \langle f\rangle\rangle$.*

Proof. Let $g(x) + \langle f\rangle \in \mathcal{R}$. Let ℓ be the largest integer such that $p^{\ell}(g(x) + \langle f\rangle) \neq 0$. By Lemma 2.1.1, $J(\bar{\mathcal{R}}) = \langle h(x) + \langle f\rangle\rangle$. By Lemma 1.2.1 and Lemma 2.1.2 and the fact that $p^{\ell}(g(x) + \langle f\rangle) \in \langle p^{a-1} + \langle f\rangle\rangle$, it can be shown that $\langle p^{a-1}h(x)^{t-1} + \langle f\rangle\rangle \subset \langle g(x) + \langle f\rangle\rangle$. So $\langle p^{a-1}h(x)^{t-1} + \langle f\rangle\rangle$ is contained in any principal ideal. Since $J(\mathcal{R})$ annihilates $\langle p^{a-1}h(x)^{t-1} + \langle f\rangle\rangle$, $soc(\mathcal{R}) = \langle p^{a-1}h(x)^{t-1} + \langle f\rangle\rangle$. It is clearly simple. ■

Lemma 2.1.2 tells us when the alphabet is a finite field, then $\mathcal{R}$ is a chain ring. However, $\mathcal{R}$ is not a chain ring in general. As a counter example, consider $\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}$. We have $x^2 - 1 = (x + 1)^2 - 2(x + 1)$. Clearly, $(x + 1) \notin \langle 2\rangle$ in $\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}$. Assume $2 \in \langle x + 1\rangle$. Then $2 = g_1(x)(x + 1) + g_2(x)(x^2 - 1) \in \mathbb{Z}_4[x]$. Evaluating at $x = -1$, we get $2 = 0$ in $\mathbb{Z}_4$. This is a contradiction. Thus we have shown $\langle 2\rangle \not\subset \langle x + 1\rangle$ and $\langle x + 1\rangle \not\subset \langle 2\rangle$. By Lemma 2.1.1, $J\left(\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}\right) = \langle 2, x + 1\rangle$. Since $J\left(\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}\right)$ is 2-generated, by Lemma 1.1.1 $\frac{\mathbb{Z}_4[x]}{\langle x^2-1\rangle}$ is not a chain ring.

The next theorem shows exactly when $\mathcal{R}$ is a chain ring based on the parameters $a, t, h(x)$ and $\beta(x)$ of $f(x)$.

Theorem 2.1.4 *The ring $\mathcal{R}$ is a chain ring if and only if any one of the conditions is met*

1. $a = 1$
2. $t = 1$
3. $\beta(x) \notin \langle p, h(x)\rangle$.

Proof. Assume $a = 1$. By Lemma 2.1.2, $\mathcal{R}$ is a chain ring.

Assume $t = 1$ then $h(x) = f(x) - p\beta(x) \in \langle p, f(x)\rangle$. So, $h(x) + \langle f\rangle \in \langle p + \langle f\rangle\rangle$. By Lemma 2.1.1, $J\,(\mathcal{R}) = \langle p + \langle f\rangle\rangle$. Hence, by Lemma 1.1.1, $\mathcal{R}$ is a chain ring.

Assume $\beta(x) \notin \langle p, h(x)\rangle$. Then $\beta(x) + \langle f\rangle \notin J(\mathcal{R})$ which implies $\beta(x) + \langle f\rangle$ is a unit in $\mathcal{R}$. So, $\langle p + \langle f\rangle\rangle = \langle h(x)^t + \langle f\rangle\rangle$ which implies $p + \langle f\rangle \in \langle h(x) + \langle f\rangle\rangle$. By Lemma 2.1.1, $J(\mathcal{R}) = \langle h(x) + \langle f\rangle\rangle$. Hence, by Lemma 1.1.1, $\mathcal{R}$ is a chain ring.

Now assume $a > 1$, $t > 1$ and $\beta(x) \in \langle p, h(x)\rangle$. We want to show that $\mathcal{R}$ is not a chain ring so assume the contrary. This implies $\langle p + \langle f\rangle\rangle \subset \langle h(x) + \langle f\rangle\rangle$ or $\langle h(x) + \langle f\rangle\rangle \subset \langle p + \langle f\rangle\rangle$. So, $p \in \langle h(x), f(x)\rangle$ or $h(x) \in \langle p, f(x)\rangle$. First, assume $p \in \langle h(x), f(x)\rangle$ which implies $\beta(x) \in \langle p, h(x)\rangle = \langle p, h(x), f(x)\rangle = \langle h(x), f(x)\rangle$. So,

$$f(x) = h(x)^t + p\beta(x) = h(x)^t + p(\gamma(x)h(x) + \alpha(x)f(x))$$

for some $\gamma(x), \alpha(x) \in GR(p^a, m)[x]$ and

$$f(x)(1 - p\alpha(x)) = h(x)\left(h(x)^{t-1} + p\gamma(x)\right).$$

Since $(1 - p\alpha(x))$ is invertible in $GR(p^a, m)[x]$, $f(x) \in \langle h(x)\rangle$. So, $p \in \langle h(x), f(x)\rangle = \langle h(x)\rangle$. Since $a > 1$, $p \neq 0$. This is a contradiction since p cannot be a nonzero multiple of $h(x)$.

Next, assume $h(x) \in \langle p, f(x)\rangle$. Then,

$$h(x)^t = [\gamma(x)p + \alpha(x)f(x)]^t = f(x) - p\beta(x)$$

for some $\gamma(x), \alpha(x) \in GR(p^a, m)[x]$. This implies,

$$\overline{[\alpha(x)f(x)]^t} = \overline{f(x)}.$$

Since $t > 1$, by comparing degrees we see this is a contradiction. Hence, $\mathcal{R}$ is not a chain.

■

Below are two examples that show the distinctions between the particular cases in Theorem 2.1.4.

Example 2.1.5 *Let $a > 1, p = 2, s > 0$ and $f(x) = x^{2^s} + 1$. Then*

$$\begin{aligned} x^{2^s} + 1 &= (x + 1 - 1)^{2^s} + 1 \\ &= (x+1)^{2^s} - \binom{2^s}{2^s - 1}(x+1)^{2^s - 1} + \cdots - \binom{2^s}{1}(x+1) + 1 + 1 \\ &= (x+1)^{2^s} + 2\beta(x) \end{aligned}$$

where $\beta(x) = (x+1)q(x) + 1$ for some $q(x) \in \mathcal{R}$. In [14] it was shown that $\frac{GR(p^a,m)[x]}{\langle f(x)\rangle}$ is a chain ring with the maximal ideal $\langle x + 1\rangle$.

Example 2.1.6 *Let $a > 1, p = 2, s > 0$ and $f(x) = x^{2^s} - 1$. Then*

$$\begin{aligned} x^{2^s} - 1 &= (x+1-1)^{2^s} - 1 \\ &= (x+1)^{2^s} - \binom{2^s}{2^s-1}(x+1)^{2^s-1} + \cdots - \binom{2^s}{1}(x+1) + 1 - 1 \\ &= (x+1)^{2^s} + 2\beta(x) \end{aligned}$$

where $(x+1) | \beta(x)$. In [37] it was shown that $\frac{GR(p^a,m)[x]}{\langle f(x) \rangle}$ is local with the maximal ideal $\langle 2, (x+1) \rangle$ and is not a chain ring.

Theorem 2.1.4 shows that $\mathcal{R}$ is not a principal ideal ring in general. Through the next series of results we will show the existence of a particular generating set which turns out to be a minimal strong Groebner basis (see Definition 2.1.12).

Let $g(x) \in GR(p^a, m)[x]$ and n be the largest integer such that $\deg(g(x)) \geq n \deg(h(x))$. By the division algorithm, we can find $q_n(x), r_1(x) \in GR(p^a, m)[x]$ such that

$$g(x) = q_n(x)h(x)^n + r_1(x),$$

where $r_1(x) = 0$ or $\deg(r_1(x)) < n \deg(h(x))$. Note that $\deg(q_n(x)) < \deg(h(x))$. Next we can find $q_{n-1}(x), r_2(x) \in GR(p^a, m)[x]$ such that

$$r_1(x) = q_{n-1}(x)h(x)^{n-1} + r_2(x)$$

where $r_2(x) = 0$ or $\deg(r_2(x)) < (n-1)\deg(h(x))$. Note that $\deg(q_{n-1}(x)) < \deg(h(x))$. We can continue this process until we have $q_n(x), q_{n-1}(x), \ldots, q_0(x) \in GR(p^a, m)[x]$ where

$$g(x) = q_n(x)h(x)^n + \cdots + q_1(x)h(x) + q_0(x)$$

where for $0 \leq i \leq n$, either $\deg(q_i(x)) < \deg(h(x))$ or $q_i(x) = 0$. With some manipulation $g(x)$ can be represented in the following form

$$g(x) = p^{j_0}h(x)^{i_0}\alpha_0(x) + \cdots + p^{j_r}h(x)^{i_r}\alpha_r(x) \tag{2.1}$$

where $0 \leq r \leq a-1$ and

- $\alpha_i(x) \notin \langle p, h(x) \rangle$
- $0 \leq j_0 < \cdots < j_r \leq a-1$
- $i_0 > \cdots > i_r \geq 0.$

Since $f(x)$ is regular and monic, $g(x)$ can be divided by $f(x)$ initially. Then it is not hard to see that for some $q(x) \in GR(p^a, m)[x]$

$$g(x) = q(x)f(x) + p^{j_0}h(x)^{i_0}\alpha_0(x) + \cdots + p^{j_r}h(x)^{i_r}\alpha_r(x)$$

where r, $\alpha_i(x)$, j_e and i_ℓ are as above with $t > i_0$.

In [21] and [33], a unique generating set for an ideal of $\frac{GR(p^a,m)[x]}{\langle x^{p^s}-1\rangle}$ was developed. The polynomial $x^{p^s} - 1$ is of the type $f(x)$ is. Notice $x^{p^s} - 1 = (x-1)^{p^s} + p\beta(x)$. We will now find a similar generating set for an ideal of $\mathcal{R}$.

Definition 2.1.7 (cf. [21, Definition 6.1]) *Let* $C \lhd \mathcal{R}$. *For* $0 \leq i \leq a-1$, *define*

$$Tor_i(C) = \{\mu(v) : \quad p^i v \in C\}.$$

$Tor_i(C)$ is called the i^{th} *torsion code* of C. $Tor_0(C) = \mu(C)$ is usually called the residue code of C. Note that for a code C over $GR(p^a, m)$, we have $Tor_i(C) \subset Tor_{i+1}(C)$.

Lemma 2.1.8 *Let* $C \lhd \mathcal{R}$. *Then*

$$Tor_i(C) = \langle h(x)^{T_i} + \langle f \rangle\rangle \subset \frac{GR(p,m)[x]}{\langle f(x)\rangle}$$

for some $0 \leq T_i \leq t$.

Proof. Since $C \lhd \mathcal{R}$, $Tor_i(C) \lhd \frac{GR(p,m)[x]}{\langle \bar{f}(x)\rangle}$. The claim follows by Lemma 2.1.2. ■

Definition 2.1.9 *In Lemma 2.1.8,* T_i *is the* i^{th} *torsional degree of* C *which we denote by* $T_i(C)$. *The torsional degrees form a non-increasing sequence, i.e.,* $t \geq T_0(C) \geq \cdots \geq T_{a-1}(C) \geq 0$.

For any $\xi(x) + \langle f \rangle \in \mathcal{R}$, we can divide $\xi(x)$ by $f(x)$, as $f(x)$ is regular, and get $\xi(x) = q(x)f(x) + r(x)$ such that either $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. So $\xi(x) + \langle f \rangle = r(x) + \langle f \rangle$. This implies that $\mathcal{R} = \{a(x) + \langle f \rangle : a(x) \in GR(p^a, m)[x], \deg(a(x)) < \deg(f(x))\}$. Throughout the remainder for this section, the elements of $\mathcal{R}$ will be represented as polynomials of degree less than $\deg(f(x))$.

Definitions 2.1.7 and 2.1.9 and Lemma 2.1.8 are expansions to polycyclic codes of the ideas first presented in Section 6 of [21] in the context of cyclic codes. The following theorem is a generalization of Theorem 6.5 of [21].

Theorem 2.1.10 *Let $C \lhd \mathcal{R}$. Then $C = \langle F_0(x), pF_1(x), \ldots, p^{a-1}F_{a-1}(x)\rangle$ where $F_i(x) = 0$ if $T_i(C) = t$, and $F_i(x) = h(x)^{T_i(C)} + p\gamma_i(x)$ for some $\gamma_i(x) \in GR(p^a, m)[x]$, if $T_i(C) < t$.*

Proof. Denote $T_i(C)$ by T_i. If $C = 0$, we are done. So assume $C \neq 0$. Let r be the smallest nonnegative integer such that $T_r < t$. For every $0 \leq i \leq r-1$, set $F_i(x) = 0$. For $r \leq i \leq a-1$, pick $F_i(x) \in GR(p^a, m)[x]$ such that $p^iF_i(x) \in C$ and $\mu(F_i(x)) = h(x)^{T_i}$. So, $F_i(x) = h(x)^{T_i} + p\gamma_i(x)$ for some $\gamma_i(x) \in \mathcal{R}$. Note that such an $F_i(x)$ exists because $Tor_i(C) = \langle h(x)^{T_i}\rangle \lhd \frac{GR(p,m)[x]}{\langle f(x)\rangle}$. Let $g(x) \in C$. As was shown earlier (see Equation (2.1)),

$$g(x) = p^{j_0}(h(x)^{i_0}\sigma_{j_0}(x) + p\beta_0(x)) \tag{2.2}$$

for some $\sigma_{j_0}(x), \beta_0(x) \in GR(p^a, m)[x]$ where $i_0 < t$ and $\sigma_{j_0}(x) \neq 0$. Let $\sigma_0(x) = \cdots = \sigma_{j_0-1}(x) = 0$. Let

$$g_1(x) = g(x) - p^{j_0}h(x)^{i_0-T_{j_0}}\sigma_{j_0}(x)F_{j_0}(x).$$

Note that since $Tor_{j_0}(C) = \langle h(x)^{T_{j_0}}\rangle$, it follows by (2.2) and the fact that $\sigma_{j_0}(x)$ is a unit in $\frac{GR(p^a,m)[x]}{\langle f(x)\rangle}$ that $i_0 \geq T_{j_0}$. Since $T_{j_0} < t$, we have

$$\begin{aligned} g_1(x) &= p^{j_0}(h(x)^{i_0}\sigma_{j_0}(x) + p\beta_0(x)) - p^{j_0}h(x)^{i_0-T_{j_0}}\sigma_{j_0}(x)[h(x)^{T_{j_0}} + p\gamma_{j_0}(x)] \\ &= p^{j_0+1}\beta_0(x) - p^{j_0+1}h(x)^{i_0-T_{j_0}}\sigma_{j_0}(x)\gamma_{j_0}(x). \end{aligned}$$

So, $g_1(x) \in \langle p^{j_0+1}\rangle \cap C$. If $g_1(x) = 0$, let $\sigma_{j_0+1}(x) = \cdots = \sigma_{a-1}(x) = 0$ and we are done. If not, then, as was done with $g(x)$, we can view $g_1(x)$ as

$$g_1(x) = p^{j_1}(h(x)^{i_1}\sigma_{j_1}(x) + p\beta_1(x))$$

for some $\sigma_{j_1}(x), \beta_1(x) \in GR(p^a, m)[x]$ where $i_1 < t$, $j_0 < j_1$ and $\sigma_{j_1}(x) \neq 0$. Let $\sigma_{j_0+1}(x) = \cdots = \sigma_{j_1-1}(x) = 0$. Let

$$g_2(x) = g_1(x) - p^{j_1}h(x)^{i_1-T_{j_1}}\sigma_{j_1}(x)F_{j_1}(x).$$

Since $T_{j_1} < t$, we have

$$\begin{aligned} g_2(x) &= p^{j_1}(h(x)^{i_1}\sigma_{j_1}(x) + p\beta_1(x)) - p^{j_1}h(x)^{i_1-T_{j_1}}\sigma_1(x)[h(x)^{T_{j_1}} + p\gamma_{j_1}(x)] \\ &= p^{j_1+2}\beta_1(x) - p^{j_1+1}h(x)^{i_1-T_{j_1}}\sigma_1(x)\gamma_{j_1}(x). \end{aligned}$$

So $g_2(x) \in \langle p^{j_1+1}\rangle \cap C$. If $g_2(x) = 0$, then let $\sigma_{j_1+1}(x) = \cdots = \sigma_{a-1}(x) = 0$. Note that since $j_0 < j_1 < a$, this is a finite process. So

$$g(x) = \sum_{i=0}^{a-1} p^ih(x)^{i-T_i}\sigma_i(x)F_i(x) \in \langle F_0(x), pF_1(x), \ldots, p^{a-1}F_{a-1}\rangle.$$

Hence $C \subset \langle F_0(x), pF_1(x), \ldots, p^{a-1}F_{a-1}(x)\rangle$. Since $p^iF_i(x) \in C$, for all $0 \leq i \leq a-1$, we have the equality

$$C = \langle F_0(x), pF_1(x), \ldots, p^{a-1}F_{a-1}(x)\rangle.$$

■

As was stated in [33], Theorem 6.5 of [21] does not provide a unique set of generators. Neither does our generalization in Theorem 2.1.10. We now show, as in [33], that there does exist a unique set of generators given some extra constraints. Although this is a generalization of Theorem 2.5 in [33], the proof here only differs from that one in a few details. However, we present the proof in its entirety here for the sake of completeness.

We would like to point out that there is a little inaccuracy in the statement of Theorem 2.5 in [33]. Let $\mathcal{T}_m[u]$ be the set of polynomials in u whose coefficients are in $\mathcal{T}_m$. The $h_{j,\ell}(u)$ in their theorem is said to be an element of $\mathcal{T}_m[u]$ which is not necessarily true. What is true is that $h_{j,\ell}(u)$ is either 0 or a unit and that

$$h_{j,\ell}(u) = \sum_{k=0}^{T_{\ell+j}-1} c_{k,j,\ell}(u-1)^k$$

with $c_{k,j,\ell} \in \mathcal{T}_m$ and $c_{0,j,\ell} \neq 0$. It should also be pointed out that $h_{j,\ell}(u)$ is a unit precisely because $(u-1)$ is nilpotent (which is not stated but fairly easy to show) and $c_{0,j,\ell}$ is a unit.

Theorem 2.1.11 *Let $C \lhd \mathcal{R}$. Then there exist $f_0(x), f_1(x), \ldots, f_{a-1}(x) \in \mathcal{R}$ such that*

$$C = \langle f_0(x), pf_1(x), \ldots, p^{a-1}f_{a-1}(x)\rangle$$

where $f_i(x) = 0$, if $T_i(C) = t$ otherwise

$$f_i(x) = h(x)^{T_i(C)} + \sum_{j=1}^{a-1-i} p^j h(x)^{t_{i,j}} \alpha_{i,j}(x)$$

where $t_{i,j}\deg(h(x)) + \deg(\alpha_{i,j}(x)) < T_{i+j}(C)\deg(h(x))$ and each $\alpha_{i,j}(x) \notin \langle p, h(x)\rangle \setminus \{0\}$.

Furthermore, the set $\{f_0(x), pf_1(x), \ldots, p^{a-1}f_{a-1}(x)\}$ is the unique generating set with these properties.

Proof. Denote $T_i(C)$ by T_i. When $C = 0$, the result holds. Assume $C \neq 0$. By Theorem 2.1.10, $C = \langle F_0(x), pF_1(x), \ldots, p^{a-1}F_{a-1}(x)\rangle$ where $F_i(x) = 0$ when $T_i = t$, otherwise $F_i(x) =$

$h(x)^{T_i} + p\gamma_i(x)$ for some $\gamma_i(x) \in GR(p^a, m)[x]$. The torsional degrees of C form the non-increasing sequence $t \geq T_0 \geq \cdots \geq T_{a-1} \geq 0$. Since $C \neq \{0\}$ there is a least positive integer r such that $t > T_r \geq \cdots \geq T_{a-1} \geq 0$. For $0 \leq i \leq r-1$, $F_i(x) = 0$. Let $f_i(x) = 0$ for $0 \leq i \leq r-1$. For $r \leq i \leq a-1$, $F_i(x) \neq 0$. Since we are considering $p^i F_i(x)$ and $F_i(x)$ can be put in the form as shown in equation (2.1), without loss of generality we can write

$$F_i(x) = h(x)^{T_i} + \sum_{j=1}^{a-1-i} p^j \sum_{k=0}^{t-1} h(x)^k q_{i,j,k}(x)$$

where $q_{i,j,k}(x) = \sum_{l=0}^{\deg h-1} b_{i,j,k,l} x^l$ with $b_{i,j,k,l} \in \mathcal{T}_m$.

Let

$$f_{a-1}(x) = F_{a-1}(x) = h(x)^{T_{a-1}}.$$

Now,

$$\begin{aligned} F_{a-2}(x) &= h(x)^{T_{a-2}} + p\sum_{k=0}^{t-1} h(x)^k q_{a-2,1,k}(x) \\ &= h(x)^{T_{a-2}} \\ &\quad +p\left[\sum_{k=0}^{T_{a-1}-1} h(x)^k q_{a-2,1,k}(x) + h(x)^{T_{a-1}} \sum_{k=T_{a-1}}^{t-1} h(x)^{k-T_{a-1}} q_{a-2,1,k}(x)\right]. \end{aligned}$$

Let

$$\begin{aligned} f_{a-2}(x) &= F_{a-2}(x) - pf_{a-1}(x) \sum_{k=T_{a-1}}^{t-1} h(x)^{k-T_{a-1}} q_{a-2,1,k}(x) \\ &= F_{a-2}(x) - ph(x)^{T_{a-1}} \sum_{k=T_{a-1}}^{t-1} h(x)^{k-T_{a-1}} q_{a-2,1,k}(x) \\ &= h(x)^{T_{a-2}} + p \sum_{k=0}^{T_{a-1}-1} h(x)^k q_{a-2,1,k}(x) \\ &= h(x)^{T_{a-2}} + ph(x)^{t_{a-2,1}} \sum_{k=t_{a-2,1}}^{T_{a-1}-1} h(x)^{k-t_{a-2,1}} q_{a-2,1,k}(x) \end{aligned}$$

where $t_{a-2,1}$ is the smallest k such that $q_{a-2,1,k}(x) \neq 0$ if such a k exists, otherwise $\sum_{k=t_{a-2,1}}^{T_{a-1}-1} h(x)^{k-t_{a-2,a-1}} q_{a-2,1,k}(x) = 0$ and $t_{a-2,1}$ can be arbitrary. It is easy to see that

$$C = \langle F_0(x), pF_1(x), \ldots, p^{a-3}F_{a-3}(x), p^{a-2}f_{a-2}(x), p^{a-1}f_{a-1}(x)\rangle$$

and that $f_{a-2}(x)$ and $f_{a-1}(x)$ satisfy the conditions in the theorem.

We proceed by induction. Assume $f_{i+1}(x), \ldots, f_{a-1}(x)$ satisfy the conditions of the theorem and that

$$C = \langle F_0(x), pF_1(x), \ldots, p^i F_i(x), p^{i+1} f_{i+1}(x), \ldots, p^{a-1} f_{a-1}(x)\rangle.$$

After subtracting appropriate multiples of $p^{i+1}f_{i+1}(x), \ldots, p^{a-1}f_{a-1}(x)$ from $F_i(x)$ we can find an element $f_i(x)$ such that

$$\begin{aligned} f_i(x) &= h(x)^{T_i} + \sum_{j=1}^{a-1-i} p^j \sum_{k=0}^{T_{i+j}-1} h(x)^k g_{i,j,k}(x) \\ &= h(x)^{T_i} + \sum_{j=1}^{a-1-i} p^j h(x)^{t_{i,j}} \sum_{k=t_{i,j}}^{T_{i+j}-1} h(x)^{k-t_{i,j}} g_{i,j,k}(x) \end{aligned}$$

where $g_{i,j,k}(x) = \sum_{l=0}^{\deg h-1} c_{i,j,k,l}x^l$ for some $c_{i,j,k,l} \in \mathcal{T}_m$ and for fixed j, $t_{i,j}$ is the smallest k such that $g_{i,j,k}(x) \neq 0$ if such a k exists, otherwise $\sum_{k=t_{i,j}}^{T_{i+j}-1} h(x)^{k-t_{i,j}} g_{i,j,k}(x) = 0$ and $t_{i,j}$ can be arbitrary. Let $\alpha_{i,j}(x) = \sum_{k=t_{i,j}}^{T_{i+j}-1} h(x)^{k-t_{i,j}} g_{i,j,k}(x)$. If $\alpha_{i,j}(x) \neq 0$, $\alpha_{i,j}(x)$ is a unit since $\alpha_{i,j}(x) \notin \langle p, h(x)\rangle$. It is easy to see that

$$C = \langle F_0(x), pF_1(x), \ldots, p^{i-1}F_{i-1}(x), p^i f_i(x), \ldots, p^{a-1}f_{a-1}(x)\rangle$$

and $f_i(x), \ldots, f_{a-1}(x)$ satisfy the conditions in the theorem. Hence, we have $f_0(x), \ldots, f_{a-1}(x)$ such that

$$C = \langle f_0(x), pf_1(x), \ldots, p^{a-1}f_{a-1}(x)\rangle.$$

Now we show the uniqueness of such a generating set. Assume that $f_0^{'}(x), \cdots, f_{a-1}^{'}(x)$ also satisfy the conditions in the theorem. Say

$$f_i(x) = h(x)^{T_i} + \sum_{j=1}^{a-1-i} p^j \sum_{k=0}^{T_{i+j}-1} h(x)^k g_{i,j,k}(x)$$

and

$$f_i^{'}(x) = h(x)^{T_i} + \sum_{j=1}^{a-1-i} p^j \sum_{k=0}^{T_{i+j}-1} h(x)^k g_{i,j,k}^{'}(x)$$

where $g_{i,j,k}(x), g'_{i,j,k}(x) \in \mathcal{T}_m[x]$ of degree less than $h(x)$. Assume $f_i(x) - f_i^{'}(x) \neq 0$. Then for some j, k, $g_{i,j,k}(x) - g_{i,j,k}^{'}(x) \neq 0$. Let j_0 be the smallest j in the above sum such that $g_{i,j,k}(x) - g_{i,j,k}^{'}(x) \neq 0$. Then

$$p^i(f_i(x) - f_i^{'}(x)) = p^{i+j_0} \sum_{j=j_0}^{a-1-i} p^{j-j_0} \sum_{k=0}^{T_{i+j}-1} h(x)^k (g_{i,j,k}(x) - g_{i,j,k}^{'}(x)).$$

Since the difference of two distinct elements of $\mathcal{T}_m$ is not divisible by p, for all j, k in the above sum, either $g_{i,j,k}(x) - g_{i,j,k}^{'}(x)$ is 0 or not divisible by p. By the assumption on j_0 then, $p^i(f_i(x) - f_i^{'}(x)) \in C \bigcap \langle p^{i+j_0}\rangle \setminus \langle p^{i+j_0+1}\rangle$. Since this is a nonzero element of C with degree less than $T_{i+j_0}\deg(h)$, this contradicts the definition of T_{i+j_0}. Hence $f_i(x) = f_i^{'}(x)$. ■

Now, in Corollary 2.1.13, we show that if we remove the redundant generators in Theorem 2.1.11, then we obtain a result similar to [53, Theorem 4.1]. There they prove it in a slightly different setting namely $GR(p^a, m)$ is replaced by an arbitrary finite chain ring and $f(x)$ is either $x^n - 1$ or $x^n + 1$ (i.e., cyclic and negacyclic codes over a finite chain ring). We will also prove this result later in the case that $f(x)$ is an arbitrary regular polynomial.

Definition 2.1.12 (adapted from [45, Definition 4.1]) *Let* $G = \{p^{j_0} f_{j_0}(x), \ldots, p^{j_r} f_{j_r}(x)\} \subset \mathcal{R}$*, for some* $0 \leq r \leq a-1$*, such that*

1. $0 \leq j_0 < \cdots < j_r \leq a-1$,

2. $t > k_{j_0} > \cdots > k_{j_r} \geq 0$,

3. $f_{j_i}(x) = h(x)^{k_{j_i}} + \sum_{\ell=1}^{a-1-j_i} p^{\ell} h(x)^{t_{j_i,\ell}} \alpha_{j_i,\ell}(x)$ *where* $t_{j_i,\ell} \deg(h(x)) + \deg(\alpha_{j_i,\ell}(x)) < k_{j_i} \deg(h(x))$ *and each* $\alpha_{j_i,\ell}(x) \notin \langle p, h(x) \rangle \setminus \{0\}$,

4. $p^{j_{i+1}} f_{j_i}(x) \in \langle p^{j_{i+1}} f_{j_{i+1}}(x), \ldots, p^{j_r} f_{j_r}(x) \rangle$,

5. $p^{j_0} f(x) \in \langle p^{j_0} f_{j_0}(x), \ldots, p^{j_r} f_{j_r}(x) \rangle$ *in* $GR(p^a, m)[x]$.

The set G is called a generating set in standard form. Moreover, by [43, Theorem 5.4], the set G is a minimal strong Groebner basis.

Corollary 2.1.13 *Let* $C \lhd \mathcal{R}$*. There exists a generating set in standard form for* C*.*

Proof. Let $\{f_0(x), \ldots, p^{a-1} f_{a-1}(x)\}$ be a generating set for C as in Theorem 2.1.11. Let $j_0 = \min\{i | f_i(x) \neq 0\}$ and set $k_i = T_i(C)$. Then

$$C = \langle p^{j_0} f_{j_0}(x), \ldots, p^{a-1} f_{a-1}(x) \rangle.$$

Assume there exist Torsional degrees of C, T_i, T_{i+1}, such that $T_i = T_{i+1}$ for some $i \geq j_0$. It should be clear that $p^{i+1} f_{i+1}(x) \in \langle p^i f_i(x), p^{i+2} f_{i+2}(x), \ldots, p^{a-1} f_{a-1}(x) \rangle$. So after removing these unnecessary generators we have, for some r such that $1 \leq r \leq a-1$,

$$C = \langle p^{j_0} f_{j_0}(x), \ldots, p^{j_r} f_{j_r}(x) \rangle.$$

Then the properties (1)-(4) of Definition 2.1.12 are satisfied.

Now, assume $p^{j_0} f(x) \notin \langle p^{j_0} f_0(x), \ldots, p^{j_r} f_r(x)\rangle$ in $GR(p^a, m)[x]$. We consider

$$\begin{aligned} g_{j_0}(x) &= p^{j_0} f(x) - h(x)^{t-T_{j_0}} p^{j_0} f_{j_0}(x) \\ &= p^{k_0} h(x)^{z_{k_0}} \alpha_{z_{k_0}}(x) + \cdots + p^{k_e} h(x)^{z_{k_e}} \alpha_{z_{k_e}}(x) \qquad (2.3) \end{aligned}$$

where the representation (2.3) is as in (2.1). Note that $g_{j_0}(x) \in C$ when we consider $g_{j_0}(x)$ as an element of $\mathcal{R}$. If $k_0 < j_r$, say $j_{q-1} \leq k_0 < j_q$ for some $q \leq r$, then $z_{k_0} \geq T_{j_{q-1}}$ otherwise we get a contradiction to the torsional degree. Now, for an appropriate polynomial, say $\upsilon(x)$, we get

$$\begin{aligned} g_{j_{q-1}} &= g_{j_0}(x) - \upsilon(x) p^{j_{q-1}} f_{j_{q-1}}(x) \\ &= p^{\ell_0} h(x)^{y_{\ell_0}} \alpha_{y_{\ell_0}}(x) + \cdots + p^{\ell_{e'}} h(x)^{y_{\ell_{e'}}} \alpha_{y_{\ell_{e'}}}(x) \qquad (2.4) \end{aligned}$$

where the representation (2.4) is as in (2.1) and $\ell_0 > k_0$. Continuing like this, we obtain a non-zero polynomial $g(x) \in \langle p^{j_r}\rangle$ such that

$$p^{j_0} f(x) = \sum_{i=0}^{r} p^{j_i} f_i(x) \beta_i(x) + g(x),$$

where $\deg g(x) < \deg f_r(x)$. Now, in $\mathcal{R}$

$$g(x) = -\sum_{i=0}^{r} p^{j_i} f_i(x) \beta_i(x).$$

So, $g(x) \in C$. But, $T_{j_r} \deg h(x) > \deg g(x)$ which is a contradiction to the torsional degree. Hence (5) of Definition 2.1.12 holds. ■

Corollary 2.1.14 *Let $C \lhd \mathcal{R}$. Then C is at most* $\min\{a, t\}$*-generated.*

Proof. Follows from the facts that the number of distinct torsional degrees that are degrees of generators in the generating set in Corollary 2.1.13 is less than t and that the number of generators there does not exceed a. ■

Now we observe a relation between the generating sets introduced in [33, Theorem 2.5] and generating sets in standard form for cyclic codes studied in [43].

Remark 2.1.15 *By [43, Theorem 3.2] and Corollary 2.1.13, a generating set as in Theorem 2.1.11 (and in particular, in [33, Theorem 2.5]) for $C \lhd \mathcal{R}$ is actually a strong Groebner basis (see [46, Definition 3.8] for a definition). Moreover, given a generating set G as in Theorem*

2.1.11, if we remove the redundant elements from G, as described in the proof of Corollary 2.1.13, we obtain a generating set as in Corollary 2.1.13, i.e., a generating set in standard form which is a minimal strong Groebner basis, for C.

Our final result of this section shows that if one can produce a generating set in standard form, the torsional degrees can easily be found.

Theorem 2.1.16 *Let $\{p^{j_0}f_{j_0}(x), \dots, p^{j_r}f_{j_r}(x)\}$ be a generating set in standard form for $C \lhd \mathcal{R}$ where $f_{j_i}(x) = h(x)^{k_{j_i}} + p\beta_{j_i}(x)$ for some $\beta_{j_i}(x) \in \mathcal{R}$. Then for $e < j_0$, $T_e(C) = t$; for $j_i \leq e < j_{i+1}$, $T_e(C) = k_{j_i}$ and for $e \geq j_r$, $T_e(C) = k_{j_r}$.*

Proof. For $e < j_0$, $Tor_e(C) = 0$ so $T_e(C) = t$. Clearly, $T_{j_i}(C) \leq k_{j_i}$ and $T_{j_0}(C) = k_{j_0}$. Now, let $j_i \leq e < j_{i+1}$ for some i. There exists a polynomial $f_e(x) = h(x)^{T_e(C)} + p\rho(x)$ where $\deg(\rho(x)) < \deg(h(x))T_e(C)$ such that $p^e f_e(x) \in C$. In the following we are working in $GR(p^a, m)[x]$. Since $e \geq j_0$, we have

$$p^e f_e(x) \in \langle p^{j_0}f_{j_0}(x), \dots, p^{j_r}f_{j_r}(x), p^{j_0}f(x)\rangle.$$

By 2.1.12(5),

$$p^e f_e(x) \in \langle p^{j_0}f_{j_0}(x), \dots, p^{j_r}f_{j_r}(x)\rangle.$$

We know $T_e(C) \leq k_{j_i}$. Assume $T_e(C) < k_{j_i}$. By the properties in 2.1.12(2) and 2.1.12(3), $\deg f_{j_0}(x) > \cdots > \deg f_{j_i}(x) > \deg f_e(x)$ which implies

$$p^e f_e(x) \in \langle p^{j_{i+1}}f_{j_{i+1}}(x), \dots, p^{j_r}f_{j_r}(x)\rangle.$$

This is a contradiction since by the property 2.1.12(1), $e < j_{i+1} < \cdots < j_r \leq a - 1$ which implies

$$p^e f_e(x) \notin \langle p^{j_{i+1}}f_{j_{i+1}}(x), \dots, p^{j_r}f_{j_r}(x)\rangle.$$

So, $T_e(C) = k_{j_i}$. For $e \geq j_r$, the proof is similar. ■

Remark 2.1.17 *Remark 2.1.15 and Theorem 2.1.16 imply that we can go back and forth between a generating set as in Theorem 2.1.11 and a generating set in standard form. Given a generating set as in Theorem 2.1.11, we can obtain a generating set in standard form as explained in Remark 2.1.15. Conversely, suppose that we are given a generating set $G =$*

$\{p^{j_0}f_{j_0}(x),\ldots,p^{j_r}f_{j_r}(x)\}$ in standard form. We know, by Theorem 2.1.16, that $f_{j_i}(x)=h(x)^{T_{j_i}}+p\beta_{j_i}(x)$. Define $F_e(x)=0$ for $0\le e<j_0$, $F_e(x)=p^ef_{j_i}(x)$ for $j_i\le e<j_{i+1}$ and $F_e(x)=p^{j_r}f_{j_r}(x)$ for $j_r\le e<a$. Then, by Theorem 2.1.16, the set

$$G^{'}=\{F_0(x),pF_1(x),\ldots,p^{a-1}F_{a-1}(x)\}$$

is as in Theorem 2.1.10. Now applying the operations in the proof of Theorem 2.1.11 to $G^{'}$, we obtain a generating set as in Theorem 2.1.11.

2.2 Structure of the Ambient Space: General Case

In this section, we study the structure of the code ambient for polycyclic codes over a Galois ring which is the ring $\frac{GR(p^a,m)[x]}{\langle f(x)\rangle}$ where $f(x)$ is a regular monic polynomial. Throughout this section assume that $f(x)\in GR(p^a,m)[x]$ is regular. By Theorem 1.1.2, $f(x)=\delta(x)f_1(x)\cdots f_s(x)$ where $\delta(x)\in GR(p^a,m)[x]$ is a unit and $\{f_i(x)\in GR(p^a,m)[x]\}_{i=1}^s$ is a set of regular primary co-prime polynomials that are not units. By the fact that $\delta(x)$ is a unit, we may assume without loss of generality that $f_i(x)=h_i(x)^{t_i}+p\beta_i(x)$ where $h_i(x)$ is a monic basic irreducible polynomial such that $\overline{h_i}(x)=h_i(x)$. We know that $t_i\deg h_i(x)>\deg\beta_i(x)$. Since we are interested in $\frac{GR(p^a,m)[x]}{\langle f(x)\rangle}$ and $\langle f(x)\rangle=\langle\delta(x)^{-1}f(x)\rangle$, we assume $\delta(x)=1$, so $f(x)=f_1(x)\cdots f_s(x)$. Additionally, throughout this section let $\mathcal{R}=\frac{GR(p^a,m)[x]}{\langle f(x)\rangle}$ and let $\hat{f_i}(x)=\prod_{j=1,j\neq i}^s f_j(x)$ for $1\le i\le s$.

Theorem 2.2.1 *For $\mathcal{R}$, we have the following*

1. $\mathcal{R}=\bigoplus_{i=1}^s\langle\hat{f_i}(x)+\langle f\rangle\rangle$ *and* $\langle\hat{f_i}(x)+\langle f\rangle\rangle\cong\frac{GR(p^a,m)[x]}{\langle f_i(x)\rangle}$,
2. *Any maximal ideal of $\mathcal{R}$ is of the form* $\langle p\hat{f_i}(x)+f_i(x)+\langle f\rangle,h_i\hat{f_i}(x)+f_i(x)+\langle f\rangle\rangle=\langle p+\langle f\rangle,h_i(x)+\langle f\rangle\rangle$ *for some* $1\le i\le s$,
3. $J(\mathcal{R})=\bigcap_{i=1}^s\langle p+\langle f\rangle,h_i(x)+\langle f\rangle\rangle=\langle p+\langle f\rangle,\prod_{i=1}^s h_i(x)+\langle f\rangle\rangle$,
4. $soc(\mathcal{R})=\bigoplus_{i=1}^s\langle p^{a-1}h_i(x)^{t_i-1}\hat{f_i}(x)+\langle f\rangle\rangle=\langle p^{a-1}\prod_{i=1}^s h_i(x)^{t_i-1}+\langle f\rangle\rangle$.

Proof.

(1) This has been proved above.

(2) Let $\hat{e}_i(x)$ be as above. Define $\mathcal{R}_i = \frac{GR(p^a,m)[x]}{\langle f_i(x)\rangle}$. We showed that $\mathcal{R} = \bigoplus_{i=1}^{s}\langle \hat{f}_i(x) + \langle f\rangle\rangle$ and $\langle \hat{e}_i(x) + \langle f\rangle\rangle = \langle \hat{f}_i(x) + \langle f\rangle\rangle \cong \mathcal{R}_i$. The map

$$\begin{aligned} \phi_i : \mathcal{R}_i &\rightarrow \langle \hat{e}_i\rangle \\ g(x) + \langle f_i\rangle &\mapsto g(x)\hat{e}_i(x) + \langle f\rangle \end{aligned}$$

is a ring isomorphism as $\hat{e}_i(x) + \langle f\rangle$ is idempotent. Therefore the map

$$\begin{aligned} \phi : \bigoplus_{i=1}^{s}\mathcal{R}_i &\rightarrow \mathcal{R} \\ \phi(g_1(x) + \langle f_i\rangle, \ldots, g_s(x) + \langle f_s\rangle) &\mapsto \sum_{i=1}^{s} g_i(x)\hat{e}_i(x) + \langle f\rangle \end{aligned}$$

is also a ring isomorphism. The maximal ideals of $\mathcal{R}$ are $M_1, \ldots, M_s$ and

$$\phi^{-1}(M_i) = \mathcal{R}_1 \oplus \cdots \oplus \mathcal{R}_{i-1} \oplus m_i \oplus \mathcal{R}_{i+1} \oplus \cdots \mathcal{R}_s \tag{2.5}$$

where m_i is the maximal ideal of $\mathcal{R}_i$. By Lemma 2.1.1, we know that $m_i = \langle p+\langle f_i\rangle, h_i(x)+\langle f_i\rangle\rangle$. Using ϕ and (2.5), we see that $M_i = \langle p\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x) + \langle f\rangle, h_i(x)\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x) + \langle f\rangle\rangle$. Since $\hat{e}_i(x)$'s and $\hat{f}_i(x)$'s differ by units, this also implies $M_i = \langle p\hat{f}_i(x) + f_i(x) + \langle f\rangle, h_i\hat{f}_i(x) + f_i(x) + \langle f\rangle\rangle$. By (2.5), we get that $p = p\sum_{i=1}^{s}\hat{e}_i(x), h_i(x) = h_i(x)\sum_{i=1}^{s}\hat{e}_i(x) \in M_i$. So $\langle p, h_i(x)\rangle \subset \langle p\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x), h_i(x)\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x)\rangle$. Since $f_i(x)$ and $\hat{e}_j(x)$ are coprime modulo f for every $i \neq j$, we have $\langle \hat{e}_j(x) + \langle f\rangle\rangle = \langle f_i(x)\hat{e}_j(x) + \langle f\rangle\rangle$. So $\langle f_i(x) + \langle f\rangle\rangle = \langle f_i(x)\sum_{j=1}^{s}\hat{e}_j(x)+\langle f\rangle\rangle = \langle \sum_{i\neq j}\hat{e}_j(x)+\langle f\rangle\rangle$. Since $f_i(x) = h_i(x)^{t_i}+p\beta_i(x) \in \langle p+\langle f\rangle, h_i(x)+\langle f\rangle\rangle$, we get $p\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x) + \langle f\rangle, p\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x) + \langle f\rangle \in \langle p + \langle f\rangle, h_i(x) + \langle f\rangle\rangle$. Hence

$$\langle p + \langle f\rangle, h_i(x) + \langle f\rangle\rangle = \langle p\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x) + \langle f\rangle, h_i(x)\hat{e}_i(x) + \sum_{i\neq j}\hat{e}_j(x) + \langle f\rangle\rangle = M_i.$$

(3) Since $f_i(x)$ and $f_j(x)$ are coprime for every $i \neq j$, the polynomials $h_i(x)$ and $h_j(x)$ are also coprime. So $\bigcap_{i=1}^{s}\langle h_i(x) + \langle f\rangle\rangle = \langle \prod_{i=1}^{s} h_i(x) + \langle f\rangle\rangle$ and the claim follows.

(4) It is not hard to see that $h_j(x)^{t_j-1}$ is a unit in $\mathcal{R}_i$ for all $i \neq j$. As a result of this, $\prod_{i\neq j} h_j(x)^{t_j-1}$ is a unit in $\mathcal{R}_j$. So

$$\begin{aligned}
\bigoplus_{i=1}^{s}\langle p^{a-1}h_i(x)^{t_i-1}\hat{f}_i(x)+\langle f\rangle\rangle &= \bigoplus_{i=1}^{s}\langle p^{a-1}h_i(x)^{t_i-1}\hat{e}_i(x)+\langle f\rangle\rangle \\
&= \bigoplus_{i=1}^{s}\langle p^{a-1}h_i(x)^{t_i-1}\prod_{i\neq j} h_j^{t_j-1}(x)\hat{e}_i(x)+\langle f\rangle\rangle \\
&= \langle p^{a-1}\prod_{i=1}^{s} h_i(x)^{t_i-1}\hat{e}_i(x)+\langle f\rangle\rangle \\
&= \langle p^{a-1}\prod_{i=1}^{s} h_i(x)^{t_i-1}\hat{f}_i(x)+\langle f\rangle\rangle.
\end{aligned}$$

■

Theorem 2.2.2 *The following are equivalent:*

1. *$\mathcal{R}$ is not a principal ideal ring.*

2. *$a > 1$ and there exists a factor from a primary co-prime factorization of $f(x)$, $g(x)$, where $g(x) = h(x)^t + p\beta(x)$ and $h(x)$ is basic irreducible, $t > 1$ and $\beta(x) \in \langle p, h(x)\rangle$.*

3. *$a > 1$, $\bar{f}(x)$ is not square free and if $\bar{f}'(x)$ is the square free part of $\bar{f}(x)$, and we write $f(x) = f'(x)\alpha(x) + p\gamma(x)$ then $\bar{\gamma}(x) = 0$ or $\bar{\alpha}(x)$ and $\bar{\gamma}(x)$ are not co-prime.*

Proof. (1) $\Longleftrightarrow$ (2) By Theorem 1.1.2, there exists a primary coprime decomposition of $g(x)$. Then the result follows from Theorems 2.2.1 and 2.1.4.

(2)$\Rightarrow$(3) Since $t > 1$, $\bar{f}(x)$ is not square free. This also shows $h(x)|\bar{f}'(x)$ and $h(x)|\bar{\alpha}(x)$. Since $\beta(x) \in \langle p, h(x)\rangle$, we have $\bar{\beta}(x) \in \langle h\rangle$. This implies $h(x)|(g(x) \pmod{p^2})$. Since $g(x)|f(x)$, we see that $h(x)|\bar{\gamma}(x)$. So, $\bar{\alpha}(x)$ and $\bar{\gamma}(x)$ are not co-prime.

(3)$\Rightarrow$(2) Since $\bar{f}(x)$ is not square free and $\bar{\alpha}(x)$ and $\bar{\gamma}(x)$ are not co-prime there exists a basic irreducible polynomial $h(x)$ such that $h(x)^t|\bar{f}(x)$ for some $t > 1$ and $h(x)|\bar{\gamma}(x)$. So there exists a factor $g(x)$ of $f(x)$ such that $g(x) = h(x)^t + p\beta(x)$ for some $\beta(x)$. Since $h(x)|\bar{\gamma}(x)$, we have that $h(x)|\bar{\beta}(x)$. Hence, $\beta(x) \in \langle p, h(x)\rangle$. ■

Remark 2.2.3 *The equivalence in Theorem 2.2.2 of (1) and (3) was presented in [53] with an alternative proof.*

Lemma 2.2.4 *Let R be a ring with direct sum decomposition $R = \oplus_{i=1}^{n} R_i$ and I_i be and ideal of R_i for $1 \leq i \leq n$. Assume, for any positive integer i, that $I_i \lhd R_i$ is at most k-generated. Let $I = \oplus_{i=1}^{n} I_i$. Then $I \lhd R$ is at most k-generated.*

Proof. Let $I \lhd R$. Then $I = \oplus_{i=1}^{n} I_i$ for $I_i \in R_i$. Then I_i is generated by some $f_{i1}, \ldots, f_{ik} \in R_i$. Let $g_j = f_{1j} + \cdots + f_{nj}$ for $1 \leq j \leq k$. Then $\langle f_{1j}, \ldots, f_{nj} \rangle = \langle g_j \rangle$ and hence $I = \langle g_1, \ldots, g_k \rangle$. ■

Now we generalize Proposition 2.1.13 to the case where $f(x)$ is an arbitrary regular polynomial.

Theorem 2.2.5 *Let $C \lhd \mathcal{R}$. Then*

$$C = \langle p^{j_0} g_0(x), \ldots, p^{j_r} g_r(x) \rangle$$

where $0 \leq r \leq a-1$ and

1. $0 \leq j_0 < \cdots < j_r \leq a-1$
2. $g_i(x)$ *monic for* $i = 0, \ldots, r$,
3. $\deg f(x) > \deg g_0(x) > \cdots > \deg g_r(x)$,
4. $p^{j_{i+1}} g_i(x) \in \langle p^{j_{i+1}} g_{i+1}(x), \ldots, p^{j_r} g_r(x) \rangle$
5. $p^{j_0} f(x) \in \langle p^{j_0} g_0(x), \ldots, p^{j_r} g_r(x) \rangle$ *in* $GR(p^a, m)[x]$.

Proof. Follows from Proposition 2.1.13, Theorem 2.2.1 and Lemma 2.2.4. ■

The structure of the ambient space of cyclic codes over finite chain rings was studied in [44], [46], [45] and [53]. For any ideal of the ambient space, the authors of those papers came up with a special generating set called *strong Groebner basis (SGB)*. They showed that SGB can be used to determine the Hamming distance of the corresponding code. It is easy to see that their results also hold for the ideals of $\mathcal{R}$. So we have the following result.

Theorem 2.2.6 *Let $C \lhd \mathcal{R}$ where $C = \langle p^{j_0} g_{j_0}(x), \ldots, p^{j_r} g_{j_r}(x) \rangle$ is as in Theorem 2.2.5. Then $d_H(C) = d_H(\langle p^{a-1} g_{j_r}(x) \rangle) = d_H(\overline{\langle g_{j_r}(x) \rangle})$.*

Proof. For $v(x) \in C$, if $p^k v(x) \neq 0$ then $w_H(v(x)) \geq w_H(p^k v(x))$. Let $c(x) \in C$ such that $d_H(I) = w_H(c(x))$. Let ℓ be the largest integer such that $p^\ell c(x) \neq 0$. Hence, $p^\ell c(x) \in C \bigcap \langle p^{a-1} \rangle = \langle p^{a-1} g_{j_r} \rangle$. Also $w_H(c(x)) = w_H(p^k c(x))$ by the minimality of $c(x)$. Hence, $d_H(\langle p^{a-1} g_{j_r}(x) \rangle) = w_H(pc(x)) = d_H(C)$. The equality $d_H(\langle p^{a-1} g_{j_r}(x) \rangle) = d_H(\overline{\langle g_{j_r}(x) \rangle})$ follows from Lemma 1.2.1. ■

2.3 Structure and the Hamming Distance in Characteristic p^2

In Section 2.1 and Section 2.2, we study polycyclic codes over a Galois ring of characteristic p^a where a can be any positive integer. In this section, we observe that our results can be refined if we work in characteristic p^2. This leads to a generalization of the results given in [31] where the authors study cyclic codes over $GR(4, 1)$. As a result of this, we determine the structure and the Hamming distance of the cyclic codes of length p^s over $GR(p^2, m)$

Throughout this section, we work in characteristic p^2 and we assume $f(x) \in GR(p^2, m)[x]$ is a regular primary polynomial and let $\mathcal{R}_2 = \frac{GR(p^2,m)[x]}{\langle f(x) \rangle}$.

Recently, the Hamming distance of cyclic codes of length 2^s over $GR(4, 1)$ has been determined in [31]. Applying the results of Section 2.1, we extend this result in two ways. First, we consider the problem for a more general class of linear codes which are called polycyclic codes. We show how to obtain the torsional degrees of polycyclic codes over a Galois ring of characteristic p^2. This gives us the Hamming distance if the Hamming distance of the residue code is known. Second, we generalize this result of [31] to cyclic codes of length p^s over any Galois ring of characteristic p^2. We explicitly determine the Hamming distance of all cyclic codes of length p^s over $GR(p^2, n)$.

First, in Lemma 2.3.1, we classify all polycyclic codes in characteristic p^s where $f(x)$ is a regular primary polynomial. This also gives us a classification of all cyclic codes of length p^s. Then, in Lemma 2.3.2 and Lemma 2.3.3, we determine the torsional degrees of polycyclic codes. Using this together with some observations on the polynomial $x^{p^s} - 1$, we determine the Hamming distance of all cyclic codes of length p^s in characteristic p^2 in Lemma 2.3.8.

As was explained in Section 2.1, without loss of generality, we can assume that $f(x)$ is monic, $f(x) = h(x)^t + p\beta(x)$ where $\beta(x) \in GR(p^2, m)[x]$ and either $\beta(x) = 0$ or $\deg \beta(x) < t \deg h(x)$.

Also, we may assume $h(x)$ is a monic basic irreducible polynomial. Moreover, if $\beta(x) \neq 0$ we can express $\beta(x)$ as $\beta(x) = h(x)^v \beta'(x)$ such that $\beta'(x) = \sum_{j=0}^{t-1-v} \gamma_j(x) h^j(x)$ where $v < t$, $\gamma_0(x) \neq 0$,$\gamma_0(x) \notin \langle p \rangle$, $\gamma_j(x) \in GR(p^2, m)[x]$ and $\deg(\gamma_j(x)) < \deg(h(x))$ (see the explanation in Section 2.1). Since we are working in characteristic p^2 we may also assume that $\gamma_j(x) \in \mathcal{T}_m[x]$. This can be seen by noting that $p\gamma_j(x) = p\overline{\gamma_j}(x)$.

Assume $C \lhd \mathcal{R}_2$. Since C is finite we have that $C = \langle f_1(x), \ldots, f_n(x) \rangle$ for $f_i(x) \in \mathcal{R}_2$ where $\deg(f_i(x)) < \deg(f(x))$, i.e. C is finitely generated. Without loss of generality we can assume that if $p \nmid f_i(x)$ then $f_i(x)$ is monic and if $p | f_i(x)$ that the leading coefficient of $f_i(x)$ is p. We consider two cases here, when $C \not\subseteq \langle p \rangle$ and $C \subseteq \langle p \rangle$. First assume $C \not\subseteq \langle p \rangle$. In this case, it can be shown by looking at the representation (2.1) that if $p \nmid f_i(x)$ then $f_i(x) = h(x)^{k_i} + ph(x)^{\ell_i} \delta_i(x)$ and that if $p | f_i(x)$, $f_i(x) = ph(x)^{\ell_i} \delta_i(x)$, where $\delta_i(x)$ is a unit with $\ell_i \deg(h(x)) + \deg(\delta_i(x)) < k_i \deg(h(x))$ where at least one generator is not divisible by p. Let $k_i = \infty$ if not defined. Let j be such that $k_j = min\{k_i\}_{i=1}^n$. Let $g_i(x) = f_i(x) - f_j(x) h(x)^{k_i - k_j}$ if $p \nmid f_i(x)$ and $g_i(x) = f_i(x)$ if $p | f_i(x)$. Now, we see that $C = \langle g_1(x), \ldots, g_{j-1}(x), f_j(x), g_{j+1}(x), \ldots, g_n(x) \rangle$. Notice $g_i(x) \in \mathcal{R}_2 \cap \langle p \rangle$ for $i \neq j$. Again, without loss of generality we may assume for $i \neq j$ that $g_i(x) = ph(x)^{\ell'_i}$. Let j' be such that $\ell_{j'} = min\{\ell'_i\}_{i=1}^n$. So, $g_i(x) - g_{j'}(x) h(x)^{\ell'_i - \ell'_j} = 0$. Hence, $C = \langle f_j(x), g_{j'}(x) \rangle$. Finally, if $k_j \leq \ell_{j'}$ then $f_j(x) | g_{j'}(x)$ and $C = \langle f_j(x) \rangle$. Now, assume $C \subseteq \langle p \rangle$. Then $f_i(x) = ph(x)^{\ell_i} \delta_i(x)$ is a unit. Without loss of generality, we can assume that $f_i(x) = ph(x)^{\ell_i}$. As above let j be such that $\ell_j = min\{\ell_i\}_{i=1}^n$. So, $f_i(x) - f_j(x) h(x)^{\ell_k - \ell_j} = 0$. Hence, $C = \langle f_j(x) \rangle$. From this discussion we get the following lemma.

Lemma 2.3.1 *Let $C \lhd \mathcal{R}_2$. Then C can be expressed in one of the following forms.*

1. $\langle 0 \rangle$,

2. $\langle 1 \rangle$,

3. $\langle ph(x)^n \rangle$,

4. $\langle h(x)^k \rangle$,

5. $\langle h(x)^k + ph(x)^\ell \delta(x) \rangle$,

6. $\langle h(x)^k, ph(x)^n \rangle$,

7. $\langle h(x)^k + ph(x)^\ell \delta(x), ph(x)^n \rangle$

where in any case $k, \ell, n < t$, $\ell < n < k$ and $\delta(x) = \sum_{j=0}^{k-1-\ell} \eta_j(x)h(x)^j$, where $\eta_j(x) \in \mathcal{T}_m[x]$, $\eta_0(x) \neq 0$ and $\deg(\eta_j(x)) < \deg(h(x))$.

Proof. The only thing that needs justification is the fact that $\delta(x) = \sum_{j=0}^{k-1-\ell} \eta_j(x)h(x)^j$ where $\eta_j(x) \in \mathcal{T}_m[x]$, $\eta_0(x) \neq 0$ and $\deg(\eta_j(x)) < \deg(h(x))$. By the discussion before this lemma, $\delta(x)$ is a unit so, $\delta(x) \notin \langle p, h(x)\rangle$. By the discussion in Section 2.1, $\delta(x) = \sum_{j=0}^{k-1-\ell} \eta_j(x)h(x)^j$ where $\eta_j(x) \in GR(p^2, m)[x]$, $\eta_0(x) \neq 0$ and $\deg(\eta_j(x)) < \deg(h(x))$. Finally, $\eta_j(x) \in \mathcal{T}_m[x]$ since we are working in characteristic p^2 which means $p\eta_j(x) = p\overline{\eta_j}(x)$. ■

The results of Section 2.1 assume the torsional degrees of a code are known. The next three lemmas will focus on finding the torsional degrees of a code so we can apply the results of Section 2.1 with the ultimate goal of this section being the determination of the Hamming distance of a code. For the following, recall form the beginning of this section that $t, v, h(x), \beta(x), \beta'(x), \gamma_j(x)$ are parameters of $f(x)$.

Lemma 2.3.2 *Let $C \lhd \mathcal{R}_2$ and $n < t$. If $C = \langle ph(x)^n\rangle$ then $T_0(C) = t$ and $T_1(C) = n$.*

Proof. The result on $T_0(C)$ is obvious. Since every codeword is divisible by p and $h(x)^n$, clearly $T_1(C) = n$. ■

Lemma 2.3.3 *Assume $\beta(x) = 0$. Let $C \lhd \mathcal{R}_2$, $k, \ell, n < t$, $n < k$, $\delta(x) \notin \langle p, h(x)\rangle$ and* $\deg(\delta(x)) < (k - \ell)\deg(h(x))$.

1. *If $C = \langle h(x)^k\rangle$ then $T_0(C) = k$ and $T_1(C) = k$.*
2. *If $C = \langle h(x)^k + ph(x)^\ell\delta(x)\rangle$ then $T_0(C) = k$ and* $T_1(C) = \min(k, t - k + \ell)$.
3. *If $C = \langle h(x)^k, ph(x)^n\rangle$ then $T_0(C) = k$ and* $T_1(C) = \min(k, n)$.
4. *If $C = \langle h(x)^k + ph(x)^\ell\delta(x), ph(x)^n\rangle$ then $T_0(C) = k$ and* $T_1(C) = \min(k, t - k + \ell, n)$.

Proof. The results on $T_0(C)$ are obvious. We concentrate on $T_1(C)$.

(1) The only way to create a codeword divisible by p is to multiply the generator by p or by a large enough power of $h(x)$. Since $h(x)^t = f(x) = 0$ in $\mathcal{R}_2$, $h(x)^k h(x)^{t-k} = h(x)^t = f(x) = 0$.

Multiplying by any smaller multiple of $h(x)$ will not produce a polynomial divisible by p. Hence any codeword divisible by p is divisible by $ph(x)^k$ and so $T_1(C) = k$.

(2) Noting that $(h(x)^k + ph(x)^\ell\delta(x))h(x)^{t-k} = h(x)^t + ph(x)^{t-k+\ell}\delta(x) = ph(x)^{t-k+\ell}\delta(x)$ and $p\left(h(x)^k + ph(x)^\ell\delta(x)\right) = p(h(x))^k$ we see that $T_1(C) = \min(k, t-k+\ell)$ following similar arguments as in (1).

(3) This can be argued similar to (1).

(4) This can be argued similar to (2). ■

Lemma 2.3.4 *Assume $\beta(x) \neq 0$. Let $C \lhd \mathcal{R}_2$, $k, \ell, n < t$, $n < k$ and $\delta(x) = \sum_{j=0}^{k-1-\ell} \eta_j(x)h(x)^j$, where $\eta_j(x) \in \mathcal{T}_m[x]$, $\eta_0(x) \neq 0$ and $\deg(\eta_j(x)) < \deg(h(x))$.*

1. *If $C = \langle h(x)^k \rangle$ then $T_0(C) = k$ and $T_1(C) = \min(k, v)$.*

2. *If $C = \langle h(x)^k + ph(x)^\ell\delta(x) \rangle$ then $T_0(C) = k$ and*

$$T_1(C) = \begin{cases} \min(k, v, t-k+\ell), & \text{if } v \neq t-k+\ell \\ \min(k, v+z), & \text{if } v = t-k+\ell \end{cases}$$

   where $z = \min\left(\{j|\gamma_j(x) \neq \eta_j(x)\} \cup \{t\}\right)$.

3. *If $C = \langle h(x)^k, ph(x)^n \rangle$ then $T_0(C) = k$ and $T_1(C) = \min(k, v, n)$.*

4. *If $C = \langle h(x)^k + ph(x)^\ell\delta(x), ph(x)^n \rangle$ then $T_0(C) = k$ and*

$$T_1(C) = \begin{cases} \min(k, v, t-k+\ell, n), & \text{if } v \neq t-k+\ell \\ \min(k, v+z, n), & \text{if } v = t-k+\ell \end{cases}$$

   where $z = \min\left(\{j|\gamma_j(x) \neq \eta_j(x)\} \cup \{t\}\right)$.

Proof. The results on $T_0(C)$ are obvious. We concentrate on $T_1(C)$.

(1) The only way to create a codeword divisible by p is to multiply the generator by p or by a large enough power of $h(x)$. Now, $h(x)^{t-k}h(x)^k = h(x)^t = -ph(x)^v\beta'(x)$. We know $\beta'(x)$ is a unit since $\gamma_0(x) \neq 0$ so, $T_1(C) = \min(k, v)$.

(2) First,

$$\begin{aligned} h(x)^{t-k}\left(h(x)^k + ph(x)^\ell\delta(x)\right) &= h(x)^t + ph(x)^{t-k+\ell}\delta(x) \\ &= -ph(x)^v\beta'(x) + ph(x)^{t-k+\ell}\delta(x). \end{aligned}$$

If $v < t - k + \ell$ then

$$\begin{aligned} & -ph(x)^v\beta'(x) + ph(x)^{t-k+\ell}\delta(x) \\ = \quad & -ph(x)^v\left(\gamma_0(x) + \sum_{j=1}^{t-1-v}\gamma_j(x)h^j(x) - h(x)^{t-k+\ell-v}\sum_{j=0}^{k-1-\ell}\eta_j(x)h(x)^j\right). \end{aligned}$$

In this case $T_1(C) = \min(k, v)$. If $v > t - k + \ell$ then

$$\begin{aligned} & -ph(x)^v\beta'(x) + ph(x)^{t-k+\ell}\delta(x) \\ = \quad & ph(x)^{t-k+\ell}\left(\eta_0(x) + \sum_{j=1}^{k-1-\ell}\eta_j(x)h(x)^j - h(x)^{v-(t-k+\ell)}\sum_{j=0}^{t-1-v}\gamma_j(x)h^j(x)\right). \end{aligned}$$

In this case $T_1(C) = \min(k, t-k+\ell)$. Next, consider the case $v = t - k + \ell$. Here, if $\beta'(x) = \delta(x)$ then $-ph(x)^v\beta'(x) + ph(x)^{t-k+\ell}\delta(x) = 0$ so $T_1(C) = k$. Finally, if $\beta'(x) \neq \delta(x)$ then for some $0 \leq j' < t, \gamma_{j'}(x) \neq \eta_{j'}(x)$. Since $\gamma_j(x), \eta_j(x) \in \mathcal{T}_m[x]$ we have that $\gamma_z(x) - \eta_z(x)$ is not divisible by p and is therefore a unit. Then

$$\begin{aligned} & -ph(x)^v\beta'(x) + ph(x)^{t-k+\ell}\delta(x) \\ = \quad & -ph(x)^{v+z}\left(\gamma_z(x) - \eta_z(x) + \sum_{j=z+1}^{t-1-v}\gamma_j(x)h^{j-z}(x) - \sum_{j=z+1}^{k-1-\ell}\eta_j(x)h^{j-z}(x)\right). \end{aligned}$$

Since $z \leq t - 1 - v$, in this final case, $T_1(C) = \min(k, v + z)$.

(3) This can be argued similar to (1).

(4) This can be argued similar to (2). ■

Now that the torsional degrees of any code can be computed, the techniques in Section 2.1 can be applied to produce a generating set as in Theorem 2.1.11 or Definition 2.1.12. Our goal here is to show how the hamming distance can be computed. Notice in Section 2.1 that ultimately $T_{a-1}(C)$ will determine the Hamming distance of C, i.e., $d_H(C) = d_H\left(\langle h(x)^{T_1(C)}\rangle\right)$.

In the remaining part of this section, we study cyclic codes of length p^s over $GR(p^2, m)$ and show how to determine their Hamming distances. To do so we apply the results from the beginning of this section. The following two lemmas are immediate consequences of Kummer's Theorem (see [23] for the statement) which we will need for our calculations.

Lemma 2.3.5 *Let $k < p^e$ and let ℓ be the largest integer such that $p^\ell | k$. Then $p^{e-\ell} | \binom{p^e}{k}$.*

Lemma 2.3.6 *Let $0 < i < p$. We have $\binom{p^s}{ip^{s-1}} = pu \in GR(p^2, m)$, where $p \nmid u$.*

To apply the results of this section, we need to show that the ambient ring is of the correct type. To do so, we only need to show that an appropriate polynomial is used for the generator of the ideal being factored out . For cyclic codes of length p^s, this polynomial is $x^{p^s} - 1$ of course. We now show why this is an appropriate polynomial. By Lemma 2.3.5 and Lemma 2.3.6 and the fact that we are working in $GR(p^2, m)$,

$$\begin{aligned} x^{p^s} - 1 &= ((x-1)+1)^{p^s} - 1 \\ &= (x-1)^{p^s} + \binom{p^s}{p^s - 1}(x-1)^{p^s - 1} + \cdots + \binom{p^s}{1}(x-1) \\ &= (x-1)^{p^s} + \binom{p^s}{(p-1)p^{s-1}}(x-1)^{(p-1)p^{s-1}} + \cdots + \binom{p^s}{p^{s-1}}(x-1)^{p^{s-1}} \\ &= (x-1)^{p^s} + p(x-1)^{p^{s-1}} \sum_{i=0}^{p-2} \frac{\binom{p^s}{(i+1)p^{s-1}}}{p}(x-1)^{ip^{s-1}} \end{aligned}$$

We want to show that we can express $x^{p^s} - 1$ in the form needed to use the results form this section. Let $t = p^s$, $v = p^{s-1}$, $h(x) = x - 1$ and $\beta'(x) = \sum_{i=0}^{p-2} \gamma_{ip^{s-1}}(x-1)^{ip^{s-1}}$ where $\gamma_{ip^{s-1}} = \frac{\binom{p^s}{(i+1)p^{s-1}}}{p} \pmod{p}$ for $0 \leq i < p-1$ and $\gamma_j = 0$ for all other j. Note, $\gamma_j \in \mathcal{T}_m$. This shows that $x^{p^s} - 1$ is the type of polynomial we need.

The following is a special case of Lemma 2.3.1.

Lemma 2.3.7 *Let $C \lhd \frac{GR(p^2,m)[x]}{\langle x^{p^s} - 1 \rangle}$. Then C can be expressed in one of the following forms.*

1. $\langle 0 \rangle$,

2. $\langle 1 \rangle$,

3. $\langle p(x-1)^n \rangle$,

4. $\langle (x-1)^k \rangle$,

5. $\langle (x-1)^k + p(x-1)^\ell \delta(x) \rangle$,

6. $\langle (x-1)^k, p(x-1)^n \rangle$,

7. $\langle (x-1)^k + p(x-1)^\ell \delta(x), p(x-1)^n \rangle$,

where in any case $k, \ell, n < p^s$, $n < k$ *and* $\delta(x) = \sum_{j=0}^{k-1-\ell} \eta_j (x-1)^j$, *where* $\eta_j \in \mathcal{T}_m$ *and* $\eta_0 \neq 0$.

Now, restating Lemma 2.3.2 and Lemma 2.3.4 for cyclic codes of length p^s and using the fact that $d_H(C) = d_H(\overline{\langle (x-1)^{T_1(C)} \rangle})$, we determine the Hamming distance of all cyclic codes of length p^s over $GR(p^2, m)$ in the following lemma. Note that $\overline{\langle (x-1)^{T_1(C)} \rangle}$ is a cyclic code of length p^s over $\mathbb{F}_{p^m}$ and its Hamming distance is given in Theorem 3.2.6.

Lemma 2.3.8 *Let* $C \lhd \frac{GR(p^2,m)[x]}{\langle x^{p^s}-1 \rangle}$, $k, \ell, n < p^s$, $n < k$ *and* $\delta(x) = \sum_{j=0}^{k-1-\ell} \eta_j (x-1)^j$, *where* $\eta_j \in \mathcal{T}_m$ *and* $\eta_0 \neq 0$. *Then* $d_H(C) = d_H(\overline{\langle (x-1)^{T_1(C)} \rangle})$ *where* $T_0(C)$ *and* $T_1(C)$ *are as follows.*

1. *If* $C = \langle (x-1)^k \rangle$ *then* $T_0(C) = k$ *and* $T_1(C) = \min(k, p^{s-1})$.

2. *If* $C = \langle (x-1)^k + p(x-1)^\ell \delta(x) \rangle$ *then* $T_0(C) = k$ *and*

$$T_1(C) = \begin{cases} \min(k, p^{s-1}, p^s - k + \ell), & \text{if } p^{s-1} \neq p^s - k + \ell \\ \min(k, p^{s-1} + z), & \text{if } p^{s-1} = p^s - k + \ell \end{cases}$$

where $z = \min\Big(\{j | \gamma_j \neq \eta_j\} \cup \{p^s\}\Big)$.

3. *If* $C = \langle (x-1)^k, p(x-1)^n \rangle$ *then* $T_0(C) = k$ *and* $T_1(C) = \min(k, p^{s-1}, n)$.

4. *If* $C = \langle (x-1)^k + p(x-1)^\ell \delta(x), p(x-1)^n \rangle$ *then* $T_0(C) = k$ *and*

$$T_1(C) = \begin{cases} \min(k, p^{s-1}, p^s - k + \ell, n), & \text{if } p^{s-1} \neq p^s - k + \ell \\ \min(k, p^{s-1} + z, n), & \text{if } p^{s-1} = p^s - k + \ell \end{cases}$$

where $z = \min\Big(\{j | \gamma_j \neq \eta_j\} \cup \{p^s\}\Big)$.

5. *If* $C = \langle p(x-1)^n \rangle$ *then* $T_0(C) = p^s$ *and* $T_1(C) = n$.

CHAPTER 3

Repeated-Root Constacyclic Codes

We apply our results in Chapter 2 to study repeated-root constacyclic codes over Galois rings. First, we develop some computational tools to determine the Hamming distance in Section 3.1. Next, we study constacyclic codes of length np^s over the Galois ring $GR(p^a, m)$ in Section 3.2. We determine their ideal structure and compute their Hamming distance. Then, in Section 3.3, we study constacyclic codes of length $2np^s$ over $GR(p^a, m)$.

3.1 On the Hamming Weight of $(x^n + \gamma)^N$

We develop some tools, that we use in Section 3.2 and Section 3.3, to compute the Hamming distance of some constacyclic codes over finite fields.

We begin with partitioning the set $\{1, 2, \ldots, p^s - 1\}$ into three subsets. These subsets arise naturally from the technicalities of our computations as described in Section 3.2 and Section 3.3. If i is an integer satisfying $1 \leq i \leq (p-1)p^{s-1}$, then there exists a uniquely determined integer β such that $0 \leq \beta \leq p - 2$ and

$$\beta p^{s-1} + 1 \leq i \leq (\beta + 1)p^{s-1}.$$

Moreover since

$$p^s - p^{s-1} < p^s - p^{s-2} < \cdots < p^s - p^{s-s} = p^s - 1,$$

for an integer i satisfying $(p-1)p^{s-1} + 1 = p^s - p^{s-1} + 1 \leq i \leq p^s - 1$, there exists a uniquely determined integer k such that $1 \leq k \leq s - 1$ and

$$p^s - p^{s-k} + 1 \leq i \leq p^s - p^{s-k-1}. \tag{3.1}$$

Besides if i is an integer as above and k is the integer satisfying $1 \leq k \leq s-1$ and (3.1), then we have

$$\begin{aligned} &p^s - p^{s-k} < p^s - p^{s-k} + p^{s-k-1} < p^s - p^{s-k} + 2p^{s-k-1} < \cdots \\ &< p^s - p^{s-k} + (p-1)p^{s-k-1} \end{aligned}$$

and $p^s - p^{s-k} + (p-1)p^{s-k-1} = p^s - p^{s-k-1}$. So for such integers i and k, there exists a uniquely determined integer τ with $1 \leq \tau \leq p-1$ such that

$$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}.$$

Thus

$$\begin{aligned} &\{1, 2, \ldots, p^{s-1}\} \sqcup \bigsqcup_{\beta=1}^{p-2} \{i : \quad \beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1}\} \\ &\sqcup \bigsqcup_{k=1}^{s-1} \bigsqcup_{\tau=1}^{p-1} \{i : \quad p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}\} \end{aligned} \tag{3.2}$$

gives us a partition of the set $\{1, 2, \ldots, p^s - 1\}$.

Throughout this section q denotes a power of p. Let N be a positive integer and $\gamma \in \mathbb{F}_q \setminus \{0\}$. Our computations in Section 3.2 and Section 3.3 are based on expressing the Hamming weight of an arbitrary nonzero codeword in terms of $w_H((x^\eta + \gamma)^N)$. In [39], the Hamming weight of the polynomial $(x^\eta + \gamma)^N$ is given as described below. Let e, η, N and $0 \leq b_0, b_1, \ldots, b_{e-1} \leq p-1$ be positive integers such that $N < p^e$ and let $\gamma \in \mathbb{F}_q \backslash \{0\}$. Let $N = b_{e-1}p^{e-1} + \cdots + b_1 p + b_0$, $0 \leq b_i < p$, be the p-adic expansion of N. Then, by [39, Lemma 1], we have

$$w_H((x+\gamma)^N) = \prod_{d=0}^{e-1} (b_d + 1). \tag{3.3}$$

As suggested in [39], identifying x with x^η in (3.3), we obtain

$$w_H((x^\eta+\gamma)^N) = \prod_{d=0}^{e-1} (b_d + 1). \tag{3.4}$$

The following two lemmas are consequences of (3.4) and we will use them in our computations frequently.

Lemma 3.1.1 *Let $m, \eta, 1 \leq \beta \leq p-2$ be positive integers and $\gamma \in \mathbb{F}_q \backslash \{0\}$. If $m < p^s - \beta p^{s-1} - 1$, then $w_H((x^\eta + \gamma)^{m+\beta p^{s-1}+1}) \geq \beta + 2$.*

Proof. Since

$$m < p^s - \beta p^{s-1} - 1 = (p-\beta-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p + p - 1,$$

either

$$\begin{aligned} m &= Lp^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p + p - 1 \quad \text{or} \\ m &= a_{s-1}p^{s-1} + \cdots + a_1 p + a_0 \end{aligned}$$

holds, where $0 \leq L \leq p - \beta - 2$, $0 \leq a_0, a_1, \ldots, a_{s-2} \leq p - 1$ and $0 \leq a_{s-1} \leq p - \beta - 1$ are integers such that $a_\ell < p - 1$ for some $0 \leq \ell < s - 1$. According to the p-adic expansion of m, we consider the following two cases.

First, we assume that $m = Lp^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p + p - 1$. Then $m + \beta p^{s-1} + 1 = (L + \beta + 1)p^{s-1}$. So using (3.4), we get $w_H((x^\eta + \gamma)^{m+\beta p^{s-1}+1}) = L + \beta + 2 \geq \beta + 2$.

Second, we assume that $m = a_{s-1}p^{s-1} + \cdots + a_1 p + a_0$. Then the p-adic expansion of $m + \beta p^{s-1} + 1$ is of the form $m + \beta p^{s-1} + 1 = b_{s-1}p^{s-1} + \cdots + b_1 p + b_0$ where $0 \leq b_0, b_1, \ldots, b_{s-2} \leq p - 1$ and

$$b_{s-1} = a_{s-1} + \beta. \tag{3.5}$$

Let k be the least nonnegative integer with $a_k < p - 1$. Then it follows that

$$0 < b_k \leq p - 1. \tag{3.6}$$

So, using (3.4), (3.5) and (3.6), we get

$$w_H((x^\eta + \gamma)^{m+\beta p^{s-1}+1}) \geq (\beta + a_{s-1} + 1)(b_k + 1) \geq (\beta + 1)2 > \beta + 2.$$

■

Lemma 3.1.2 *Let $m, \eta, 1 \leq \tau \leq p - 1, 1 \leq k \leq s - 1$ be positive integers and $\gamma \in \mathbb{F}_q \setminus \{0\}$. If $m < p^{s-k} - (\tau - 1)p^{s-k-1} - 1$, then $w_H((x^{2\eta} + \gamma)^{m+p^s-p^{s-k}+(\tau-1)p^{s-k-1}+1}) \geq (\tau + 1)p^k$.*

Proof. Since

$$\begin{aligned} m &< p^{s-k} - (\tau - 1)p^{s-k-1} - 1 \\ &= (p - \tau + 1)p^{s-k-1} - 1 \\ &= (p - \tau)p^{s-k-1} + (p-1)p^{s-k-2} + \cdots + (p-1)p + p - 1, \end{aligned}$$

either

$$\begin{aligned} m &= Lp^{s-k-1} + (p-1)p^{s-k-2} + \cdots + (p-1)p + p - 1 \quad \text{or} \\ m &= a_{s-k-1}p^{s-k-1} + \cdots + a_1 p + a_0 \end{aligned}$$

holds, where $0 \leq L \leq p - \tau - 1$, $0 \leq a_0, a_1, \ldots, a_{s-k-2} \leq p - 1$ and $0 \leq a_{s-k-1} \leq p - \tau$ are some integers such that $0 \leq a_\ell < p - 1$ for some $0 \leq \ell < s - k - 1$. According to the p-adic expansion of m, we consider the following two cases.

First, we assume that $m = Lp^{s-k-1} + (p-1)p^{s-k-2} + \cdots + (p-1)p + p - 1$. Then the p-adic expansion of $m + p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1$ is of the form

$$m + p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 = (p-1)p^{s-1} + \cdots + (p-1)p^{s-k} + (L + \tau)p^{s-k-1}.$$

So, using (3.4), we get $w_H((x^\eta + \gamma)^{m+p^s-p^{s-k}+(\tau-1)p^{s-k-1}+1}) \geq (\tau + 1)p^k$.

Second, we assume that $m = a_{s-k-1}p^{s-k-1} + \cdots + a_1 p + a_0$. Then the p-adic expansion of $m + p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1$ is of the form

$$\begin{aligned} m + p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 &= (p-1)p^{s-1} + \cdots + (p-1)p^{s-k} \\ &\quad + b_{s-k-1}p^{s-k-1} + \cdots + b_1 p + b_0 \end{aligned}$$

where $0 \leq b_0, b_1, \ldots, b_{s-k-1} \leq p - 1$ are integers. It is easy to see that

$$b_{s-k-1} = a_{s-k-1} + \tau - 1. \tag{3.7}$$

Let ℓ_0 be the least nonnegative integer with $0 \leq a_{\ell_0} < p - 1$. Then

$$0 < b_{\ell_0} \leq p - 1. \tag{3.8}$$

Using (3.7), (3.8) and (3.4), we get

$$\begin{aligned} w_H((x^\eta + \gamma)^{m+p^s-p^{s-k}(\tau-1)p^{s-k-1}+1}) &\geq p^k(b_{s-k-1} + 1)(b_{\ell_0} + 1) \\ &\geq 2\tau p^k \\ &\geq (\tau + 1)p^k. \end{aligned}$$

■

In [39], the authors have shown that the polynomial $(x^\eta + \gamma)^N$ has the so-called *"weight retaining property"* (see [39, Theorem 1.1]). As a result of this, they gave a lower bound for the Hamming weight of the polynomial $g(x)(x^\eta+\gamma)^N$ where $g(x)$ is any element of $\mathbb{F}_q[x]$. Let η, N, γ and $g(x)$ be as above. Then, by [39, Theorem 1.3 and Theorem 6.3], the Hamming weight of $g(x)(x^\eta + \gamma)^N$ satisfies

$$w_H(g(x)(x^\eta+\gamma)^N) \geq w_H(g(x) \pmod{x^\eta+\gamma}) \cdot w_H((x^\eta+\gamma)^N). \tag{3.9}$$

Now we examine the Hamming weight of the polynomials $(x^\eta+\gamma_1)^{p^s}(x^\eta+\gamma_2)^i$, over $\mathbb{F}_q[x]$, where $0 < i < p^s$. Let $0 < i < p^s$ be an integer and $\gamma_1, \gamma_2 \in \mathbb{F}_q \setminus \{0\}$. Let

$$(x^\eta+\gamma_2)^i = a_i x^{\eta i} + a_{i-1}x^{\eta(i-1)} + \cdots + a_0\gamma_2^i$$

where $a_0, a_1, \ldots, a_i$ are the binomial coefficients. Note that

$$\begin{aligned}(x^\eta+\gamma_1)^{p^s}(x^\eta+\gamma_2)^i &= (x^{\eta p^s}+\gamma_1^{p^s})(a_i x^{\eta i} + a_{i-1}x^{\eta(i-1)}\gamma_2 + \cdots + a_0\gamma_2^i) \\ &= a_i x^{\eta(i+p^s)} + a_{i-1}x^{\eta(i-1+p^s)}\gamma_2 + \cdots + a_0 x^{\eta p^s}\gamma_2^i \\ &\quad + a_i\gamma_1^{p^s}x^{\eta i} + a_{i-1}\gamma_1^{p^s}x^{\eta(i-1)} + \cdots + a_0\gamma_1^{p^s}\gamma_2^i.\end{aligned}$$

Therefore $w_H((x^\eta+\gamma_1)^{p^s}(x^\eta+\gamma_2)^i) = 2w_H((x^\eta+\gamma_2)^i)$.

3.2 Constacyclic Codes of Length np^s

Let η and s be positive integers. Let $\gamma, \lambda \in \mathbb{F}_{p^m} \setminus \{0\}$ such that $\gamma^{p^s} = -\lambda$. All λ-cyclic codes, of length ηp^s, over $\mathbb{F}_{p^m}$ correspond to the ideals of the finite ring

$$\mathcal{R} = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{\eta p^s} - \lambda\rangle}.$$

Suppose that $x^\eta+\gamma$ is irreducible over $\mathbb{F}_{p^m}$. Then the monic divisors of $x^{\eta p^s}-\lambda = (x^\eta+\gamma)^{p^s}$ are exactly the elements of the set $\{(x^\eta+\gamma)^i : \quad 0 \leq i \leq p^s\}$. So if $x^\eta+\lambda$ is irreducible over $\mathbb{F}_{p^m}$, then the λ-cyclic codes, of length ηp^s, over $\mathbb{F}_{p^m}$, are of the form $\langle (x^\eta+\gamma)^i\rangle$ where $0 \leq i \leq p^s$. In this section, we determine the Hamming distance of all λ-cyclic codes of length ηp^s over $\mathbb{F}_{p^m}$ and $GR(p^a, m)$. In Theorem 3.2.6, we determine the Hamming distance of $\langle (x^\eta+\gamma)^i\rangle$. As a particular case, we obtain the Hamming distance of negacyclic codes of length $2p^s$ over $\mathbb{F}_{p^m}$ where x^2+1 is irreducible over $\mathbb{F}_{p^m}[x]$. Using Theorem 3.2.6 together with the results of Section 2.1 and Section 2.2, we determine the Hamming distance of a cyclic code of length p^s over $GR(p^a, m)$.

Let $C = \langle (x^\eta+\gamma)^i \rangle$ where $0 \le i \le p^s$ is an integer and $x^\eta+\gamma \in \mathbb{F}_{p^m}[x]$ is irreducible. Obviously if $i = 0$, then $C = \mathcal{R}$, i.e., C is the whole space $\mathbb{F}_{p^m}^{\eta p^s}$, and if $i = p^s$, then $C = \{0\}$. For the remaining values of i, we consider the partition of the set $\{1, 2, \ldots, p^s - 1\}$ given in (3.2).

If $0 < i \le p^{s-1}$, then $d_H(C)$ is 2 as shown in Lemma 3.2.1.

For $p^{s-1} < i < p^s$, we first find a lower bound on the Hamming weight of an arbitrary nonzero codeword of C in Lemma 3.2.2 and Lemma 3.2.4. Next in Corollary 3.2.3 and Corollary 3.2.5, we show that there exist codewords in C, achieving these previously found lower bounds. This gives us the Hamming distance of C.

We summarize our results on $\mathcal{R}$ in Theorem 3.2.6. We observe that Theorem 3.2.6 gives the Hamming distance of negacyclic codes, of length $2p^s$, over $\mathbb{F}_{p^m}$ where $p \equiv 3 \pmod 4$ and m is an odd number. We close this section by describing how to determine the Hamming distance of certain polycyclic codes, and in particular constacyclic codes, of length ηp^s over $GR(p^a, m)$.

Lemma 3.2.1 *Let $1 \le i \le p^{s-1}$ be an integer and let $C = \langle (x^\eta + \gamma)^i \rangle$. Then $d_H(C) = 2$.*

Proof. The claim follows from Lemma 1.2.1 and the fact that

$$(x^\eta + \gamma)^{p^{s-1}-i}(x^\eta + \gamma)^i = (x^\eta + \gamma)^{p^{s-1}} = x^{\eta p^{s-1}} + \gamma^{p^{s-1}} \in C.$$

■

Let $C = \langle (x^\eta + \gamma)^i \rangle$ for some integer $0 < i < p^s$. For any $0 \ne c(x) \in C$, there exists $0 \ne f(x) \in \mathbb{F}_q[x]$ such that $c(x) \equiv f(x)(x^\eta+\gamma)^i \left(\bmod\ (x^\eta + \gamma)^{p^s}\right)$. Dividing $f(x)$ by $(x^\eta+\gamma)^{p^s-i}$, we get $f(x) = q(x)(x^\eta + \gamma)^{p^s-i} + r(x)$, where $q(x), r(x) \in \mathbb{F}_q[x]$ and $0 \le \deg(r(x)) < \eta p^s - \eta i$ or $r(x) = 0$. We observe that

$$\begin{aligned} c(x) &\equiv f(x)(x^\eta + \gamma)^i \\ &\equiv (q(x)(x^\eta + \gamma)^{p^s-i} + r(x))(x^\eta + \gamma)^i \\ &\equiv q(x)(x^\eta + \gamma)^{p^s} + r(x)(x^\eta + \gamma)^i \\ &\equiv r(x)(x^\eta + \gamma)^i \left(\bmod\ (x^\eta + \gamma)^{p^s}\right). \end{aligned}$$

Consequently, for any $0 \ne c(x) \in C$, there exists $0 \ne r(x) \in \mathbb{F}_{p^m}[x]$ with $\deg(r(x)) < \eta p^s - \eta i$ such that $c(x) = r(x)(x^\eta + \gamma)^i$, where we consider this equality in $\mathbb{F}_{p^m}[x]$. Therefore the

Hamming weight of $c \in C$ is equal to the nonzero coefficients of $r(x)(x^\eta + \gamma)^i \in \mathbb{F}_q[x]$, i.e., $w_H(c) = w_H(r(x)(x^\eta + \gamma)^i)$.

In the following lemma, we give a lower bound on $d_H(C)$ when $p^{s-1} < i$.

Lemma 3.2.2 *Let $1 \leq \beta \leq p-2$ be an integer and let $C = \langle (x^\eta + \gamma)^{\beta p^{s-1}+1} \rangle$. Then $d_H(C) \geq \beta + 2$.*

Proof. Let $0 \neq c(x) \in C$, then there exists $0 \neq f(x) \in \mathbb{F}_q[x]$ such that

$$c(x) \equiv f(x)(x^\eta + \gamma)^{\beta p^{s-1}+1} \left(\text{mod } (x^\eta + \gamma)^{p^s}\right).$$

We may assume that $\deg(f(x)) < \eta p^s - \eta\beta p^{s-1} - \eta = (p-\beta)\eta p^{s-1} - \eta$. We choose m to be the largest nonnegative integer with $(x^\eta + \gamma)^m | f(x)$. Clearly $\deg(f(x)) < (p-\beta)\eta p^{s-1} - \eta$ implies $m < (p-\beta)p^{s-1} - 1$. So, by Lemma 3.1.1, we get

$$w_H((x^\eta + \gamma)^{m+\beta p^{s-1}+1}) \geq \beta + 2. \tag{3.10}$$

For $f(x) = g(x)(x^\eta + \gamma)^m$, we have $g(x) \pmod{x^\eta + \gamma} \neq 0$ by our choice of m, so

$$w_H(g(x) \pmod{(x^\eta + \gamma)}) > 0. \tag{3.11}$$

Now using (3.10), (3.11) and (3.9), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H(g(x)(x^\eta + \gamma)^{m+\beta p^{s-1}+1}) \\ &\geq w_H(g(x) \pmod{(x^\eta + \gamma)}) w_H((x^\eta + \gamma)^m) \\ &\geq \beta + 2. \end{aligned}$$

■

Next we show that the lower bound given in Lemma 3.2.2 is achieved when $p^{s-1} < i \leq (p-1)p^{s-1}$ and this gives us the exact value of $d_H(C)$.

Corollary 3.2.3 *Let $1 \leq \beta \leq p-2$, $\beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1}$ be integers and let $C = \langle (x^\eta + \gamma)^i \rangle$. Then $d_H(C) = \beta + 2$.*

Proof. Lemma 3.2.2 and $C \subset \langle (x^\eta + \gamma)^{\beta p^{s-1}+1} \rangle$ imply $d_H(C) \geq \beta + 2$. We know, by (3.4), that $w_H((x^\eta + \gamma)^{(\beta+1)p^{s-1}}) = \beta + 2$. Clearly $(x^\eta + \gamma)^{(\beta+1)p^{s-1}} \in C$ as $(\beta+1)p^{s-1} \geq i$. Thus $d_H(C) \leq \beta + 2$. Hence $d_H(C) = \beta + 2$.

■

Having covered the range $p^{s-1} < i \leq (p-1)p^{s-1}$, now we give a lower bound on $d_H(C)$ when $(p-1)p^{s-1} < i < p^s$ in the following lemma.

Lemma 3.2.4 *Let $1 \leq \tau \leq p-1$, $1 \leq k \leq s-1$ be integers and let $C = \langle (x^\eta + \gamma)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} \rangle$. Then $d_H(C) \geq (\tau+1)p^k$.*

Proof. Let $0 \neq c(x) \in C$, then there is $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ such that

$$c(x) \equiv f(x)(x^\eta + \gamma)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} \left(\text{mod } (x^\eta + \gamma)^{p^s}\right).$$

We may assume that

$$\deg(f(x)) < \eta p^{s-k} - \eta(\tau-1)p^{s-k-1} - \eta. \tag{3.12}$$

Let m be the largest nonnegative integer with $(x^\eta + \gamma)^m | f(x)$. Then there exists $g(x) \in \mathbb{F}_{p^m}[x]$ such that $f(x) = g(x)(x^\eta + \gamma)^m$. By (3.12), we have $m < p^{s-k} - (\tau-1)p^{s-k-1} - 1$. So, by Lemma 3.1.2, we get

$$w_H((x^\eta + \gamma)^{m + p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}) \geq p^k(\tau+1). \tag{3.13}$$

The maximality of m implies $x^\eta + \gamma \nmid g(x)$ and therefore $g(x) \pmod{x^\eta + \gamma} \neq 0$. So we have

$$w_H(g(x) \pmod{(x^\eta + \gamma)}) > 0. \tag{3.14}$$

Now using (3.9), (3.13) and (3.14), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H(g(x)(x^\eta + \gamma)^{m + p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}) \\ &\geq w_H(g(x) \pmod{(x^\eta + \gamma)}) w_H((x^\eta + \gamma)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1+m}) \\ &\geq p^k(\tau+1). \end{aligned}$$

This completes the proof. ■

For $(p-1)p^{s-1} < i < p^s$, we determine $d_H(C)$ in Corollary 3.2.5 where we show the existence of a codeword that achieves the lower bound given in Lemma 3.2.4.

Corollary 3.2.5 *Let $1 \leq \tau \leq p-1$, $1 \leq k \leq s-1$ and i be integers such that*

$$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}.$$

Let $C = \langle (x^\eta + \gamma)^i \rangle$. Then $d_H(C) = (\tau+1)p^k$.

Proof. Lemma 3.2.4 and $C \subset \langle (x^{\eta} + \gamma)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} \rangle$ implies $d_H(C) \geq (\tau + 1)p^k$. We know, by (3.4), that $w_H((x^{\eta} + \gamma)^{p^s - p^{s-k} + \tau p^{s-k-1}}) = (\tau + 1)p^k$. Clearly $(x^{\eta} + \gamma)^{p^s - p^{s-k} + \tau p^{s-k-1}} \in C$ as $p^s - p^{s-k} + \tau p^{s-k-1} \geq i$. So $d_H(C) \leq (\tau + 1)p^k$. Thus we have shown $d_H(C) = (\tau + 1)p^k$. ■

We summarize our results in the following theorem.

Theorem 3.2.6 *Let p be a prime number, $\mathbb{F}_{p^m}$ a finite field of characteristic p, $\gamma \in \mathbb{F}_q \setminus \{0\}$ and η be a positive integer. Suppose that $x^{\eta} + \gamma \in \mathbb{F}_q[x]$ is irreducible. Then the λ-cyclic codes over $\mathbb{F}_q$, of length ηp^s, are of the form $C[i] = \langle (x^{\eta} + \gamma)^i \rangle$, where $0 \leq i \leq p^s$ and $\lambda = -\gamma^{p^s}$. If $i = 0$, then C is the whole space $\mathbb{F}_{p^m}^{\eta p^s}$ and if $i = p^s$, then C is the zero space $\{\mathbf{0}\}$. For the remaining values of i, if $p = 2$, then*

$$d_H(C[i]) = \begin{cases} 1, & \text{if } \ i = 0, \\ 2, & \text{if } \ 1 \leq i \leq 2^{s-1}, \\ 2^{k+1}, & \text{if } \ 2^s - 2^{s-k} + 1 \leq i \leq 2^s - 2^{s-k} + \tau 2^{s-k-1}, \\ & \text{where } \ 1 \leq k \leq s-1, \end{cases}$$

if p is odd, then

$$d_H(C[i]) = \begin{cases} 2, & \text{if } \ 1 \leq i \leq p^{s-1}, \\ \beta + 2, & \text{if } \ \beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1}, \text{ where } \ 1 \leq \beta \leq p-2, \\ (\tau+1)p^k, & \text{if } \ p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}, \\ & \text{where } \ 1 \leq \tau \leq p-1 \ \text{ and } \ 1 \leq k \leq s-1. \end{cases}$$

Remark 3.2.7 *If we replace η with 1 and γ with -1 in Theorem 3.2.6, then we obtain the main results of [16] and [47]. Namely, we obtain [16, Theorem 4.11] and [47, Theorem 3.4].*

Theorem 3.2.6 is still useful when the polynomial $x^{\eta} + \gamma$ is reducible over the alphabet $\mathbb{F}_{p^m}$.

Remark 3.2.8 *Note that $\langle (x^{\eta} + \gamma)^i \rangle$, $0 \leq i \leq p^s$ are ideals of $\mathcal{R}$ independent of the fact that $x^{\eta} + \gamma$ is irreducible. So our results from Lemma 3.2.1 to Corollary 3.2.5 hold even when the polynomial $x^{\eta} + \gamma$ is reducible over $\mathbb{F}_{p^m}$. But then, the cases considered above do not cover all the λ-cyclic codes of length p^s. In other words, if $x^{\eta} + \gamma$ is reducible, then there are λ-cyclic codes other than $\langle (x^{\eta} + \gamma)^i \rangle$, $0 \leq i \leq p^s$ and their Hamming distance is not determined here.*

Now we will apply Theorem 3.2.6 to a particular case. Namely, we will consider the negacyclic codes over $\mathbb{F}_{p^m}$ of length $2p^s$ where p is an odd prime. In order to apply Theorem 3.2.6, the polynomial x^2+1 must be irreducible over $\mathbb{F}_{p^m}$. A complete irreducibility criterion for x^2+1 is given in the following lemma.

Lemma 3.2.9 *Let p be an odd prime and m be a positive integer. The polynomial $x^2+1 \in \mathbb{F}_{p^m}[x]$ is irreducible if and only if $p = 4k+3$ for some $k \in \mathbb{N}$ and m is odd.*

Proof. Follows from the order of the multiplicative group of $\mathbb{F}_{p^m}$. ■

Let C be a negacyclic code of length $2p^s$ over $\mathbb{F}_{p^m}$. If x^2+1 is irreducible over $\mathbb{F}_{p^m}$, then the Hamming distance of C is given in the following theorem.

Theorem 3.2.10 *Let $p = 4k+3$ be a prime for some $k \in \mathbb{N}$ and let $m \in \mathbb{N}$ be an odd number. Then the negacyclic codes over $\mathbb{F}_{p^m}$, of length $2p^s$, are of the form $C[i] = \langle (x^2+1)^i \rangle$, where $0 \leq i \leq p^s$, and*

$$d_H(C[i]) = \begin{cases} 2, & \text{if } 1 \leq i \leq p^{s-1}, \\ \beta+2, & \text{if } \beta p^{s-1}+1 \leq i \leq (\beta+1)p^{s-1}, \text{ where } 1 \leq \beta \leq p-2, \\ (\tau+1)p^k, & \text{if } p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}, \\ & \text{where } 1 \leq \tau \leq p-1 \text{ and } 1 \leq k \leq s-1. \end{cases}$$

For the other values of p and m, x^2+1 is reducible over $\mathbb{F}_{p^m}$ and in this case, we determine the minimum Hamming distance of C in Section 3.3.

Now we describe how to determine the Hamming distance of certain polycyclic codes of length ηp^s over $GR(p^a, m)$ and, in particular, this gives us the Hamming distance of certain constacyclic codes of length ηp^s. Let $\gamma_0, \lambda_0 \in GR(p^a, m)$ be units such that $\overline{\gamma}_0 = \gamma$, $\overline{\lambda}_0 = \lambda$ and $\gamma_0^{p^s} = -\lambda_0$. According to our assumption in the beginning of this section, we have that $x^\eta + \overline{\gamma}_0$ is irreducible.

Let $f(x) = (x^\eta + \gamma_0)^{p^s} + p\beta(x) \in GR(p^a, m)[x]$ with $\deg(\beta(x)) < \eta p^s$. Note that $f(x)$ in this form is a primary regular polynomial so the techniques of Section 2.1 can be applied.

Let $\mathcal{R}_0 = \frac{GR(p^a,m)[x]}{\langle f(x) \rangle}$. Let $C = \langle p^{j_0} g_0(x), \ldots, p^{j_r} g_r(x) \rangle \lhd \mathcal{R}_0$ where the generators are as in Theorem 2.2.5. As was done in (2.1), we can express $g_r(x)$ in the canonical form

$$g_r(x) = p^0 (x^\eta + \gamma_0)^{e_0} \alpha_0(x) + \cdots + p^{a-1} (x^\eta + \gamma_0)^{e_{a-1}} \alpha_{a-1}(x)$$

where each $\alpha_i(x)$ is either a unit or 0. For $0 \neq g_r(x)$, we have $\alpha_0(x) \neq 0$ since $p \nmid g_r(x)$. Therefore $\alpha_0(x)$ is a unit. So, by Theorem 2.2.6, we deduce that $d_H(C) = d_H(\overline{\langle g_r(x) \rangle}) = d_H(\overline{\langle (x^\eta + \gamma)^{e_0} \rangle})$. Now $d_H(\overline{\langle (x^\eta + \gamma)^{e_0} \rangle})$ can be determined using Theorem 3.2.6.

Remark 3.2.11 *Let $\gamma, \gamma_0, \lambda, \lambda_0$ be as above. The λ_0-cyclic codes of length ηp^s over $GR(p^a, m)$ are the ideals of the ring $\frac{GR(p^a,m)[x]}{\langle x^{\eta p^s} - \lambda_0 \rangle}$. Since $x^{\eta p^s} - \lambda_0 = (x^\eta + \gamma_0)^{p^s} + p\beta'(x)$, for some $\beta(x) \in GR(p^a, m)[x]$ with $\deg(\beta'(x)) < \eta p^s$, we can determine the Hamming distance of the λ_0-cyclic codes of length ηp^s over $GR(p^a, m)$ as described above.*

3.3 Constacyclic Codes of Length $2np^s$

We assume that p is an odd prime number, η and s are positive integers, $\mathbb{F}_{p^m}$ is a finite field of characteristic p and $\lambda, \xi, \psi \in \mathbb{F}_{p^m} \setminus \{0\}$ throughout this section.

Suppose that $\psi^{p^s} = \lambda$ and $x^{2\eta} - \psi$ factors into two irreducible polynomials over $\mathbb{F}_{p^m}$ as

$$x^{2\eta} - \psi = (x^\eta - \xi)(x^\eta + \xi). \tag{3.15}$$

In this section, we compute the Hamming distance of λ-cyclic codes, of length $2\eta p^s$, over $\mathbb{F}_{p^m}$ where (3.15) is satisfied. Next, we determine the Hamming distance of certain polycyclic codes, and in particular certain constacyclic codes, of length ηp^s over $GR(p^a, m)$. We know that λ-cyclic codes of length $2\eta p^s$ over $\mathbb{F}_{p^m}$ correspond to the ideals of the finite ring

$$\mathcal{R} = \frac{\mathbb{F}_{p^m}[x]}{\langle x^{2\eta p^s} - \lambda \rangle}.$$

Note that, by Proposition 2.2.1, we have $\mathcal{R} = \langle x^{\eta p^s} + \xi^{p^s} \rangle \oplus \langle x^{\eta p^s} - \xi^{p^s} \rangle$ and $\langle x^{\eta p^s} + \xi^{p^s} \rangle \cong \frac{\mathbb{F}_{p^m}[x]}{\langle x^{\eta p^s} - \xi^{p^s} \rangle}$, $\langle x^{\eta p^s} - \xi^{p^s} \rangle \cong \frac{\mathbb{F}_{p^m}[x]}{\langle x^{\eta p^s} + \xi^{p^s} \rangle}$. Moreover, by Proposition 2.2.1, the maximal ideals of $\mathcal{R}$ are $\langle x^\eta - \xi \rangle$ and $\langle x^\eta + \xi \rangle$. Since the monic polynomials dividing $x^{2\eta p^s} - \lambda$ are exactly the elements of the set $\{(x^\eta - \xi)^i (x^\eta + \xi)^j : \quad 0 \leq i, j \leq p^s\}$, the λ-cyclic codes, of length $2\eta p^s$, over $\mathbb{F}_{p^m}$ are of the form $\langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$, where $0 \leq i, j \leq p^s$ are integers.

Let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. If $(i, j) = (0, 0)$, then $C = \mathcal{R}$. If $(i, j) = (p^s, p^s)$, then $C = \{0\}$. For the remaining values of (i, j), we consider the partition of the set $\{1, 2, \ldots, p^s - 1\}$ given in (3.2).

In order to simplify and improve the presentation of our results, from Lemma 3.3.4 till Corollary 3.3.21, we consider only the cases where $i \geq j$ explicitly. We do so because the cases where $j > i$ can be treated similarly as the corresponding case of $i > j$.

Now we give an overview of the results in this section. If $i = 0$, or $j = 0$, or $0 \leq i, j \leq p^{s-1}$, then the Hamming distance of C can easily found to be 2 as shown in Lemma 3.3.1 and Lemma 3.3.2.

If $0 < j \leq p^{s-1}$ and $p^{s-1} + 1 \leq i \leq p^s$, then $d_H(C)$ is computed in Lemma 3.3.4, Corollary 3.3.5, Lemma 3.3.6 and Corollary 3.3.7.

If $p^{s-1} + 1 \leq j \leq i \leq (p-1)p^{s-1}$, then $d_H(C)$ is computed in Lemma 3.3.8 and Corollary 3.3.9.

If $p^{s-1} + 1 \leq j \leq (p-1)p^{s-1} < i \leq p^s - 1$, then $d_H(C)$ is computed in Lemma 3.3.10 and Corollary 3.3.11.

If $(p-1)p^{s-1} + 1 \leq j \leq i \leq p^s - 1$, then $d_H(C)$ is computed in Lemma 3.3.12, Corollary 3.3.13, Lemma 3.3.14 and Corollary 3.3.15.

Finally if $i = p^s$ and $0 < j < p^s - 1$, then $d_H(C)$ is computed from Lemma 3.3.16 till Corollary 3.3.21.

At the end of this section, we summarize our results in Theorem 3.3.22.

We begin our computations with the case where $i = 0$ or $j = 0$.

Lemma 3.3.1 *Let* $0 < i, j \leq p^s$ *be integers, let* $C = \langle (x^\eta - \xi)^i \rangle$ *and* $D = \langle (x^\eta + \xi)^j \rangle$. *Then* $d_H(C) = d_H(D) = 2$.

Proof. Since

$$\begin{aligned} (x^\eta - \xi)^{p^s - i}(x^\eta - \xi)^i &= x^{\eta p^s} - \xi^{p^s} \in C \quad \text{and} \\ (x^\eta + \xi)^{p^s - j}(x^\eta + \xi)^j &= x^{\eta p^s} + \xi^{p^s} \in D, \end{aligned}$$

we have $d_H(C), d_H(D) \leq 2$. On the other hand, $d_H(C), d_H(D) \geq 2$ by Lemma 1.2.1. Hence $d_H(C) = d_H(D) = 2$. ■

Lemma 3.3.2 *Let* $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$, *for some integers* $0 \leq i, j \leq p^{s-1}$ *with* $(i, j) \neq (0, 0)$. *Then* $d_H(C) = 2$.

Proof. By Lemma 1.2.1, we have $d_H(C) \geq 2$ and

$$(x^\eta - \xi)^i (x^\eta + \xi)^j (x^\eta - \xi)^{p^{s-1}-i} (x^\eta + \xi)^{p^{s-1}-j} = x^{2\eta p^{s-1}} - \xi^{2p^{s-1}} \in C$$

implies that $d_H(C) \leq 2$. Hence $d_H(C) = 2$. ■

Let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$ for some integers $0 \leq i, j \leq p^s$ with $(0,0) \neq (i, j) \neq (p^s, p^s)$. Let $0 \neq c(x) \in C$, then there exists $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ such that $c(x) \equiv f(x)(x^\eta - \xi)^i (x^\eta + \xi)^j \left(\bmod x^{2\eta p^s} - \lambda\right)$. Dividing $f(x)$ by $(x^\eta - \xi)^{p^s-i}(x^\eta + \xi)^{p^s-j}$, we get

$$f(x) = q(x)(x^\eta - \xi)^{p^s-i}(x^\eta + \xi)^{p^s-j} + r(x),$$

where $q(x), r(x) \in \mathbb{F}_q[x]$ and, either $r(x) = 0$ or $\deg(r(x)) < 2\eta p^s - \eta i - \eta j$. Since

$$\begin{aligned} c(x) &\equiv f(x)(x^\eta - \xi)^i (x^\eta + \xi)^j \\ &\equiv (q(x)(x^\eta - \xi)^{p^s-i}(x^\eta + \xi)^{p^s-j} + r(x))(x^\eta - \xi)^i (x^\eta + \xi)^j \\ &\equiv q(x)(x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^s} + r(x)(x^\eta - \xi)^i (x^\eta + \xi)^j \\ &\equiv r(x)(x^\eta - \xi)^i (x^\eta + \xi)^j \left(\bmod (x^{2\eta p^s} - \lambda)\right), \end{aligned}$$

we may assume, without loss of generality, that $\deg(f(x)) < 2\eta p^s - \eta i - \eta j$. Moreover $w_H(r(x)(x^\eta - \xi)^i (x^\eta + \xi)^j) = w_H(c)$ as $\deg(r(x)(x^\eta - \xi)^i (x^\eta + \xi)^j) < 2\eta p^s$.

Let i_0 and j_0 be the largest integers with $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Then there exists $g(x) \in \mathbb{F}_{p^m}[x]$ such that $f(x) = (x^\eta - \xi)^{i_0}(x^\eta + \xi)^{j_0} g(x)$ and $(x^\eta - \xi) \nmid g(x)$, $(x^\eta + \xi) \nmid g(x)$. Clearly $\deg(f(x)) < 2\eta p^s - \eta i - \eta j$ implies $i_0 + j_0 < 2p^s - i - j$. Therefore $i_0 < p^s - i$ or $j_0 < p^s - j$ must hold.

So if $i_0 \geq p^s - i$, then $j_0 < p^s - j$. For such cases, the following lemma will be used in our computations.

Lemma 3.3.3 *Let i, j, i_0, j_0 be nonnegative integers such that $i \geq j$, $i_0 \geq p^s - i$ and $j_0 < p^s - j$. Let $c(x) = (x^\eta - \xi)^{i_0+i}(x^\eta + \xi)^{j_0+j} g(x)$ with $x^\eta - \xi \nmid g(x)$ and $x^\eta + \xi \nmid g(x)$. Then $w_H(c(x)) \geq 2w_H((x^{2\eta} - \xi^2)^{j_0+j})$.*

Proof. Since $i_0 \geq p^s - i$ and $-j_0 \geq -p^s + j + 1$, we have $i_0 - j_0 \geq j - i + 1$ or equivalently $i_0 - j_0 + i - j \geq 1$. So $c(x) = (x^{2\eta} - \xi^2)^{j_0+j}(x^\eta - \xi)^{i_0-j_0+i-j} g(x)$. Dividing $(x^\eta - \xi)^{i_0-j_0+i-j} g(x)$ by $x^{2\eta} - \xi^2$, we get

$$(x^\eta - \xi)^{i_0-j_0+i-j} g(x) = (x^{2\eta} - \xi^2) q(x) + r(x) \tag{3.16}$$

for some $q(x), r(x) \in \mathbb{F}_q[x]$ with $r(x) = 0$ or $\deg(r(x)) < 2\eta$. Let θ_1 and θ_2 be any roots of $x^\eta - \xi$ and $x^\eta + \xi$, respectively, in some extension of $\mathbb{F}_{p^m}$. Obviously θ_1 and θ_2 are roots of $(x^{2\eta} - \xi^2)q(x)$. First we observe that $r(\theta_1) = 0$ as θ_1 is a root of LHS of (3.16). Second we observe that $r(\theta_2) \neq 0$ as θ_2 is not a root of LHS of (3.16). So it follows that $r(x)$ is a nonzero and nonconstant polynomial implying $w_H(r(x)) \geq 2$. Therefore

$$w_H((x^\eta - \xi)^{i_0-j_0+i-j}g(x) \left(\text{mod } (x^{2\eta} - \xi^2)\right)) = w_H(r(x)) \geq 2. \tag{3.17}$$

Using (3.9) and (3.17), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H((x^{2\eta} - \xi^2)^{j_0+j}(x^\eta - \xi)^{i_0-j_0+i-j}g(x)) \\ &\geq w_H((x^{2\eta} - \xi^2)^{j_0+j})w_H((x^\eta - \xi)^{i_0-j_0+i-j}g(x) \left(\text{mod } (x^{2\eta} - \xi^2)\right)) \\ &\geq 2w_H((x^{2\eta} - \xi^2)^{j_0+j}). \end{aligned}$$

■

Now we have the machinery to obtain the Hamming distance of C for the ranges $p^{s-1} < i \leq p^s$ and $0 < j \leq p^s$.

In what follows, for a particular range of i and j, we first give a lower bound on $d_H(C)$ in the related lemma. Then in the next corollary, we determine $d_H(C)$ by showing the existence of a codeword that achieves the previously found lower bound.

We compute $d_H(C)$ when $0 < j \leq p^{s-1} < i \leq 2p^{s-1}$ in the following lemma and corollary.

Lemma 3.3.4 *Let $C = \langle (x^\eta - \xi)^{p^{s-1}+1}(x^\eta + \xi)\rangle$. Then $d_H(C) \geq 3$.*

Proof. Pick $0 \neq c(x) \in C$ where $c(x) \equiv f(x)(x^\eta - \xi)^{p^{s-1}+1}(x^\eta + \xi) \left(\text{mod } (x^{2\eta p^s} - \lambda)\right)$ for some $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ with $\deg(f(x)) < 2\eta p^s - \eta p^{s-1} - 2\eta$. Let i_0 and j_0 be the largest integers with $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Then $f(x)$ is of the form $f(x) = (x^\eta - \xi)^{i_0}(x^\eta + \xi)^{j_0}g(x)$ for some $g(x) \in \mathbb{F}_{p^m}[x]$ with $x^\eta - \xi \nmid g(x)$ and $x^\eta + \xi \nmid g(x)$. Note that $i_0 < p^s - p^{s-1} - 1$ or $j_0 < p^s - 1$ holds.

If $i_0 < p^s - p^{s-1} - 1$, then, by Lemma 3.1.1,

$$w_H((x^\eta - \xi)^{i_0+p^{s-1}+1}) \geq 3. \tag{3.18}$$

Moreover the inequality

$$w_H(g(x)(x^\eta + \xi)^{j_0+1} \ (\text{mod } (x^\eta - \xi))) > 0 \tag{3.19}$$

holds since $x^\eta - \xi \nmid g(x)$. Now using (3.9), (3.18) and (3.19), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H(f(x)(x^\eta - \xi)^{p^{s-1}+1}(x^\eta + \xi)) \\ &= w_H((x^\eta - \xi)^{i_0+p^{s-1}+1}(x^\eta + \xi)^{j_0+1}g(x)) \\ &\geq w_H((x^\eta - \xi)^{i_0+p^{s-1}+1})w_H((x^\eta + \xi)^{j_0+1}g(x) \pmod{(x^\eta - \xi)}) \\ &\geq 3. \end{aligned} \tag{3.20}$$

If $i_0 \geq p^s - p^{s-1} - 1$, then $j_0 < p^s - 1$. Clearly $w_H((x^{2\eta} - \xi^2)^{j_0+j}) \geq 2$. So, by Lemma 3.3.3, we have

$$w_H(c(x)) \geq 2w_H((x^{2\eta} - \xi^2)^{j_0+j}) \geq 4. \tag{3.21}$$

Now combining (3.20) and (3.21), we obtain $w_H(c(x)) \geq 3$, and hence $d_H(C) \geq 3$. ■

Corollary 3.3.5 *Let i, j be integers with $2p^{s-1} \geq i > p^{s-1} \geq j > 0$ and let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. Then $d_H(C) = 3$.*

Proof. Since $C \subset \langle (x^\eta - \xi)^{p^{s-1}+1}(x^\eta + \xi) \rangle$, we know, by Lemma 3.3.4, that $d_H(C) \geq 3$. For $(x^\eta - \xi)^{2p^{s-1}}(x^\eta + \xi)^{2p^{s-1}} \in C$, we have

$$(x^\eta - \xi)^{2p^{s-1}}(x^\eta + \xi)^{2p^{s-1}} = (x^{2\eta} - \xi^2)^{2p^{s-1}} = x^{4\eta p^{s-1}} - 2\xi^{2p^{s-1}}x^{2\eta p^{s-1}} + \xi^{4p^{s-1}}.$$

So $d_H(C) \leq 3$ and hence $d_H(C) = 3$. ■

For $2p^{s-1} < i < p^s$ and $0 < j \leq p^{s-1}$, $d_H(C)$ is computed in the following lemma and corollary.

Lemma 3.3.6 *Let $C = \langle (x^\eta - \xi)^{2p^{s-1}+1}(x^\eta + \xi) \rangle$. Then $d_H(C) \geq 4$.*

Proof. Pick $0 \neq c(x) \in C$ where $c(x) \equiv f(x)(x^\eta - \xi)^{2p^{s-1}+1}(x^\eta + \xi) \left(\text{mod } (x^{2\eta p^s} - \lambda)\right)$ for some $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ with $\deg(f(x)) < 2\eta p^s - 2\eta p^{s-1} - 2\eta$. Let i_0 and j_0 be the largest integers with $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Then $f(x)$ is of the form $f(x) = (x^\eta - \xi)^{i_0}(x^\eta + \xi)^{j_0}g(x)$ for some $g(x) \in \mathbb{F}_{p^m}[x]$ with $x^\eta - \xi \nmid g(x)$ and $x^\eta + \xi \nmid g(x)$. Note that $i_0 < p^s - 2p^{s-1} - 1$ or $j_0 < p^s - 1$ holds since $\deg(f(x)) < 2\eta p^s - 2\eta p^{s-1} - 2\eta$.

If $i_0 < p^s - 2p^{s-1} - 1$, then, by Lemma 3.1.1, we have

$$w_H((x^\eta - \xi)^{i_0+2p^{s-1}+1}) \geq 4. \tag{3.22}$$

Since $x^\eta - \xi \nmid g(x)$,

$$w_H(g(x)(x^\eta + \xi)^{j_0+1} \ (\mathrm{mod}\ (x^\eta - \xi))) > 0 \tag{3.23}$$

holds. Now using (3.22), (3.23) and (3.9), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H(f(x)(x^\eta - \xi)^{2p^{s-1}+1}(x^\eta + \xi)) \\ &= w_H((x^\eta - \xi)^{i_0+2p^{s-1}+1}(x^\eta + \xi)^{j_0+1}g(x)) \\ &\geq w_H((x^\eta + \xi)^{j_0+1}g(x) \ (\mathrm{mod}\ (x^\eta - \xi)))w_H((x^\eta - \xi)^{i_0+2p^{s-1}+1}) \\ &\geq 4. \end{aligned}$$

If $i_0 \geq p^s - 2p^{s-1} - 1$, then $j_0 < p^s - 1$. Clearly $w_H((x^{2\eta} - \xi^2)^{j_0+1}) \geq 2$. So, by Lemma 3.3.3, we have $w_H(c(x)) \geq 2w_H((x^{2\eta} - \xi^2)^{j_0+1}) \geq 4$. Hence $d_H(C) \geq 4$. ■

Corollary 3.3.7 *Let $2p^{s-1} < i < p^s$ and $0 < j \leq p^{s-1}$ be integers, and let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. Then $d_H(C) = 4$.*

Proof. Since $C \subset \langle (x^\eta - \xi)^{2p^{s-1}+1}(x^\eta + \xi) \rangle$, we know, by Lemma 3.3.6, that $d_H(C) \geq 4$. For $(x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^{s-1}} \in C$, we have $w_H((x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^{s-1}}) = 4$. Thus $d_H(C) \leq 4$ and hence $d_H(C) = 4$. ■

Next we consider the cases where $p^{s-1} < j \leq i \leq p^s$. We begin with computing $d_H(C)$ when $p^{s-1} < j \leq i \leq (p-1)p^{s-1}$ in the following lemma and corollary.

Lemma 3.3.8 *Let $1 \leq \beta' \leq \beta \leq p - 2$ be integers and $C = \langle (x^\eta - \xi)^{\beta p^{s-1}+1}(x^\eta + \xi)^{\beta' p^{s-1}+1} \rangle$. Then $d_H(C) \geq \min\{\beta + 2, 2(\beta' + 2)\}$.*

Proof. Let $0 \neq c(x) \in C$. Then there exists $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ such that $c(x) \equiv f(x)(x^\eta - \xi)^{\beta p^{s-1}+1}(x^\eta + \xi)^{\beta' p^{s-1}+1} \left(\mathrm{mod}\ (x^{2\eta p^s} - \lambda)\right)$. We may assume that $\deg(f(x)) < 2\eta p^s - \eta\beta p^{s-1} - \eta\beta' p^{s-1} - 2\eta$. We consider the cases $\beta = \beta'$ and $\beta < \beta'$ separately.

First, we assume that $\beta = \beta'$. Then $C = \langle (x^{\eta} - \xi)^{\beta p^{s-1}+1}(x^{\eta} + \xi)^{\beta' p^{s-1}+1} \rangle = \langle (x^{2\eta} - \xi^2)^{\beta p^{s-1}+1} \rangle$. Let m be the largest nonnegative integer with $(x^{2\eta} - \xi^2)^m | f(x)$. We have $m < p^s - \beta p^{s-1} - 1$ as $\deg(f(x)) < 2\eta p^s - 2\eta\beta p^{s-1} - 2\eta$. So, by Lemma 3.1.1, we get

$$w_H((x^{2\eta} - \xi^2)^{\beta p^{s-1}+1+m}) \geq \beta + 2. \tag{3.24}$$

Clearly $f(x)$ is of the form $f(x) = (x^{2\eta} - \xi^2)^m g(x)$ for some $g(x) \in \mathbb{F}_{p^m}[x]$ where $x^{2\eta} - \xi^2 \nmid g(x)$. So $g(x) \left(\text{mod } (x^{2\eta} - \xi^2)\right) \neq 0$ and therefore

$$w_H(g(x) \left(\text{mod } (x^{2\eta} - \xi^2)\right)) > 0. \tag{3.25}$$

So if $\beta = \beta'$, then using (3.24), (3.25) and (3.9), we get

$$\begin{aligned} w_H(c(x)) &= w_H((x^{2\eta} - \xi^2)^{m+\beta p^{s-1}+1} g(x)) \\ &\geq w_H(g(x) \left(\text{mod } (x^{2\eta} - \xi^2)\right)) w_H((x^{2\eta} - \xi^2)^{m+\beta p^{s-1}+1}) \\ &\geq \beta + 2. \end{aligned}$$

Second, we assume that $\beta' < \beta$. For $c(x) \equiv f(x)(x^{\eta} - \xi)^{\beta p^{s-1}+1}(x^{\eta} + \xi)^{\beta' p^{s-1}+1} \left(\text{mod } (x^{2\eta p^s} - \lambda)\right)$, let i_0 and j_0 be the largest integers with $(x^{\eta} - \xi)^{i_0} | f(x)$ and $(x^{\eta} + \xi)^{j_0} | f(x)$. Since $\deg(f(x)) < 2\eta p^s - \eta\beta p^{s-1} - \eta\beta' p^{s-1} - 2\eta$, we have $i_0 + j_0 < 2p^s - \beta p^{s-1} - \beta' p^{s-1} - 2$. Thus $i_0 < p^s - \beta p^{s-1} - 1$ or $j_0 < p^s - \beta' p^{s-1} - 1$ holds.

If $i_0 < p^s - \beta p^{s-1} - 1$, then, by Lemma 3.1.1, we have

$$w_H((x^{\eta} - \xi)^{i_0 + \beta p^{s-1}+1}) \geq \beta + 2. \tag{3.26}$$

Note that $(x^{\eta} + \xi)^{j_0 + \beta' p^{s-1}+1} g(x) \ (\text{mod } (x^{\eta} - \xi)) \neq 0$ since $x^{\eta} - \xi \nmid (x^{\eta} + \xi)^{j_0 + \beta' p^{s-1}+1} g(x)$. Therefore

$$w_H((x^{\eta} + \xi)^{j_0 + \beta' p^{s-1}+1} g(x) \ (\text{mod } (x^{\eta} - \xi))) > 0. \tag{3.27}$$

Using (3.9), (3.26) and (3.27), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H((x^{\eta} - \xi)^{i_0 + \beta p^{s-1}+1}(x^{\eta} + \xi)^{j_0 + \beta' p^{s-1}+1} g(x)) \\ &\geq w_H((x^{\eta} + \xi)^{j_0 + \beta' p^{s-1}+1} g(x) \ (\text{mod } (x^{\eta} - \xi))) w_H((x^{\eta} - \xi)^{i_0 + \beta p^{s-1}+1}) \qquad (3.28) \\ &\geq \beta + 2. \end{aligned}$$

If $i_0 \geq p^s - \beta p^{s-1} - 1$, then $j_0 < p^s - \beta' p^{s-1} - 1$. By Lemma 3.3.3, we get

$$w_H(c(x)) \geq 2 w_H((x^{2\eta} - \xi^2)^{j_0 + \beta' p^{s-1}+1}). \tag{3.29}$$

For $w_H((x^{2\eta} - \xi^2)^{j_0+\beta' p^{s-1}+1})$, we use Lemma 3.1.1 and get

$$w_H((x^{2\eta} - \xi^2)^{j_0+\beta' p^{s-1}+1}) \geq \beta' + 2. \tag{3.30}$$

Combining (3.29) and (3.30), we obtain

$$w_H(c(x)) \geq 2(\beta' + 2). \tag{3.31}$$

So if $\beta' < \beta$, then, by (3.28) and (3.31), we get that $w_H(c(x)) \geq \min\{\beta + 2, 2(\beta' + 2)\}$. In both cases, namely $\beta = \beta'$ and $\beta' < \beta$, we have shown that $d_H(C) \geq \min\{\beta + 2, 2(\beta' + 2)\}$. ■

Corollary 3.3.9 *Let $j \leq i$, $1 \leq \beta' \leq \beta \leq p - 2$ be integers such that*

$$\begin{aligned} \beta p^{s-1} + 1 \quad &\leq \quad i \quad \leq \quad (\beta + 1)p^{s-1} \quad \textit{and} \\ \beta' p^{s-1} + 1 \quad &\leq \quad j \quad \leq \quad (\beta' + 1)p^{s-1}. \end{aligned}$$

Let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. Then $d_H(C) = \min\{\beta + 2, 2(\beta' + 2)\}$.

Proof. We know, by Lemma 3.3.8, that $d_H(C) \geq \min\{\beta + 2, 2(\beta' + 2)\}$. So it suffices to show $d_H(C) \leq \min\{\beta + 2, 2(\beta' + 2)\}$.

First, $(\beta + 1)p^{s-1} \geq i, j$ implies that $(x^\eta - \xi)^{(\beta+1)p^{s-1}}(x^\eta + \xi)^{(\beta+1)p^{s-1}} = (x^{2\eta} - \xi^2)^{(\beta+1)p^{s-1}} \in C$. By (3.4), we get $w_H((x^{2\eta} - \xi^2)^{(\beta+1)p^{s-1}}) = \beta + 2$. Therefore

$$d_H(C) \leq \beta + 2. \tag{3.32}$$

Second, we consider $(x^\eta - \xi)^{p^s}(x^\eta + \xi)^{(\beta'+1)p^{s-1}} \in C$. Using (3.4) and the fact that $p^s > (\beta' + 1)p^{s-1}$, we get

$$w_H((x^\eta - \xi)^{p^s}(x^\eta + \xi)^{(\beta'+1)p^{s-1}}) = 2w_H((x^\eta + \xi)^{(\beta'+1)p^{s-1}}) = 2(\beta' + 2).$$

So

$$d_H(C) \leq 2(\beta' + 2). \tag{3.33}$$

Combining (3.32) and (3.33), we deduce that $d_H(C) \leq \min\{\beta + 2, 2(\beta' + 2)\}$. Therefore $d_H(C) = \min\{\beta + 2, 2(\beta' + 2)\}$. ■

The following lemma and corollary deal with the case where $p^{s-1} < j \leq (p-1)p^{s-1} < i < p^s$.

Lemma 3.3.10 *Let* $1 \leq \tau \leq p-1$, $1 \leq \beta \leq p-2$, $1 \leq k \leq s-1$ *be integers and* $C = \langle (x^\eta - \xi)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}(x^\eta + \xi)^{\beta p^{s-1}+1}\rangle$. *Then* $d_H(C) \geq 2(\beta+2)$.

Proof. Let $0 \neq c(x) \in C$. Then there exists $0 \neq f(x) \in \mathbb{F}_q[x]$ such that $c(x) \equiv (x^\eta - \xi)^{p^s-p^{s-k}+(\tau-1)p^{s-k-1}+1}(x^\eta + \xi)^{\beta p^{s-1}+1} f(x) \ \left(\text{mod}\ (x^{2\eta p^s} - \lambda)\right)$ and $\deg(f(x)) < \eta p^s + \eta p^{s-k} - \eta(\tau-1)p^{s-k-1} - \eta\beta p^{s-1} - 2\eta$. Let i_0 and j_0 be the largest integers with $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Then $f(x)$ is of the form $f(x) = (x^\eta - \xi)^{i_0}(x^\eta+\xi)^{j_0} g(x)$ for some $g(x) \in \mathbb{F}_{p^m}[x]$ such that $x^\eta - \xi \nmid g(x)$ and $x^\eta + \xi \nmid g(x)$. Clearly $i_0 + j_0 < p^s + p^{s-k} - (\tau-1)p^{s-k-1} - \beta p^{s-1} - 2$. So $i_0 < p^{s-k} - (\tau-1)p^{s-k-1} - 1$ or $j_0 < p^s - \beta p^{s-1} - 1$ holds.

If $i_0 < p^{s-k} - (\tau-1)p^{s-k-1} - 1$, then, by Lemma 3.3.3, we have

$$w_H((x^\eta - \xi)^{i_0 + p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}) \geq (\tau+1)p^k. \tag{3.34}$$

Since $x^\eta - \xi \nmid g(x)$,

$$w_H((x^\eta + \xi)^{j_0 + \beta p^{s-1}+1} g(x) \ (\text{mod}\ (x^\eta - \xi))) > 0. \tag{3.35}$$

Using (3.34), (3.35) and (3.9), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H((x^\eta - \xi)^{i_0 + p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}(x^\eta + \xi)^{j_0+\beta p^{s-1}+1} g(x)) \\ &\geq w_H((x^\eta + \xi)^{j_0+\beta p^{s-1}+1} g(x) \ (\text{mod}\ (x^\eta - \xi))) w_H((x^\eta - \xi)^{i_0 + p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}) \\ &\geq (\tau+1)p^k \\ &\geq 2p \\ &\geq 2(\beta+2). \end{aligned}$$

If $i_0 \geq p^{s-k} - (\tau-1)p^{s-k-1} - 1$, then $j_0 < p^s - \beta p^{s-1} - 1$. So, by Lemma 3.3.3, we get

$$w_H(c(x)) \geq 2 w_H((x^{2\eta} - \xi^2)^{j_0 + \beta p^{s-1}+1}). \tag{3.36}$$

For $w_H((x^{2\eta} - \xi^2)^{j_0 + \beta p^{s-1}+1})$, we use Lemma 3.1.1 and get

$$w_H((x^{2\eta} - \xi^2)^{j_0 + \beta p^{s-1}+1}) = \beta + 2. \tag{3.37}$$

Combining (3.36) and (3.37), we obtain $w_H(c(x)) \geq 2(\beta+2)$. So $d_H(C) \geq 2(\beta+2)$. ■

Corollary 3.3.11 *Let* i, j, $1 \leq \tau \leq p-1$, $1 \leq \beta \leq p-2$ *and* $1 \leq k \leq s-1$ *be integers such that*

$$\begin{aligned} p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \ &\leq \ i \ \leq \ p^s - p^{s-k} + \tau p^{s-k-1} \quad \textit{and} \\ \beta p^{s-1} + 1 \ &\leq \ j \ \leq \ (\beta+1)p^{s-1}. \end{aligned}$$

Let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. *Then* $d_H(C) = 2(\beta+2)$.

Proof. Since $\langle (x^\eta - \xi)p^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}(x^\eta + \xi)^{\beta p^{s-1}+1}\rangle \supset C$, we know, by Lemma 3.3.10, that $d_H(C) \geq 2(\beta + 2)$. So it suffices to show $d_H(C) \leq 2(\beta + 2)$. We consider $(x^\eta - \xi)^{p^s}(x^\eta + \xi)^{(\beta+1)p^{s-1}} \in C$. Note that $w_H((x^\eta - \xi)^{(\beta+1)p^{s-1}}) = \beta + 2$ by (3.4). So, using the fact that $p^s > (\beta + 1)p^{s-1}$, we obtain $w_H((x^\eta - \xi)^{p^s}(x^\eta + \xi)^{(\beta+1)p^{s-1}}) = 2(\beta + 2)$. So $d_H(C) \leq 2(\beta + 2)$, and hence $d_H(C) = 2(\beta + 2)$. ■

From Lemma 3.3.12 till Corollary 3.3.15, we compute $d_H(C)$ when $(p-1)p^{s-1} < j \leq i < p^s$.

Lemma 3.3.12 *Let* $1 \leq k \leq s-1, 1 \leq \tau^{'} \leq \tau \leq p-1,$

$$\begin{aligned} i &= p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 \quad \textit{and} \\ j &= p^s - p^{s-k} + (\tau^{'} - 1)p^{s-k-1} + 1 \end{aligned}$$

be integers and $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. *Then* $d_H(C) \geq \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$.

Proof. Let $0 \neq c(x) \in C$. Then there exists $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ such that $c(x) \equiv f(x)(x^\eta - \xi)^i(x^\eta + \xi)^j \pmod{(x^{2\eta p^s} - \lambda)}$ and $\deg(f(x)) < 2\eta p^s - i\eta - j\eta$. Let i_0 and j_0 be the largest integers with $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Then $f(x)$ is of the form $f(x) = (x^\eta - \xi)^{i_0}(x^\eta + \xi)^{j_0} g(x)$ for some $g(x) \in \mathbb{F}_{p^m}[x]$ with $x^\eta - \xi \nmid g(x)$ and $x^\eta + \xi \nmid g(x)$. Clearly $i_0 + j_0 < 2p^s - i - j$ and therefore $i_0 < p^s - i$ or $j_0 < p^s - j$ holds.

If $i_0 < p^s - i$, then by Lemma 3.1.2, we have

$$w_H((x^\eta - \xi)^{i_0 + i}) \geq (\tau + 1)p^k. \tag{3.38}$$

Since $x^\eta - \xi \nmid g(x)$, we have $g(x)(x^\eta + \xi)^{j_0 + j} \not\equiv 0 \pmod{(x^\eta - \xi)}$ and therefore

$$w_H(g(x)(x^\eta + \xi)^{j + j_0} \pmod{(x^\eta - \xi)}) > 0. \tag{3.39}$$

Using (3.38), (3.39) and (3.9), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H((x^\eta - \xi)^{i + i_0}(x^\eta + \xi)^{j + j_0} g(x)) \\ &\geq w_H(g(x)(x^\eta + \xi)^{j + j_0} \pmod{(x^\eta - \xi)}) w_H((x^\eta - \xi)^{i + i_0}) \\ &\geq (\tau + 1)p^k. \end{aligned} \tag{3.40}$$

If $i_0 \geq p^s - i$, then $j_0 < p^s - j$. So, by Lemma 3.3.3, we have

$$w_H(c(x)) \geq 2 w_H((x^{2\eta} - \xi^2)^{j_0 + j}). \tag{3.41}$$

For $w_H((x^{2\eta} - \xi^2)^{j_0+j})$, we use Lemma 3.1.2 and get

$$w_H((x^{2\eta} - \xi^2)^{j_0+j}) \geq (\tau^{'} + 1)p^k. \tag{3.42}$$

Combining (3.41) and (3.42), we obtain

$$w_H(c(x)) \geq 2(\tau^{'} + 1)p^k. \tag{3.43}$$

Now, using (3.40) and (3.43), we deduce that $w_H(c(x)) \geq \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$. Hence $d_H(C) \geq \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$. ■

Corollary 3.3.13 *Let $j \leq i$, $1 \leq k \leq s-1$, $1 \leq \tau^{'} \leq \tau \leq p-1$ be integers such that*

$$\begin{array}{rcccl} p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 & \leq & i & \leq & p^s - p^{s-k} + \tau p^{s-k-1} \quad \textit{and} \\ p^s - p^{s-k} + (\tau^{'} - 1)p^{s-k-1} + 1 & \leq & j & \leq & p^s - p^{s-k} + \tau^{'} p^{s-k-1}. \end{array}$$

Let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. Then $d_H(C) = \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$.

Proof. Since $\langle (x^\eta - \xi)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} (x^\eta + \xi)^{p^s - p^{s-k} + (\tau^{'}-1)p^{s-k-1}+1} \rangle \supset C$, we have, by Lemma 3.3.12, that $d_H(C) \geq \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$. So it suffices to show $d_H(C) \leq \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$.

First, we consider $(x^\eta - \xi)^{p^s} (x^\eta + \xi)^{p^s - p^{s-k} + \tau^{'} p^{s-k-1}} \in C$. Since

$$w_H((x^\eta + \xi)^{p^s - p^{s-1} + \tau^{'} p^{s-k-1}}) = (\tau^{'} + 1)p^k,$$

we have $w_H((x^\eta - \xi)^{p^s} (x^\eta + \xi)^{p^s - p^{s-1} + (\tau^{'}-1)p^{s-k-1}}) = 2(\tau^{'} + 1)p^k$. So

$$d_H(C) \leq 2(\tau^{'} + 1)p^k \tag{3.44}$$

Second, we consider $(x^{2\eta} - \xi^2)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} \in C$. By Lemma 3.4, we get

$$w_H((x^{2\eta} - \xi^2)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1}) = (\tau + 1)p^k.$$

Thus

$$d_H(C) \leq (\tau + 1)p^k. \tag{3.45}$$

Now combining (3.44) and (3.45), we deduce that $d_H(C) \leq \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$. Hence $d_H(C) = \min\{2(\tau^{'} + 1)p^k, (\tau + 1)p^k\}$. ■

Lemma 3.3.14 *Let* $1 \leq k^{'} < k \leq s-1$, $1 \leq \tau^{'}, \tau < p-1$,

$$\begin{aligned} i &= p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 \quad \textit{and} \\ j &= p^s - p^{s-k^{'}} + (\tau^{'} - 1)p^{s-k^{'}-1} + 1 \end{aligned}$$

be integers and $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. *Then* $d_H(C) \geq 2(\tau^{'} + 1)p^{k^{'}}$.

Proof. Let $0 \neq c(x) \in C$. Then there exists $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ such that $c(x) \equiv (x^\eta - \xi)^i (x^\eta + \xi)^j f(x) \left(\text{mod } (x^{2\eta p^s} - \lambda)\right)$ and $\deg(f(x)) < 2\eta p^s - i\eta - j\eta$. Let i_0 and j_0 be the largest integers with $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Then $f(x)$ is of the form $f(x) = (x^\eta - \xi)^{i_0}(x^\eta + \xi)^{j_0} g(x)$ for some $g(x) \in \mathbb{F}_{p^m}[x]$ with $x^\eta - \xi \nmid g(x)$ and $x^\eta + \xi \nmid g(x)$. Clearly $i_0 + j_0 < 2p^s - i - j$. So $i_0 < p^s - i$ or $j_0 < p^s - j$ holds.

If $i_0 < p^s - i$, then, by Lemma 3.1.2, we have

$$w_H((x^\eta - \xi)^{i+i_0}) \geq (\tau + 1)p^k \geq 2(\tau^{'} + 1)p^{k^{'}}. \tag{3.46}$$

Since $x^\eta - \xi \nmid g(x)$, we have $(x^\eta + \xi)^{j_0+j} g(x) \ (\text{mod } (x^\eta - \xi)) \neq 0$ and therefore

$$w_H((x^\eta + \xi)^{j_0+j} g(x) \ (\text{mod } (x^\eta - \xi))) > 0. \tag{3.47}$$

Using (3.46), (3.47) and (3.9), we obtain

$$\begin{aligned} w_H(c(x)) &= w_H((x^\eta - \xi)^{i_0+i}(x^\eta + \xi)^{j_0+j} g(x)) \\ &\geq w_H((x^\eta + \xi)^{j_0+j} g(x) \ (\text{mod } (x^\eta - \xi))) w_H((x^\eta - \xi)^{i_0+i}) \\ &\geq 2(\tau^{'} + 1)p^{k^{'}}. \end{aligned}$$

If $i_0 \geq p^s - i$, then $j_0 < p^s - j$. So, by Lemma 3.3.3, we have

$$w_H(c(x)) \geq 2 w_H((x^{2\eta} - \xi^2)^{j_0+j}). \tag{3.48}$$

For $w_H((x^{2\eta} - \xi^2)^{j_0+j})$, we use Lemma 3.1.2 and get

$$w_H((x^{2\eta} - \xi^2)^{j_0+j}) \geq (\tau^{'} + 1)p^{k^{'}}. \tag{3.49}$$

Now combining (3.48) and (3.49), we obtain $w_H(c(x)) \geq 2(\tau^{'} + 1)p^{k^{'}}$. Hence $d_H(C) \geq 2(\tau^{'} + 1)p^{k^{'}}$. ■

Corollary 3.3.15 *Let $i, j, 1 \leq k^{'} < k \leq s-1, 1 \leq \tau^{'}, \tau \leq p-1$ be integers such that*

$$\begin{array}{rcccl} p^s - p^{s-k} + (\tau - 1)p^{s-k-1} + 1 & \leq & i & \leq & p^s - p^{s-k} + \tau p^{s-k-1} \quad \textit{and} \\ p^s - p^{s-k^{'}} + (\tau^{'} - 1)p^{s-k^{'}-1} + 1 & \leq & j & \leq & p^s - p^{s-k^{'}} + \tau^{'} p^{s-k^{'}-1}. \end{array}$$

Let $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$. Then $d_H(C) = 2(\tau^{'} + 1)p^{k^{'}}$.

Proof. Since $\langle (x^\eta - \xi)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} (x^\eta + \xi)^{p^s - p^{s-k^{'}} + (\tau^{'}-1)p^{s-k^{'}-1}+1} \rangle \supset C$, we know, by Lemma 3.3.14, that $d_H(C) \geq 2(\tau^{'} + 1)p^{k^{'}}$. So it suffices to show $d_H(C) \leq 2(\tau^{'} + 1)p^{k^{'}}$. We consider $(x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^s - p^{s-k^{'}} + \tau^{'} p^{s-k^{'}-1}} \in C$. By (3.4), we have

$$w_H((x^\eta + \xi)^{p^s - p^{s-k^{'}} + \tau^{'} p^{s-k^{'}-1}}) = (\tau^{'} + 1)p^{k^{'}}.$$

Moreover since $(x^\eta - \xi)^{p^s} = x^{\eta p^s} - \xi^{p^s}$ and $p^s > p^s - p^{s-k^{'}} + \tau^{'} p^{s-k^{'}-1}$, we get

$$w_H((x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^s - p^{s-k^{'}} + \tau^{'} p^{s-k^{'}-1}}) = 2(\tau^{'} + 1)p^{k^{'}}.$$

So $d_H(C) \leq 2(\tau^{'} + 1)p^{k^{'}}$ and therefore $d_H(C) = 2(\tau^{'} + 1)p^{k^{'}}$. ■

Finally it remains to consider the cases where $i = p^s$ and $0 < j < p^s$.

Lemma 3.3.16 *Let $C = \langle (x^\eta - \xi)^{p^s}(x^\eta + \xi) \rangle$. Then $d_H(C) \geq 4$.*

Proof. Pick $0 \neq c(x) \in C$. Then there exists $0 \neq f(x) \in \mathbb{F}_{p^m}[x]$ such that $c(x) \equiv f(x)(x^\eta - \xi)^{p^s}(x^\eta + \xi) \ \big(\mathrm{mod}\ (x^{2\eta p^s} - \lambda)\big)$ and $\deg(f(x)) < 2\eta p^s - \eta p^s - \eta = \eta p^s - \eta$. Let i_0 and j_0 be the largest nonnegative integers such that $(x^\eta - \xi)^{i_0} | f(x)$ and $(x^\eta + \xi)^{j_0} | f(x)$. Clearly $i_0 + j_0 < p^s - 1$ as $\deg(f(x)) < \eta p^s - \eta$. So, since $i_0 \geq p^s - p^s = 0$ and $j_0 < p^s - 1$, by Lemma 3.3.3, we get $w_H(c(x)) \geq 2 w_H((x^{2\eta} - \xi^2)^{j_0+1})$. Obviously $w_H((x^{2\eta} - \xi^2)^{j_0+1}) \geq 2$ and therefore $w_H(c(x)) \geq 4$. Hence $d_H(C) \geq 4$. ■

Corollary 3.3.17 *Let $0 < j \leq p^{s-1}$ be an integer and $C = \langle (x^\eta - \xi)^{p^s}(x^\eta + \xi)^j \rangle$. Then $d_H(C) = 4$.*

Proof. Since $\langle (x^\eta - \xi)^{p^s}(x^\eta + \xi) \rangle \supset C$, we know, by Lemma 3.3.16, that $d_H(C) \geq 4$. So it suffices to show $d_H(C) \leq 4$. We consider $(x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^{s-1}} \in C$. Clearly $w_H((x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^{s-1}}) = 4$. So $d_H(C) \leq 4$ and hence $d_H(C) = 4$. ■

For $i = p^s$ and $p^{s-1} < j < p^s$, the Hamming distance of C is computed in the following lemmas and corollaries. Their proofs are similar to those of Lemma 3.3.16 and Corollary 3.3.16.

Lemma 3.3.18 *Let* $1 \leq \beta \leq p-2$ *be an integer and* $C = \langle (x^\eta - \xi)^{p^s}(x^\eta + \xi)^{\beta p^{s-1}+1} \rangle$. *Then* $d_H(C) \geq 2(\beta+2)$.

Corollary 3.3.19 *Let* $1 \leq \beta \leq p-2$, $\beta p^{s-1} + 1 \leq j \leq (\beta+1)p^{s-1}$ *be integers. Let* $C = \langle (x^\eta - \xi)^{p^s}(x^\eta + \xi)^j \rangle$. *Then* $d_H(C) = 2(\beta+2)$.

Lemma 3.3.20 *Let* $1 \leq \tau \leq p-1, 1 \leq k \leq s-1, j$ *be integers and* $C = \langle (x^\eta - \xi)^{p^s}(x^\eta + \xi)^{p^s - p^{s-k} + (\tau-1)p^{s-k-1}+1} \rangle$. *Then* $d_H(C) \geq 2(\tau+1)p^k$.

Corollary 3.3.21 *Let* $1 \leq \tau \leq p-1, 1 \leq k \leq s-1, j$ *be integers such that*

$$p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq j \leq p^s - p^{s-k} + \tau p^{s-k-1}.$$

Let $C = \langle (x^\eta - \xi)^{p^s}(x^\eta + \xi)^j \rangle$. *Then* $d_H(C) = 2(\tau+1)p^k$.

We summarize our results in the following theorem.

Theorem 3.3.22 *Let p be an odd prime, a, s, n be arbitrary positive integers. Let* $\lambda, \xi, \psi \in \mathbb{F}_{p^m} \setminus \{0\}$ *such that* $\lambda = \psi^{p^s}$. *Suppose that the polynomial* $x^{2\eta} - \psi$ *factors into two irreducible polynomials as* $x^{2\eta} - \psi = (x^\eta - \xi)(x^\eta + \xi)$. *Then all* λ*-cyclic codes, of length* $2\eta p^s$*, over* $\mathbb{F}_{p^m}$ *are of the form* $\langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle \subset \mathbb{F}_{p^m}[x]/\langle x^{2\eta p^s} - \lambda \rangle$, *where* $0 \leq i, j \leq p^s$ *are integers. Let* $C = \langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle \subset \mathbb{F}_{p^m}[x]/\langle x^{2\eta p^s} - \lambda \rangle$. *If* $(i, j) = (0, 0)$, *then C is the whole space* $\mathbb{F}_{p^m}^{2\eta p^s}$, *and if* $(i, j) = (p^s, p^s)$, *then C is the zero space* $\{\mathbf{0}\}$. *For the remaining values of* (i, j), *the Hamming distance of C is given in Table 3.1.*

Remark 3.3.23 *There are some symmetries in most of the cases, so we made the following simplification in Table 3.1. For the cases with *, i.e., the cases except 2 and 7, we gave the Hamming distance of C when* $i \geq j$. *The corresponding case with* $j \geq i$ *has the same Hamming distance. For example in 1*, the corresponding case is* $i = 0$ *and* $0 \leq j \leq p^s$, *and the Hamming distance is* 2. *Similarly in 6*, the corresponding case is* $\beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1}$ *and* $p^s - p^{s-k} + (\tau-1)p^{s-k-1} + 1 \leq j \leq p^s - p^{s-k} + \tau p^{s-k-1}$, *and the Hamming distance is* $2(\beta+2)$.

Table 3.1: The Hamming distance of all non-trivial constacyclic codes, of the form $\langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle$, of length $2\eta p^s$ over $\mathbb{F}_{p^m}$. The polynomials $x^\eta - \xi$ and $x^\eta + \xi$ are assumed to be irreducible. The parameters $1 \leq \beta^{'} \leq \beta \leq p-2$, $1 \leq \tau^{(2)} < \tau^{(1)} \leq p-1$, $1 \leq \tau, \tau^{(3)}, \tau^{(4)} \leq p-1$, $1 \leq k \leq s-1$, $1 \leq k^{''} < k^{'} \leq s-1$ below are integers. For the cases with *, i.e., the cases except 2 and 7, see Remark 3.3.23

Case	**i**	**j**	$\mathbf{d_H(C)}$
1*	$0 < i \leq p^s$	$j = 0$	2
2	$0 \leq i \leq p^{s-1}$	$0 \leq j \leq p^{s-1}$	2
3*	$p^{s-1} < i \leq 2p^{s-1}$	$0 < j \leq p^{s-1}$	3
4*	$2p^{s-1} < i \leq p^s$	$0 < j \leq p^{s-1}$	4
5*	$\beta p^{s-1} + 1 \leq i \leq (\beta + 1)p^{s-1}$	$\beta^{'} p^{s-1} + 1 \leq j \leq (\beta^{'} + 1)p^{s-1}$	$\min\{\beta + 2,$ $2(\beta^{'} + 2)\}$
6*	$p^s - p^{s-k} + (\tau - 1)p^{s-k-1}$ $+1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}$	$\beta p^{s-1} + 1 \leq j \leq (\beta + 1)p^{s-1}$	$2(\beta + 2)$
7	$p^s - p^{s-k} + (\tau - 1)p^{s-k-1}$ $+1 \leq i \leq p^s - p^{s-k} + \tau p^{s-k-1}$	$p^s - p^{s-k} + (\tau - 1)p^{s-k-1}$ $+1 \leq j \leq p^s - p^{s-k} + \tau p^{s-k-1}$	$(\tau + 1)p^k$
8*	$p^s - p^{s-k} + (\tau^{(1)} - 1)p^{s-k-1}$ $+1 \leq i \leq \quad p^s - p^{s-k}$ $+\tau^{(1)} p^{s-k-1}$	$p^s - p^{s-k} + (\tau^{(2)} - 1)p^{s-k-1}$ $+1 \leq j \leq \quad p^s - p^{s-k}$ $+\tau^{(2)} p^{s-k-1}$	$\min\{$ $2(\tau^{(2)} + 1)p^k,$ $(\tau^{(1)} + 1)p^k\}$
9*	$p^s - p^{s-k^{'}} + (\tau^{(3)} - 1)p^{s-k^{'}-1}$ $+1 \leq i \leq \quad p^s - p^{s-k^{'}}$ $+\tau^{(3)} p^{s-k^{'}-1}$	$p^s - p^{s-k^{''}} + (\tau^{(4)} - 1)p^{s-k^{''}-1}$ $+1 \leq j \leq \quad p^s - p^{s-k^{''}}$ $+\tau^{(4)} p^{s-k^{''}-1}$	$2(\tau^{(4)} + 1)p^{k^{''}}$
10*	$i = p^s$	$\beta p^{s-1} + 1 \leq j \leq (\beta + 1)p^{s-1}$	$2(\beta + 2)$
11*	$i = p^s$	$p^s - p^{s-k} + (\tau - 1)p^{s-k-1}$ $+1 \leq j \leq \quad p^s - p^{s-k}$ $+\tau p^{s-k-1}$	$2(\tau + 1)p^k$

The results in Table 3.1 still hold when the polynomials $x^\eta + \xi$ and $x^\eta - \xi$ are reducible except the fact that the cases in Table 3.1 do not cover all the λ-cyclic codes of length $2\eta p^s$ over $\mathbb{F}_{p^m}$.

Remark 3.3.24 *Note that $\langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle, 0 \leq i, j \leq p^s$ are ideals of $\mathcal{R}$ independent of the fact that $x^\eta - \xi$ and $x^\eta - \xi$ are irreducible over $\mathbb{F}_{p^m}$. So the above results from Lemma 3.3.4 till Corollary 3.3.21 hold even when the polynomials $x^\eta - \xi$ and $x^\eta + \xi$ are reducible. But in this case, there are more λ-cyclic codes than the ones of the form $\langle (x^\eta - \xi)^i (x^\eta + \xi)^j \rangle, 0 \leq i, j \leq p^s$ and their Hamming distance is not given in this paper.*

In the last part of this section, we determine the Hamming distance of some polycyclic codes of length $2\eta p^s$ over $GR(p^a, m)$ whose canonical images are as above. In particular, this gives us the Hamming distance of certain constacyclic codes of length $2\eta p^s$ over $GR(p^a, m)$. Let λ_0, $\xi_0 \in GR(p^a, m)$ be units and $\overline{\lambda}_0 = \lambda$, $\overline{\xi}_0 = \xi$. So $\xi_0^{2p^s} = \lambda_0$ and, $x^\eta - \overline{\xi}_0$ and $x^\eta + \overline{\xi}_0$ are irreducible. The polynomial $x^{2\eta p^s} - \lambda_0$ factors into two coprime polynomials as

$$x^{2\eta p^s} - \lambda_0 = x^{2\eta p^s} - \xi_0^{2p^s} = (x^{\eta p^s} - \xi_0^{p^s})(x^{\eta p^s} + \xi_0^{p^s}).$$

Let $f_1(x) = (x^\eta - \xi_0)^{p^s} + p\beta_1(x)$ and $f_2(x) = (x^\eta - \xi_0)^{p^s} + p\beta_2(x)$ with $\deg(\beta_1(x)), \deg(\beta_2(x)) < \eta p^s$. Let $f(x) = f_1(x) f_2(x)$ and $\mathcal{R}_0 = \frac{GR(p^a,m)[x]}{\langle f(x) \rangle}$. Note that $f_1(x)$ and $f_2(x)$ are primary regular polynomials and therefore we can use the arguments of Section 2.2.

By Proposition 2.2.1, we get $\mathcal{R}_0 = \langle f_1(x) \rangle \oplus \langle f_2(x) \rangle$. Additionally, by Proposition 2.2.1, we know that $\langle f_1(x) \rangle \cong \frac{GR(p^a,m)[x]}{\langle f_2(x) \rangle}$ and $\langle f_2(x) \rangle \cong \frac{GR(p^a,m)[x]}{\langle f_1(x) \rangle}$ are local rings and the maximal ideals of $\mathcal{R}_0$ are $\langle p, x^\eta + \xi_0 \rangle$ and $\langle p, x^\eta - \xi_0 \rangle$.

Now given $g(x) \in \mathcal{R}_0$, we will see how to determine $\overline{\langle g(x) \rangle} \subset \mathcal{R}$. Since

$$\overline{\langle g(x) \rangle} = \overline{\langle (x^\eta - \xi)^{j_0} (x^\eta + \xi)^{j_1} \rangle},$$

we have $\bar{g}(x) = (x^\eta - \bar{\xi})^{j_0} (x^\eta + \bar{\xi})^{j_1} u(x)$ where $u(x)$ is a unit in $\mathcal{R}$. In order to determine j_0, we consider the substitution $x^i = (x^\eta - \xi_0 + \xi_0)^{d_i} x^{\ell_i}$ for every $i \geq \eta$, we get

$$\begin{aligned} g(x) &= a_L x^L + \cdots + a_\eta x^\eta + a_{\eta-1} x^{\eta-1} + \cdots + a_0 \\ &= (x^\eta - \xi_0)^{d_L} h_{d_L}(x) + (x^\eta - \xi_0)^{d_L - 1} h_{d_L - 1}(x) + \cdots + h_0(x) \end{aligned}$$

where $h_i(x)$ are polynomials such that $\deg(h_i(x)) < \eta$ for $d_L \geq i \geq 0$. Then j_0 is the least integer with the property $p \nmid h_{j_0}(x)$. Similarly, via the substitution $x^i = (x^\eta + \xi_0 - \xi_0)^{d_i} x^{\ell_i}$ for every $i \geq \eta$, the integer j_1 can be determined.

Let $C = \langle g_1(x), \ldots, g_r(x)\rangle \lhd \mathcal{R}_0$ be a polycyclic code, where the generators are as in Theorem 2.2.5. By Theorem 2.2.6, we have $d_H(C) = d_H(\overline{\langle g_r(x)\rangle})$. The canonical image $\overline{\langle g_r(x)\rangle}$ of $\langle g_r(x)\rangle$ can be determined as described above. Say $\overline{\langle g_r(x)\rangle} = \overline{\langle (x^\eta - \xi)^{\hat{i}}(x^\eta + \xi)^{\hat{j}}\rangle}$ for some $0 \le \hat{i}, \hat{j} \le p^s$. Then $d_H(\overline{\langle (x^\eta - \xi)^{\hat{i}}(x^\eta + \xi)^{\hat{j}}\rangle})$ can be determined using Theorem 3.3.22.

Remark 3.3.25 *Note that $x^{\eta p^s} - \xi_0^{p^s} = (x^\eta - \xi_0)^{p^s} + p\hat{\beta}_1(x)$ and $x^{\eta p^s} + \xi_0^{p^s} = (x^\eta + \xi_0)^{p^s} + p\hat{\beta}_2(x)$ for some $\hat{\beta}_1(x), \hat{\beta}_2(x) \in \mathcal{R}_0$. In the above setup, if we take $f_1(x) = (x^\eta - \xi_0)^{p^s} + p\hat{\beta}_1(x)$ and $f_2(x) = (x^\eta + \xi_0)^{p^s} + p\hat{\beta}_2(x)$, then we obtain the Hamming distance of λ-cyclic codes of length $2\eta p^s$ over $GR(p^a, m)$.*

CHAPTER 4

Matrix Product Codes

Constructing linear codes having the best possible parameters is one of the most important areas in coding theory. In this chapter, we study a method that has been proven to be effective in finding codes over finite fields with best known parameters.

In [27], Hernando and Ruano introduced a new method, which is called matrix product codes with polynomial units, to construct linear codes over finite fields having best known parameters. We show that using nested constituent codes and a non-constant matrix in their construction is crucial. We prove a lower bound on the Hamming distance of matrix product codes with polynomial units when the constituent codes are nested. This generalizes the technique used to construct the record-breaking examples of [27]. Contrary to a similar construction previously introduced, this bound is not sharp and need not hold when the constituent codes are not nested. We give a comparison of this construction with a similar method introduced in [50]. We also construct new binary codes having the same parameters, as the examples of [27], but non-equivalent to them.

4.1 Motivation: The Main Problem of Coding Theory

Recall that, a linear code C of length n, dimension k and Hamming distance d is called an (n,k,d) code. The integers n,k,d are called the parameters of the linear code.

One of the most common applications of Coding Theory is channel coding for reliable communication. This makes it possible for two parties to communicate over a noisy channel. Here we describe the model very briefly. Textbooks in coding theory such as [3, 28, 38] provide more detailed information.

An (n, k, d) linear code C over $\mathbb{F}_q$, with a generator matrix G, can be used to achieve reliable communication over a noisy channel as follows. A message m is represented by a vector of length k. Then m is encoded into a codeword $c \in C$ by $c = mG$. The codeword c is sent over the channel and it can be decoded back to m on the receiver's side. This system can correct errors as many as $\lfloor \frac{d-1}{2} \rfloor$ in each message. Obviously, this adds a redundancy of $n - k$ letters to the message m. However it is this redundancy that makes the message immune up to $\lfloor \frac{d-1}{2} \rfloor$ errors. The more Hamming distance C has, the more errors it can correct. But, for a fixed n, increasing d forces k to decrease. Less k means more redundancy which means less efficient use of the communication channel. So there is a trade-off between k and d. Thus, there is the problem of finding the best possible values of the parameters for a linear linear code over a fixed alphabet. This problem is called *the main problem of Coding Theory*. More explicitly, the problem is, given $\mathbb{F}_q$, n, k, finding the largest possible value of d such that there is an (n, k, d) linear code over $\mathbb{F}_q$. The current state-of-the-art can be found at [24].

In the above sense, linear codes having the best possible parameters are called *optimal codes*. As can be seen in [24], there are still cases where construction of an optimal code is unknown. The obvious approach to cover these gaps is exhaustive search. However, for large values of n, there are too many cases which makes it infeasible to search the whole space. So, various code construction methods have been introduced to tackle this problem. Some of these methods guarantee a lower bound for the Hamming distance of the resulting code. Consequently, beginning the search with a large lower bound narrows down the search space and sometimes gives linear codes that have best parameters than the previously known ones. In the following two sections, we study two such code construction methods.

4.2 Matrix Product Codes

Matrix Product Codes have been introduced by Özbudak and Stichtenoth in [50]. They showed that many optimal codes can be found with their method. Via method, short linear codes are combined to produce longer linear codes. Below, we explain their construction.

Let C be a linear code of length m and dimension k over $\mathbb{F}_q$. Let $W_1, W_2, \ldots, W_k$ be linear codes over $\mathbb{F}_q$ with the same length n. Suppose that each W_i has dimension e_i. The codes $W_1, W_2, \ldots, W_k$ are called the *constituent codes*. Fix a basis $c^{(1)}, c^{(2)}, \ldots, c^{(k)}$ for C. Let

$G \in \mathbb{F}_q^{k \times n}$ be the matrix whose i^{th} row is the codeword $c^{(i)}$ for all $1 \leq i \leq k$. So, clearly, G is a generator matrix of C. Let

$$C_j = \text{span}\{c^{(1)}, c^{(2)}, \dots, c^{(k)}\} \subset \mathbb{F}_q^m.$$

Clearly, C_j is a linear code of length m and has dimension k. Now, we define M to be the set of all $n \times k$ matrices over $\mathbb{F}_q$ whose j^{th} column is a codeword of W_j for all $1\ le j \leq k$. Then M is a linear subspace of dimension $e_1 + e_2 + \cdots + e_k$.

Let W be the linear code of length mn and dimension $e_1 + e_2 + \cdots + e_k$ over $\mathbb{F}_q$ defined as

$$W = \{A \cdot G : \ A \in M\}.$$

It has been shown in [50] that

$$d_H(W) \geq \min\{d_H(W_i)d(C_i) : \ 1 \leq i \leq k\}.$$

4.3 Matrix Product Codes with Polynomial Units

In [27], Hernando and Ruano introduced a method to construct longer linear codes using shorter ones. This method is similar to matrix product codes. Using their method, they found several linear codes having best known parameters hence improving the entries of code tables at [24]. In this section we explain their construction.

Let $C_1, \dots, C_s \subset \mathcal{R}$ be cyclic codes of length m over $\mathbb{F}_q$. Let s and ℓ be positive integers such that $s \leq \ell$ and let $A = (a_{ij}) \in \mathcal{R}^{s \times \ell}$ be an $s \times \ell$ matrix having full rank. Then

$$C = [C_1 \cdots C_s]A = \{[c_1, \dots, c_s]A : \quad c_i \in C_i\}$$

is called a *matrix product code with polynomial units*. Let $1 \leq i \leq s$ and let C_i be an $[m, k_i, d_i]$ cyclic code with the generator polynomial $f_i(x)$. Then C is a linear code of length ℓm over $\mathbb{F}_q$ and the dimension of C is $k_1 + \cdots + k_s$ (cf. [27, Proposition 1]).

Let R be a commutative ring with 1 and let $W \subset R^n$ be an R-module, i.e., W is a linear code of length n over R. The Hamming weight of $w = (w_1, \cdots, w_n) \in W$ is defined as

$$W_H(w) = |\{i : \ w_i \neq 0\}|. \tag{4.1}$$

The Hamming distance of W is defined as

$$D_H(W) = \min\{W_H(w) : \ w \in W \setminus \{0\}\}. \tag{4.2}$$

Throughout the paper when V is a linear code over $\mathbb{F}_q$, its Hamming distance, denoted by $d_H(V)$, and the Hamming weight of the codeword $v \in V$, denoted by $w_H(v)$, are used in the usual sense (see [38, Chapter 1]). In particular, if W is a module over $\mathcal{R}$ and $w \in W$, then W is also a linear code over $\mathbb{F}_q$ and, $W_H(w)$ in (4.1) and $D_H(W)$ in (4.2) are different from $w_H(w)$ and $d_H(W)$, respectively.

The matrices used in the above construction can be grouped into two classes. This plays an important role on the Hamming distance of the resulting codes.

Definition 4.3.1 *Let $A = (a_{ij}) \in \mathcal{R}^{s\times\ell}$. It is clear that there exist uniquely determined $a_{ij}^{(0)}, a_{ij}^{(1)}, \ldots, a_{ij}^{(m-1)} \in \mathbb{F}_q$ such that*

$$a_{ij} = a_{ij}^{(0)} + a_{ij}^{(1)}x + \cdots + a_{ij}^{(m-1)}x^{m-1}.$$

Throughout the paper we say that A is constant if $a_{ij}^{(1)} = a_{ij}^{(2)} = \cdots = a_{ij}^{(m-1)} = 0$ for all entries $a_{ij} \in \mathcal{R}$ of A. Similarly, A is non-constant if there exists at least one entry $a_{ij} \in \mathcal{R}$ such that $a_{ij} \neq a_{ij}^{(0)}$.

4.4 Construction of Good Codes via Nested Codes

In [27], using the above construction, some linear codes whose parameters are better than the previously known ones were constructed (see the examples in Section 4.5 for details). This construction is based on choosing nested codes C_1 and C_2 as the constituent codes and using an appropriate 2×2 matrix. We consider a generalization of this construction in Theorem 4.4.3 to the case of $s \times \ell$ matrices and we show that the resulting codes satisfy the bound given in [27, Proposition 2]. In Remark 4.4.4, we observe that this bound is not sharp. Moreover we notice, in Remark 4.4.5, that when the constituent codes are not nested, this bound does not hold in general.

The main result of this section is Theorem 4.4.3 and, for its proof, we need the following preliminaries.

The following fact is well-known when R is a field. However when R is a commutative ring with 1, we could not find a direct reference for its proof in algebra textbooks. Therefore we provide a short proof using some results from [35]. This fact is fundamentally used in the proof of Lemma 4.4.2.

Proposition 4.4.1 *Let R be a commutative ring with* 1. *Let M be a square matrix over R. Then M is invertible if and only if M has full rank.*

Proof. Say M is an $n \times n$ matrix. Note that we can view M as a linear map from $\mathcal{R}^n$ to $\mathcal{R}^n$, say with respect to the standard basis. M has full rank if and only if M is an isomorphism. By [35, Proposition 4.18], M is an isomorphism if and only if the determinant of M is a unit in $\mathcal{R}$. By [35, Proposition 4.16], the determinant of M is a unit in $\mathcal{R}$ if and only if M is invertible. Hence M has full rank if and only if M is invertible. ■

Lemma 4.4.2 *Let $A = (a_{ij}) \in \mathcal{R}^{s \times \ell}$ be a matrix of full rank. Let C_{R_i} be the $\mathcal{R}$-module spanned by the first i rows of A. We denote the Hamming distance of C_{R_i} by D_i, whose definition is given in (4.2). Suppose that $D_i = \ell - i + 1$. Let $C_i \subset \mathcal{R}$ be cyclic codes of length m with $C_1 \supset C_2 \supset \cdots \supset C_s$ and consider codewords $c_i \in C_i$ for $1 \leq i \leq s$. Let $w = (w_1, w_2, \ldots, w_\ell) = (c_1, c_2, \ldots, c_s)A$. If w has r entries, which are* 0, *i.e., $w_{j_1} = w_{j_2} = \cdots = w_{j_r} = 0$ for some integers $j_1, \ldots, j_r$, then $c_i \in C_{r+1}$ for every $i \in \{1, \ldots, s\}$.*

Proof. It suffices to show that $c_i \in C_{r+1}$ for all $i \in \{1, 2, \ldots, r\}$ as $c_i \in C_{r+1}$ for all $i > r$. Assume that $w_{j_1} = w_{j_2} = \cdots = w_{j_r} = 0$. Writing this as a system of linear equations, we get

$$\begin{array}{rcl} c_1 a_{1j_1} + c_2 a_{2j_1} + \cdots + c_s a_{sj_1} & = & 0 \\ c_1 a_{1j_2} + c_2 a_{2j_2} + \cdots + c_s a_{sj_2} & = & 0 \\ \vdots & \vdots & \vdots \\ c_1 a_{1j_r} + c_2 a_{2j_r} + \cdots + c_s a_{sj_r} & = & 0. \end{array} \tag{4.3}$$

Let $i, e \in \{1, \ldots, r\}$ and let $G = (a_{ij_e}) \in \mathcal{R}^{r \times r}$. Keeping $c_i a_{ij_e}$'s, for $i \leq r$, on the left hand side of (4.3) and putting the rest at the right hand side, we write these equalities in matrix form as

$$(c_1, c_2, \ldots, c_r)G = (\kappa_1, \kappa_2, \ldots, \kappa_r), \tag{4.4}$$

where $\kappa_e = -(c_{r+1} a_{r+1 j_e} + c_{r+2} a_{r+2 j_e} + \cdots + c_s a_{s j_e}) \in C_{r+1}$ for all $r + 1 \leq e \leq s$.

Now we show that G has maximum row rank. If that was not the case, i.e., if its rows were linearly dependent, there would be $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r) \in \mathcal{R}^r \setminus \{(0, 0, \ldots, 0)\}$ such that $\alpha G = (0, 0, \ldots, 0)$. Then $\beta = (\alpha_1, \ldots, \alpha_r, 0 \ldots, 0)A \in C_{R_r}$ would have at least r zeros contradicting the assumption that $D_r = \ell - r + 1$.

By Proposition 4.4.1, G is invertible since G has full rank. Therefore, using (4.4), we get

$$(c_1, c_2, \ldots, c_r) = (\kappa_1, \kappa_2, \ldots, \kappa_r)G^{-1} \in C_{r+1} \times \ldots \times C_{r+1}$$

and the claim follows. ■

Recall that the constituent codes $C_1, \ldots, C_s$ are $[n, k_i, d_i]$ cyclic codes. Now we show that when the constituent codes $C_1, \ldots, C_s$ are nested then the Hamming distance of the resulting matrix product code can always be bounded from below by some number depending on C_i and the matrix A. This also justifies and generalizes the construction method of the examples of [27] in which record-breaking binary codes are given.

Theorem 4.4.3 *Let A, C_i, D_i be as in Lemma 4.4.2 and let $d_i = d_H(C_i)$. Let $C = [C_1 \cdots C_s]A$. Then we have*

$$d_H(C) \geq \min\{d_1 D_1, \ldots, d_s D_s\}. \tag{4.5}$$

Proof. Let $w = (w_1, \ldots, w_\ell) = (c_1, \ldots, c_s)A \in C \setminus \{0\}$. Suppose that $w_i \neq 0$ for all i. Then, since $w_i \in C_1$ for all i, we have $w_H(w) \geq d_1 D_1$. If some of the w_i's are 0, say r of them, then by Lemma 4.4.2, we get $c_i \in C_{r+1}$ for all $1 \leq i \leq s$. This implies that $w_i \in C_{r+1}$ for all $1 \leq i \leq s$. Therefore, for each of the $s - r$ entries w_i, which are nonzero, we have $w_H(w_i) \geq d_{r+1}$. Thus $w_H(w) \geq (s - r)d_{r+1} \geq \min\{sd_1, (s-1)d_2, \ldots, (s-i+1)d_i, \ldots, d_s\}$. ■

Remark 4.4.4 *Suppose that the constituent codes are nested. The bound (4.5) is shown to be sharp, in [26, Theorem 1], for matrix product codes introduced in [50]. However it is not sharp when A is non-constant. To see this, let A, C_1, C_2 be as in Example 1 of Section 4.5. The Hamming distance of C_1 is $d_1 = 11$ and the Hamming distance of C_2 is $d_2 = 47$. Clearly, $D_1 = 2$ and $D_2 = 1$ (see the statement of Lemma 4.4.2 for the definition of D_1 and D_2). The Hamming distance of $C = [C_1\ C_2]A$ is 27. Note that $27 > \min\{D_1 d_1, D_2 d_2\} = 22$.*

Remark 4.4.5 *The bound (4.5) need not hold true when the constituent codes $C_1, \ldots, C_s$ are not nested. As a demonstration, we consider the following example. Let $C_1 = \langle x + 1\rangle \subset GR(p^a, m)[x]$ and $C_2 = \langle x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\rangle \subset GR(p^a, m)[x]$. Obviously $d_1 = d_H(C_1) = 2$ and $C_2 = \{0, x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\}$. So $d_2 = d_H(C_2) = 7$. Let $A = \begin{bmatrix} 1 & 1 + x^2 + x^4 \\ 0 & 1 \end{bmatrix} \in (GR(p^a, m)[x])^{2\times 2}$. Clearly A has full rank over $GR(p^a, m)[x]$. Let*

R_1 and R_2 be the first and the second rows of A, respectively. Let $C_{R_1} = span\{R_1\}$ and $C_{R_2} = span\{R_1, R_2\}$. Note that C_{R_1} and C_{R_2} are regarded as linear codes over the ring $GR(p^a, m)[x]$. Clearly $D_1 = D_H(C_{R_1}) = 2$ and $D_2 = D_H(C_{R_2}) = 1$. Let $C = [C_1\ C_2] \cdot A$. Now we consider $x + 1 \in C_1$ and $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in C_2$. Then

$$c = [x + 1, x^6 + x^5 + x^4 + x^3 + x^2 + x + 1] \cdot A = [x + 1, x^6] \in C.$$

So $d_H(C) \leq w_H(c) = 3$. On the other hand, we have $\min\{D_1 \cdot d_1, D_2 \cdot d_2\} = 4$.

4.5 Three Examples and Construction of Non-Equivalent Good Codes

In this section, we show that the matrix product codes with polynomial units construction allows us to construct non-equivalent good codes. For this, we examine the three examples of [27] in detail. There are essentially three different constructions given in [27] and the rest of the codes are derived from the third code by puncturing, shortening or extending it. For each of these three constructions, we observe that, by changing one entry in the matrix A, we can obtain codes with the same Hamming distance but having a different weight distribution. In particular, for each example of [27], we present another example with weight distribution having less number of codewords of minimum weight than the ones in [27]. Next, we deduce that using non-constant matrices is a very important part of the construction of [27].

Below, we consider the three examples given in [27, page 366] where

$$\begin{aligned} A &= \begin{bmatrix} 1 & g \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \hat{A} = \begin{bmatrix} 1 & \hat{g} \\ 0 & 1 \end{bmatrix}, \\ C_1 &= \langle f_1(x) \rangle \quad \text{and} \quad C_2 = \langle f_2(x) \rangle, \\ C &= [C_1\ C_2]A \quad \text{and} \quad \hat{C} = [C_1\ C_2]\hat{A} \end{aligned} \tag{4.6}$$

and $g, \hat{g} \in \mathcal{R}$ are units. In the examples, C denotes the linear code given in the examples of [27] and $\hat{C}$ denotes the new linear code that we found by changing $g(x)$ to $\hat{g}(x)$. The weight distributions of C and $\hat{C}$ are given in the Appendix.

Example 1:

- $C_1, C_2 \subset \frac{\mathbb{F}_2[x]}{\langle x^{47}+1 \rangle}$
- $f_1(x) = x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^5 + x^4 + 1$

- $f_2(x) = (x^{47} + 1)/(x + 1)$
- $g(x) = x^{20} + x^{19} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^4 + x^3 + x^2 + 1$
- $\hat{g}(x) = x^{45} + x^{42} + x^{41} + x^{37} + x^{35} + x^{31} + x^{29} + x^{27} + x^{25} + x^{20} + x^{19} + x^{14} + x^{11} + x^9 + x^7 + x^4 + x^3 + x^2 + x$

C and $\hat{C}$ are $[94, 25, 27]$ codes. C has 1222 codewords of Hamming weight 27 and $\hat{C}$ has only 611 codewords of Hamming weight 27.

Example 2:

- $f_1(x) = x^{25} + x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + x^{16} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$
- $f_2(x) = (x^{51} + 1)/(x^2 + x + 1)$
- $g(x) = x^{20} + x^{15} + x^{14} + x^{10} + x^9 + x^7 + 1$
- $\hat{g} = x^{47} + x^{45} + x^{44} + x^{40} + x^{38} + x^{36} + x^{35} + x^{34} + x^{31} + x^{29} + x^{22} + x^{21} + x^{17} + x^{16} + x^{15} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$

C and $\hat{C}$ are $[102, 28, 28]$ codes. C has 1173 codewords of Hamming weight 28 and $\hat{C}$ has only 663 codewords of Hamming weight 28.

Example 3:

- $f_1(x) = x^{24} + x^{23} + x^{21} + x^{19} + x^{18} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + 1$
- $f_2(x) = (x^{51} + 1)/(x^2 + x + 1)$
- $g(x) = x^{50} + x^{49} + x^{48} + x^{46} + x^{44} + x^{43} + x^{42} + x^{41} + x^{38} + x^{37} + x^{36} + x^{34} + x^{32} + x^{29} + x^{27} + x^{25} + x^{24} + x^{19} + x^{17} + x^{15} + x^{13} + x^{12} + x^{10} + x^8 + x^5 + x + 1$
- $\hat{g} = x^{48} + x^{39} + x^{35} + x^{30} + x^{28} + x^{25} + x^{23} + x^{22} + x^{21} + x^{17} + x^{14} + x^{13} + x^{12} + x^8 + x^6 + x^3 + x^2$

C and $\hat{C}$ are $[102, 29, 28]$ codes. C has 2142 codewords of Hamming weight 28 and $\hat{C}$ has only 1836 codewords of Hamming weight 28.

Now considering the above examples, we show that using constant matrices is crucial. We take the same constituent codes and instead of the matrix A, as defined in (4.6), which is non-constant, we consider all constant invertible 2×2 matrices (i.e., matrices having full rank) over $\mathbb{F}_2$, which are

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$A_4 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad A_5 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad A_6 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Using MAGMA, we found that the Hamming distances of the resulting product codes are much less than the Hamming distances of the original codes given in the examples. We present our results in Table 4.1. The actual examples of [27] are given in the first row.

Table 4.1: Examples of codes with constant matrices and the actual examples of [27]. C_1 and C_2 are as in the examples of [27] and the matrices A_i are as above. A stands for the matrix used in the examples of [27].

Example 1	
Matrix	$d_H(C)$
A	**27**
A1	11
A2	11
A3	11
A4	11
A5	22
A6	22

Example 2	
Matrix	$d_H(C)$
A	**28**
A1	10
A2	10
A3	10
A4	10
A5	20
A6	20

Example 3	
Matrix	$d_H(C)$
A	**28**
A1	9
A2	9
A3	9
A4	9
A5	18
A6	18

4.6 Comparison with Other Methods

We compare the constructions of [27] and [50] in the following remarks.

Remark 4.6.1 *The construction introduced in [27] is essentially different from the construction in [50] in the sense that given the same constituent codes, we can not obtain the code* *produced by the method of [27] via the construction given in [50] in general. To see this, let C, C_1, C_2, A be as in Example 1 in Section 4.5. In what follows, we will show that it is impossible to obtain a linear code equivalent to C using the construction of [50]. Namely, we claim that there is no matrix M, over $\mathbb{F}_2$, such that*

$$D = \left\{ \begin{bmatrix} c_0^1 & c_0^2 \\ \vdots & \vdots \\ c_{m-1}^1 & c_{m-1}^2 \end{bmatrix} M : \quad c^i = (c_0^i, \ldots, c_{m-1}^i) \in C_i \right\}$$

and C are equivalent linear codes. If such a matrix exists, then M must be a 2×2 matrix as the codeword length of D must be 94. Let M_1 be the linear code generated by the first row of M_1 and let M_2 be the linear code generated by the two rows of M. We have $d_H(M_2) = 1$, since M has full rank, and $d_H(M_1) = 1$ or $d_H(M_1) = 2$. Since the constituent codes are nested, i.e., $C_1 \supset C_2$, using [26, Theorem 1], we get $d_H(D) = 11$, if $d_H(M_1) = 1$, and $d_H(D) = 22$, if $d_H(M_1) = 2$. This implies that C and D can not be equivalent because $d_H(C) = 27$.

Remark 4.6.2 *When the matrix $A = (a_{ij}) \in \mathcal{R}^{s\times\ell}$, used in the construction of matrix product codes with polynomial units, is a constant matrix, the constructions introduced in [50] and [27] are essentially the same. More precisely, with the conventions of Section 4.3, consider $C = [C_1 \cdots C_s]A$ where A is constant. Now, using the method of [50], we will construct another code $C^{'}$ and we will show that C and $C^{'}$ are equivalent. Let*

$$C^{'} = \left\{ \begin{bmatrix} v_0^1 & v_0^2 & \ldots & v_0^s \\ \vdots & \vdots & & \vdots \\ v_{m-1}^1 & v_{m-1}^2 & \ldots & v_{m-1}^s \end{bmatrix} A : \quad (v_0^i, \ldots, v_{m-1}^i) \in C_i \right\}.$$

Let $c^i = c_0^i + c_1^i x + \cdots + c_{m-1}^i x^{m-1} \in C^i$ and let

$$\begin{aligned} w &= [c^1, \ldots, c^s] \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1\ell} \\ a_{21} & a_{22} & \ldots & a_{2\ell} \\ \vdots & \vdots & & \vdots \\ a_{s1} & a_{s2} & \ldots & a_{s\ell} \end{bmatrix} \\ &= [(c_0^1 a_{11} + c_0^2 a_{21} + \cdots + c_0^s a_{s1}) + \cdots + (c_{m-1}^1 a_{11} + c_{m-1}^2 a_{21} + \cdots + c_{m-1}^s a_{s1}) x^{m-1}, \\ &\quad \ldots, (c_0^1 a_{1\ell} + c_0^2 a_{2\ell} + \cdots + c_0^s a_{s\ell}) + \cdots + (c_{m-1}^1 a_{1\ell} + c_{m-1}^2 a_{2\ell} + \cdots + c_{m-1}^s a_{s\ell}) x^{m-1}] \in C. \end{aligned}$$

Let

$$w^{'} = \begin{bmatrix} c_0^1 & c_0^2 & \dots & c_0^s \\ c_1^1 & c_1^2 & \dots & c_1^s \\ \vdots & \vdots & & \vdots \\ c_{m-1}^1 & c_{m-1}^2 & \dots & c_{m-1}^s \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1\ell} \\ a_{21} & a_{22} & \dots & a_{2\ell} \\ \vdots & \vdots & & \vdots \\ a_{s1} & a_{s2} & \dots & a_{s\ell} \end{bmatrix} \in C^{'}.$$

It is not hard to see that w and $w^{'}$ correspond to the same codeword under an appropriate permutation. Via this permutation, we deduce that C contains a linear code equivalent to $C^{'}$. Since the lengths and dimensions of C and $C^{'}$ are equal, it follows that C and $C^{'}$ are equivalent codes.

As a demonstration of Remark 4.6.2 we refer the reader to Table 4.1. The codes in Table 4.1 constructed via the matrices A_i's are essentially the same as the ones in [7, 50] and therefore the distance bound (4.5) is sharp for them. Consequently, their Hamming distances are not as good as the ones constructed by A

The construction introduced in [27], in certain cases, not only yields a linear code with better parameters but also allows us to get other linear codes having different weight distributions. We have also seen that choosing non-constant matrices is a very important part of the construction, which distinguishes it from existing methods. This construction turns out to be a very interesting and promising way of combining cyclic codes to produce longer linear codes.

REFERENCES

[1] Taher Abualrub, Ali Ghrayeb, Nuh Aydin and Irfan Siap. On the Construction of Skew Quasi-Cyclic Codes *IEEE Trans. Inform. Theory*, 56(5):2081-2090, 2010.

[2] Taher Abualrub and Robert Oehmke. On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory*, 49(9):2126–2133, 2003.

[3] Elwyn R. Berlekamp. *Algebraic coding theory*. McGraw-Hill Book Co., New York, 1968.

[4] Gilberto Bini and Flaminio Flamini. *Finite commutative rings and their applications*. The Kluwer International Series in Engineering and Computer Science, 680. Kluwer Academic Publishers, Boston, MA, 2002.

[5] Jason Thomas Blackford. Negacyclic codes over Z_4 of even length. *IEEE Trasns. Inform. Theory*, 49(6):1417–1424, 2003.

[6] Jason Thomas Blackford and Dwijendra K. Ray-Chaudhuri. A transform approach to permutation groups of cyclic codes over Galois rings. *IEEE Trans. Inform. Theory*, 46(7):2350–2358, 2000.

[7] Tim Blackmore and Graham H. Norton. Matrix-product codes over $\mathbb{F}_q$. *Appl. Algebra Engrg. Comm. Comput.*, 12(6):477–500, 2001.

[8] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[9] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Des. Codes Cryptogr.*, 6(1):21–35, 1995.

[10] Guy Castagnoli, James L. Massey, Philipp A. Schoeller, and Niklaus von Seemann. On repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):337–342, 1991.

[11] J. Cazaran and A. V. Kelarev. On finite principal ideal rings. *Acta Math. Univ. Comenian. (N.S.)*, 68(1):77–84, 1999.

[12] Jilyana Cazaran and Andrei V. Kelarev. Generators and weights of polynomial codes. *Arch. Math. (Basel)*, 69(6):479–486, 1997.

[13] Jose I. I. Curto, Hakan Özadam and Ferruh Özbudak . On matrix product codes with polynomial units. *submitted*.

[14] Hai Q. Dinh. Negacyclic codes of length 2^s over Galois rings. *IEEE Trans. Inform. Theory*, 51(12):4252–4262, 2005.

[15] Hai Q. Dinh. Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$. *IEEE Trans. Inform. Theory*, 53(1):147–161, 2007.

[16] Hai Q. Dinh. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl.*, 14(1):22–40, 2008.

[17] Hai Q. Dinh. Constacyclic codes of length 2^s over Galois extension rings of $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory*, 55(4):1730–1740, 2009.

[18] Hai Q. Dinh. Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. *J. Algebra*, 324(5):940–950, 2010.

[19] Hai Q. Dinh, Sergio R. López-Permouth, and Steve Szabo. On the structure of cyclic and negacyclic codes over finite chain rings. In Patrick Solé, editor, *Codes Over Rings*, volume 6 of *Series on Coding Theory and Cryptology*, pages 22–59. World Scientific Publ Co Pte Ltd, 2009.

[20] Hai Quang Dinh and Sergio R. López-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*, 50(8):1728–1744, 2004.

[21] Steven T. Dougherty and Young Ho Park. On modular cyclic codes. *Finite Fields Appl.*, 13(1):31–57, 2007.

[22] Dummit, David S. and Foote, Richard M. Abstract algebra, Third Edition. John Wiley & Sons Inc., 2004.

[23] Andrew Granville. Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers. In *Organic mathematics (Burnaby, BC, 1995)*, volume 20 of *CMS Conf. Proc.*, pages 253–276. Amer. Math. Soc., Providence, RI, 1997.

[24] Markus Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at *http://www.codetables.de*.

[25] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé. The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, 40(2):301–319, 1994.

[26] Fernando Hernando, Kristine Lally, and Diego Ruano. Construction and decoding of matrix-product codes from nested codes. *Appl. Algebra Engrg. Comm. Comput.*, 20(5-6):497–507, 2009.

[27] Fernando Hernando and Diego Ruano. New linear codes from matrix-product codes with polynomial units. *Advances in mathematics of communications*, 4(3):363–367, August 2010.

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

[29] Claude Shannon. A mathematical theory of communication. *Bell System Tech.*. J. 27, 379â423 and 623â656, (1948).

[30] Hungerford, Thomas W. Algebra. *Graduate Texts in Mathematics*, Springer-Verlag, 1974.

[31] Xiaoshan Kai and Shixin Zhu. On the distance of cyclic codes of length 2^e over $\mathbb{Z}_4$. *Discrete Math.*, 310(1):12–20, 2010.

[32] Pramod Kanwar and Sergio R. López-Permouth. Cyclic codes over the integers modulo p^m. *Finite Fields Appl.*, 3(4):334–352, 1997.

[33] Han Mao Kiah, Ka Hin Leung, and San Ling. Cyclic codes over GR(p^2, m) of length p^k. *Finite Fields Appl.*, 14(3):834–846, 2008.

[34] P. Vijay Kumar, Tor Helleseth, A. R. Calderbank, and A. Roger Hammons, Jr. Large families of quaternary sequences with low correlation. *IEEE Trans. Inform. Theory*, 42(2):579–592, 1996.

[35] Serge Lang. *Algebra*. Springer, Third edition, 2002.

[36] Lidl, Rudolf and Niederreiter, Harald. Finite Fields. *Encyclopedia of Mathematics and its Applications*, vol. 20, Cambridge University Press, 1997.

[37] Sergio R. López-Permouth and Steve Szabo. On the Hamming weight of repeated root cyclic and negacyclic codes over Galois rings. *Adv. Math. Commun.*, 3(4):409–420, 2009.

[38] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Publishing Co., Amsterdam, 1977.

[39] James L. Massey, Daniel J. Costello, and Jørn Justesen. Polynomial weights and code constructions. *IEEE Trans. Information Theory*, IT-19:101–110, 1973.

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

[41] A. A. Nechaev. Linear recurrent sequences over commutative rings. *Diskret. Mat.*, 3(4):105–127, 1991.

[42] A. A. Nechaev and D. A. Mikhaĭlov. A canonical system of generators of a unitary polynomial ideal over a commutative Artinian chain ring. *Diskret. Mat.*, 13(4):3–42, 2001.

[43] G. H. Norton and A. Sălăgean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields Appl.*, 9(2):237–249, 2003.

[44] Graham H. Norton and Ana Sălăgean. On the Hamming distance of linear codes over a finite chain ring. *IEEE Trans. Inform. Theory*, 46(3):1060–1067, 2000.

[45] Graham H. Norton and Ana Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Appl. Algebra Engrg. Comm. Comput.*, 10(6):489–506, 2000.

[46] Graham H. Norton and Ana Sălăgean. Strong Gröbner bases for polynomials over a principal ideal ring. *Bull. Austral. Math. Soc.*, 64(3):505–528, 2001.

[47] Hakan Özadam and Ferruh Özbudak. A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p. *Adv. Math. Commun.*, 3(3):265–271, 2009.

[48] Hakan Özadam and Ferruh Özbudak. The minimum Hamming distance of cyclic codes of length $2p^s$. *Applied algebra, algebraic algorithms, and error-correcting codes*, Lecture Notes in Computer Science vol. 5527, 92–100, Springer, 2009.

[49] Sergio R. López-Permouth, Hakan Özadam, Ferruh Özbudak and Steve Szabo. Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes *Finite Fields Appl.*, to appear, http://dx.doi.org/10.1016/j.ffa.2012.10.002 , 2012.

[50] Ferruh Özbudak and Henning Stichtenoth. Note on Niederreiter-Xing's propagation rule for linear codes. *Appl. Algebra Engrg. Comm. Comput.*, 13(1):53–56, 2002.

[51] Vera S. Pless and Zhongqiang Qian. Cyclic codes and quadratic residue codes over Z_4. *IEEE Trans. Inform. Theory*, 42(5):1594–1600, 1996.

[52] Ron M. Roth and Gadiel Seroussi. On cyclic MDS codes of length q over GF(q). *IEEE Trans. Inform. Theory*, 32(2):284–285, 1986.

[53] Ana Sălăgean. Repeated-root cyclic and negacyclic codes over a finite chain ring. *Discrete Appl. Math.*, 154(2):413–419, 2006.

[54] Li-zhong Tang, Cheong Boon Soh, and Erry Gunawan. A note on the q-ary image of a q^m-ary repeated-root cyclic code. *IEEE Trans. Inform. Theory*, 43(2):732–737, 1997.

[55] J. H. van Lint. Repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):343–345, 1991.

[56] Gerardo Vega and Jacques Wolfmann. Some families of $\mathbb{Z}_4$-cyclic codes. *Finite Fields Appl.*, 10(4):530–539, 2004.

[57] Jacques Wolfmann. Negacyclic and cyclic codes over Z_4. *IEEE Trans. Inform. Theory*, 45(7):2527–2532, 1999.

[58] Jacques Wolfmann. Binary images of cyclic codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, 47(5):1773–1779, 2001.

[59] Karl-Heinz Zimmermann. On generalizations of repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 42(2):641–649, 1996.

APPENDIX A

APPENDIX

A.1 Weight Distribution of the Examples in Section 4.5

The weight distribution of a linear code D consists of pairs of non-negative integers of the form (δ, γ) which means that D has exactly γ codewords of Hamming weight δ.

Example 1: The weight distribution of C is

[(0, 1), (27, 1222), (28, 940), (30, 6251), (31, 21244), (32, 22372), (34, 73696), (35, 259534), (36, 212252), (38, 497260), (39, 1422032), (40, 975156), (42, 1621876), (43, 3926380), (44, 2278372), (46, 2700432), (47, 5516392), (48, 2700432), (50, 2278372), (51, 3926380), (52, 1621876), (54, 975156), (55, 1422032), (56, 497260), (58, 212252), (59, 259534), (60, 73696), (62, 22372), (63, 21244), (64, 6251), (66, 940), (67, 1222), (94, 1)].

The weight distribution of $\hat{C}$ is

[(0, 1), (27, 611), (28, 1316), (30, 5499), (31, 23406), (32, 23876), (34, 74824), (35, 257607), (36, 203980), (38, 498012), (39, 1420904), (40, 983428), (42, 1624132), (43, 3928918), (44, 2282884), (46, 2690656), (47, 5514324), (48, 2690656), (50, 2282884), (51, 3928918), (52, 1624132), (54, 983428), (55, 1420904), (56, 498012), (58, 203980), (59, 257607), (60, 74824), (62, 23876), (63, 23406), (64, 5499), (66, 1316), (67, 611), (94, 1)].

Example 2:

The weight distribution of C is

[(0, 1), (28, 1173), (30, 6477), (32, 34221), (34, 140358), (36, 496859), (38, 1552083), (40, 3892626), (42, 8812069), (44, 16080351), (46, 26517807), (48, 34884646), (50, 42113556), (52, 40867014), (54, 36031670), (56, 25656876), (58, 16567962), (60, 8568731), (62, 4026195), (64, 1493892), (66, 510238), (68, 138423), (70, 35343), (72, 5610), (74, 969), (76, 153), (78, 153)]

The weight distribution of $\hat{C}$ is

[(0, 1), (28, 663), (30, 7497), (32, 31365), (34, 142857), (36, 489872), (38, 1564017), (40, 3890127), (42, 8851424), (44, 16068162), (46, 26380566), (48, 34975154), (50, 42145890), (52, 40848552), (54, 36118574), (56, 25570890), (58, 16541952), (60, 8588995), (62, 4021809), (64, 1510008), (66, 507501), (68, 141024), (70, 31569), (72, 5559), (74, 1224), (76, 204)]

Example 3:

The weight distribution of C is

[(0, 1), (28, 2142), (30, 12342), (32, 67167), (34, 273171), (36, 1012707), (38, 3061122), (40, 7939578), (42, 17388858), (44, 32577984), (46, 52116696), (48, 70966806), (50, 83016882), (52, 83016882), (54, 70966806), (56, 52116696), (58, 32577984), (60, 17388858), (62, 7939578), (64, 3061122), (66, 1012707), (68, 273171), (70, 67167), (72, 12342), (74, 2142), (102, 1)]

The weight distribution of $\hat{C}$ is

[(0, 1), (28, 1836), (30, 13668), (32, 64107), (34, 284493), (36, 990437), (38, 3071526), (40, 7927848), (42, 17439552), (44, 32594508), (46, 51956556), (48, 71099542), (50, 82991382), (52, 82991382), (54, 71099542), (56, 51956556), (58, 32594508), (60, 17439552), (62, 7927848), (64, 3071526), (66, 990437), (68, 284493), (70, 64107), (72, 13668), (74, 1836), (102, 1)]

VITA

PERSONAL INFORMATION

Name	:	Hakan
Last Name	:	Özadam
Nationality	:	Turkish Citizen
e-mail	:	hakan.ozadam@gmail.com

EDUCATION

Degree	Institution	Year
PhD	METU, Department of Cryptography	2012
MS	METU, Department of Cryptography	2008
BS	METU, Department of Computer Engineering	2006
BS	METU, Department of Mathematics	2005

WORK EXPERIENCE

Research Assistant, Department of Mathematics, METU, 2005-2011

FOREIGN LANGUAGES

English (Fluent), Spanish (Basics)

PUBLICATIONS

1. S. R. López-Permouth, H. Özadam, F. Özbudak and S. Szabo, "Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes", Finite Fields and

Their Applications, vol. 19, no. 1, pp. 16-38, 2013.

2. H. Özadam and F. Özbudak, " A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p", Advances in mathematics of communications, vol. 3, no. 3, pp. 265-271, 2009.

3. H. Özadam and F. Özbudak "The Minimum Hamming Distance of Cyclic Codes of Length $2p^s$", in Proceedings of AAECC 18, Springer Lecture Notes in Computer Science, vol. 5527, pp. 92-100, 2009.